Technical reference for Microsoft SharePoint Foundation 2010

Microsoft Corporation

Published: May 2011

Author: Microsoft Office System and Servers Team (itspdocs@microsoft.com)

Abstract

This book includes information about the Microsoft SharePoint Foundation 2010 provider for Windows PowerShell and other helpful reference information about general settings, security, and tools. The audiences for this book are business application specialists, line-of-business specialists, information architects, IT generalists, program managers, and infrastructure specialists who are planning a solution based on SharePoint Foundation 2010.

The content in this book is a copy of selected content in the SharePoint Foundation 2010 technical library (*http://go.microsoft.com/fwlink/?LinkId=181463*) as of the publication date. For the most current content, see the technical library on the Web.

Microsoft

Contents

Getting help

Every effort has been made to ensure the accuracy of this book. This content is also available online in the Office System TechNet Library, so if you run into problems you can check for updates at:

http://technet.microsoft.com/office

If you do not find your answer in our online content, you can send an e-mail message to the Microsoft Office System and Servers content team at:

itspdocs@microsoft.com

If your question is about Microsoft Office products, and not about the content of this book, please search the Microsoft Help and Support Center or the Microsoft Knowledge Base at:

http://support.microsoft.com

Technical reference for SharePoint Foundation 2010

Published: May 12, 2010

Technical reference includes information about Windows PowerShell for Microsoft SharePoint Foundation 2010 and other useful reference information about general settings, security, and tools.

In this section:

- Windows PowerShell for SharePoint Foundation 2010 (Available on TechNet at *http://technet.microsoft.com/library/570ba120-85f7-4690-95ba-3a1651a92447(Office.14).aspx*)
- System Center Operations Manager knowledge articles (SharePoint Foundation 2010)
- User permissions and permission levels (SharePoint Foundation 2010)
- Database types and descriptions (SharePoint Foundation 2010)
- User experience on read-only sites (SharePoint Foundation 2010)
- Language packs (SharePoint Foundation 2010)
- SharePoint 2010 Administration Toolkit (SharePoint Foundation 2010)
- Peoplepicker-peopleeditoronlyresolvewithinsitecollection: Stsadm property (SharePoint Foundation 2010)

Other Resources

Stsadm command-line tool (Windows SharePoint Services)
(*http://technet.microsoft.com/en-us/library/cc288981(office.12).aspx*)

System Center Operations Manager knowledge articles (SharePoint Foundation 2010)

Published: May 12, 2010

The articles in this section are knowledge articles for the Microsoft SharePoint Foundation 2010 management pack for Microsoft System Center Operations Manager 2007. Typically, you would see these articles after clicking a link in an alert in the Operations Manager console. You can use these articles to help you troubleshoot and resolve problems in SharePoint Foundation 2010.

In this section:

- ULS not enough free disk space - Event 6457 (SharePoint 2010 Products)
- Access denied for writing to registry - Event 6588 (SharePoint 2010 Products)
- Access denied for writing to disk - Event 6589 (SharePoint 2010 Products)
- Application pool account must be registered as Kerberos - Event 6590 (SharePoint 2010 Products)
- SMTP service not running - Event 6599 (SharePoint 2010 Products)
- Event handler failed to load - Event 6644 (SharePoint 2010 Products)
- Product Help Library Permission - Event 6769 (SharePoint 2010 Products)
- Cannot resolve name of the outbound SMTP server - Event 6856 (SharePoint 2010 Products)
- Cannot connect to SMTP host - Event 6857 (SharePoint 2010 Products)
- Error occurred while communicating with SMTP server - Event 6858 (SharePoint 2010 Products)
- SharePoint lists cannot receive e-mail - Event 6872 (SharePoint 2010 Products)
- E-mail service cannot deliver e-mail - Event 6873 (SharePoint 2010 Products)
- Event receiver failed - Event 6875 (SharePoint 2010 Products)
- Backup timer job could not be created - Event 7035 (SharePoint 2010 Products)
- Central Administration update failed - Event 7037 (SharePoint 2010 Products)
- Throttling starts alert- Events 8032 8062 (SharePoint 2010 Products)
- Cannot retrieve end point - Event 8070 (SharePoint 2010 Products)
- Log folder does not exist - Event 8074 (SharePoint 2010 Products)
- Usage timer job failed - Event 8075 (SharePoint 2010 Products)
- Business Data Connectivity Service - BDC database adapter connection exception - Event 8080 (SharePoint 2010 Products)
- Business Data Connectivity Service - BDC Web service proxy generations exception - Event 8082 (SharePoint 2010 Products)
- Business Data Connectivity Service - BDC Proxy - unexpected exception - Event 8085 (SharePoint 2010 Products)
- Business Data Connectivity Service - SQL exception - Event 8086 (SharePoint 2010 Products)
- ULS trace log reaching maximum size - Event 8094 (SharePoint 2010 Products)
- ULS usage log reaching maximum size - Event 8095 (SharePoint 2010 Products)
- STS signing certificate missing - Event 8303 (SharePoint 2010 Products)
- STS cannot sign credentials - Event 8304 (SharePoint 2010 Products)
- Claims cannot establish endpoint - Event 8305 (SharePoint 2010 Products)
- STS claims provider error - Event 8307 (SharePoint 2010 Products)
- Administration service is not running (SharePoint 2010 Products)
- Document conversion launcher unavailable (SharePoint 2010 Products)
- Document conversion load balancer unavailable (SharePoint 2010 Products)

- Knowledge article is not yet available (SharePoint 2010 Products)
- Sandboxed code is running (SharePoint 2010 Products)
- SharePoint Administration service is disabled (SharePoint 2010 Products)
- SharePoint Foundation 2010 search is not running (SharePoint 2010 Products)
- SharePoint Health Analyzer has detected an error or warning (SharePoint 2010 Products)
- SharePoint Timer service could not start (SharePoint 2010 Products)
- SharePoint Timer service is not running (SharePoint 2010 Products)
- SQL Server remote access is disabled (SharePoint 2010 Products)
- Tracing service is not running (SharePoint 2010 Products)
- Web application taking too long to render a page (SharePoint 2010 Products)
- Web application unavailable (SharePoint 2010 Products)
- Web site unavailable (SharePoint 2010 Products)

ULS not enough storage for log directory - Event 2150 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: ULS not enough storage for log directory

Event ID: 2150

Summary: The Microsoft SharePoint Foundation Tracing (SPTracev4) service is used by Microsoft SharePoint Foundation 2010 to manage usage log output. When usage logging is turned on, administrators can specify the path that is used to store the usage logs. This log file is used by many applications that are built on top of SharePoint Foundation 2010. This event occurs when not enough free space is available for logging.

Symptoms: One or more of the following symptoms might appear:

- The usage log shows no new usage data.
- This event appears in the event log: Event ID: 2150 Description: Failed to create a usage log file at <Log Location>. There must be at least <# of GBs needed to resume logging> GB of free space if the usage logs are on System Drive.
-

Cause: The configured log location does not have enough free disk space for logging.

Resolution: Free up disk space or relocate the usage log

- SharePoint Foundation 2010 could not write to the usage log. This usage log contains information that is helpful for usage tracking and reporting.

To free up disk space:

1. Use Disk Cleanup to free up disk space where the usage log files are stored.
2. Verify whether the trace log has enough disk space to run properly.
3. If disk space is inadequate, try to clean the Temp folders on the drive.
4. If this procedure does not solve the problem, you can relocate the usage log file to a partition that has more drive space.

To relocate the log file:

1. On the SharePoint Central Administration Web site, on the Quick Launch, click **Monitoring** and in the **Reporting** section click **Usage Logging**.
2. On the Usage Logging page, in the **Logging Settings** section, type the new location for the usage log file.
3. Click **OK**.

To check the usage log file:

1. To verify that Microsoft SharePoint Foundation 2010 can create and write to the usage log file, on the Central Administration page click **Monitoring**, and in the **Reporting** section click **Usage Logging**.
2. On the Usage Logging page, in the **Logging Settings** section, copy the path of the usage log file.
3. In Windows Explorer, navigate to the usage log file by using the copied path. Usage log files are in binary format and the contents cannot be easily viewed and understood. The file size of the usage log increases over time and confirms that usage logging is working.

Event log flooding - Events 2158 2159 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Event log flooding

Event ID: 2158 or 2159

Summary: Event log flood protection prevents repeated events from being logged to the Windows event log. When an event is logged several times in a short period, flood protection prevents future events of the same type from being logged.

Symptoms: This event appears in the event log: Event ID: 2158 or 2159 Description: Event [Event ID] ([Event Provider Name]) of severity [Event Severity] occurred [Number of occurrences] more time(s) and was suppressed in the event log.

Cause: The same event is being logged repeatedly, triggering event log flood protection. You can identify which event is being logged repeatedly in the Event Description text of Event ID 2158 or 2159.

SQL Server database login failed - Event 3351 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SQL Server database login failed

Event ID: 3351

Summary: Microsoft SharePoint Foundation uses Microsoft SQL Server 2008 databases to store most of the content for SharePoint Foundation Web sites and configuration settings, and uses a service account to communicate with the database on behalf of a user request. Note that a Web application might be associated with one or many databases. This error — SQL Server database login failed — means that SharePoint Foundation cannot log on to SQL Server 2008 by using the specified service account user name and password.

Symptoms: The following symptom might appear:

- This event appears in the event log: Event ID: 3351 Description: SQL database login failed. Additional error information from SQL Server is included below.

Cause: The user name or password for the Microsoft SharePoint Foundation service account was invalid before the session or became invalid during the session.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following procedures.

Resolution: Grant correct permissions to the database access account

- To resolve this issue, assign the database access account and then verify that the account has correct permission in SQL Server.

To assign the database access account:

1. On the Central Administration Web page, on the Quick Launch, click **Security**, and in the **General Security** section click **Configure service accounts**.
2. In the **Credential Management** section, in the upper drop-down list click the correct Web application pool for your Web application.
3. In the **Select an account for this component** drop-down list, click the domain account with which you want to associate this Web application pool, or click **Register new managed account** to associate a new domain account with this application pool.
4. Click **OK** to save changes.

To verify that the account has correct permissions in SQL Server:

1. Connect to the computer that is running SQL Server by using an account with Administrator permissions.
2. In SQL Server Management Studio, in the **Object Explorer** navigation pane, expand the **Security** node, and then click the **Logins** node. The name of the database access account indicates that it is a SQL login.
3. If the account exists, in the **Object Explorer** navigation pane, expand the **Databases** node, expand the configuration database node (for example, WSS_Config), expand the **Security** node, and then click **Roles**.
4. Expand the **Database Roles** node, right-click **db_owner**, and select **Properties**.
5. In the **Database Roles Properties** dialog box, check whether the database access account is in the **Members of this role** list. If the account is not listed, click **Add**.

To verify that any database issues have been resolved:

1. In the SharePoint Management Shell, run the Windows PowerShell command **Get-SPSite | Format-Table -Property ID,WebApplication,ContentDatabase** to obtain a list of the sites for each Web application to list all sites in the various databases, and locate one site in each database.
2. Browse to the site.

Backup failed due to insufficient permissions - Event 3353 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Backup failed due to insufficient permissions

Event ID: 3353

Summary: This error occurs when the account that is performing the backup does not have sufficient permissions to write to the backup folder.

When you back up a Web application, you back up the content databases and settings for the Web application, including all sites in the site collections, files in document libraries, files attached to lists, security and permission settings, and feature settings. The backup process creates files that contain all of this data.

Similarly, when you back up a site collection, site, or list, the contents of those structures will be written to files or packages, and the restore or import process will use these files to recover the objects.

Symptoms: This event might appear in the event log: Event ID: 3353 Description: Unable to write to the backup folder.

Cause: One or more of the following might be the cause:

1. The SQL Server service account does not have Full Control access to the backup folder.
2. The SharePoint Timer Service account does not have Full Control access to the backup folder.
3. If the backup or restore was performed by using Windows PowerShell, the user who performed the backup operation did not have Full Control access to the backup folder.

Resolution: Verify permissions

- Ensure that the following are given the Full Control file share and NTFS permissions for the backup shared folder:
  - The account used by the SQL Server service account.
  - The Windows SharePoint Services Timer V4 (SPTimerV4) account.
  - The logged on account, if you are using Windows PowerShell to perform the backup or restore.
  - If the backup folder is a network share, ensure that all accounts that are listed above have access to both the share and the folder itself.
  - If you are performing a backup or restore operation between two SharePoint farms, services on both farms must have the permissions described above.

- For more information, see Configuring permissions for backup and recovery (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/d77b0854-08e5-4ea3-bf58-773264530c26(Office.14).aspx*).

Other Resources

View diagnostic logs (SharePoint Foundation 2010)
(*http://technet.microsoft.com/library/28a72c44-2c3a-459d-aa64-918c3a71c858(Office.14).aspx*)

Cannot connect to SQL Server - Event 3355 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Cannot connect to SQL Server

Event ID: 3355

Summary: Microsoft SharePoint Foundation 2010 uses Microsoft SQL Server 2008 databases to store configuration settings and most of the content for the Microsoft SharePoint Foundation Web site. For example, all pages in the site, files in document libraries, files attached to lists, and information in lists are stored in the content database, and security and permission settings along with other configuration settings are stored in the configuration database in SQL Server.

SharePoint Foundation 2010 uses a service account to communicate with the database on behalf of a user request. This service account can be either a specific user name or password (domain name and password), or a predefined system account, such as Local System or Network Service. When a SQL Server database is created, a value for the maximum database size is set. Each database has a separate database size setting. Note that a Web application might be associated with one or many databases.

This error indicates that Microsoft SharePoint Foundation could not connect to the SQL Server database.

Symptoms: One or more of the following symptoms might appear:

- Attempts to communicate with SQL Server fail and no content from databases hosted on the SQL Server can be accessed.
- This event appears in the event log: Event ID: 3355 Cannot connect to SQL Server. <Server Name> not found. Additional error information from SQL Server is included below.

Cause: One or more of the following might be the cause:

1. The SQL Server might be offline.
2. The SharePoint Foundation database access account might not have the necessary permissions to communicate with the SQL Server.
3. A firewall that runs on either the local server or on SQL Server might be blocking network communications.

Resolution: Grant correct permissions to the database access account

- You must be a member of the Farm Administrators group to perform this task.

Assign the database access account:

1. On the Central Administration home page, click **Security** and in the **General Security** section click **Configure service accounts**.

2. On the Service Accounts page, in the **Credential Management** section, in the upper drop-down list click the correct Web application pool for your Web application.
3. In the **Select an account for this component** drop-down list, click the domain account that you want to associate with this Web application pool, or click **Register new managed account** to associate a new domain account with this application pool.
4. Click **OK** to save changes.

Verify that the account has correct permissions in SQL Server:

1. Connect to the computer that runs SQL Server by using an account that has Administrator permissions.
2. In SQL Server Management Studio, **Object Explorer** navigation pane, expand the **Security** node, and then expand the **Logins** node. The name of the database access account indicates that it is a SQL login.
3. If the account exists, in the **Object Explorer** navigation pane, expand the **Databases** node, expand the configuration database node, expand the **Security**, and then click **Roles**.
4. Expand the **Database Roles** node, right-click **db_owner** role and select **Properties**.
5. In the **Database Role Properties** dialog box, check whether the database access account is in the **Members of this role** list. If the account is not listed, click **Add**.

Verify that any database issues are resolved:

1. In the SharePoint Management Shell, run the Windows PowerShell command **Get-SPSite | Format-Table -Property ID,WebApplication,ContentDatabase** to obtain a list of the sites for each Web application to list all sites in the various databases, and locate one site in each database.
2. Browse to that site, and ensure that the appropriate page rendered. An Access Denied page with an option to request access, or the option to log on as a different user, indicates that the operation completed successfully.
3. On the Central Administration page, on the Quick Launch, click **Application Management** and in the **Site Collections** section click **Specify quota templates**.
4. On the Quota Templates page, create a new quota template. The specific settings are not relevant to this verification test. You are creating the template to verify that it can be accessed in step 7.
5. Click **OK** to save the quota template.
6. Refresh the browser window, and then return to the Quota Templates page. If the quota template that you created can be selected, access to the SQL Server 2008 configuration database in Microsoft SharePoint Foundation is restored.
7. Click **Delete** to delete the quota template.

The application pool account cannot add user accounts to Active Directory - Event 3359 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: The application pool account cannot add user accounts to Active Directory

Event ID: 3359

Summary: The Internet Information Services (IIS) application pool creates identities based on Active Directory users, and associates these identities by using a set of permissions. This lets users in an Active Directory organizational unit (OU) inherit those permissions.

Symptoms: One or more of the following symptoms might appear:

- Account creation mode does not work correctly, which prevents user data from being added or read.
- User accounts are not automatically created in Active Directory.
- The event appears in the event log: Event ID: 3359 Description: The application pool account has insufficient permissions to add user accounts to Active Directory.

Cause: The account that is used by the application pool does not have the appropriate level of permissions that are required to add new user accounts to Active Directory.

Resolution: Determine the OU in which the application pool account creates new user accounts

1. Verify that you meet the following minimum requirements: See **Add-SPShellAdmin**.
2. On the **Start** menu, click **All Programs**.
3. Click Microsoft SharePoint 2010 Products.
4. Click SharePoint 2010 Management Shell.
5. At the Windows PowerShell command prompt, type the following:

```
$wa=Get-SPWebApplication
$wa.Parent.CreateActiveDirectoryAccounts
$wa.Parent.ActiveDirectoryDomain
$wa.Parent.ActiveDirectoryOrganizationalUnit
```

Note:

We recommend that you use Windows PowerShell when performing command-line administrative tasks. The Stsadm command-line tool has been deprecated, but is included to support compatibility with previous product versions.

Resolution: Add the correct permissions to the OU

1. On a server that has the Active Directory tools installed, open the Active Directory Users and Computers snap-in as a user who has sufficient domain permissions, such as domain administrator. To open Active Directory Users and Computers, click **Start**, click **Run**, and then type **dsa.msc**.
2. In the console tree, right-click the OU for which you want to delegate control.
3. Click **Delegate Control** to start the Delegation of Control Wizard, and then follow the instructions in the wizard.
4. In the **Welcome** pane, click **Next**.
5. In the **Users and Groups** pane, click **Add**.
6. In the **Enter the object names to select** box, type the user name that you plan to use for the administration application pool identity, and then click **OK**.
7. Click **Next**.
8. In the Tasks to Delegate pane, select the Create, delete, and manage user accounts and Read all user information check boxes, and then click Next.
9. Click **Finish**.

Active Directory organization unit unregistered - Event 3360 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Active Directory organization unit (OU) unregistered

Event ID: 3360

Summary: This error indicates that the Active Directory organizational unit (OU) that was created for account creation mode does not exist.

Symptoms: One or more of the following symptoms might appear:

- Account creation mode does not work correctly, which prevents user data from being added or read.
- This event appears in the event log: Event ID: 3360 Description: The Active Directory organization unit <OU Name> registered in Windows SharePoint Services 4.0 does not exist.

Cause: This can occur due to an error during provisioning or a run-time error that either caused the OU specified during farm configuration to not be created, or caused it to be renamed or deleted. Until this OU is created and registered, you cannot create a new site collection or add additional users.

Resolution: Add the OU to Active Directory

- You must be logged on as a domain administrator to perform this procedure.
- Click **Start**, click **Run**, and then type **dsa.msc**.
- Expand the **Domains** node.
- Right-click the domain, click **New**, and then click **Organizational Unit**.
- Type the OU name from event 7037 in the **<insert OU here>** box.
- Right-click the OU, and then click **Delegate Control**.
- Add the application pool account for the Web application that is being used for account creation.
- Click Create, delete, and manage accounts.
- Click **Next**.
- Click **Finish**.

SQL Server database is full - Event 3758 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SQL Server database is full

Event ID: 3758

Summary: Microsoft SharePoint Foundation uses Microsoft SQL Server 2008 databases to store most of the content for SharePoint Foundation Web site and configuration settings, and uses a service account to communicate with the database on behalf of a user request. When a SQL Server database is created, a value for the maximum database size is set. Each database has a separate database size setting. Note that a Web application might be associated with one or many databases. This error indicates that the database has reached the size of its maximum size setting.

Symptoms: The following symptom might appear:

- Users cannot add or update any content in SharePoint Foundation.
- Administrators cannot update any SharePoint Foundation settings.
- This event appears in the event log: Event ID: 3758 Description: Database full error on SQL Server instance <instance name> in database <database name>. Additional error information from SQL Server is included below. <SQL error message>

Cause: The database has reached its maximum size.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following tasks.

Resolution: Increase the size of the SQL Server database

- SharePoint Foundation cannot write to a database that has reached its maximum size. Increase the maximum size setting for the full database that is named in the event message.

To increase the database size:

1. In SQL Server Management Studio, in the **Object Explorer** navigation pane, expand the server node, and then expand the **Databases** node.
2. Right-click the database you want, and then click **Properties**. The database name is provided in the event message.
3. In the **Database Properties** dialog box, in the navigation pane, click **Files**.
4. In the **Database files** section, in the **Autogrowth** column, click the ellipsis for the database file.

5. In the **Change Autogrowth** dialog box, in the **Maximum File Size** section, if the **Restricted File Growth** option is selected, increase the maximum file size in the box to the right. You can also configure the database to grow without restrictions by selecting the **Unrestricted File Growth** option.
6. Click **OK** to save changes.

To verify that database issues are resolved:

1. In the SharePoint Management Shell, run the Windows PowerShell command **Get-SPSite | Format-Table -Property ID,WebApplication,ContentDatabase** to obtain a list of the sites for each Web application to list all sites in the various databases, and locate one site in each database.
2. Browse to the site.
3. Try to add content to the site. For example, add a list item or a document. SharePoint Foundation uses different errors under different editing circumstances, so if adding content to the site fails, check the event log for an error message such as those in the following table.

Log Name:	**Application**
Source:	Microsoft-Windows SharePoint-Windows SharePoint Services 4
Date:	4/2/2009 6:34:13 AM
Event ID:	3758
Task Category:	Database
Level:	Critical
Keywords:	
User:	Domain\Myuser
Computer:	MyServer
Description:	Database full error on SQL Server instance 'CO137' in database 'wss_2'. Additional error information from SQL Server is included below. Could not allocate space for object 'dbo.AllDocs'.'AllDocs_Url' in database 'wss_2' because the 'PRIMARY' filegroup is full. Create disk space by deleting unneeded files, dropping objects in the filegroup, adding additional files to the filegroup, or setting autogrowth on for existing files in the filegroup.

Database could not be accessed - Event 3760 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Database could not be accessed

Event ID: 3760

Summary: Microsoft SharePoint Foundation 2010 uses Microsoft SQL Server 2008 databases to store most of the content for the Web site and configuration settings. For example, all pages in the site, files in document libraries, files attached to lists, and information in lists are stored in the content database, and security and permission settings along with other configuration settings are stored in the configuration database in SQL Server.

SharePoint Foundation 2010 uses a service account to communicate with the database on behalf of a user request. This service account can be either a specific domain name/user name and password, or a predefined system account, such as Local System or Network Service. When a SQL Server database is created, a value for the maximum database size is set. Each database has a separate database size setting. Note that a Web application might be associated with one or many databases.

Symptoms: The following symptoms might appear:

- Content in the database is not available and attempts to access the database generate errors.
- This event appears in the event log: Event ID: 3760 Description: SQL Database '<database name>' on SQL Server instance '<instance name>' not found. Additional error information from SQL Server is included below. <error information>

Cause: One or more of the following might cause this:.

- The SQL Server user login failed.
- The database has been deleted or renamed.
- The database is currently unavailable because it is in an offline or loading state.

Important:

You must be a member of the local Administrators group to perform this task.

Resolution: Verify that SQL Server is running

- On the database server, in the Services snap-in, verify that the SQL Server (MSSQLSERVER) service is running.

Resolution: Verify that the user account can connect to SQL Server

- Log onto Microsoft SQL Server Management Studio as the account provided in the error details and click **Connect** and then **Database Engine**.
- Type the server name provided in the error details and click **Connect**.

Resolution: Verify that the database exists

- In Microsoft SQL Server Management Studio, expand the server node.
- Expand the Databases node.
- Verify that the database exists.

Note:

You must be a member of the Farm Administrators SharePoint group to perform these tasks.

Resolution: Restore database

- If the SQL Server database is not present or accessible on the computer that is running SQL Server, restore the database from a backup and reconnect it to SharePoint Foundation 2010.

To restore the database from a backup:

1. On the SharePoint Central Administration Web site, click **Backup and Restore** and in the **Farm Backup and Restore** section click **Restore from a backup**.
2. On the Restore from Backup page, type the backup path in the **Backup Directory Location** text box, select the backup you want to restore, and then click **Next**.
3. Select the database from the list and then click **Next**.

   Important:

   The backup must include the database and the accompanying Web application.
4. In the **Restore Options** section, select the **Same** configuration option. This action overwrites the existing database.
5. Click Start Restore.

To reconnect the database in Central Administration:

1. On the Central Administration page, click **Application Management** and in the **Databases** section click **Manage Content databases**.
2. On the Manage Content Databases page, click **Add a content database** and in the **Web Application** section select the Web application.
3. Under **Database Name and Authentication**, type the name of the server in the **Database Server** text box and type the database name in the **Database Name** text box.
4. Click **OK** to save the changes.

To verify that any database issues have been resolved:

1. In the SharePoint Management Shell, run the Windows PowerShell command `Get-SPSite | Format-Table -Property ID,WebApplication,ContentDatabase` to obtain a list of the sites for each Web application to list all sites in the various databases, and locate one site in each database.
2. Browse to that site and make sure that the appropriate page rendered. An Access Denied page with an option to request access, or the option to log on as a different user, indicates that the operation completed successfully.
3. On the Central Administration page, click **Application Management** and in the **Site Collections** section click **Specify Quota Templates**.
4. On the Quota Templates page, create a new quota template. The specific settings are not relevant to this verification test. You are creating the template to verify that it can be accessed in step 7.
5. Click **OK** to save the quota template.
6. Refresh the browser window, and then return to the Quota Templates page. If the quota template that you created can be selected, access to the SharePoint Foundation 2010 configuration database has been restored.
7. Click **Delete** to delete the quota template.

Content deployment job failed - Events 4958 5323 5325 5335 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Content deployment job failed

Event ID: 4958 5323 5325 and 5325

Summary: A content deployment job has failed. Content might not have been correctly deployed from the source environment to the target environment.

Symptoms: One or more of the following messages appear in the event log:

- Event ID: 4958 Description: Publishing: Content deployment job failed. Error: '<error>'.
- Event ID: 5323 Description: Failed to transfer files to destination server for Content Deployment job '<job name>'. Exception was: '<exception>'.
- Event ID: 5325 Description: Failed import operation for Content Deployment job '<job name>'. Exception was: '<exception>'.
- Event ID: 5326 Description: Failed import operation for Content Deployment job '<job name>'. Exception was: '<exception>'.

Cause: Content deployment can fail for various reasons. The specific reasons for this failure are contained in the content deployment report on the Content Deployment Paths and Jobs page in Central Administration.

Resolution: View the content deployment job status

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **General Application Settings**.
3. On the General Application Settings page, in the **Content Deployment** section, click **Manage content deployment paths and jobs**.
4. On the Manage Content Deployment Paths and Jobs page, confirm the status of the job. If the job failed, you can view the job details by clicking **Failed**.
5. On the Content Deployment Report page, in the **Errors and Warnings** section, you can view the error details.

You can also download the error details by clicking **Download Report** in the **Quick Links** section of the Content Deployment Report page.

Resolution: Rerun the content deployment job

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.

2. On the Central Administration Home page, click **General Application Settings**.
3. On the General Application Settings page, in the **Content Deployment** section, click **Manage content deployment paths and jobs**.
4. On the Manage Content Deployment Paths and Jobs page, click the arrow next to the job, and then click **Run Now**.
5. You can refresh the page to see the status of the job in progress. If the job failed, you can view the job details by clicking **Failed**.
6. On the Content Deployment Report page, in the **Errors and Warnings** section, you can view the error details.

You can also download the error details by clicking **Download Report** in the **Quick Links** section of the Content Deployment Report page.

Content database is Read-Only - Event 4971 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Content database is Read-Only

Event ID: 4971

Summary: Microsoft SharePoint Foundation 2010 stores most of the content of the Web application — including site collections, sites, lists, documents, and permissions — in content databases. A single Web application can be associated with one or many content databases.

Symptoms: One or more of the following symptoms might appear:

- Users cannot add or update content in SharePoint Foundation 2010 sites.
- The following event appears in the event log: Event ID: 4971 Description: Cannot update database on SQL Server instance '<instance name>'. Database is read/only. Additional error information from SQL Server is included below. <additional information>

Cause: SQL Server provides the option of setting a database to read-only mode, in which data can be read from the database but data cannot be added, changed, or removed. If a content database is in read-only mode, you might observe the symptoms described.

Resolution: Set the database to read/write

- If you verify that the content database is in read-only mode, set the SQL Server Management Studio database to read/write.

To verify that the database is read-only:

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **Application Management**.
3. On the Application Management page, in the **Databases** section, click **Manage content databases**.
4. On the Manage Content Databases page, select the Web application from the **Web Application** list.
5. If **Yes** appears in the **Database Read-Only** column for the content database, set the content database to read/write.

To set the content database to read/write:

1. Verify that the user account that is performing this procedure is a member of the **db_owner** fixed database role for the content database.
2. Open SQL Server Management Studio and connect to the database server.

3. In Object Explorer, expand **Databases**.
4. Right-click the database that you want to set to read/write, and then click **Properties**.
5. In the **Database Properties** dialog box, on the **Options** properties page, under **State**, select **False** from the drop-down list next to **Database Read-Only**, and then click **OK**.
6. Click **Yes**.

Insufficient SQL Server database permissions - Event 5214 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Insufficient SQL Server database permissions

Event ID: 5214

Summary: Microsoft SharePoint Foundation uses Microsoft SQL Server 2008 databases to store most of the content for the Web site and configuration settings. For example, all pages in the site, files in document libraries, files attached to lists, and information in lists are stored in the content database, and security and permission settings along with other configuration settings are stored in the configuration database in SQL Server.

SharePoint Foundation uses a service account to communicate with the database on behalf of a user request. This service account can be either a specific user name and password (domain name and password) or a predefined system account, such as Local System or Network Service. This error occurs when the service account specified in SharePoint Foundation has not been granted sufficient permissions in the SQL Server database.

Symptoms: The following symptom might appear:

- This event appears in the event log: Event ID: 5214 Insufficient SQL database permissions for user '<username>' in database <database name> on SQL Server instance <instance name>. Additional error information from SQL Server is included below.

Cause: One or more of the following might be the cause:

- The service account to which SharePoint Foundation is set does not have sufficient permissions to the database to which it is trying to connect.
- The service account is not set up properly in SharePoint Foundation.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following tasks.

Resolution: Grant correct permissions to the database access account

- To resolve this issue, assign the database access account and then verify the account has correct permission in SQL Server.

To assign the database access account:

1. On the Central Administration Web site, click **Security** and in the **General Security** section click **Configure Service Accounts**.
2. On the Configure Service Accounts page, in the **Credential Management** section, select the correct Web application pool for your Web application.
3. In the **Select an account for this component** section, select the domain account that you want to associate with this Web application pool, or click **Register new managed account** to associate a new domain account with this application pool.

   Note:

   You can use a local account for the Web application pool only if SharePoint Foundation and SQL Server are running on the same computer.

4. Click **OK** to save changes.

To verify that account has correct permissions in SQL Server:

1. Connect to the computer that runs SQL Server by using an account with SQL Server administrator permissions.
2. In SQL Server Management Studio, in the **Object Explorer** navigation pane, expand the **Security** node, and then click the **Logins** node. The name of the database access account indicates that it is a SQL login.
3. If the account exists, open the database node, open the **Security** node, and then click **Roles**.
4. Expand the **Database Roles** node, right-click **db_owner**, and select **Properties**.
5. In the **Database Roles Properties** dialog box, check whether the database access account is in the **Members of this role** list. If the account is not listed, click **Add**.

To verify that any database issues have been resolved:

1. In the SharePoint Management Shell, run the Windows PowerShell command **Get-SPSite | Format-Table -Property ID,WebApplication,ContentDatabase** to obtain a list of the sites for each Web application to list all sites in the various databases, and locate one site in each database.
2. Browse to the site.

Unable to write to trace log - Event 5401 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Unable to write to trace log

Event ID: 5401

Summary: Unified Logging Service (ULS) trace logs contain diagnostic information about what is happening on a Microsoft SharePoint Foundation 2010 server. This information can be used to diagnose problems on your server if they occur.

Symptoms: The following symptoms might appear:

- ULS trace log files are not created.
- This event appears in the event log: Event ID: 5401 Tracing Service failed to create the trace log file at <Log Location>. Error <Error Number>: <Error Description>.

Cause: This error occurs when the tracing service cannot create a new log file.

Resolution: Check the event log

- This error can occur for multiple reasons. The error number and error description describe the cause of the error in more detail; use the information in the error description to determine the most appropriate troubleshooting steps.

Unknown SQL exceptions - Event 5586 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Unknown SQL exceptions

Event ID: 5586

Summary: Microsoft SharePoint Foundation uses Microsoft SQL Server 2008 databases to store configuration settings and most of the content for the Web site. For example, all pages in the site, files in document libraries, files attached to lists, and information in lists are stored in the content database, and security and permission settings along with other configuration settings are stored in the configuration database in SQL Server 2008.

Microsoft SharePoint Foundation uses a service account to communicate with the database on behalf of a user request. This service account can be either a specific user name or password (domain name and password), or a predefined system account, such as Local System or Network Service. When a SQL Server database is created, a value for the maximum database size is set. Each database has a separate database size setting. Note that a Web application might be associated with one or many databases.

Symptoms: The following symptom might appear:

- This event appears in the event log: Event ID: 5586 Description: Database full error on SQL Server instance <instance name> in database <database name>. Additional error information from SQL Server is included below. <SQL error message>.

  Note:

  The description changes depending on the SQL Error code.

Cause: One or more of the following might be the cause:

1. Insufficient SQL Server database permissions
2. SQL Server database is full
3. Incorrect MDAC version
4. SQL Server database not found
5. Incorrect version of SQL Server
6. SQL Server collation is not supported
7. Database is read-only

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following tasks.

Resolution: Grant correct permissions to the database access account

- To resolve this issue, assign the database access account and then verify the account has correct permission in SQL Server.

To assign the database access account:

1. On the SharePoint Central Administration Web site, click **Security**, and in the **General Security** section click **Configure Service Accounts**.
2. On the Configure Service Accounts page, in the **Credential Management** section, select the correct Web application pool for your Web application.
3. In the **Select an account for this component** section, select the domain account that you want to associate with this Web application pool, or click **Register new managed account** to associate a new domain account with this application pool.
4. Click **OK** to save changes.

To verify that the account has correct permission in SQL Server:

1. Connect to the computer on which SQL Server runs by using an account with administrator permissions.
2. In SQL Server Management Studio, in the **Object Explorer** navigation pane, expand the **Security** node, and then expand the **Logins** node. The name of the database access account indications that it is a SQL logon account; for example, ##MS_PolicyTsqlExecutionLogin##.
3. If the account exists, expand the **Databases** node, expand the **Security** node, and then click **Roles**.
4. Expand the **Database Roles** node, right-click **db_owner**, and select **Properties**.
5. In the **Database Roles Properties** dialog box, check whether the database access account is in the **Members of this role** list. If the account is not listed, click **Add**.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following tasks.

Resolution: Increase the size of the SQL Server database

- SharePoint Foundation cannot write to a database that has reached its maximum size. One solution is to increase the maximum size setting for the database that is full, which is named in the event message.

To increase the database size:

1. In SQL Server Management Studio, in the **Object Explorer** navigation pane, expand the server node, expand the **Databases** node, right-click the database you want, and then click **Properties**. The database name is provided in the event message.
2. In the **Properties** dialog box, in the navigation pane, click **Files**.

3. In the **Database files** dialog box, in the **Autogrowth** column, click the ellipsis for the database file.
4. In the **Change Autogrowth** dialog box, under **Maximum File Size**, if the **Restricted File Growth (MB)** option is selected, increase the maximum file size in the box to the right. You can also configure the database to grow without restrictions by selecting the **Unrestricted File Growth** option.
5. Click **OK** to save changes.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following tasks.

Resolution: Restore database

- If the SQL Server database is not present or accessible on the computer that is running SQL Server, restore the database from a backup and reconnect it to SharePoint Foundation 2010.

To restore the database from a backup:

1. Copy the database backup to the SQL Server host.
2. Restore the database by using the **RESTORE SQL Server** command. For more information about the **RESTORE** command, see http://msdn.microsoft.com/en-us/library/ms186858(SQL.90).aspx.

To reconnect the database in Central Administration:

3. On the Central Administration page, click **Application Management** and in the **Databases** section, click **Manage content databases**.
4. On the Manage Content Databases page, click **Add a content database** and in the **Web Application** section select the Web application.
5. In the **Database Name and Authentication** section, type the name of the server in the **Database Server** text box and the database name in the **Database Name** text box.
6. Click **OK** to save the changes.

Resolution: Install correct SQL Server version

- The computer that hosts the database server role must have Microsoft SQL Server 2005 Service Pack 3 Cumulative Update (CU) 3 or SQL Server 2008 Service Pack 1 CU 2 installed. You can either install or upgrade the server to the correct version of SQL Server.

Note:

You must have db_owner permissions to the database to perform the following task.

Resolution: Select the correct SQL Server collation

1. Connect to the computer on which SQL Server is running by using an account with db_owner permissions to the database.
2. In SQL Server Management Studio, in the **Object Explorer** navigation pane, expand the **Databases** node. Right-click the specific database that was indicated in event 4972, and then click **Properties**.
3. On the **General** tab, the collation is listed in the **Maintenance** section.
4. To change the collation, open the **Options** page.
5. Select the correct collation from the **Collation** box.

Resolution: Change database to Read / Write

- Change the database so that it can be both read from and written to (read/write) by performing the following steps to increase the size of the database.

  Note:

  You must have db_owner access to the database to perform this action.

To increase the size of the database:

1. In SQL Server Management Studio, in the **Object Explorer** navigation pane, expand the server node, and then expand the Databases node.
2. Right-click the database you want, and then click **Properties**. The database name is provided in the event message.
3. In the **Database Properties** dialog box, in the navigation pane, click **Files**.
4. In the **Database files** section, in the **Autogrowth** column, click the ellipsis for the database file.
5. In the **Change Autogrowth** dialog box, in the **Maximum File Size** section, if the **Restricted File Growth** option is selected, increase the maximum file size in the box to the right. You can also configure the database to grow without restrictions by selecting the **Unrestricted File Growth** option.
6. Click **OK** to save changes.

Verify that any database issues have been resolved

1. In the SharePoint Management Shell, run the Windows PowerShell command **Get-SPSite | Format-Table -Property ID,WebApplication,ContentDatabase** to obtain a list of the sites for each Web application to list all sites in the various databases, and locate one site in each database.
2. Browse to the site.

SharePoint Foundation failed to create a site - Event 6141 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SharePoint Foundation failed to create a site

Event ID: 6141

Summary: In Microsoft SharePoint Foundation 2010, administrators can create new SharePoint sites. Site owners and — depending on the site settings — site visitors can create subsites. This alert indicates that an attempt to create a new SharePoint site has failed.

Symptoms: This event might appear in the event log: Event ID: 6141 Description: The site <Site Name> could not be created. The following exception occurred: <Exception Details>.

Cause: One or more of the following could cause this:.

- A configuration error.
- The user does not have sufficient permission to create the site.
- The user attempted to create a site with a non-valid character in the site name, such as '+'.

To determine the specific error, see the exception text in the event description.

Resolution: User must request access

- If Event 6141 has the description of: 'The site %SiteURL% could not be created. The following exception occurred: Access denied.' This means the user does not have permission to create a SharePoint site. Users will need to request access to the SharePoint site so that a SharePoint Administrator can update their permissions.

Instruct the user to follow these steps:

- On the home page of the site, in the upper right corner of the page, click next to “Welcome, <user name>”.
- Click Request Access.
- On the Request Access page, type a deception of your request, if needed, and click **Send Request**.

Resolution: User must use a different URL

- If Event 6141 has the description of: 'The site %SiteURL% could not be created. The following exception occurred: Invalid character in Web name %SiteName%.' This means the user attempted to create the site using an invalid character. Instruct the user to recreate the site without the special character such as '+' in the site name.

Unable to load authentication provider - Event 6143 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Unable to load authentication provider

Event ID: 6143

Summary: To authenticate users, Microsoft SharePoint 2010 Products uses the authentication providers that are provided by Windows Server 2008 R2 — such as forms authentication or Web single sign-on (SSO) authentication — by other versions of Windows, and by third-party vendors.

When using Kerberos v5 authentication, the service account used by the Internet Information Services (IIS) application pool for your Web application must be registered in Active Directory as a Service Principal Name (SPN) on the domain on which the front-end Web server is a member.

This error indicates that the role manager or membership provider that is specified for a particular Web application is incorrectly configured.

Symptoms: One or more of the following symptoms might appear:

- User authentication fails to work correctly, which prevents users from accessing content.
- User tokens are not updated by using correct role memberships, which prevents users from accessing content that they would expect to have access to, based on their roles.
- Event 6143 might appear in the event log with one of the following descriptions:
    - Description: Cannot get Membership Provider with name <Membership Provider Name>. The membership provider for this process was not properly configured. You must configure the membership provider in the .config file for every SharePoint process.
    - Description: Cannot get Role Manager with name <Role Manager Name>. The role manager for this process was not properly configured. You must configure the role manager in the .config file for every SharePoint process.

Cause: The role manager or membership provider specified for a particular Web application may be incorrectly configured.

Resolution: Verify the authentication mode

1. On the Central Administration Home page Quick Launch, click **Security**.
2. On the Security page, in the General Security section, click Specify authentication providers.
3. On the Authentication Providers page, ensure that the correct Web application is selected. If it is not, select the Web application that you want to review.
4. On the Authentication Providers page, click the zone for which you want to change authentication settings.

5. On the Edit Authentication page, in the **Authentication Type** section, review the selected authentication type.
6. If **Windows** is selected, review the settings in the **IIS Authentication Settings** section. If **Forms** or **Web Single Sign-On** is selected, review the settings in the **Membership Provider Name** and **Role Manager Name** sections.
7. Click **Cancel** to close without saving changes.

Resolution: Configure Kerberos v 5 authentication mode

1. You only need to perform this procedure if you are using Kerberos v 5 authentication.
2. You must be a member of the SharePoint Administrators group to perform this task.
3. Contact a domain administrator and ensure that the service account used by the application pool is the registered SPN for all domains listed with the Web application.

   Note:

   If you do not have a specific need for Kerberos v5 authentication, or if you cannot configure the SPN, use NTLM authentication instead. If you use Kerberos v5 authentication and cannot configure the SPN, only server administrators will be able to authenticate to the site. To change the authentication type, see the "Configure NTLM authentication mode" procedure later in this article

For more information about how to configure SharePoint 2010 Products to use Kerberos v5 authentication, see the Microsoft Knowledge Base article 832769, How to configure a Windows SharePoint Services virtual server to use Kerberos v5 authentication and how to switch from Kerberos v5 authentication back to NTLM authentication (*http://go.microsoft.com/fwlink/?LinkId=188483&clcid=0x409*).

Resolution: Configure NTLM authentication mode

1. On the Central Administration Home page Quick Launch, click **Security**.
2. On the Security page, in the General Security section, click Specify authentication providers.
3. On the Authentication Providers page, ensure that the correct Web application is selected. If it is not, select the Web application that you intend to review.
4. On the Authentication Providers page, click the zone for which you want to change authentication settings.
5. On the Edit Authentication page, in the **Authentication Type** section, select **Windows authentication**.
6. Under **IIS Authentication Settings**, ensure that the **Integrated Windows authentication** check box is selected, and then click **NTLM**.
7. Click **OK** to save changes.

Resolution: Configure Forms or Web Single Sign-On authentication mode

1. You only need to perform this procedure if you are using Kerberos v 5 authentication.
2. You must be a member of the SharePoint Administrators group to perform this task.
3. Review the documentation for the forms or Web SSO provider. Ensure that the correct components for the provider are installed on the server and that the settings for the provider are correctly set up in the Web.config file of the IIS directory for the Web application. Record the membership provider name and role manager from the Web.config file.
4. On the Central Administration Home page Quick Launch, click **Security**.
5. On the Security page, in the General Security section, click Specify authentication providers.
6. On the Authentication Providers page, click on the correct zone.
7. On the Edit Authentication page, in the **Claims Authentication** section, record the **ASP.NET Membership provider name**. Make sure that this is the same name specified in the Web.config file.
8. Record the **ASP.NET Role manager name**. Make sure that this is the same name specified in the Web.config file.

Insufficient permissions to write to the configuration data cache - Event 6395 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Insufficient permissions to write to the configuration data cache

Event ID: 6395

Summary: Several features of Microsoft SharePoint Foundation 2010 rely on scheduled background processes called timer jobs. Administrators can configure and schedule timer jobs by using SharePoint Central Administration. When you use the Services on Server page of the SharePoint Central Administration Web site to start or stop a service, a timer job performs this action.

To improve the performance of SharePoint Foundation 2010, most of the data in the configuration database in SQL Server 2008 is kept in a local file-system cache, called the configuration data cache. SharePoint Foundation 2010 uses the timer service to keep this cache synchronized with the configuration database.

This error indicates that a permissions issue is preventing specific trusted accounts from writing to the %systemdrive%\Users\AllUsers\Microsoft\SharePoint\Config directory.

Symptoms: The following message might appear in the event log: Event ID: 6395 Insufficient permissions to write to the configuration data cache. More information is included below.

Cause: The configuration cache directory has security settings that prevent write access to its contents. Although configuration objects can be updated farm-wide, the objects are not updated locally.

Resolution: Assign sufficient permissions to the configuration data cache

- Make sure that the WSS_ADMIN_WPG and WSS_RESTRICTED_WPG local groups have been granted permissions to write to the %systemdrive%\Users\All Users\Microsoft\SharePoint\Config directory. You must have Modify permissions to the directory in order to perform this task.

Alternate access mapping update failed - Event 6397 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Alternate access mapping update failed

Event ID: 6397

Summary: Several features of Microsoft SharePoint Foundation 2010 rely on scheduled background processes called timer jobs. Administrators can configure and schedule timer jobs by using SharePoint Central Administration. When you use the Services on Server page of the SharePoint Central Administration Web site to start or stop a service, a timer job performs this action.

To improve the performance of SharePoint Foundation 2010, much of the data in the configuration database in SQL Server 2008 is kept in a local file-system cache, called the configuration data cache. SharePoint Foundation 2010 uses the timer service to keep this cache synchronized with the configuration database. Alternate access mapping is a feature of Microsoft SharePoint Foundation 2010 for administrators to configure a load-balanced system by mapping an incoming URL to alternate URLs that are used by SharePoint Foundation.

This error occurs when the timer job that is used to update alternate access mappings failed on the specified server.

Symptoms: One or more of the following symptoms might appear:

- The alternate access mapping settings for Web applications on the local server might not be current.
- This event appears in the event log: Event ID: 6397 Alternate Access Mapping failed to be updated. Web Application affected: <Web Application>. Current user: <User Name>. More information is provided below.

Cause: The alternate access mapping specified in the configuration cache was not applied to the IIS settings of the local machine.

Note:

You must be a member of the Farm Administrators SharePoint group on the Central Administration site to perform the following task.

Resolution: Complete the alternate access mapping update

- The event string for event 6397 provides the alternate access mapping that failed. Try to re-create the mapping by using the Central Administration site.

To view or change alternate access mapping settings:

1. On the Central Administration page, click Application Management and in the Web Applications section click Configure alternate access mappings.
2. To edit the mapping, click the mapping you want to change.

To verify that the alternate access mapping is correct:

- If the SharePoint Administration Service was restarted, in the SharePoint Management Shell, run the Windows PowerShell command **Start-SPAdminJob** to ensure that all tasks required by the administration service were completed.

Service Instance timer execution failed - Event 6398 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SPServiceInstance timer execution failed

Event ID: 6398

Summary: Several features of Microsoft SharePoint Foundation 2010 rely on scheduled background processes called timer jobs. Administrators can configure, schedule, and view the status of timer jobs by using the SharePoint Central Administration Web site.

Symptoms: The following symptom might appear:

- This event appears in the event log: Event ID: 6398 The Execute method of job definition <Job Definition Name> (ID Job ID) threw an exception. More information is included below. %n%n <Job Details>

Most Common Job Definitions:

- **SPPasswordManagementJobDefinition**

Purpose: Sends e-mail and logs events for expiring passwords and password changes. This timer job ensures that managed passwords are changed before they expire.

- **SPGeneratePasswordJobDefinition**

Purpose: Generates new password for an account, updates the account password, and then launches jobs to deploy the new password to everything that uses it.

- **SPAdminAppPoolCredentialDeploymentJobDefinition**

Purpose: Updates the credentials for the administration Internet Information Services (IIS) 7.0 application pool in the farm.

- **SPContentAppPoolCredentialDeploymentJobDefinition**

Purpose: Updates the credentials for a content IIS application pool on all servers in the farm.

- **SPWindowsServiceCredentialDeploymentJobDefinition**

Purpose: Updates the credentials for a Windows service on every computer in the farm where the service is running.

- **SPMasterPassphraseDeploymentJobDefinition**

Purpose: Tells all the front-end Web applications the new passphrase-derived key. This job is run when the administrator decides to change the passphrase of the farm.

Cause: One or more of the following might be the cause:

- The third-party timer job cannot be found or is corrupt.
- The Microsoft SharePoint Foundation 2010 timer job cannot be found, or is corrupt.

- Most Common Job Causes:
  - **SPPasswordManagementJobDefinition**

Issue: Password change timer jobs (SPGeneratePasswordJobDefinition) have not been scheduled or updated for farm credentials. Any additions or changes made recently to the password change schedules for any credentials in the farm will not be updated to match the changes until this job completes successfully.

  - **SPGeneratePasswordJobDefinition**

Issue: A scheduled timer job to create a new password for a farm credential failed. The current credential value might no longer be valid and has to be updated manually in the Active Directory account. If the credentials for the account are still valid, this timer job should be restarted.

  - **SPAdminAppPoolCredentialDeploymentJobDefinition**

Issue: The new credentials for the Central Administration Web application pool have not been updated on the local machine to match the current value that was configured for the farm. This might prevent the Central Administration Web application from starting.

  - **SPContentAppPoolCredentialDeploymentJobDefinition**

Issue: The new credentials for the application pool have not been updated on the local machine to match the current value that was configured for the farm. This might prevent the application pool from starting.

  - **SPWindowsServiceCredentialDeploymentJobDefinition**

Issue: The new credentials for the service have not been updated on the local machine to match the current value that was configured for the farm. This might prevent the service from starting.

  - **SPMasterPassphraseDeploymentJobDefinition**

Issue: The master passphrase for the farm has not been updated on the local machine to match the current value that was configured for the farm. This might prevent decryption or encryption of the farm encryption key until it is updated locally.

Resolution: Determine appropriate resolution

- Review the job definition name found in the event description to determine the appropriate resolution:
  - **SPPasswordManagementJobDefinition**

Resolution: Restart this timer job.

  - **SPGeneratePasswordJobDefinition**

Resolution: Restart this timer job to manually force a password reset.

  - **SPAdminAppPoolCredentialDeploymentJobDefinition**

Resolution: Restart this timer job to run administrator deployment jobs locally, in order to manually force a password reset.

  - **SPContentAppPoolCredentialDeploymentJobDefinition**

Resolution: Restart this timer job to run administrator deployment jobs locally, in order to manually force a password reset.

- **SPWindowsServiceCredentialDeploymentJobDefinition**

Resolution: Restart this timer job to run administrator deployment jobs locally, in order to manually force a password reset.

- **SPMasterPassphraseDeploymentJobDefinition**

Resolution: Restart this timer job to run administrator deployment jobs locally, in order to manually force a password reset.

For all other timer job resolutions, follow the steps in the next section. To resolve this issue, use the resolution that corresponds to the cause you identified in the "Symptoms" section. After performing the resolution steps, see the "Verify" section to confirm that the feature is operating properly.

Note:

You must be a member of the Farm Administrators SharePoint group to perform these tasks.

Resolution: Configure faulty timer job

- If the faulty assembly cannot be found or is corrupt, and if it is not a SharePoint Foundation 2010 assembly, and if the timer definition is a recurring job, you must disable the faulty timer job.

To disable the faulty timer job:

1. On the Central Administration page, click **Monitoring** and in the **Timer Jobs** section click **Review Job Definitions**.
2. Locate the timer job in the list and click the timer definition name.
3. On the Edit Timer Job page, click **Disable**.

Disabled timer jobs are displayed as **Disabled** in the **Schedule Type** column.

To enable the faulty timer job:

1. On the Central Administration page, click **Monitoring** and in the **Timer Jobs** section click **Review Job Definitions**.
2. Locate the timer job in the list and click the timer definition name.
3. On the Edit Timer Job page, click **Enable**.

Note:

To perform the following procedure, you must be a member of the Administrators group on the local computer.

Resolution: Repair Windows SharePoint Services installation

- If the faulty assembly cannot be found or is corrupt, and is a Microsoft SharePoint Foundation assembly, you must repair the SharePoint Foundation installation to restore or repair the assembly.

Note:

Repairing the installation requires that you restart the server. Web application modifications and other settings changes will be preserved.

To repair the SharePoint Foundation installation:

- Run the Microsoft SharePoint Foundation 2010 setup wizard, select the **Repair** option, and click **Continue**.

To verify that the timer job is working:

- If the timer job was a recurring job, go to the Timer Job Definition page, and enable the timer job. The job should run at the next normally scheduled interval.
- If the timer job was a one-time-only job, retry the command that triggered the timer job.

ULS not enough free disk space - Event 6457 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: ULS not enough free disk space

Event ID: 6457

Summary: The Microsoft SharePoint Foundation Tracing (SPTracev4) service is used by Microsoft SharePoint Foundation 2010 to manage trace message output. When trace logging is turned on, administrators can specify the path that is to be used to store the trace logs. This log file is used by many applications that are built on top of SharePoint Foundation. The trace log contains information that is useful for diagnosing server problems. SharePoint Foundation 2010 could not write to the trace log. This event occurs when not enough free space is available for logging.

Symptoms: The following symptoms might appear:

- The trace log shows no new data.
- This event appears in the event log: Event ID: 6457 Description: Not enough free disk space available. The tracing service has temporarily stopped outputting trace messages to the log file. Tracing will resume when more than <# of MBs needed to resume logging> MB of disk space becomes available.

Cause: The configured log location does not have sufficient free disk space for logging.

Resolution: Free up disk space

1. Use Disk Cleanup to free up disk space where the trace logs are stored.
2. Verify that the trace log has enough disk space to run properly.
3. If the trace log does not have enough disk space, clean up the Temp folders on the drive.
4. If this procedure does not solve the problem, it is also possible to relocate the trace log file to a partition that has more drive space.

Resolution: Relocate the log file

1. On the SharePoint Central Administration Web site, click **Monitoring** and in the **Reporting** section, click **Configure diagnostic logging**.
2. On the Diagnostic Logging page, in the **Trace Log** section, type the new location for the trace log files in the **Path** text box.
3. Click **OK**.

Access denied for writing to registry - Event 6588 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Access denied for writing to registry

Event ID: 6588

Summary: This error occurs when an Internet Information Services application pool that is used by Microsoft SharePoint Foundation 2010 attempts to update a registry key and is denied access because the service account that is used by the application pool has inadequate permissions.

Symptoms: The following symptoms might appear:

- Registry keys might not be updated correctly to reflect configured settings.
- This event appears in the event log: Event ID: 6588 Description: The application pool account <Account Name> cannot write registry key <Key Name> at <Key Location>. Additional information is below.

Cause: The service account for the IIS application pool that SharePoint Foundation 2010 does not have appropriate access permissions to write to a registry key.

Resolution: Grant correct permissions to the application pool account

- The Web application pool account does not have sufficient permissions to write to the registry or to a file on disk. First, try to fix SharePoint Foundation 2010 permissions by using the Psconfig command-line tool. If that does not solve the problem, use the following procedures in order. First determine which account is used for the Web application.

  Note:

  You must be a member of the Farm Administrators SharePoint group to perform the following procedures.

To fix SharePoint Foundation 2010 permissions:

1. Open a Command Prompt window and at the command prompt, type:

cd /d %commonprogramfiles%\Microsoft Shared\Web server extensions\14\BIN

2. Fix the permissions on the server by entering the following command:

psconfig -cmd secureresources

3. Restart IIS and make the changes by entering the following command at the command prompt:**iisreset /noforce**

To determine the account for the Web application:

1. In the IIS Manager, in the **Connections** pane, expand the server node and then click **Application Pools**.
2. In the reading pane, in Features View, in the **Identity** column, note the account for the application pool that you identified.

To manually set the required group account for the Web application pool account on the computer:

1. Click Start, click Administrative Tools, and then click Computer Management.
2. In the tree view, expand **Local Users and Groups**, and then click the **Groups** folder.
3. In the reading pane list, right-click **WSS_WPG** and click **Add to Group**.
4. In the **WSS_WPG Properties** dialog box, add the Web application pool account by clicking **Add**.

To grant required permissions for the Web application pool account to a folder:

1. On the SharePoint Foundation computer, locate the folder identified in event 6588 or 6589.
2. Right-click the folder and select **Properties**.
3. In the **Properties** dialog box, on the **Security** tab, in the **Group or user names** section, select **Everyone**, and then click **Edit**.

   Note:

   Incorrectly editing the registry might severely damage the system. Before making changes to the registry, back up any valued data on the computer.

4. In the **Permissions for <foldername>** dialog box, click **Add** to add the Web application pool account. The account requires Write permission.

To grant the required permissions for the Web application pool account to a registry key:

1. Click the **Start** button, click **All Programs**, click **Accessories**, and then click **Run**.
2. Type **regedit**, and then click **OK**.
3. In the Registry Editor, in the tree view, locate the registry key that is identified in event 6588 or 6589.
4. Right-click the registry key and select **Permissions**.
5. In the **Permissions** dialog box, click **Add** to add the Web application pool account. The account will require Write permission.

To verify:

- Retry the operation that previously failed.

Access denied for writing to disk - Event 6589 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Access denied for writing to disk

Event ID: 6589

Summary: This error occurs when anInternet Information Services (IIS) 7.0 application pool used by Microsoft SharePoint Foundation 2010 attempts to update a file or folder and is denied access because the service account used by the application pool has inadequate permissions.

Symptoms: The following symptoms might appear:

- Files might not be updated correctly to reflect configured settings.
- This event appears in the event log: Event ID: 6589 Description: The application pool account <Account Name> has insufficient permissions to write file <File Name> at <File Location>. Additional information is below.

Cause: The service account for the IIS application pool that SharePoint Foundation 2010 uses does not have appropriate permissions to write to a file or folder in the NTFS file system.

Resolution: Grant correct permissions to the application pool account

- The Web application pool account does not have sufficient permissions to write to the registry or to a file on disk. First, try to fix SharePoint Foundation 2010 permissions by using the Psconfig command-line tool. If that does not solve the problem, use the following procedures in order. First determine which account is used for the Web application.
-

  Note:

  You must be a member of the Farm Administrators SharePoint group to perform the following procedures.

To fix SharePoint Foundation 2010 permissions:

1. Open a Command Prompt window and at the command prompt, type:

cd /d %commonprogramfiles%\Microsoft Shared\Web server extensions\14\BIN

2. Fix the permissions on the server by entering the following command:

psconfig -cmd secureresources

3. Restart IIS and make the changes by entering the following command at the command prompt: **iisreset /noforce**

To determine the account for the Web application:

1. In the IIS Manager, in the **Connections** pane, expand the server node and then click **Application Pools**.
2. In the reading pane, in Features View, in the **Identity** column, note the account for the application pool that you identified.

To manually set the required group account for the Web application pool account on the computer:

1. Click Start, click Administrative Tools, and then click Computer Management.
2. In the tree view, expand **Local Users and Groups** and click **Groups**.
3. In the reading pane list, right-click **WSS_WPG** groups and click **Add to Group**.
4. In the **WSS_WPG Properties** dialog box, add the Web application pool account by clicking **Add**.

To grant required permissions for the Web application pool account to a folder:

1. On the SharePoint Foundation computer, locate the folder identified in event 6588 or 6589.
2. Right-click the folder and select **Properties**.
3. In the **Properties** dialog box, on the **Security** tab, in the **Group or user names** section, select **Everyone**, and then click **Edit**.

   Note:

   Incorrectly editing the registry might severely damage the system. Before making changes to the registry, back up any valued data on the computer.

4. In the **Permissions for <foldername>** dialog box, click **Add** to add the Web application pool account. The account requires Write permission.

To grant the required permissions for the Web application pool account to a registry key:

1. Click the **Start** button, click **All Programs**, click **Accessories**, and then click **Run**.
2. Type **regedit**, and then click **OK**.
3. In the Registry Editor, in the tree view, locate the registry key identified in event 6588 or 6589.
4. Right-click the registry key and select **Permissions**.
5. In the **Permission** dialog box, click **Add** to add the Web application pool account. The account will require Write permission.

To verify:

- Retry the operation that previously failed.

Application pool account must be registered as Kerberos - Event 6590 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Application pool account must be registered as Kerberos

Event ID: 6590

Summary: Microsoft SharePoint Foundation 2010 can use the authentication providers that are provided by Windows Server 2008 to authenticate users. For example, Microsoft SharePoint Foundation can use forms-based authentication or Web single sign-on.

When using the Kerberos version 5 authentication protocol, the service account that is used by the Internet Information Services (IIS) application pool for your Web application must be registered in Active Directory Domain Services (AD DS) as an SPN on the domain on which the front end Web server is a member.

Symptoms: This event appears in the event log: Event ID: 6590 Description: The application pool account has insufficient permissions to add user accounts to Active Directory. When using Kerberos authentication, the service account used by the Internet Information Services (IIS) application pool for your Web application must be registered in Active Directory as a Service Principal Name (SPN) on the domain on which the Web front-end is a member.

Cause: One or more of the following might be the cause:

- If using Kerberos v5 authentication, the Web application pool account is not a registered security provider name.
- If using either forms-based authentication or Web single sign-on, the authentication provider could not be loaded because no membership provider name was specified.
- The Web application pool must be restarted for changes to be saved.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following action.

Resolution: Determine which authentication type the site is using

1. On the SharePoint Central Administration Web site, on the Quick Launch click **Security** and in the **General Security** section click **Specify Authentication Providers**.
2. On the Authentication Providers page, select the correct Web application. To select a Web application, click the **Web Application** drop-down list arrow and

click **Change Web Application**. In the **Select Web Application** dialog box, click the correct Web application.

3. On the Authentication Providers page, click the zone for the site from the list.
4. On the Edit Authentication page, the authentication type is displayed in the **IIS Authentication Settings** section.

Resolution: Register the application pool account as an SPN

- The Web application pool account is not a registered security provider name (SPN). Contact a domain administrator and make sure that the service account that is used by the application pool is the registered SPN for all domains listed with the Web application.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following tasks.

Resolution: Specify membership provider name and a role manager

1. On the Central Administration page, on the Quick Launch click **Security** and in the **General Security** section click **Specify authentication providers**.
2. On the Authentication Providers page, select the zone for which you want to change authentication settings.
3. On the Edit Authentication page, in the **Authentication Type** section select either the **Forms** or **Web single sign-on** authentication option. Windows authentication is selected by default.
4. Click **Save**.
5. In the **Membership Provider Name** section, type the name in the **Membership provider name** text box.
6. In the **Role Manager Name** section, type the name in the **Role manager name** text box.
7. Click **Save**.

Resolution: Edit authentication settings for a zone

1. On the Central Administration page, on the Quick Launch click **Security**, and in the **General Security** section click **Specify authentication providers**.
2. On the Authentication Providers page, select the zone for which you want to change authentication settings.
3. On the Edit Authentication page, in the **Authentication Type** section select the authentication option. Windows authentication is selected by default.
4. In the **IIS Authentication Settings** section, select the setting. **Integrated Windows authentication — NTLM** is selected by default. If you select **Negotiate (Kerberos)** you must perform additional steps to configure authentication.
5. Click **Save**.

SMTP service not running - Event 6599 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SMTP service is not running

Event ID: 6599

Summary: Microsoft SharePoint 2010 Products sends alerts and other SharePoint 2010 Products administration messages by using a Simple Mail Transfer Protocol (SMTP) mail server. When SharePoint 2010 Products is configured to receive incoming e-mail, the SMTP service delivers e-mail messages to a drop folder. A SharePoint timer job scans the drop folder and inserts the messages into SharePoint lists.

Symptoms: One or more of the following symptoms might appear:

- SharePoint 2010 Products does not receive incoming e-mail.
- Some front-end Web servers receive incoming e-mail while others do not.
- This event appears in the event log: Event ID: 6599 Description: there was an error connecting to the Windows SMTP service.

Cause: Automatic configuration for incoming e-mail is enabled and the Windows SMTP service is not installed on one or multiple servers, or the Windows SMTP service is not running on one or multiple servers.

Note:

The SMTP server is not installed by default. SMTP can be added by using the Features Summary area of Server Manager in Windows Server 2008 R2.

Resolution: Configure outgoing e-mail settings in Central Administration

Note:

SMTP is turned off by default in SharePoint Foundation 2010.

On the Central Administration Home page, click System Settings, and in the E-Mail and Text Messages (SMS) section, click Configure Outgoing E-Mail Settings.

1. On the Outgoing E-Mail Settings page, in the **Mail Settings** section, type the correct SMTP server in the **Outbound SMTP server** box.

Resolution: Enable and configure the SMTP service

- Perform the steps in the following article: Configure SMTP E-mail (IIS 7) (http://technet.microsoft.com/en-us/library/cc772058(WS.10).aspx).

Resolution: Start the SMTP service

Note:

In Internet Information Services (IIS) 6.0 Manager, connect to the SMTP server.

Expand the server node, and look for the SMTP virtual server used by SharePoint 2010 Products.

1. Right-click the correct virtual server, and then click **Start**.

Event handler failed to load - Event 6644 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Event handler failed to load

Event ID: 6644

Summary: In Microsoft SharePoint Foundation 2010, you can bind an event handler to an event host (such as an entire site, a list, or a document library). By binding an event handler to an event host, you can use document library events to start other processes, such as workflow processes.

Symptoms: This event appears in the event log: Event ID: 6644 Description: Event manager error: <error>.

Cause: One or more of the following might be the cause:

- The custom event receiver assembly cannot be found, or it is corrupted.
- The SharePoint Foundation 2010 assembly cannot be found, or it is corrupted.

Resolution: Contact the manufacturer of the faulty custom event receiver

- If the faulty assembly is corrupted, and it is not a SharePoint Foundation 2010 assembly, contact the manufacturer of the faulty event receiver assembly for more information.

Resolution: Repair your product installation

1. Repairing the installation will require you to restart the server. Web application modifications and other changes to settings will be preserved.

   Note:

   You must be a member of the Administrators group on the local computer to perform this task.

To repair the Microsoft SharePoint Foundation 2010 installation:

i. In Control Panel, open **Programs and Features**.

ii. Select your installation of SharePoint Foundation 2010 from the list, and then click **Change**.

iii. In the SharePoint Products Configuration Wizard, select **Repair**, and then click **Continue**.

iv. After completing the changes in the SharePoint Products Configuration Wizard, verify that the event handler assembly is either repaired or removed from all farm servers.

v. Retry the operation that triggered the event handler. These events should not continue to appear in the Windows event log.

Product Help Library Permission - Event 6769 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Product Help Library Permissions

Event ID: 6769

Summary: Microsoft SharePoint Foundation requires that specific permissions be set on the Product Help Library to correctly display Help to users. For this event ID the SCOM monitor monitors the permission configuration for this library. The Product Help Library is located in the Help Site Collection under the SharePoint Central Administration Web application.

Symptoms: The following symptoms might appear:

- End users cannot access the product Help.
- This event appears in the event log: Event ID: 6769 Description: Unable to refresh permissions for Product Help Library Site Collection.

Cause: A problem with refreshing permissions for the Product Help Library Site Collection.

Resolution: Reset Permissions

- Reset the permission configuration by using a Psconfig job or a Windows PowerShell cmdlet.

To reset the permission configuration by using a Psconfig job:

- Open a Command Prompt window and at the command prompt, type **psconfig -cmd helpcollections-install**.

To reset the permission configuration by using a Windows PowerShell cmdlet:

- Click Start, click All Programs, click Microsoft SharePoint 2010 Products, and then click SharePoint Management Shell. A Command Prompt window opens.
- Type the Windows PowerShell command **Install-SPHelpCollection -All**.

Cannot resolve name of the outbound SMTP server - Event 6856 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Cannot resolve name of the outbound SMTP server

Event ID: 6856

Summary: Microsoft SharePoint Foundation 2010 sends alerts and other administration messages by using an SMTP mail server. You can specify which SMTP server to use, and you can set the e-mail address to use for sending alerts and receiving replies for all sites, by using the Outgoing E-Mail Settings page of the SharePoint Central Administration Web site.

Symptoms: The following symptoms might appear:

- Cannot send e-mail by using SPUtility.SendEmail
- Cannot send e-mail messages, including alert e-mail, confirmation e-mail, invitation e-mail, and e-mail about exceeding quota
- This event appears in the event log: Event ID: 6856 Description: Cannot resolve name of SMTP host <host id>.

Cause: One or more of the following might be the cause:

- Microsoft SharePoint Foundation cannot connect to the SMTP host.
- SharePoint Foundation 2010 cannot resolve the name of the outbound SMTP server.

To resolve this issue, use the resolution that corresponds to the cause that you identify. After performing the resolution, see the “Verify that an e-mail message is sent” section at the end of this article to confirm that the feature is operating properly.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following actions.

Resolution: Start and configure the SMTP service

1. Start the Internet Information Services Manager 6.0 Manager and in the tree view expand the name of the server.
2. Right-click the SMTP virtual server that is used by SharePoint Foundation (for example, Default SMTP Virtual Server), and then click **Start**.
3. To configure the virtual server, right-click the virtual server and click **Properties**.
4. On the Delivery tab, click Outbound Security.

5. In the **Outbound Security** dialog box, either the **Anonymous access** or **Integrated Windows Authentication** option is selected. If Integrated Windows authentication is selected, make sure that the SharePoint Foundation Central Administration application pool account has access to the SMTP service. Select the **Account** and **Password** check boxes, and type the Windows account name and password that grants you access to the computer to which you connect.

Resolution: Configure outgoing e-mail settings in Central Administration

1. On the Central Administration page, click **System Settings** and in the **E-Mail** section click **Configure Outgoing E-Mail Settings**.
2. On the Outgoing E-Mail Settings page, in the **Mail Settings** section, type the correct SMTP server in the **Outbound SMTP server** text box.

Verify that an e-mail alert is sent

3. Navigate to a SharePoint Foundation Web site that has a list of any type.
4. Click an item in the list.
5. Click an item in the list and on the ribbon, click **Share & Track**.
6. Click **Alert Me** and from the menu select **For this item**.
7. In the **New Alert** dialog box, in the **Send Alerts To** section, type the account name in the **Users** text box.
8. After verifying other settings, click **OK**.

An e-mail message is sent to the e-mail Inbox informing you that you have created a new alert.

Cannot connect to SMTP host - Event 6857 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Cannot connect to SMTP host

Event ID: 6857

Summary: Microsoft SharePoint Foundation 2010 sends alerts and other administration messages by using an SMTP mail server. You can specify which SMTP server to use to send the alerts, and you can set the e-mail address to use for sending alerts and receiving replies for all sites, by using the Outgoing E-Mail Settings page on the SharePoint Central Administration Web site.

Symptoms: The following symptoms might appear:

- Cannot send e-mail by using SPUtility.SendEmail
- Cannot send e-mail messages, including alert e-mail, confirmation e-mail, invitation e-mail, e-mail about exceeding quota
- This event appears in the event log: Event ID: 6857 Description: Cannot resolve name of SMTP host <host id>.

Cause: One or more of the following might be the cause:

- Microsoft SharePoint Foundation cannot connect to the SMTP host.
- SharePoint Foundation cannot resolve name of the outbound SMTP server.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following actions.

Resolution: Start and configure the SMTP service

1. In Internet Information Services (IIS) 6.0 Manager, connect to the SMTP server.
2. Expand the server node and look for the SMTP virtual server that is used by SharePoint Foundation.
3. Right-click the correct virtual server and click **Start**.
4. To configure the virtual server, open the virtual server's properties.
5. On the **Delivery** tab, click Outbound **Security**.
6. In the **Outbound Security** dialog box, select either **Anonymous access** or **Integrated Windows Authentication**. If you select Integrated Windows authentication, make sure that the SharePoint Foundation Central Administration application pool account is authenticated on the SMTP server by selecting the **Account** and **Password** check boxes.

Resolution: Configure outgoing e-mail settings in Central Administration

1. On the Central Administration page, click **System Settings** and in the **E-Mail** section click **Configure Outgoing E-Mail Settings**.
2. On the Outgoing E-Mail Settings page, in the **Mail Settings** section, type the correct SMTP server in the **Outbound SMTP server** text box.

Error occurred while communicating with SMTP server - Event 6858 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Error occurred while communicating with SMTP server

Event ID: 6858

Summary: Microsoft SharePoint Foundation 2010 sends alerts and other administration messages by using an SMTP mail server. You can specify which SMTP server to use to send the alerts, and you can set the e-mail address to use for sending alerts and receiving replies for all sites, by using the Outgoing E-Mail Settings page on the SharePoint Central Administration Web site.

Symptoms: The following symptoms might appear:

- Cannot send e-mail using SPUtility.SendEmail
- Cannot send e-mail messages, including alert e-mail, confirmation e-mail, invitation e-mail, e-mail about exceeding quota
- This event appears in the event log: Event ID: 6858 Description: Cannot resolve name of SMTP host <host id>.

Cause: One or more of the following might be the cause:

- Microsoft SharePoint Foundation cannot connect to the SMTP host.
- SharePoint Foundation cannot resolve name of the outbound SMTP server.

To resolve this issue, use the resolution that corresponds to the cause that you identify. After performing the resolution, see the “Verify that an e-mail alert is sent” section at the end of this article to confirm that the feature is operating properly.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following actions.

Resolution: Start and configure the SMTP service

1. In Internet Information Services (IIS) 6.0 Manager, connect to the SMTP server.
2. Expand the server node and look for the SMTP virtual server used by SharePoint Foundation.
3. Right-click the correct virtual server, and then click **Start**.
4. To configure the virtual server, open the virtual server's properties.
5. On the Delivery tab, click Outbound Security.

6. In the **Outbound Security** dialog box, select either **Anonymous access** or **Integrated Windows Authentication**. If you selected Integrated Windows Authentication, make sure that the Windows SharePoint Services Central Administration application pool account is authenticated on the SMTP server by selecting the **Account** and **Password** check boxes.

Resolution: Configure outgoing e-mail settings in Central Administration

1. On the Central Administration page, click **System Settings** and in the **E-Mail** section click **Configure Outgoing E-Mail Settings**.
2. On the Outgoing E-Mail Settings page, in the **Mail Settings** section type the correct SMTP server in the **Outbound SMTP server** text box.

Verify that an e-mail alert is sent

1. Navigate to a SharePoint Foundation Web site that has a list of any type.
2. Click an item in the list.
3. Click an item in the list and on the ribbon, click **Share & Track**.
4. Click **Alert Me** and from the menu select **For this item**.
5. In the **New Alert** dialog box, in the **Send Alerts To** section, type the account name in the **Users** box.
6. After verifying other settings, click **OK**.

An e-mail message is sent to the e-mail Inbox informing you that you have created a new alert.

SharePoint lists cannot receive e-mail - Event 6872 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SharePoint lists cannot receive e-mail

Event ID: 6872

Summary: The Microsoft SharePoint 2010 Products incoming e-mail service processes e-mail messages to be added to SharePoint lists. The service processes mail that the Windows Simple Mail Transfer Protocol (SMTP) service added to a drop folder.

Symptoms: One or more of the following symptoms might appear:

- SharePoint lists do not receive incoming e-mail.
- Duplicate items appear in lists that are receiving incoming e-mail.
- This event appears in the event log: Event ID: 6872 Description: the incoming email service cannot access the drop directory or doesn't have sufficient permissions.

Cause: One or more of the following might be the cause:

1. The SharePoint timer service does not have read permissions on the drop folder.
2. The specified drop folder specified doesn't exist.
3. The SharePoint timer service does not have write permissions on the drop folder.

Resolution: Configure the drop directory in IIS

- In the Internet Information Services (IIS) 6.0 Manager snap-in, expand the Server node.
- In the **SMPT Virtual Server** node, double-click **Domains**.
- Right-click the domain, and then click **Properties**.
- Record the location of the drop directory. If no drop directory exists, create one.
- Grant the SharePoint timer service permissions to the drop directory.

Resolution: Configure the incoming email settings

- On the Central Administration Home page, click **System Settings**.
- On the System Settings page, in the E-Mail and Text Messages (SMS) section, click Configure incoming email settings.
- On the Configure Incoming E-mail Settings page, if the **Advanced** option is selected in the **Directory Management Service** section, type the location of the drop directory from the previous procedure in the **E-mail drop folder** box, and then click **OK**.

E-mail service cannot deliver e-mail - Event 6873 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: E-mail service cannot deliver e-mail

Event ID: 6873

Summary: The Microsoft SharePoint 2010 Products e-mail service processes e-mail destined for insertion into SharePoint lists. The service processes mail that the Windows Simple Mail Transfer Protocol (SMTP) service added to a drop folder.

Symptoms: One or more of the following symptoms might appear:

- SharePoint lists do not receive e-mail.
- This event appears in the event log: Event ID: 6599 Description: an error occurred while processing incoming email

Cause: One or more of the following might be the cause:

- There is no corresponding SharePoint list for the recipient of an e-mail.
- The sender does not have sufficient permissions to add content to the SharePoint list.

Resolution: Verify that the list is configured to receive e-mail

1. In the list provided in the event details, on the **List** menu, click **List Settings**.
2. On the List Settings page, under **Communications**, click **Incoming e-mail settings**.
3. Verify the following:
   - The correct e-mail address is entered in the **E-mail address** box.
   - The Yes option is selected under Allow this document library to receive e-mail?

Resolution: Grant the sender the appropriate permissions to the recipient list

1. In the list provided in the event details, on the **List** menu, click **List Settings**.
2. On the List Settings page, under Permissions and Management, click Permissions for this list.
3. Verify that the user account provided in the event details has at least **Contributor** permissions to the list.

Event receiver failed - Event 6875 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Event receiver failed

Event ID: 6875

Summary: In Microsoft SharePoint Foundation 2010, you can bind an event handler to an event host (such as an entire site, a list, or a document library). By binding an event handler to an event host, you can use document library events to start other processes, such as workflow processes.

Symptoms: This event appears in the event log: Event ID: 6875 Description: Error loading and running event receiver <receiver name> in <receiver location>. Additional information is below. <additional information>.

Cause: One or more of the following might be the cause:

- The custom event receiver assembly cannot be found, or it is corrupted.
- The SharePoint Foundation 2010 assembly cannot be found, or it is corrupted.

Resolution: Contact the manufacturer of the faulty event receiver

1. If the faulty assembly is corrupted, and it is not a SharePoint Foundation 2010 assembly, contact the manufacturer of the faulty event receiver assembly for more information.

Resolution: Repair your product installation

1. Repairing the installation will require you to restart the server. Web application modifications and other changes to settings will be preserved.

   Note:

   You must be a member of the Administrators group on the local computer to perform this task.

To repair SharePoint Foundation 2010 installation:

i. In Control Panel, open **Programs and Features**.

ii. Select your installation of SharePoint Foundation 2010 from the list, and then click **Change**.

iii. In the SharePoint Products Configuration Wizard, select **Repair**, and then click **Continue**.

iv. After completing the changes in the SharePoint Products Configuration Wizard, verify that the event handler assembly is either repaired or removed from all farm servers.

v. Retry the operation that triggered the event handler. These events should not continue to appear in the Windows event log.

Backup timer job could not be created - Event 7035 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Backup timer job could not be created

Event ID: 7035

Summary: When you back up a Web application, you back up the content databases and settings for the Web application, including all sites in the site collections, files in document libraries, files attached to lists, security and permission settings, and feature settings. The backup process creates files that contain all of this data. The restore process uses these files to restore the content databases and settings for the Web application.

Similarly, when you back up a site collection, site, or list, the contents of those structures will be written to files or packages, and the restore or import process will use these files to recover the objects.

Symptoms: One or more of the following symptoms might appear:

- One or more warning notifications will appear under the Readiness section of the Backup and Restore Job Status or Granular Backup Job Status pages in Central Administration.
- The following event appears in the event log: Event ID: 7035 Description: The same item is already in the process of being backed up or restored. To check the status of that process, go to the backup/restore job status page in the administration site.

Cause: An existing backup/restore timer job has failed or was not fully completed, and the SharePoint Timer Service or SharePoint Admin Service are not started.

Verify that the Timer and SharePoint Administration services are running

1. Ensure that the following services are started:
    i. The SharePoint Timer V4 service must be started on all front-end Web servers and application servers in the farm.
    ii. The SharePoint Administration V4 service must be started on the server that is running the Central Administration Web site.

Resolution: Verify that the previous backup or restore timer job completed successfully

- Verify that the user account that is performing this procedure is a member of the Farm Administrators SharePoint group.
- On the Central Administration Home page, click **Backup and Restore**.

- On the Backup and Restore page, under **Farm Backup and Restore**, click **Check backup and restore job status**.
- On the Backup and Restore Job Status page, under **Readiness**, verify that there are no backup or restore jobs in progress, that the Timer service is running, and that the Administration service is running.
- Click the **Back** button in the browser.
- On the Backup and Restore page, under **Granular Backup**, click **Check granular backup job status**.
- On the Granular Backup Job Status page, under **Readiness**, verify that there are no backup jobs in progress, there are no export jobs in progress, and the Timer service is running.
- Check the status of any current jobs in the **Site Collection Backup** and **Content Export** sections.

Central Administration update failed - Event 7037 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Central Administration update failed

Event ID: 7037

Summary: This error indicates that the Microsoft SharePoint Foundation 2010 timer job to update Central Administration on a specific URL was not created, or the local registry–based URL for the Central Administration was not updated.

Symptoms: One or more of the following symptoms might appear:

- Local server URL settings for the Central Administration Web site do not match the configured settings.
- This event appears in the event log: Event ID: 7037 Description: Error creating timer job to update central administration url location at <URL>.

Cause: One or more of the following might be the cause:

- The timer job that updates the Central Administration settings failed to be created. This failure may be caused by a communication failure with the configuration database while the configuration object was created.
- The Central Administration URL registry location on the local server failed to be updated because of registry key permission issues.

Resolution: Grant permissions to the appropriate hive location in registry

- Make sure that the local administrators and farm administrators groups have full control permissions on the local registry–based URL for the Central Administration.
-

  Note:

  Incorrectly editing the registry might severely damage the system. Before making changes to the registry, back up any valued data on the computer.

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. In Registry Editor, in the tree view, locate the following registry key:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\14.0\WSS\CentralAdministrationURL.
3. Right-click the registry key, and then click **Permissions**.
4. Make sure that the **Administrators** and **WSS_ADMIN_WPG** local groups have **Allow Full Control** permissions, and no **Deny** permissions have been set. Do not remove or change permissions for any other group or user entry for this registry key.

Resolution: Restart the update of the Central Administration Web site port

1. Verify that you meet the following minimum requirements: See **Add-SPShellAdmin**.
2. On the **Start** menu, click **All Programs**.
3. Click Microsoft SharePoint 2010 Products.
4. Click SharePoint 2010 Management Shell.
5. At the Windows PowerShell command prompt, type the following command:

   Set-SPCentralAdministration -Port <Int32>

Where:

- <*Int32*> is the new port number.

For more information, see Set-SPCentralAdministration (*http://technet.microsoft.com/library/a8bf87b6-18e6-4ba0-ada9-91ee9f4199ec(Office.14).aspx*).

Note:

We recommend that you use Windows PowerShell when performing command-line administrative tasks. The Stsadm command-line tool has been deprecated, but is included to support compatibility with previous product versions.

Throttling starts alert- Events 8032 8062 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SPServer throttling starts

Event ID: 8032 or 8062

Summary: The front-end Web throttling feature is introduced in Microsoft SharePoint Foundation 2010 to keep the server from running out of resources for high-priority server jobs. Throttling monitors performance counters on the server and begins to reject low-priority jobs by returning a 503 error message when the counter values exceed or drop lower than predefined thresholds.

Symptoms: The following symptoms might appear:

- Users receive a 503 error in the browser: The server is busy now. Try again later.
- This event appears in the event log: Event ID: 8032 Description: Http throttling starts because a heavy load was detected on <server name> the web app name. The excessive performance counters include: <performance counter name>.
- This event appears in the event log: Event ID: 8062 Description: Http throttling on <server name> stops because there is no heavy load detected now. <# of requests> requests have been throttled during the throttling period.

Cause: CPU usage, available memory, ASP.NET queue length, and ASP.NET queue wait time, have exceed or dropped lower than the predefined threshold on the front-end Web servers.

Resolution: Change the throttling threshold

1. Click Start, click All Programs, click Microsoft SharePoint 2010 Products, and then click SharePoint Management Shell. A Command Prompt window opens.
2. Enter the following Windows PowerShell command to read the threshold value for performance counters.

Disable-SPWebApplicationHttpThrottling URL

3. Enter the following command to obtain the current setting of the performance counter thresholds.

Get-SPWebApplicationHttpThrottlingMonitors URL

4. Review the thresholds and decide whether you have to change the current values to less-restrictive thresholds. For example, the following Windows PowerShell command can be used to set the CPU percentage threshold to 75 percent.

Set-SPWebApplicationHttpThrottlingMonitor URL -Category Processor -Counter "% Processor Time" -instance _Total -Max 75

Resolution: Disable the throttling feature

1. On the SharePoint Central Administration Web site, in the **Application Management** section click **Manage web applications**.
2. On the **Web Application** tab of the ribbon, click **General Settings** and select **Resource Throttling** to turn off HTTP throttling.

   Note:

   Turning off the throttling feature puts the server at risk of running out of resources to serve high-priority jobs in case of high workload. We do not recommend that you ordinarily turn off the throttling feature.

Resolution: Upgrade hardware

- Review your capacity plan. You can take different actions can be taken as remedies depending on the reason that throttling is triggered:

1. Add more memory
2. Upgrade CPU
3. Upgrade front-end Web servers
4. Add more front-end Web servers
5. Upgrade SQL Server host servers

Cannot retrieve end point - Event 8070 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Cannot retrieve end points

Event ID: 8070

Summary: The Application Discovery and Load Balancer Service Application is unable to retrieve the list of end points for a service application from the remote farm.

Symptoms: This event appears in the event log: Event ID: 8070 Description: An exception occurred when trying to call GetEndPoints: <EndPoint Name>.

Cause: One or more of the following might be the cause:

- This farm does not have permissions to connect to the remote farm.
- Network errors or connectivity issues prevent this operation from succeeding.

Note:

You must be a member of the Farm Administrators SharePoint group on the Central Administration site to perform the following task.

Resolution: Ensure that this farm has permissions to connect to the remote farm

- Contact the administrator of the remote farm to ensure that the following is true:
  - This farm has been added as a trusted farm in the remote farm.
  - This farm's service account has permissions to access the topology service on the remote farm.
- Ensure that the remote farm has been added as a trusted farm on this farm.
- To establish the trust between two server farms, each farm must add the other farm's public root certificate to the list of trusted root authorities by using the **New-SPTrustedRootAuthority**Windows PowerShell command. For more information, see New-SPTrustedRootAuthority (*http://technet.microsoft.com/library/25458530-4f0d-491c-80d3-61b8f1f0dd7e(Office.14).aspx*).

Resolution: Ensure that there are no network issues in connecting to the remote farm

- Ping the servers in the remote farm to ensure that they are available.
- Contact the remote farm administrator to ensure that there are no connectivity issues on that farm.

Log folder does not exist - Event 8074 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Log folder does not exist

Event ID: 8074

Summary: The logging folder specified in the error message does not exist or cannot be accessed.

Symptoms: This event appears in the event log: Event ID: 8074 Description: Unable to access directory <directoryname> on server <servername>. Ensure that this directory exists and that the account <domain>\<username> can access it.

Cause: One or more of the following might be the cause:

- The folder does not exist.
- The SharePoint 2010 Tracing Service (SPTraceV4) account does not have permissions to read and write to this folder.

Resolution: Verify that usage logging folder exists

- Log on to the server that is listed in the event.
- Navigate to the folder that is listed in the event.
- If the folder does not exist, create the folder.
- Verify that the SharePoint 2010 Tracing Service (SPTraceV4) account has read, write, and delete permission to the folder.

Usage timer job failed - Event 8075 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Usage timer job failed

Event ID: 8075

Summary: The Usage Data Processing timer job failed.

Symptoms: This event appears in the event log: Event ID: 8075 Description: The Usage Data Processing timer job failed. You can rerun this job using the Timer Job Status page in the SharePoint Central Administration site.

Cause: One or more of the following might be the cause:

- Usage logging is not enabled.
- The farm service account does not have sufficient permissions to the log folder.
- The disk on which the log folder is located is full.
- The logging database does not exist or cannot be written to.
- There were network issues between the farm server and the database server.

Resolution: Verify that usage logging is running on all servers in the farm

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators SharePoint group.
2. On the Central Administration Home page, under **System Settings**, click **Manage servers in this farm**.
3. On the Servers in Farm page, in the **Server** section, record the names of all the servers in the farm.
4. For each server in the farm, do the following: In the Services snap-in, verify that the SharePoint 2010 Tracing Service (SPTraceV4) service is enabled and started. If it is not started, start it.
5. From the **Log On** tab, record the Run As account for each service.

Resolution: Verify that usage logging folder exists

1. Log on to the server that is listed in the event.
2. Navigate to the folder that is listed in the event.
3. If the folder does not exist, create the folder.
4. Verify that the SharePoint 2010 Tracing Service (SPTraceV4) Run As account has read, write, and delete permissions to the folder.

Resolution: Verify that the logging database exists

- Verify that the user account that is performing this procedure is a member of the Farm Administrators SharePoint group.
- On the Central Administration Home page, click **Monitoring**.
- On the Monitoring page, in the **Reporting** section, click **Configure usage and health data logging**.
- On the Configure web analytics and health data collection page, in the **Usage Data Collection Settings** section, record the server and location of the log folder from the **Log file location** box.
- In the **Logging Database Server** section, record the location of the logging database from the **Database Server** and **Database Name** boxes.
- In SQL Server Management Studio, connect to the database server.
- Expand the **Databases** node, and verify that the database exists and that it is online.

Resolution: Rerun the timer job

- Verify that the user account that is performing this procedure is a member of the Farm Administrators SharePoint group.
- On the Central Administration Home page, click **Monitoring**.
- On the Monitoring page, in the **Reporting** section, click **Configure usage and health data logging**.
- On the Job Definitions page, click the Microsoft SharePoint Foundation Usage Data Processing timer job.
- On the Edit Timer Job page, click **Run Now**.

Business Data Connectivity Service - BDC database adapter connection exception - Event 8080 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Business Data Connectivity Service - BDC database adapter connection exception

Event ID: 8080

Summary: The Business Data Connectivity service runtime reads the metadata defined in the service application model, establishes a connection with the external data source, and calls the appropriate methods defined in the application model for any of the operations. This event is logged if this connection cannot be established for a database. None of the operations triggered by client applications will be executed, and the data may be rendered obsolete.

Symptoms: This event appears in the event log: Event ID: 8080 Description: The BDC service application %1 failed to open connection using %2.

Cause: One or the more of the following might be the cause:

- The Business Data Connectivity service application model does not have the correct connection properties for the external data source.
- The external data source is currently not functioning and is not responding.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following procedure.

Resolution: Verify that the external data source connection properties are correct

1. On the Central Administration Home page, click **Application Management**.
2. On the Application Management page, in the **Service Applications** section, click **Manage service applications**.
3. On the Service Applications page, select the **BDC Service Application**.
4. On the **Edit** tab, in the **View** group, click **External systems**.
5. Click the external system to view its instances.

   Tip:

   By default, the only instances of external system types that are configurable are databases and Web services.

6. Select the external system name.
7. Edit or view the settings.

For more information about the settings that are available for configuring a database external system, see Configure an instance of an external system (*http://technet.microsoft.com/library/541e5ea6-adf7-496c-a7cb-b1ea4fb4e6e3(Office.14).aspx#configinstance*).

For more information about managing BDC models, see Manage BDC models (*http://technet.microsoft.com/library/f2d973ee-b8e0-4e5f-9363-24c78bbd0011(Office.14).aspx*).

Resolution: Verify that the network connection to the external data source is working

- Open a Command Prompt window on the application server and type **PING**<*servername*>, where <*servername*> is the database server that hosts the external data source.

Business Data Connectivity Service - BDC Web service proxy generations exception - Event 8082 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Business Data Connectivity Service - BDC Web service proxy generation exception

Event ID: 8082

Summary: While working with a Web service, the Business Data Connectivity service will first obtain a proxy and then call the appropriate methods based on the metadata defined in the application model. This event is logged when the Business Data Connectivity service fails to obtain a proxy to a Web service. This will affect data synchronization between the client computer and the external data source.

Symptoms: The following event appears in the event log: Event ID: 8082 Description: The Business Data Connectivity Service Could not obtain a proxy to WebService for External Data Source '% ExternalDataSourceName %.

Cause: One or the more of the following might be the cause:

- The Business Data Connectivity service application model does not have the correct connection properties for the external data source.
- The external data source is down and is not responding.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following action.

Resolution: Verify that the external data source connection properties as defined in the application model are correct

1. On the Central Administration Home page, click **Application Management**.
2. On the Application Management page, in the **Service Applications** section, click **Manage service applications**.
3. On the Service Applications page, select the **BDC Service Application**.
4. On the **Edit** tab, in the **View** group, click **External systems**.

   Tip:

   By default, the only external system type that is configurable is a Web service. By default, the only instances of external system types that are configurable are databases and Web services.

5. Point to the external system, click the arrow that appears, and then click **Settings**.
6. Edit or view the settings.

For more information about how to configure and manage an external data source, see Configure an instance of an external system (*http://technet.microsoft.com/library/541e5ea6-adf7-496c-a7cb-b1ea4fb4e6e3(Office.14).aspx#configinstance*) in the article "Manage external systems (SharePoint Foundation 2010)."

For more information about managing BDC models, see Manage BDC models (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/f2d973ee-b8e0-4e5f-9363-24c78bbd0011(Office.14).aspx#deleteamodel*).

Resolution: Verify that the external data source is accessible

- From the application server, ping the database server that hosts the external data source to confirm that the servers can communicate over the network.

Business Data Connectivity Service - BDC Proxy - unexpected exception - Event 8085 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Business Data Connectivity Service - BDC proxy unexpected exception

Event ID: 8085

Summary: When a Web server receives a request from a client computer, it routes the request to an application server through a load balancer. The load balancer maintains a list of available servers for a given service application. If the Business Data Connectivity service application on one or more application servers does not respond, the load balancer drops the application server from the list of available servers and this event is logged.

If the Business Data Connectivity service application is enabled on more than one application server, the client computers may not be affected. If the service application is enabled on only one application server, the client computers that rely on the metadata in the Business Data Connectivity metadata store will fail to read or write data from the external data sources defined in the metadata. The load balancer will ping the service application periodically and will automatically re-enlist it when it responds.

Symptoms: The client computers fail to read or write data from the external data sources.

Cause: One or the more of the following might be the cause:

- The application server is not accessible or the Business Data Connectivity service application model does not have the correct connection properties for the external data source.
- The external data source is currently not functioning and is not responding.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following actions.

Resolution: Verify that the application server is available

1. On the Central Administration Home page, in the **System Settings** section, click **Manage servers in this farm**.
2. On the Servers in Farm page, verify that the status of the server on which the Business Data Connectivity service runs is **No Action Required**.

Resolution: Verify that the Business Data Connectivity service application is provisioned correctly

1. On the Central Administration Home page, click **Application Management**.
2. On the Application Management page, in the **Service Applications** section, click **Manage service applications**.
3. On the Service Applications page, find the **Business Data Connectivity Service Application**, and in the **Status** column, verify that the service proxy status is **Started**.

Business Data Connectivity Service - SQL exception - Event 8086 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Business Data Connectivity Service - SQL exception

Event ID: 8086

Summary: The Business Data Connectivity service application connects to the metadata store to allow users to manage the metadata in the metadata store. This event is logged when the service application fails to connect to the database. The Business Data Connectivity metadata in the metadata store will not be accessible. This will impact importing and exporting application models or updating properties for any of the Business Data Connectivity objects by using the Business Data Connectivity Service Application Proxy page in the SharePoint Central Administration Web site.

Symptoms: This event appears in the event log: Event ID: 8086 Description: The BDC service application %name% error occurred because of a database exception.

Cause: One or the more of the following might be the cause:

- The metadata database server is down or not accessible because of network issues.
- The connection information for the Business Data Connectivity service application metadata database is incorrect.
- The Business Data Connectivity service application metadata database was not provisioned correctly.

Resolution: Verify the availability of the metadata database server

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **Application Management**.
3. On the Application Management page, in the **Service Applications** section, click **Manage service applications**.
4. On the Service Applications page, select the **Business Data Connectivity Service Application**, and click **Properties** on the ribbon.
5. Verify that the database server listed on the Properties page is available and can be connected to from SharePoint 2010 Products.

ULS trace log reaching maximum size - Event 8094 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: ULS trace log reaching maximum size

Event ID: 8094

Summary: The SharePoint 2010 Tracing Service (SPTracev4) is used by Microsoft SharePoint Foundation 2010 to manage trace message output. When trace logging is enabled, administrators can specify the path used to store the trace log file. This log file is used by many applications that are built on SharePoint Foundation 2010. This event occurs when the configured log file location is low on space. It serves as a warning that logging may stop soon unless more space is made available or the space allocated to logging is increased.

Symptoms: This event appears in the event log: Event ID: 8094 Description: Trace logs are reaching to the configured storage limit [configured limit]. Please increase the maximum storage settings. Otherwise, older files will be deleted once the limit is reached.

Cause: The configured log file location has insufficient free disk space for logging, or the maximum space allocated for logging is too low.

Resolution: Increase the space limit for log files

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **Monitoring**.
3. On the Monitoring page, in the **Reporting** section, click **Configure diagnostic logging**.
4. In the **Trace Log** section, in the **Maximum storage space for Trace Logs (GB)** box, type a larger number of gigabytes (GB) you want to allocate to the log files. When log files reach this size on disk, older log files will automatically be deleted
5. Click **OK**.

Resolution: Change the location of the log files

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **Monitoring**.
3. On the Monitoring page, in the **Reporting** section, click **Configure diagnostic logging**.
4. In the **Trace Log** section, in the **Path** box, type the new location for the log file on a drive or partition that has sufficient disk space.
5. Click **OK**.

Resolution: Free disk space

1. Use the Disk Cleanup tool to free disk space where the trace log files are stored.
2. Verify that the tracing service has sufficient disk space to write the log file.
3. If the trace logging service has insufficient disk space to write the log files, delete the contents of the Temp folders on the drive.

ULS usage log reaching maximum size - Event 8095 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: ULS usage log reaching maximum size

Event ID: 8095

Summary: The SharePoint 2010 Tracing Service (SPTracev4) is used by Microsoft SharePoint Foundation 2010 to manage usage log output. When usage logging is enabled, administrators can specify the path used to store the usage log file. This log file is used by many applications that are built on SharePoint Foundation 2010. This event occurs when the configured log file location is low on space. It serves as a warning that logging may stop soon unless more space is made available or the space allocated to logging is increased.

Symptoms: This event appears in the event log: Event ID: 8095 Description: Usage logs are reaching to the configured storage limit [configured limit]. Please increase the maximum storage settings. Otherwise, older files will be deleted once the limit is reached.

Cause: The configured log file location has insufficient free disk space for logging, or the maximum space allocated for logging is too low.

Resolution: Increase the space limit for log files

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **Monitoring**.
3. In the Reporting section, click Configure usage and health data collection.
4. On the Configure web analytics and health data collection page, in the **Usage Data Collection Settings** section, type a larger number of gigabytes (GB) to allocate to the log files. When log files reach this size on the disk, older log files will automatically be deleted.
5. Click **OK**.

Resolution: Change the location of the log file

1. On the Central Administration Home page, click **Monitoring**.
2. In the Reporting section, click Configure usage and health data collection.
3. On the Configure web analytics and health data collection page, in the **Usage Data Collection Settings** section, type a new location for the log file on a drive or partition that has sufficient disk space.
4. Click **OK**.

Resolution: Free disk space

1. Run the Disk Cleanup tool to free disk space where the usage log files are stored.
2. Verify that the usage logging service has sufficient disk space to write the log file.
3. If the usage logging service has insufficient disk space to write the log file, delete the contents of the Temp folders on the drive.

To check the usage log file

4. On the Central Administration Home page, click **Monitoring**, and in the **Reporting** section, click **Configure usage and health data collection**.
5. On the Configure web analytics and health data collection page, in the **Usage Data Collection Settings** section, copy the path of the usage log file.
6. In Windows Explorer, navigate to the usage log file by using the copied path. Usage log files are in binary format and the contents cannot be easily viewed and understood. The file size of the usage log increases over time and confirms that usage logging is working.

STS signing certificate missing - Event 8303 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Security Token Service signing certificate missing

Event ID: 8303

Summary: The Security Token service (STS) signing certificate that Microsoft SharePoint 2010 Products uses to authenticate users is missing.

Symptoms: One or more of the following symptoms might appear:

- Users are unable to log in to SharePoint 2010 Products.
- This event appears in the event log: Event ID: 8303 Description: The Access Data Services is no longer available. [Session: <session ID> User: <username>].

Cause: One of the following might be the cause:

- The STS signing certificate that is included with SharePoint 2010 Products is missing.
- The self-signed STS signing certificate, or the external certificate that you are using, is missing.

Resolution: Import a new STS signing certificate from the SharePoint 2010 Products farm

1. Retrieve the root certificate of your SharePoint 2010 Products farm.
2. Export the root certificate.
3. Use the **makecert** utility to generate a new STS signing certificate, based on the root certificate.
4. Import the new certificate into the certificate store for your operating system.

Resolution: Import a new self-signed STS signing certificate or external certificate

1. Retrieve the root certificate of your SharePoint 2010 Products farm.
2. Export the root certificate.
3. Regenerate the certificate.
4. Import the new certificate into the certificate store for your operating system.

STS cannot sign credentials - Event 8304 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Security Token Service cannot sign credentials

Event ID: 8304

Summary: The Security Token service (STS) cannot sign user credentials.

Symptoms: One or more of the following symptoms might appear:

- Users are unable to log on to Microsoft SharePoint Foundation 2010.
- Logon fails.
- People Picker fails to search or resolve and return an error message.
- This event appears in the event log: Event ID: 8307 Description: An exception occurred when trying to create signing credential: <exception>.

Cause: An error occurred with the claims provider that is specified in the exception description.

Resolution: Import a new STS signing certificate from the SharePoint 2010 Products farm

1. Retrieve the root certificate of your Microsoft SharePoint 2010 Products farm.
2. Export the root certificate.
3. Use the **makecert** utility to generate a new STS signing certificate based on the root certificate.
4. Import the new certificate into the certificate store for your operating system.

Resolution: Import a new self-signed STS signing certificate or external certificate

1. Retrieve the root certificate of your SharePoint 2010 Products farm.
2. Export the root certificate.
3. Regenerate the certificate.
4. Import the new certificate into the certificate store for your operating system.

Claims cannot establish endpoint - Event 8305 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Security Token Service claims cannot establish an endpoint

Event ID: 8305

Summary: The Security Token service (STS) claims authentication cannot establish an endpoint.

Symptoms: One or more of the following symptoms might appear:

- Users are unable to log on to Microsoft SharePoint Foundation 2010.
- Logon fails.
- This event appears in the event log: Event ID: 8305 Description: An exception occurred when trying to establish endpoint for context: <exception>.

Cause: The claims provider is not configured correctly.

To confirm that the STS service is running by using Windows PowerShell

1. Verify that you meet the following minimum requirements: See **Add-SPShellAdmin**.
2. On the **Start** menu, click **All Programs**.
3. Click Microsoft SharePoint 2010 Products.
4. Click SharePoint 2010 Management Shell.
5. At the Windows PowerShell command prompt, type the following command:

   Get-SPServiceApplicationPool | Where {$_.DisplayName -eq *<DisplayName>*}| Format-List

Where:

- *<DisplayName>* is the display name of the STS service application pool. By default, this value is "SecurityTokenServiceApplicationPool".

6. Verify that the `Status` of the application pool is `Online`.

Resolution: Revert changes to the Web.config file

1. If the Web.config file was modified, try manually reverting to the previous version, or — if you backed up the file — restore the backup.

STS claims provider error - Event 8307 (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Security Token Service claims provider error

Event ID: 8307

Summary: The Security Token service (STS) experienced an error.

Symptoms: One or more of the following symptoms might appear:

- Users are unable to log on to Microsoft SharePoint Foundation 2010.
- Logon fails.
- People Picker fails to search or resolve and return an error message.
- This event appears in the event log: Event ID: 8307 Description: An exception occurred in <Claim Provider Name> claim provider when calling <Method Name>: <Exception>.

Cause: An error occurred with the claims provider that is specified in the exception description.

Resolution: Disable the claims provider

1. Disable the claims provider that caused the error and contact the manufacturer of the claims provider for help resolving the error. For more information, see Configure claims authentication (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/ef8c3024-26de-4d06-9204-3c6bbb95fb14(Office.14).aspx*)

   Important:

   Some SharePoint Foundation 2010 components might require the claims provider and might not function correctly if it is disabled. For example, shared service applications might fail during a call because the security modules expect that the system claims were added by this provider.

Administration service is not running (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Administration service is not running

Event ID: No event ID

Summary: The Microsoft SharePoint Foundation Administration service is required to run on all servers in a Microsoft SharePoint Foundation 2010 farm. This service performs multiple operations on the local server computers that require local administrator permissions for operations; for example, creating and deleting Web applications and service applications, and starting and stopping services. If this service is not running on any server in a SharePoint Foundation 2010 farm, administrative operations can fail or partially succeed.

Cause: One or more of the following might be the cause:

- The SharePoint Foundation Administration service was stopped by an administrator on a particular computer.
- The user name or password for the account that the SharePoint Foundation Administration service is set to run as is incorrect.
- An error condition in the SharePoint Foundation Administration service caused the service to terminate.

Resolution: Start the administration service

- Start the SharePoint Foundation Administration service by using the Services Microsoft Management Console (MMC) snap-in in Windows. Click **Start**, click **Run** and type the following:

services.msc

Resolution: Check the service account

- If the service fails to start, ensure that the user name and account have membership in the Administrators group on the local computer.

Resolution: Repair the configuration

- If the service could not be started, try to repair the SharePoint Foundation configuration on that server by running the SharePoint Products and Technologies Configuration Wizard.

Document conversion launcher unavailable (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Document conversion launcher unavailable

Event ID: None

Summary: The Document Conversions Launcher Service starts document conversions on an application server. If the Document Conversions Launcher Service stops, the Document Conversions Load Balancer Service continues and any document conversion will fail. To resume the document conversion process, you must restart the Document Conversions Launcher Service.

Symptoms: One or more of the following symptoms might appear:

- Documents are not being converted.
- The Document Conversions Launcher Service is not running.

Cause: The Document Conversions Launcher service is no longer running. This can happen when an administrator unintentionally stops the service or the server runs out of RAM.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following task.

Resolution: Restart the services

1. On the SharePoint Central Administration Home page, in the **System Settings** section, click **Manage services on server**.
2. On the Services on Server page, click **Document Conversions Launcher Service**.
3. In the **Select Server** section, verify that the server that you want is selected. If it is not selected, on the **Server** menu, click **Change Server**.
4. On the Select Server page, click the name of the server on which you want to run the Document Conversions Launcher Service.
5. In the **Communication Scheme** section, select the scheme that you want the launcher to use for communication. The default is **http**.
6. In the **Port Number** section, type the port number that you want the launcher to use for communication. Choose a port number that is not used by other services on the server, but which is open in the firewall on the server.
7. Click **OK**.

Document conversion load balancer unavailable (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Document conversion load balancer unavailable

Event ID: None

Summary: The Document Conversions Load Balancer Service manages the availability of document converters. Stopping the service stops the document conversion process and turns off the Document Conversions Launcher Service. To resume the document conversion process, you must restart the Document Conversions Load Balancer Service, and then start the Document Conversions Launcher Service.

Symptoms: One or more of the following symptoms might appear:

- Documents are not being converted.
- Only one server seems to be converting documents.
- The Document Conversions Load Balancer Service is not running.

Cause: The Document Conversions Load Balancer Service is no longer running. This can occur when an administrator unintentionally stops the service or the server runs out of RAM.

Note:

You must be a member of the Farm Administrators SharePoint group to perform the following task.

Resolution: Restart the Document Conversions Load Balancer Service

1. On the SharePoint Central Administration Home page, in the **System Settings** section, click **Manage services on server**.
2. On the Services on Server page, click Document Conversions Load Balancer Service.
3. In the **Select Server** section, verify that the server that you want is selected. If it is not selected, on the **Server** menu, click **Change Server**.
4. On the Select Server page, click the name of the server on which you want to run the Document Conversions Load Balancer Service.
5. In the **Communication Scheme** section, select the scheme that you want the load balancer to use for communication. The default is **http**.
6. In the **Port Number** section, type the port number that you want the load balancer to use for communication. Choose a port number that is not used by other services on the server, but which is open in the firewall on the server.
7. Click **OK**.

Resolution: Restart the Document Conversions Launcher Service

1. On the SharePoint Central Administration Home page, in the **System Settings** section, click **Manage services on server**.
2. On the Services on Server page, click **Document Conversions Launcher Service**.
3. In the **Select Server** section, verify that the server that you want is selected. If it is not selected, on the **Server** menu, click **Change Server**.
4. On the Select Server page, click the name of the server on which you want to run the Document Conversions Launcher Service.
5. In the **Communication Scheme** section, select the scheme that you want the launcher to use for communication. The default is **http**.
6. In the **Port Number** section, type the port number that you want the launcher to use for communication. Choose a port number that is not used by other services on the server, but which is open in the firewall on the server.
7. Click **OK**.

Knowledge article is not yet available (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Knowledge article is not yet available

Event ID: None

Summary: The Microsoft System Center Operations Manager Management Pack monitors Microsoft SharePoint Foundation 2010. System Center Operations Manager raised an alert because of a problem in SharePoint Foundation 2010.

The link in the alert would go to a knowledge article with more details about how to resolve the problem. However, the knowledge article is not yet available. The article will be made available at a later date. To resolve the problem, try one or more of the following, in the order given (click the link to go to the procedure in this article):

- View and resolve SharePoint Health Analyzer alerts by using Central Administration
- Review the Windows Event log.
- Review the diagnostic log.
- Review the Management Pack Guide and the product documentation.
- Restart the affected service.
- Restart the application pool
- Restart Internet Information Services.
- Restart the affected server.
- Contact Microsoft Support.

View and resolve SharePoint Health Analyzer alerts by using Central Administration

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. In Central Administration, on the Home page, click **Monitoring**.
3. On the Monitoring page, in the **Health Status** section, click **Review problems and solutions**.
4. On the Review problems and solutions page, click the alert that you want to view and resolve.
5. To resolve the problem, follow the guidance given in the **Remedy** section of the **Review problems and solutions** dialog box. Keep the dialog box open so you can run the rule again to confirm the resolution.
6. After following the guidance given in the **Remedy** section, in the **Review problems and solutions** dialog box for the alert, click **Reanalyze Now** to confirm the resolution. If the problem is resolved, the alert status changes to **4-Success**.

Restart the application pool

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer.
2. Perform the steps in the following article: Recycle an Application Pool on Demand (*http://go.microsoft.com/fwlink/?LinkId=168806*).

Sandboxed code is running (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SPServiceInstance sandboxed code is running

Event ID: No event ID

Summary: The SharePoint Sandboxed Code Host is a Windows NT service that runs on each Microsoft SharePoint Foundation server.

Symptoms: You are unable to perform requests that require the execution of user code or activation of sandboxed solutions that contain user code. The task that fails depends on the topology and on the server that has the stopped service.

Cause: The SharePoint Sandboxed Code Host service is not running.

Resolution: Start the service on the given server

- You can restart the SharePoint Sandboxed Code Host on a specific server by using the following command at an elevated command prompt:

  net start spusercodev4

SharePoint Administration service is disabled (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SharePoint Administration service is disabled

Event ID: No event ID

Summary: The SharePoint Administration service V4 (SPAdminV4) is disabled, which prevents local server administration timer jobs from changing local server settings to match farm-wide settings.

Cause: The SharePoint Administration service V4 (SPAdminV4) is disabled and cannot be started.

Resolution: Disable the throttling feature

- If you want the SharePoint Administration service V4 (SPAdminV4) to run in the environment, set the service to start automatically and then start the service. This can be achieved by using either the Services Microsoft Management Console (MMC) snap-in (services.msc) or, in the Command Prompt window, by using the following two commands in order and executed by a farm administrator who is also a member of the Administrators group on the local computer.

```
SC CONFIG SPAdminV4 start= auto
SC START SPAdminV4
```

Resolution: Execute administration timer jobs without starting administration service

- If you do not want the SharePoint Administration service V4 (SPAdminV4) to be set to run in the environment — for example because of least-privilege considerations — the administration timer jobs can be executed directly on the local server without starting the administration service. To execute the timer jobs immediately, in SharePoint Management Shell, run the following Windows PowerShell command:

```
Start-SPAdminJob
```

Note:

The **Start-SPAdminJob** operation must be run on all computers in the farm where the SharePoint Administration service V4 (SPAdminV4) is not run. Run this command to perform provisioning and other administrative tasks that would typically be performed by using the SharePoint Foundation Timer service (SPTimer_V4).

SharePoint Foundation 2010 search is not running (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SharePoint Foundation search is not running

Event ID: No event ID

Summary: The Microsoft SharePoint Foundation 4 Search service (SPSearch4) is a Windows NT service that runs on each server that hosts a search service application.

Symptoms: One or more of the following symptoms might appear:

- The Microsoft SharePoint Foundation 4 Search service (SPSearch4) is stopped.
- You are unable to perform tasks when you attempt to use the crawl, query, or administration search functionality. The task that fails depends on the topology and on which server has the stopped service.

Cause: The Microsoft SharePoint Foundation 4 Search (SPSearch4) service is not running.

Resolution: Start the service on the server

- You can restart the Microsoft SharePoint Foundation 4 Search (SPSearch4) service on a specific server by typing the following command at an elevated command prompt:

  net start spsearch4

SharePoint Health Analyzer has detected an error or warning (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SharePoint Health Analyzer has detected an error or warning

Event ID: None

Summary: The SharePoint Health Analyzer has detected an error or warning that affects the performance, availability or security of the farm. For instructions for fixing the error or warning condition, review the error message and explanation..

Resolution: View and resolve SharePoint Health Analyzer alerts by using Central Administration

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. In Central Administration, on the Home page, click **Monitoring**.
3. On the Monitoring page, in the **Health Status** section, click **Review problems and solutions**.
4. On the Review problems and solutions page, click the alert that you want to view and resolve.
5. To resolve the problem, follow the guidance given in the **Remedy** section of the **Review problems and solutions** dialog box. Keep the dialog box open so you can run the rule again to confirm the resolution.
6. After following the guidance given in the **Remedy** section, in the **Review problems and solutions** dialog box for the alert, click **Reanalyze Now** to confirm the resolution. If the problem is resolved, the alert status changes to **4-Success**.

SharePoint Timer service could not start (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SharePoint Services Timer service could not start

Event ID: None

Summary: Microsoft SharePoint Foundation 2010 uses the Windows SharePoint Services Timer V4 (SPTimerV4) service to run most system tasks. The timer service is restarted when the farm service account changes, and it is restarted daily during the timer service recycle job. If SharePoint Foundation 2010 cannot start the timer service, updates to the farm configuration will be not be synchronized to the local server.

Symptoms: Frequently recurring timer jobs, such as Immediate Alerts and Workflow, do not run. Updates to the farm configuration are not synchronized to the local server.

Cause: SharePoint Foundation 2010 cannot start the Windows SharePoint Services Timer V4 (SPTimerV4) service.

Resolution: Start the timer service

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer.
2. Open a Command Prompt window, type the following command at the command prompt, and then press ENTER:

net start sptimerv4

3. If the service does not start, ensure that the service identity account is configured correctly by using the "Verify the service account" procedure later in this article.

Resolution: Verify the service account

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer.
2. Click Start, click Administrative Tools, and then click Services.
3. In the **Services** snap-in, right-click the Windows SharePoint Services Timer V4 service, and then click **Properties**.
4. In the **Service Properties** dialog box, on the **Log On** tab, type the password for the account, confirm the password, and then click **OK**.
5. Right-click the service, and then click **Start**.

SharePoint Timer service is not running (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Windows SharePoint Services Timer service is not running

Event ID: None

Summary: Microsoft SharePoint Foundation 2010 uses the Windows SharePoint Services Timer V4 (SPTimerV4) service to run most system tasks.

Symptoms: Frequently recurring timer jobs, such as Immediate Alerts and Workflow, do not run. Updates to the farm configuration are not synchronized to the local server.

Cause: The Windows SharePoint Services Timer V4 (SPTimerV4 service is not running.

Resolution: Start the timer service

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer.
2. Open a Command Prompt window, type the following command at the command prompt, and then press ENTER:

net start sptimerv4

3. If the service does not start, ensure that the service identity account is configured correctly by using the "Verify the service account" procedure later in this article.

Resolution: Verify the service account

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer.
2. Click Start, click Administrative Tools, and then click Services.
3. Right-click Windows SharePoint Services Timer V4, and then click Properties.
4. On the **Log On** tab, confirm that the account being used is a domain user account and is a member of the following:
   - **dbcreator** fixed SQL Server server role
   - **securityadmin** fixed SQL Server server role
   - **db_owner** fixed database role for all databases in the server farm
5. If the account has sufficient permissions, confirm the password by typing the password for the account, retyping the password in the **Confirm password** box, and then clicking **OK**.
6. Start the service by right-clicking the service name in the Services console, and then clicking **Start**.

SQL Server remote access is disabled (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: SQL Server remote access is disabled

Event ID: None

Summary: Microsoft SharePoint 2010 Products uses Microsoft SQL Server 2008 Express to store data, to which remote access is disabled by default. Depending on your farm setup, there is the possibility that a remote computer will need access to the SQL Server 2008 Express database.

Symptoms: Connecting to SQL Server 2008 Express from a remote server fails.

Cause: Remote access is disabled

Resolution: Enable remote access

1. Enable remote access. For more information, see How to configure SQL Server 2005 to allow remote connections (*http://go.microsoft.com/fwlink/?LinkId=188484&clcid=0x409*).

Tracing service is not running (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Tracing service is not running

Event ID: No event ID

Summary: The Microsoft SharePoint Foundation Tracing (SPTrace) service is a required service on all Microsoft SharePoint Foundation servers. If this service is stopped, error messages are not logged on the server.

Symptoms: No trace output is being recorded in the trace logs and no errors are being logged to the Windows log.

Cause: One or more of the following might be the cause:

- An administrator accidentally stopped the SharePoint Foundation Tracing service.
- An upgrade that was started on this server could not be completed.

Resolution: Start the Trace service

1. Log on to the SharePoint Foundation server as an administrator.
2. In a Command Prompt window, type the following at the command prompt:

net start SPTrace

Web application taking too long to render a page (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Web application taking too long to render a page

Event ID: None

Summary: The Microsoft SharePoint Foundation 2010 Executing Time/Page Request performance counter monitors how long a Web application takes to render a Web page. This performance counter threshold can be exceeded when the network temporarily experiences congestion or a peak in demand from the computer that is running Microsoft SQL Server. If the threshold is exceeded even when the network is not congested, the Web application is consuming too much memory.

Symptoms: One or more of the following symptoms might appear:

- Pages take too long to render.
- The Executing Time/Page Request performance counter threshold is frequently exceeded.

Cause: One or more of the following might be the cause:

- SharePoint Foundation 2010 is configured incorrectly.
- The server hardware is insufficient to handle user requests.

Resolution: Implement configuration best practices

- Follow the recommendations for the top configuration best practices in Best practices for operational excellence (*http://technet.microsoft.com/en-us/library/cc850692.aspx*).

Resolution: Tune Web server performance

- Follow the recommendations for physical architecture and tuning that can help improve the performance of Web servers in Tune Web server performance (Office SharePoint Server) (*http://technet.microsoft.com/en-us/library/cc298550.aspx*).

Web application unavailable (SharePoint 2010 Products)

Published: May 12, 2010

Alert Name: Web application unavailable

Event ID: None

Summary: This monitor attempts to access the Web application from the System Center Operations Manager (SCOM) server by using the Run as administrator account. The monitor is changed to an error state when the SCOM server receives a status code greater than 400.

Symptoms: The SCOM server receives a status code greater than 400.

Cause: One or more of the following might be the cause:

- The Web application is unavailable.
- The Run as administrator account does not have sufficient permission to access the Web application.

Resolution: Verify that the Web application exists and is running

1. In the Internet Information Services (IIS) snap-in, expand the server node and the **Sites** node.
2. Select the Web site for the Web application and ensure that the site is running. If it is not running, start it. If you cannot start it, go to the next step.
3. Select the **Application Pools** node. In the right-pane, ensure that the application pool for the Web application is started. If it is not, start it. If you cannot start it, go to the next step to check the Identity account.
4. Right-click the application pool, and then click **Advanced Settings**.
5. In the **Advanced Settings** dialog box, in the **Process Model** section, ensure that the Identity account has sufficient permissions to run the Web application.
6. You might have to update the password for the Identity account. To do this, click the ellipsis next to the account.
7. In the Application Pool Identity dialog box, click Set.
8. In the **Set Credentials** dialog box, type the account name and password, and then click **OK**.
9. In the IIS snap-in, try to start the application pool. If it does not start, the account does not have sufficient permissions. If it does start, then start the Web site.

Resolution: Confirm that the Run as administrator account has sufficient permissions

1. On the Central Administration Home page, click **Security**, and in the **Users** section, click **Specify web application user policy**.
2. On the Authentication Providers page, select the correct Web application. To select a Web application, click the arrow next to the **Web Application** list, and then click **Change Web Application**. In the **Select Web Application** dialog box, click the correct Web application.
3. Click the Run as administrator account. This is the account that is specified as the Identity account in the above resolution. If the account is not listed, go to the next step.
4. Click Add Users.
5. On the Edit Users page, in the **Permission Policy Levels** section, select the **Full Control – Has full control** check box.
6. Click **Save**.

Web site unavailable (SharePoint 2010 Products)

Published: May 12, 2010

If a Web page is not available, SharePoint 2010 Products cannot render the Web page and users cannot access it.

Alert Name: Web site unavailable

Event ID: None

Summary: If a Web page is not available, SharePoint 2010 Products cannot render the Web page and users cannot access it.

Symptoms: The SharePoint 2010 Products Web site is down, or pages on the Web site do not render.

Cause: One or more of the following might be the cause:

- The Web site is unavailable.
- The management pack Run as administrator account does not have permission to access SharePoint 2010 Products Web site.

Resolution: Verify that the Web site appears in the site collection

1. On the Central Administration Web site, on the Quick Launch, click **Application Management**.
2. On the Application Management page, in the **Site Collections** section, click **View all site collections**.
3. If the relative URL of the site collection is invalid, run Management Pack discovery.
4. If the problem persists after running Management Pack discovery, verify the following:
    - The SharePoint Foundation server that is hosting the Web site is running and can be accessed on the network.
    - Internet Information Services (IIS) is running.

Resolution: Confirm that the Run as administrator account has sufficient permissions

1. On the Central Administration Home page, click **Security** and in the **Users** section, click **Specify web application user policy**.
2. On the Authentication Providers page, select the correct Web application. To select a Web application, click the **Web Application**, and then click **Change Web Application**. In the **Select Web Application** dialog box, click the correct Web application.

3. Click the Run as administrator account. This is the account that is specified as the Identity account in Information Internet Services (IIS) for the Web application that runs the Web site. If the account is not listed, click **Add Users**.
4. On the Edit Users page, in the **Permission Policy Levels** section, select the **Full Control – Has full control** check box.
5. Click **Save**.

SharePoint Health Analyzer rules reference (SharePoint Foundation 2010)

Updated: July 8, 2010

The articles in this section are articles for the SharePoint Health Analyzer. Typically, you would see these articles after clicking a link in an alert in the SharePoint Health Analyzer in Central Administration. You can use these articles to help you troubleshoot and resolve problems in Microsoft SharePoint Foundation 2010.

In this section:

- Web Applications using Claims authentication require an update (*http://technet.microsoft.com/library/9d2d8945-5a6f-45dc-91bd-b588720ba745(Office.14).aspx*)

This article provides information about the SharePoint Health Analyzer rule "Web Applications using Claims authentication require an update", and describes how to update Claims Authentication.

- Automatic update setting inconsistent across farm servers (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Automatic update setting inconsistent across farm servers", and describes how to configure automatic update settings to be consistent across the farm.

- Diagnostic logging is set to verbose (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Diagnostic logging is set to verbose", and describes how to configure diagnostic logging.

- The server farm account should not be used for other services (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "The server farm account should not be used for other services", and describes how to change the account that is used for other services.

- One or more services have started or stopped unexpectedly (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "One or more services have started or stopped unexpectedly", and describes how to start the service that is not running.

- Databases used by SharePoint have fragmented indices (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Databases used by SharePoint have fragmented indices", and describes how to reorganize and rebuild indexes.

- Content databases contain orphaned items (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Content databases contain orphaned items", and describes how to remove orphan sites from the content.

- Outbound e-mail has not been configured (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Outbound e-mail has not been configured", and describes how to configure outgoing e-mail settings in Central Administration.

- Some health analyzer rules do not have associated timer jobs (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Some health analyzer rules do not have associated timer jobs", and describes how to create the health data collection timer jobs.

- Drives are running out of free space (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Drives are running out of free space", and describes how to free disk space on the server computer.

- The paging file size should exceed the amount of physical RAM in the system (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "The paging file size should exceed the amount of physical RAM in the system", and describes how to increase the minimum size of the paging file.

- Built-in accounts are used as application pool or service identities (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Built-in accounts are used as application pool or service identities", and describes how to change the identity that is used for the service or application pool.

- Web Analytics: Monitors the health of the Report Consolidator component (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Web Analytics: Monitors the health of the Report Consolidator component", and describes how to enable data trimming to improve the performance of the Report Consolidator.

- Web Analytics: Verifies that when the Web Analytics is installed and running, usage logging is enabled in the farm (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule " Web Analytics: Verifies that when the Web Analytics is installed and running, usage logging is enabled in the farm", and describes how to enable usage logging.

- Web Analytics: Verifies that a web application is serviced by at most one Web Analytics service application proxy (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Web Analytics: Verifies that a web application is serviced by at most one Web Analytics service application proxy", and describes how to disassociate other Web Analytics service application proxies.

- Web Analytics: Verifies that the SQL Server Service Broker is enabled for the Web Analytics staging databases (SharePoint Foundation 2010)

This article provides information about the SharePoint Health Analyzer rule "Web Analytics: Verifies that the SQL Server Service Broker is enabled for the Web Analytics staging databases", and describes how to enable the service broker queue.

Web Applications using Claims authentication require an update (SharePoint Foundation 2010)

Published: May 12, 2010

Rule Name: Web Applications using Claims authentication require an update

Event ID: None

Summary: Web applications that use claims-based authentication are at risk for a potential security vulnerability that might allow users to elevate privileges. Web servers that host Web applications that use claims-based authentication are potentially vulnerable.

Cause: This can happen when you deploy a Microsoft ASP.NET 2.0-based Web application to a Web site that is hosted on a server running Microsoft SharePoint Foundation 2010 and you have Internet Information Services (IIS) 7.0 or IIS 7.5 running in Integrated mode on the server.

If you deploy partially trusted Web Parts or create external lists on the SharePoint site, these Web Parts or external lists can have more permissions than they should have. This issue might create a security risk on the SharePoint site. For example, these Web Parts or external lists may unexpectedly generate database requests or HTTP requests.

This issue occurs because of a change in the ASP.NET 2.0 authentication component. The change causes the partially trusted Web Parts or external lists to impersonate the application pool account. Therefore, the Web Parts have full permission to access the SharePoint site.

Resolution: Install the update

- To download the update, go to KB979917 - QFE for SharePoint issues - Perf Counter fix & User Impersonation (*http://code.msdn.microsoft.com/KB979917*).
- For more information about update, see Knowledge Base article 979917 (*http://support.microsoft.com/kb/979917*).

Automatic update setting inconsistent across farm servers (SharePoint Foundation 2010)

Published: June 4, 2010

Rule Name: Automatic update setting inconsistent across farm servers

Summary: Servers in the SharePoint farm do not have the same Automatic Update settings configured.

Cause: One or more servers in the farm have Automatic Update settings that are different from the other servers in the farm.

Resolution: Ensure all servers in the farm have the same Automatic Update settings

- Choose an Automatic Update setting that is consistent on each server on the farm. On each server in the farm, open the Automatic Update settings page and ensure the settings are configured according to the planned consistent setting.

1. Click **Start**, click **All Programs**, and then click **Windows Update**.
2. On the Windows Update Control Panel page, click **Change settings**.
3. On the **Choose how Windows can install updates** screen, make sure that the update settings are what you want. Change the update settings if necessary.

   Note:

   If you cannot change the update settings, the update settings may be locked because of group policy. If this is the case, ensure that the same group policy is being applied to other servers in the farm.

Diagnostic logging is set to verbose (SharePoint Foundation 2010)

Published: June 4, 2010

Rule Name: Diagnostic logging is set to verbose

Summary: SharePoint Foundation writes diagnostic logging information to record activity on the server. The logs contain information that can help you diagnose server problems. This rule occurs when diagnostic logging is set to verbose. The verbose setting is appropriate when you have to diagnose a server problem, but you should turn off verbose logging during normal operations.

Cause: One or more categories of diagnostic logging are set to verbose.

Resolution: Reset diagnostic logging to the default level

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **Monitoring**.
3. On the Monitoring page, in the **Reporting** section, click **Configure diagnostic logging**.
4. In the Event Throttling section, in the Least critical event to report to the event log list and Least critical event to report to the trace log list, select Reset to default.
5. Click **OK**.

The server farm account should not be used for other services (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: The server farm account should not be used for other services

Summary: The account that is used to run the SharePoint 2010 Timer service and other system services in the SharePoint farm should not be used for other services in the farm.

Cause: The Farm Account, which is used for the SharePoint 2010 Timer service and the Central Administration site, is highly privileged and should not be used for other services on any computers in the server farm. Services in the farm were found to use this account.

Resolution: Change the account that is used for other services

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators SharePoint group.
2. On the Central Administration home page, click **Security**, and then in the **General Security** section, click **Configure service accounts**.
3. On the Service Accounts page, in the **Credential Management** section, in the upper drop-down list, click the service for which you want to update credentials.
4. In the **Select an account for this component** list, click the domain account that you want to associate with this service.
5. If you want to register the account that you selected on the SharePoint Foundation 2010 farm, click **Register Managed Account**.
6. Click **OK**.

One or more services have started or stopped unexpectedly (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: One or more services have started or stopped unexpectedly

Summary: A critical service required for the SharePoint farm to function is not running.

Cause: One or more critical services are not running on the specified server.

Resolution: Start the service that is not running

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer.
2. Click Start, click Administrative Tools, and then click Services.
3. Right-click the service that you want to start, and then click **Start**.

Databases used by SharePoint have fragmented indices (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Databases used by SharePoint have fragmented indices

Summary: Microsoft SharePoint Foundation 2010 uses Microsoft SQL Server to store most of the content for the Web site and configuration settings. One or more of the databases used by SharePoint Foundation have fragmented indexes. A fragmented index can cause degradation in performance.

Cause: Database indexes can fragment over time as a result of insert and update operations performed by SharePoint Foundation. We recommend that you periodically delete and rebuild these indexes to improve system performance.

Resolution: Reorganize and rebuild indexes

1. To correct index fragmentation, you can reorganize an index or rebuild an index. For information, see Reorganizing and Rebuilding Indexes (*http://go.microsoft.com/fwlink/?LinkID=160083&clcid=0x409*).

Other Resources

Example: Index fragmentation with insert/updates, measuring it and fixing it (*http://go.microsoft.com/fwlink/?LinkId=195327&clcid=0x409*)

Content databases contain orphaned items (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Content databases contain orphaned items

Summary: The SharePoint Health Analyzer has detected some sites in a content database that are not referenced in the configuration database. These sites may not be accessible.

Cause: A restore operation that was not completed can result in sites in a content database that are not referenced in the SharePoint configuration database.

Resolution: Remove orphaned sites from the content databases

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **Monitoring**.
3. On the Monitoring page, in the **Health Analyzer** section, click **Review problems and solutions**.
4. On the Review problems and solutions page, click the alert for the failing rule, and then click **Fix Now**. Keep the dialog box open so you can run the rule again to confirm the resolution.

   Note:

   The Fix Now feature removes all orphans from the content database.
5. After following the steps in the **Remedy** section, in the **Review problems and solutions** dialog box for the alert, click **Reanalyze Now** to confirm the resolution. If the problem is resolved, the rule is not flagged as a failing rule on the Review problems and solutions page.

Outbound e-mail has not been configured (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Outbound e-mail has not been configured

Summary: An outgoing e-mail server has not been configured on this SharePoint Foundation deployment. With no SMPT server configured for outgoing e-mail, SharePoint Foundation cannot send e-mail messages, including alert e-mail, confirmation e-mail, invitation e-mail, and e-mail about exceeding quotas.

Cause: An SMPT e-mail server has not yet been configured in the farm.

Resolution: Configure outgoing e-mail settings in Central Administration

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **System Settings**.
3. On the System Settings page, in the E-Mail and Text Messages (SMS) section, click Configure outgoing e-mail settings.
4. On the Outgoing E-Mail Settings page, in the **Mail Settings** section, type the SMTP server information in the **Outbound SMTP server** box, and then specify the addresses and the character set that you want to use.
5. Click **OK**.

Some health analyzer rules do not have associated timer jobs (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Some health analyzer rules do not have associated timer jobs

Summary: The timer jobs that run SharePoint Health Analyzer rules do not exist on this SharePoint Foundation 2010 deployment.

Cause: Some or all of the SharePoint Health Analyzer rules may not run if the health data collection timer jobs are not configured.

Resolution: Create the health data collection timer jobs

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **Monitoring**.
3. On the Monitoring page, in the **Health Analyzer** section, click **Review problems and solutions**.
4. On the Review problems and solutions page, click the alert for the failing rule, and then click **Fix Now**.
5. After following the guidance given in the **Remedy** section, in the **Review problems and solutions** dialog box for the alert, click **Reanalyze Now** to confirm the resolution. If the problem is resolved, the rule is not flagged as a failing rule on the Review problems and solutions page.

Drives are running out of free space (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Drives are running out of free space

Summary: Disk drives on one or more of the servers in the farm are running out of disk space.

Note:

This rule checks disk space as a proportion of the RAM on the computer. When disk space is less than twice the RAM on the computer, the health rule triggers an error. When disk space is less than five times the RAM on the computer, the health rule triggers a warning. Accordingly, server computers with lots of RAM are more likely to experience a failure of this rule.

Resolution: Free disk space on the server computer

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer.
2. Run the Disk Cleanup tool to free disk space on the server computer.

Resolution: Decrease the number of days to store log files

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. On the Central Administration Home page, click **Monitoring**.
3. On the Monitoring page, in the **Reporting** section, click **Configure diagnostic logging**.
4. On the Diagnostic Logging page, in the **Trace Log** section, in the **Number of days to store log files** box, type a smaller number.
5. Click **OK**.

The paging file size should exceed the amount of physical RAM in the system (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: The paging file size should exceed the amount of physical RAM in the system

Summary: The paging file size on some servers in the SharePoint farm is smaller than the total physical memory that is available on the servers.

Cause: A Windows best practice is to set the paging file size to equal to or greater than the total amount of available physical memory. Garbage collection is typically more effective at automatic recovery of heap memory when managed heap size approximates paging file size. When paging file size is smaller than RAM size, new allocations of managed memory are granted, which leads to more garbage collection and higher CPU usage.

Resolution: Increase the minimum size of the paging file

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the local computer.
2. On the Server Manager page, click **Change System Properties**.
3. In the **System Properties** dialog box, on the **Advanced** tab, in the **Performance** section, click **Settings**.
4. In the **Performance Options** dialog box, on the **Advanced** tab, in the **Virtual memory** section, click **Change**.
5. In the **Virtual Memory** dialog box, select the **Automatically manage paging file size for all drives** check box, or clear the check box and specify a paging file size that is equal to or greater than the physical memory that is available on the computer.
6. When you have made the changes that you want, click **OK**, and then restart the computer to apply the changes.

Built-in accounts are used as application pool or service identities (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Built-in accounts are used as application pool or service identities

Summary: Built-in or local computer accounts are used as an application pool identity or service identity.

Cause: Using built-in accounts as application pool identities or as service identities is not supported in a farm configuration. Built-in accounts include Network Service, Local Service, and Local System.

Resolution: Change the identity that is used for the service or application pool

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators SharePoint group.
2. On the Central Administration Home page, click **Security**.
3. On the Security page, in the **General Security** section, click **Configure service accounts**.
4. On the Service Accounts page, in the **Credential Management** section, in the upper drop-down list, click the service or application pool for which you want to change the identity.
5. In the **Select an account for this component** list, click the domain user account that you want to associate with the service or application pool.

If you want to register the account that you selected on the SharePoint Foundation 2010 farm, click **Register Managed Account**.

6. Click **OK**.

Web Analytics: Monitors the health of the Report Consolidator component (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Web Analytics: Monitors the health of the Report Consolidator component

Summary: Typically, the Report Consolidator component should not take more than two hours to run. This rule is triggered if it takes longer than five hours.

Cause: The Report Consolidator component takes longer than five hours to run.

Resolution: Enable data trimming by using Windows PowerShell

1. You can enable data trimming using the **Set-WebAnalyticsServiceApplication** cmdlet. When data trimming is enabled, the number of rows of data in the tables in the reporting database is trimmed to 20,000 rows per day per component (site, site collection, Web application, etc.). This decreases the time that the Reporting Component takes to run.
2. Verify that you meet the following minimum requirements: See **Add-SPShellAdmin**.
3. On the **Start** menu, click **All Programs**.
4. Click Microsoft SharePoint 2010 Products.
5. Click SharePoint 2010 Management Shell.
6. At the Windows PowerShell command prompt, type the following command:

   Set-SPWebAnalyticsServiceApplication [-Identity <GUID>]-EnableDataTrimming

Where:

- *<GUID>* is GUID identifier of the Web Analytics service application. If you only have one Web Analytics service application, you do not need to specify the GUID.

For more information, see Set-SPWebAnalyticsServiceApplication (*http://technet.microsoft.com/library/eafa4ad8-5991-44c4-93c9-0beb60d586df(Office.14).aspx*).

Note:

We recommend that you use Windows PowerShell when performing command-line administrative tasks. The Stsadm command-line tool has been deprecated, but is included to support compatibility with previous product versions.

Web Analytics: Verifies that when the Web Analytics is installed and running, usage logging is enabled in the farm (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Web Analytics: Verifies that when the Web Analytics is installed and running, usage logging is enabled in the farm

Summary: The Web Analytics service application collects and reports on usage information such as page views, unique visitors, search queries issued, etc. If you require this service application, you must enable usage logging to ensure that logging of this data occurs.

Cause: Usage logging is not enabled for the Web Analytics service application.

Resolution: Enable usage logging for the Web Analytics service application

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.

   Note:

   The usage and health data settings are farm-wide and cannot be set for individual servers in the farm.

2. In Central Administration, on the Home page, click **Monitoring**.
3. On the Monitoring page, in the Reporting section, click Configure usage and health data collection.
4. On the Configure usage and health data collection page, in the **Usage data collection** section, select the **Enable usage data collection** check box.
5. In the **Event Selection** section, select the events that you want to log by selecting the check boxes next to the events in the **Events to log** list. Ensure that at least the following events are selected:
   i. Page Requests
   ii. Search Query Usage
   iii. Site Inventory Usage
   iv. Rating Usage
6. In the **Usage data collection settings** section, type the path of the folder you want usage and health information to be written to in the **Log file location** box. The path that you specify must exist on all farm servers.

7. Type the maximum disk space for the logs in gigabytes (from 1 through 20 GB) in the **Maximum log file size** box.
8. Click **OK** to save the settings and enable usage logging.

Web Analytics: Verifies that a web application is serviced by at most one Web Analytics service application proxy (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Web Analytics: Verifies that a Web application is serviced by at most one Web Analytics service application proxy

Summary: When a Web application is associated with a Web Analytics service application, the Web Analytics service application logs and processes the usage data for that Web application. When a Web application is associated with multiple Web Analytics service applications, the Web Analytics service applications log and process the data for the Web application in an unpredictable way. We recommend that you use only one Web Analytics service application to log and process the data for the Web application.

Cause: Multiple Web Analytics service applications were created in the same farm and some Web applications were associated with more than one of those Web Analytics service applications.

Resolution: Disassociate other Web Analytics service applications

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators SharePoint group.
2. In Central Administration, on the home page, under **Application Management**, click **Manage Web applications**.
3. On the Web Applications page, click the Web application that is in the Health Analyzer alert, and then click **Service Connections**.
4. In the **Configure Service Application Associations** dialog box, clear all but one of the Web Analytics service application check boxes.

   Note:

   If the check boxes are not available, do the following:

   1. Record the connections that are listed in the default view.
   2. Select [custom] from the Edit the following group of connections list box.
   3. Clear all but one of the Web Analytics service application check boxes, and ensure that you select all of the other service applications that were in the default view.
5. Click **OK**.

Web Analytics: Verifies that the SQL Server Service Broker is enabled for the Web Analytics staging databases (SharePoint Foundation 2010)

Published: July 8, 2010

Rule Name: Web Analytics: Verifies that the SQL Server Service Broker is enabled for the Web Analytics staging databases

Summary: The service broker queue for the Web Analytics databases is not enabled. This causes Web Analytics data to not be processed.

Cause: This could be because of a recent SQL Server databases attach or detach or a backup or restore operation.

Resolution: Enable the service broker queue

- In Central Administration, on the Review problems and solutions page, click the rule, and then click **Repair Automatically**.

Installation reference (SharePoint Foundation 2010)

Published: July 8, 2010

In this section:

- Setup command-line reference (SharePoint Foundation 2010)
- Config.xml reference (SharePoint Foundation 2010)
- Psconfig command-line reference (SharePoint Foundation 2010)
- Windows PowerShell commands (SharePoint Foundation 2010)

Setup command-line reference (SharePoint Foundation 2010)

Published: July 8, 2010

In SharePoint 2010 Products, the Setup command-line tool is used for very few operations, and most of these are for IT administrators only.

In this article:

How to use a Setup command-line switch

To run Setup from the command line, type a space after the command, followed by a forward slash (/) and the name of the switch, and sometimes followed by another space and one or more parameters. For example:

```
setup.exe /<switch> [parameter]
```

The parameters are specific instructions that give the program more information about how to execute the command. The table in the next section contains several examples of switches.

Available switches and parameters

In SharePoint 2010 Products, Setup recognizes the following command-line options.

Switch or parameter	Description
`/config [path and file name]`	Specifies the configuration file that Setup uses during the installation. By default, the Config.xml file that is stored in the core product folder directs Setup to install that product. You can edit the Config.xml file to make additional customizations to the installation, or you can point to a different configuration file. The product DVD contains examples of Config.xml files. The example files are stored in the Files folder at the root of the DVD, in folders that correspond to different scenarios. For example, the Files\SetupFarmSilent folder contains a Config.xml file for use in setting up a server farm in silent mode.

Switch or parameter	Description

	Use */config* on the Setup command line to point to the location of the default Config.xml file for a particular product or to point to a custom configuration file.
	Examples
	To point to a customized Config.xml file:
	`\\<server>\<share>\setup.exe /config \\<server>\<share>\<folder>\config.xml`
	where <folder> is the folder that contains the Config.xml file.
	Or, to point to a different configuration file:
	`\\<server>\<share>\setup.exe /config \\<server>\<share>\Files\SetupFarmSilent\config.xml`

/modify [ProductID]	The **/modify** switch is used with a modified Config.xml file to run Setup in maintenance mode and make changes to an existing Office installation, such as adding or removing features.
	Look up the value of [ProductID] in the Setup.xml file for the product that you want to modify. The Setup.xml file is located in the core product folder at the root of the network installation point or product DVD. For example, the Setup.xml file for SharePoint Foundation 2010 is located in the Wss.en-us folder.
	In Setup.xml, [ProductID] is equal to the value of the *Id* attribute of the *Setup* element. For example:
	`- <Setup Id="Wss" Type="Product" ProductCode="{40120000-1110-0000-0000-0000000FF1CE}">`
	This switch cannot be used to change the configuration of the server (such as from a stand-alone configuration to a server farm configuration). To change the configuration, you must uninstall and reinstall.
	Examples
	`\\<server>\<share>\setup.exe /modify wssmui.en.us /config \\<server>\<share>\<folder>config.xml`
	In this example, Setup at the root of the DVD is run in maintenance mode to modify SharePoint Foundation, as specified with the **wss** product ID. If a Config.xml file is not specified, Setup uses the Config.xml in the same folder as the Setup.exe file.
	`\\<server>\<share>\setup.exe /modify wss`

/repair [ProductID]	Runs Setup to repair the files that are needed for the specified product. Running Setup in repair mode only affects the program files and does not repair your server

Switch or parameter	Description
	configuration or any sites. Look up the value of [ProductID] in the Setup.xml file for the product that you want to modify. The Setup.xml file is located in the core product folder at the root of the network installation point or product DVD. For example, the Setup.xml file for SharePoint Foundation 2010 is located in the Global folder at the root of the DVD. **Note:** You should also run the SharePoint Products Configuration Wizard after you run `setup.exe /repair` to complete the repair of the configuration. If you are using a stand-alone configuration, you can run `psconfig.exe -setup` from the command line to repair the configuration instead of using the wizard. If you are in a server farm configuration, you should use the full wizard interface. For more information, see the Help for the SharePoint Products Configuration Wizard. **Example** `\\<server>\<share>\setup.exe /repair Wss`
`/uninstall [ProductID]`	Removes the specified product from the user's computer. Look up the value of [ProductID] in the Setup.xml file for the product that you want to modify. Look up the value of [ProductID] in the Setup.xml file for the product that you want to modify. The Setup.xml file is located in the core product folder at the root of the network installation point or product DVD. For example, the Setup.xml file for SharePoint Foundation 2010 is located in the Global folder at the root of the DVD. Example `\\<server>\<share>\setup.exe /uninstall WSS`

Run Setup with a Config.xml file at a command prompt

Running Setup with a configuration file lets you specify configuration choices (such as a data location or server role) during a quiet installation. For example, you can use the Config.xml file to:

- Perform a silent installation.
- Install by using a common configuration across multiple servers.
- Perform an automated or scripted installation.

Use the following procedure to run Setup with a configuration file at a command prompt.

1. On the drive that contains the product DVD, change to the root directory to locate the Setup.exe file.
2. Run Setup with the selected Config.xml file.

setup /config<path and file name>

> **Note:**
>
> You can select one of the example files that are included in the Microsoft SharePoint Foundation 2010 product DVD, or customize your own configuration file.

3. Press ENTER.

For more information, see Install SharePoint Foundation by using Windows PowerShell (*http://technet.microsoft.com/library/8528643d-27bc-4592-8a21-0c5b1cea466d(Office.14).aspx*).

Psconfig command-line reference (SharePoint Foundation 2010)

Published: July 8, 2010

In SharePoint 2010 Products, you can use the Psconfig command-line tool as an alternative interface to perform several operations that control how SharePoint 2010 Products are configured. You must be a member of the Administrators group on the local computer to perform these operations.

In this article

How to use Psconfig commands

When you run Psconfig at a command prompt, you can specify commands to control how the tool runs. To run Psconfig at a command prompt, navigate to the %COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\14\bin folder, and then type the commands by using the following syntax:

```
psconfig.exe -cmd <command> [optional parameters]
```

The reference table in the next section contains several examples. Help is also available from the command-line interface. To view Help, at the command prompt, type:

```
psconfig.exe -?
```

To view Help about a specific command, type:

```
psconfig.exe -help <command name>
```

The commands in Psconfig must be run in a specific order to run successfully. If you use the SharePoint Products Configuration Wizard to configure an installation, it calls the commands (also known as configuration tasks) in the correct order for you. However, if you use the command line to run Psconfig, you must make sure that you are performing the tasks in the correct order. The Psconfig commands must be performed in the following order:

1. **configdb**
2. **helpcollections**

3. **secureresources**
4. **services**
5. **installfeatures**
6. **adminvs**
7. **evalprovision** (only for stand-alone installations)
8. **applicationcontent**
9. **upgrade**

Important:

If Psconfig detects that the server farm has to be upgraded, it will automatically start an upgrade when you run it (even if you did not select the upgrade command).

You can specify all the commands to run in a single command-line string. If you do this, Psconfig runs all the commands in the correct order. For example, at the command prompt, you can run a command similar to the following:

```
psconfig.exe -cmd configdb <parameters>
-cmd helpcollections <parameters>
-cmd secureresources <parameters>
-cmd services <parameters>
-cmd installfeatures <parameters>
-cmd adminvs <parameters>
-cmd evalprovision <parameters>
-cmd applicationcontent <parameters>
```

For more information about how to configure a server or server farm from the command line, see the Microsoft SharePoint Foundation 2010 TechCenter.

Available commands and parameters

In the SharePoint Products Configuration Wizard, the following command-line options are recognized.

Command	Description, parameters, and examples
?	Displays the commands available for use with Psconfig. Example **psconfig.exe -?**
help <command name>	Displays the commands available for use with Psconfig. If a command name is specified, displays help for that command. **Example** psconfig.exe -help adminvs

Command	Description, parameters, and examples
`adminvs`	Manages the SharePoint Central Administration Web application on the local computer. Takes the following optional parameters: *[-provision]* Provisions the SharePoint Central Administration Web application on this server. Provisioning creates a new SharePoint Central Administration Web application and an application pool running under the server farm administrator's account. *[-unprovision]* Unprovisions the SharePoint Central Administration Web application from this server. Unprovisioning removes the SharePoint Central Administration Web application and its application pool. *[-port <port number>]* The SharePoint Central Administration Web application port is a global setting to the server farm. When changing the port, a SharePoint Timer service job is dispatched to synchronize the port for all SharePoint Central Administration Web applications in the server farm. If a port is not specified, the port that is used for existing SharePoint Central Administration Web applications in the server farm is used. If a SharePoint Central Administration web Application has not been provisioned in the server farm, the default port selected will be random if a port is not specified. *[-windowsauthprovider <enablekerberos | onlyusentlm>]* The SharePoint Central Administration Web application authentication provider is a global setting to the server farm. When you change the authentication provider, a SharePoint Timer service job will be dispatched to synchronize the provider on all SharePoint Central Administration Web Applications in the server farm. If *onlyusentlm* is specified, NTLM will be the exclusive authentication provider for all SharePoint Central Administration Web applications. All other authentication providers are disabled and NTLM will be the only authentication provider allowed. If *enablekerberos* is specified, Kerberos authentication is enabled for all SharePoint Central Administration Web applications. If an authentication provider is not specified, the provider that is used for existing SharePoint Central Administration Web applications in the server farm will be used. If a SharePoint Central Administration Web application has not been provisioned in the server farm, the Kerberos authentication provider will be enabled if an authentication provider is not

Command	Description, parameters, and examples

	specified.
	Examples
	`psconfig.exe -cmd adminvs -provision -port 8080 -windowsauthprovider onlyusentlm`
	`psconfig.exe -cmd adminvs -unprovision`

`applicationcontent`	Manages shared application content. Takes the following required parameter: -install Copies shared application data (for example, resource files and Web application binaries) to existing Web application virtual directories. **Example** `psconfig.exe -cmd applicationcontent -install`
`configdb`	Creates, connects, or disconnects this server from the server farm. Takes the following optional parameters: [-create] Creates a new configuration database and therefore establishes a new server farm. If this server is already connected to a configuration database, the server will be disconnected first, and then the new configuration database will be created. [-disconnect] Disconnects this server from the configuration database and therefore disconnects this server from the server farm. [-connect] Connects to an existing configuration database and therefore joins this server to an existing server farm. If this server is already connected to a configuration database, the server will be disconnected first, and then connected to the existing configuration database. *[-server <SQLServerName>]* The computer that is running Microsoft SQL Server where the configuration database is located. *[-database <SQLDatabaseName>]* The configuration database name. *[-dbuser <value>]* The user name that is used for SQL authentication. *[-dbpassword <value>]* The password that is used for SQL authentication. *[-user <Domain\User>]*

Command	Description, parameters, and examples

	The server farm administrator user account.
	[-password <Password>]
	The server farm administrator user account password.
	[-addomain <value>]
	The Active Directory domain name that is used for the server farm.
	[-adorgunit <value>]
	The Active Directory organization unit name that is used for the server farm.
	[-admincontentdatabase <SQLAdminContentDatabaseName>]
	The Central Administration Web application content database name.
	Examples
	`psconfig.exe -cmd configdb -create -server <Server_name> -database <Database_name>`
	`-dbuser <DOMAIN\username> -dbpassword <password>`
	`-user <DOMAIN\username> -password <password>`
	`-addomain <domain_name> -adorgunit <org_unit>`
	`-admincontentdatabase <Database_name>`
	`psconfig.exe -cmd configdb -disconnect`
	`psconfig.exe -cmd configdb -connect -server <Server_name> -database <Database_name>`
	`-dbuser <DOMAIN\username> -dbpassword <password>`

`evalprovision`	Provisions this server as a stand-alone (evaluation mode) server. Takes the following required and optional parameters: -provision Performs stand-alone mode provisioning on this server. *[-port <port number>]* The port number assigned to the default SharePoint Web application. If not specified, port 80 is used. If a SharePoint Web application already exists and is using the port, the existing site will be overwritten. If an existing site is using the port and is not a SharePoint Web application, the site will be disabled and a new SharePoint Web application will be created that uses the port. *[-overwrite]* Specifies whether to overwrite any existing Microsoft SharePoint Foundation 2010 Web site during installation. If not specified, the site is not deleted.

Command	Description, parameters, and examples
	Example `psconfig.exe -cmd evalprovision -provision -port 1100`
`helpcollections`	Manages help collections. Takes the following required parameter: *-installall* Installs all available help collections. **Example** `psconfig.exe -cmd helpcollections -installall`
`installfeatures`	Registers any SharePoint Products and Technologies features located on the file system of this server with the server farm. **Example** `psconfig.exe -cmd installfeatures`
`quiet`	Runs the SharePoint Products Configuration Wizard in quiet mode. Output is written to the log file that is named PSCONFIG.EXE_MM_DD_YY_HH_MM_SS_MS.log, where "_MM_DD_YY_HH_MM_SS_MS" is the full date and time that the utility was run. The log file is stored in the %COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\14\LOGS directory. **Example** `psconfig.exe -cmd quiet`
`secureresources`	Performs SharePoint 2010 Products resource security enforcement on the server. For example, security is enforced on files, folders, and registry keys. **Example** `psconfig.exe -cmd secureresources`
`services`	Manages SharePoint 2010 Products services. Takes the following optional parameters: *[-install]* Registers the services in the server farm that are located on this server. *[-provision]* Provisions the services that are located on this server and sets the services as online if SharePoint 2010 Products are installed in stand-alone mode. Provisioning services also ensures that they are registered. **Note:** The *[-provision]* parameter is supported only for a single server, stand-alone installation. Do not use this parameter for a farm installation.

Command	Description, parameters, and examples

	Example
	`psconfig.exe -cmd services -install`
	`psconfig.exe -cmd services -provision`

`setup`	Performs configuration for SharePoint 2010 Products based on the installation mode. Also repairs the configuration. If the product is installed in stand-alone mode, stand-alone configuration is complete. If the product is not in stand-alone mode, you must complete the initial configuration by using the SharePoint Products Configuration Wizard instead of the Psconfig command-line tool. To run the wizard, on the **Start** menu, point to **All Programs**, point to **Administrative Tools**, and then click **SharePoint Products Configuration Wizard**. If you want to repair a stand-alone installation, first run **setup /repair** (for more information, see the Setup Help system), and then **psconfig.exe -setup**. For server farm installations, after you run **setup /repair**, use the SharePoint Products Configuration Wizard instead of the Psconfig command-line tool. Takes the following optional parameter: *[-lcid <1033>]* The locale ID (LCID) that specifies the installation language. **Example** `psconfig.exe -cmd setup`
`standaloneconfig`	Performs a stand-alone configuration for SharePoint Products and Technologies. Takes the following optional parameters: *[-lcid <1033>]* The locale ID (LCID) that specifies the installation language. **Example** `psconfig.exe -cmd standaloneconfig`
`upgrade`	Performs an upgrade of SharePoint 2010 Products. This command is automatically run when you run the SharePoint Products Configuration Wizard if the product has to be upgraded. Takes the following optional parameters: *[-wait]* If specified, the SharePoint Products Configuration Wizard does not return until the upgrade is complete. If not specified, the wizard returns after dispatching a SharePoint Timer Service job to perform the upgrade. To view the upgrade job status, you can access the SharePoint Central Administration Web site by using your Web browser. *[-force]*

Command	Description, parameters, and examples
	If specified, the SharePoint Products Configuration Wizard stops any currently running upgrade actions, and then restarts upgrade. *[-reghostonupgrade]* If specified, the SharePoint Products Configuration Wizard will reset all content to the site definition version during the upgrade. *[-inplace <v2v|b2b>]* If specified, the SharePoint Products Configuration Wizard will perform an in-place upgrade. If *v2v* is specified, an in-place version to version upgrade is performed. If *b2b* is specified, an in-place build to build upgrade is performed. *[-preserveolduserexperience]* If set to false, the SharePoint Products Configuration Wizard will update sites to use the latest SharePoint user experience. If you do not specify this parameter, the default is true. *[-passphrase]* Passphrase used to join the server farm. The Passphrase value must be the same on all servers in the farm if the farm is to function correctly. **Example** `psconfig.exe -cmd upgrade -inplace v2v -wait`

Config.xml reference (SharePoint Foundation 2010)

Updated: November 4, 2010

When you want to control how Microsoft SharePoint Foundation 2010 is installed, use the Config.xml file and the Setup command-line tool. For example, you can use the Config.xml file to do the following:

- Perform a silent installation of SharePoint Foundation 2010.
- Install SharePoint Foundation 2010 by using a common configuration across multiple servers.
- Perform an automated or scripted installation of SharePoint Foundation 2010.

In this article:

Customizing Config.xml

To control the installation, first edit the Config.xml file in a text editor to include the elements that you need with the appropriate settings for those elements. Then run

```
setup.exe /config [path and file name]
```

to specify that Setup will run and use the options that you set in the Config.xml file.

Important:

Use a text editor, such as Notepad, to edit Config.xml. Do not use a general-purpose XML editor such as Microsoft Office Word 2007.

The product DVD contains examples of Config.xml files. The example files are stored in the Files folder at the root of the DVD, in folders that correspond to different scenarios. The folders are as follows:

- **Setup** Contains a Config.xml file for use in setting up a clean installation. You must run the Psconfig command-line tool after you run Setup to finish configuring the server or server farm.
- **SetupFarmSilent** Contains a Config.xml file for use in setting up a server farm in silent mode.

- **SetupSilent** Contains a Config.xml file for use in setting up a clean installation for a single server (stand-alone, with Windows Internal Database) in silent mode.
- **SetupUpgradeSilent** Contains a Config.xml file for use in upgrading an existing server farm in place.

For more information about the differences among the various upgrade scenarios, see Determine upgrade approach (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/3402b490-e613-4ede-93e7-ea41083f07cf(Office.14).aspx*).

Config.xml element quick reference

The following table contains a list of the elements in Config.xml. These elements can appear in any order, except for Configuration Element, which must be first, and elements such as Command Element, whose order in Config.xml affects how they are processed during installation.

Element	Description
Configuration Element	Top-level element.
ARP Element	Values that control the text and behavior of **Add or Remove Programs** in Control Panel for the product.
Command Element	Runs a command during installation.
Display Element	The level of UI that Setup displays to the user.
Logging Element	Options for the type of logging that Setup performs.
DATADIR Element	The location to use to store the data files.
Package Element	The package or product to install.
Setting Element	Values for Windows Installer properties.

How it works

Setup looks for a copy of Config.xml in the same folder as Setup.exe. If a copy is not found there, Setup uses the Config.xml file that resides in the core Files folder for the product that you are installing.

You can also use the **/config** Setup command-line option to specify the location of the Config.xml file. For example:

\\<server>\<share>\setup.exe /config \\<server>\<share>\<folder>\config.xml

Config.xml file format

XML elements in Config.xml begin with an angle bracket (<) and end with a forward slash and an angle bracket (/>).

The basic element format is as follows:

<element_name [attribute_name="value"] [attribute_name="value"] … />

For example:

```
<Display Level="none" CompletionNotice="no" />
```

Elements and attributes are case-sensitive. Attribute values must be enclosed in quotation marks (") and are not case-sensitive.

An element definition can span multiple lines. Spaces, carriage returns, line feeds, and tab characters are ignored within an element definition.

For example:

```
<Display
   Level="none"
   CompletionNotice="no"
/>
```

Tip:

For long element definitions, put attributes on separate lines and use indentation to make the file easier to read.

The Configuration Element element is a special case and is required. All other elements are contained within the Configuration Element element, and the element is closed with **</Configuration>**.

The following example shows a configuration file for a clean installation of the Microsoft SharePoint Foundation 2010 package:

```
<Configuration>
  <Package Id="sts">
    <Setting Id="SETUPTYPE" Value="CLEAN_INSTALL"/>
  </Package>
  <DATADIR Value="%CommonProgramFiles%\Microsoft Shared\Web Server
Extensions\14\Data"/>
  <Logging Type="verbose" Path="%temp%" Template="Microsoft SharePoint
Foundation 2010 Setup *.log"/>
  <Setting Id="UsingUIInstallMode" Value="1"/>
  <Setting Id="SETUP_REBOOT" Value="Never"/>
</Configuration>
```

Comments can be added anywhere and are delimited by an angle bracket, exclamation point, and two hyphens (<!--) and two hyphens and an angle bracket (-->).

For example:

```
<!-- Install Microsoft SharePoint Server for clean install, using UI-->
<Configuration>
  <Package Id="sts">
    <Setting Id="LAUNCHEDFROMSETUPSTS" Value="Yes"/>
  </Package>
  <Package Id="spswfe">
    <Setting Id="SETUPCALLED" Value="1"/>
  </Package>
  <Logging Type="verbose" Path="%temp%" Template="SharePoint Server
Setup(*).log"/>
    <!--<PIDKEY Value="Enter Product Key Here" />-->
    <Setting Id="SERVERROLE" Value="SINGLESERVER"/>
    <Setting Id="USINGUIINSTALLMODE" Value="1"/>
    <Setting Id="SETUPTYPE" Value="CLEAN_INSTALL"/>
    <Setting Id="SETUP_REBOOT" Value="Never"/>
  <!-- Tells Setup.exe not to reboot -->
</Configuration>
```

Config.xml element reference

The following conventions are used in the descriptions in this reference:

bold	Element or attribute name
regular	Text to be entered exactly as shown
italic	Placeholder for a value to be added
x|y	Choose between multiple values
[*x*]	Optional value

Configuration Element

Top-level element. This element is required, and all other elements must appear within this element.

Syntax

```
<Configuration>
  <Package Id="ID">
  ...
  </Package>
  ...
</Configuration>
```

Attributes

Attribute	Value	Description
Package ID	Package ID	The package that is being installed.

Remarks

The **Package Id** attribute identifies the product and technologies that are affected by this Config.xml file.

Example

The Package ID for SharePoint Foundation 2010 is **sts**. Use the **sts** Package ID in Config.xml to specify SharePoint Foundation 2010 by entering the following:

```
<Configuration>
   <Package Id="sts">
   ...
   </Package>
   ...
</Configuration>
```

ARP Element

Specifies values that control the text and behavior of **Add or Remove Programs** in Control Panel for the product.

Syntax

<ARP attribute**="**value**"** [attribute**="**value**"**] **... />**

Attributes

Attribute	Value	Description
ARPCOMMENTS	*text*	Additional text; can be up to 255 characters, although all characters might not display.
ARPCONTACT	*text*	List of technical support contacts.
ARPNOMODIFY	**Yes**	Prevents users from modifying the product installation by making the **Change** button unavailable.
	No (default)	Allows users to modify the product installation.
ARPNOREMOVE	**Yes**	Prevents users from removing the product by making the **Remove** button unavailable.
	No (default)	Allows users to remove the product.
ARPURLINFOABOUT	*URL*	URL for the product's home page.
ARPURLUPDATEINFO	*URL*	URL for information about product updates.
ARPHELPLINK	*URL*	URL of a Web site from which users can receive technical support.
ARPHELPTELEPHONE	*text*	Phone numbers for technical support.

Command Element

Specifies a command line to run. The **Command** element commands are processed only during initial installations and uninstallations. If **Command** element commands are used for customizations after the initial installation, they are ignored.

Syntax

<Command
Path="*path*"
  [**QuietArg="***arguments***"**]
  [**Args="***args***"**]
  [**ChainPosition="Before" | "After**"(default)]
  [**Wait="***mseconds***"**]
  [**Execute**="Install"(default) | "Uninstall"]
  [**Platform**="x86"(default) | "x64"]
/>

Attributes

You can specify double-quotation marks (") in the **Path** and **Args** attributes by specifying two double-quotation marks together ("").

Attribute	Value	Description
Path	*path*	Fully qualified path of the executable Windows Installer package.
QuietArg	*string*	String of arguments to be appended to the command line when Display Element**Level=None**.
Args	*string*	String of arguments to be passed to the executable.
ChainPosition	**Before**	This command is executed before the primary product installation.
	After (default)	This command is executed after the primary product installation.
Wait	*mseconds*	When you install with the Display Element**Level** attribute set to *Full* or *Basic*, this is the number of milliseconds to wait after you run the program before you continue the installation. The default is 0 (zero), which indicates no waiting.
Execute	**Install** (default)	Setup executes this command when the primary product is installed.
	Uninstall	Setup executes this command when the primary product is uninstalled.
Platform	**x86** (default)	Specifies that this program requires the Intel x86 platform. This command runs only if the computer on which the installation is run matches this platform requirement.
	x64	Specifies that this program requires a 64-bit processor that supports the x64 extensions to the x86 architecture. This command runs only if the computer on which the installation is run matches this platform requirement.

Remarks

The **Command** element in the Config.xml file is intended to be used only for initial product installations and uninstallations. The **Command** element commands are processed only during initial installations and uninstallations. If **Command** element commands are used for customizations after the initial installation, they are ignored.

The command line can be specified to run an arbitrary command or to run a lightweight executable that you want to run when this product is installed.

The **Command** element in Config.xml does not provide the software deployment capabilities that an enterprise software deployment and management tool provides, such

as the ability to track deployment progress and troubleshoot problems. Therefore, we recommend that you limit the use of the **Command** element in Config.xml to run only a lightweight executable program or arbitrary command that will not make changes to the computer or that does not require user input. For example, you can run a utility to copy logs or a command to launch a Welcome page at the end of installation.

The command line can be specified for a chained installation or an executable that runs when this product is installed. If this is specified, you must specify a command line for Setup instead of a single .msi file.

If there are two or more **Command** elements in the Config.xml file, they will run in the order in which they are specified in Config.xml.

Important:

Chaining is not as reliable as installing each product separately. For example, if you chain two installations together and one of the products fails or encounters an unexpected error, the primary installation and the chained installation might not be completed successfully. Therefore, we do not recommend that you use the chaining approach. The recommended method for installing multiple products together in enterprise environments is to use a deployment management program, such as Microsoft System Center Configuration Manager 2010 or Microsoft Systems Management Server (SMS) 2003, or a third-party tool, instead of chaining.

The use of **Args** and **QuietArg** is as follows:

- The **Args** attribute is always appended to the command. This can include switches such as **/install** or **Company=***MyCorporation*.
- The **QuietArg** attribute is also appended if Setup is running silently (with **Display** set as `Display="none"`

). In such cases, you can specify the **QuietArg** attribute with the **"/quiet"** switch. For example, you can use: `QuietArg="/quiet"`

.

- If the value of the **Args** element includes quotation marks, you can enclose the complete value in single (') quotation marks as shown in the following example:`Args='"/param value"'`

The following statements apply to the **Wait** attribute:

- Setting the **Wait** attribute to 0 milliseconds indicates no waiting after you run the program before you continue the installation. The command will execute and move on immediately.

Return codes are only respected if the **Wait** value is nonzero. If you specify 0, Setup will not wait to continue the installation after it runs the specified program. Therefore, there is no return code to report in that case.

- Setting the **Wait** attribute to any positive nonzero value will wait exactly the number of milliseconds you specify. If the process ends earlier than the specified time, Setup will continue. If the process has not ended when the specified time is up, Setup will fail.

- Setting the **Wait** attribute to -1 indicates to wait indefinitely. This can be problematic because if the command process stops responding (hangs), Setup will stop responding and will wait indefinitely for the command to run.

Example

```
<Command Path="\\server\share\myscript.exe" Args='/id "123 abc"' QuietArg="/q"
Wait="3000">
<Command Path="\\<server>\<share>\setup.exe /config
\\<server>\<share>\<folder>\config.xml"
```

DATADIR Element

The location to use to store the data files, including the search index files.

Syntax

<**DATADIR Value**="*path*"/>

Attributes

Attribute	Value	Description
Value	path	Setup stores the data files in the location that is specified.

Remarks

You can use system environment variables in the path. If this element is not specified, the data is stored in the following path:

%ProgramFiles%\Microsoft SQL Server\MSSQL$SHAREPOINT\Data

Example

```
<DATADIR Value="d:\data"/>
```

Display Element

The level of UI that Setup displays to the user.

Syntax

<Display
Level="None" | **"Basic"** | **"Full"**(default)
CompletionNotice="Yes"(default) | **"No"**
SuppressModal="Yes" | **"No"**(default)
NoCancel="Yes" | **"No"**(default)
AcceptEula="Yes" | **"No"**(default)
/>

Attributes

Attribute	Value	Description
Level	**None**	No Setup UI is displayed.
	Basic	Setup displays the Welcome screen, the Microsoft Software License Terms page (if it is needed), a progress bar, and the completion notice (if it is allowed).
	Full (default)	Setup displays all UI to the user.
CompletionNotice	**Yes**	Only applies if **Level** is set to *Basic* or *None*. Setup displays the completion notice.
	No (default)	Only applies if **Level** is set to *Basic*. Setup does not display the completion notice.
SuppressModal	**Yes**	Only applies if **Level** is set to *Basic*. Setup does not display error messages and other dialog boxes that might interrupt the installation.
	No (default)	Only applies if **Level** is set to *Basic*. Setup displays errors and other dialog boxes as needed.
NoCancel	**Yes**	If **Level** is set to *Full* or *Basic*, disables the cancel button (X in the upper-right corner of the progress dialog box).
	No (default)	If **Level** is set to *Full* or *Basic*, allows the user to cancel the installation from the progress bar.
AcceptEULA	**Yes**	The Microsoft Software License Terms are accepted on behalf of the user. Setup

		does not display the Microsoft Software License Terms page.
	No (default)	If **Level** is not set to *None*, Setup displays the Microsoft Software License Terms page.

Remarks

If this element is not defined, the default settings are used. If an invalid value is specified, Setup ends the installation.

Note:

The **Display** element is used by Setup only if Setup finds the Config.xml file in the same folder as Setup.exe, or if you specify the Config.xml file by using the Setup **/config** command-line option.

Example

```
<Display Level="basic"
   CompletionNotice="yes"
   SupressModal="no"
   AcceptEula="yes"
/>
```

Logging Element

Specifies the type of logging that Setup performs.

Syntax

<Logging
Type="Off" | **"Standard"**(default) | **"Verbose"**
Path="*path***"**
Template="*filename***.txt"**
/>

Attributes

Attribute	Value	Description
Type	**Off**	Setup does no logging.
	Standard (default)	Setup writes installation information to the log file.

	Verbose	Setup writes all installation information to the log file.
Path	*Path*	The fully qualified path of the folder used for the log file. You can use environment variables. The default is **%temp%**.
Template	*filename*.**txt**	The name of the log file. If you insert the string ***** anywhere in the file name, a unique log file is created for each installation that is performed by Setup (see the explanation that follows). If ***** is not included and the file name that is specified already exists, log information is appended to the existing file. The .txt file name extension must be included. The default template is **SetupExe(*).log**.

Remarks

You can specify a * anywhere in the **Template** value. Setup inserts a string in that location that has the following format:

YYYYMMDDHHMMSSxxx

where:

1. YYYY = Year
2. MM = Month
3. DD = Day
4. HH = Hour
5. MM = Minutes
6. SS = Seconds
7. *xxx* = a unique string generated by Setup

Note:

The **Logging** element is used by Setup only if you specify the Config.xml file by using the Setup **/config** command-line option. If you do not specify a Config.xml file to use, then Setup uses the default logging options.

Example

```
<Logging Type="standard" Path="%temp%"
   Template="MyLog(*).txt"
/>
```

With this example, Setup creates a log file every time that it installs the product. Setup uses unique file names such as the following:

```
%temp%\MyLog(20060428110717CFC).txt
%temp%\MyLog(20060429113143C70).txt
```

Package Element

The package or product to install.

The Package ID for SharePoint Foundation 2010 is **sts**.

Setting Element

Allows you to specify values for Windows Installer properties.

Syntax

<Setting Id="*name***" Value="***value***" />**

Attributes

Attribute	Value	Description
Id	*name*	The name of the Windows Installer property.
Value	*value*	The value to assign to the property.

Values

The following Setting IDs are used for server installations:

ID	Accepted values	Description
REBOOT	ReallySuppress	Specifies (for Windows Installer) whether to allow a reboot after Setup is completed. Use ReallySuppress to specify no reboot. Must be specified at the global level, not per package.
SETUP_REBOOT	Never, AutoAlways, Always, AutoIfNeeded, IfNeeded	Specifies (for Setup) whether to allow a reboot after Setup is completed. Use Never to specify no reboot. Must be specified at the global level, not per package.
SETUPTYPE	CLEAN_INSTALL, V2V_INPLACE_UPG	Specifies whether to install a new copy of the product or technology

	RADE	(CLEAN_INSTALL), install the new version and upgrade the previous version in place (V2V_INPLACE_UPGRADE). Must be specified at the global level, not per package.
SETUPCALLED	0 | 1	Use as part of the Package Id attribute.
SERVERROLE	SINGLESERVER, APPLICATION	Specifies the type of server that you are installing to: stand-alone (SINGLESERVER) or application (APPLICATION).
USINGUIINSTALLMODE	0 | 1	Specifies whether you are performing a silent installation (0) or using the user interface for Setup (1).

Remarks

Not all Windows Installer properties can be specified in the **Setting** element. If a blocked property is specified, Setup ends the installation process. If a supported property is specified, Setup passes the property directly to Windows Installer.

Example

```
<Setting Id="REBOOT" Value="ReallySuppress" />
```

Windows PowerShell commands (SharePoint Foundation 2010)

Published: July 8, 2010

This article discusses the Windows PowerShell cmdlets that are needed to install Microsoft SharePoint Foundation 2010 on a stand-alone server or on a server farm.

In this article:

For information about the commands and syntax that are used in scripted deployment of a SharePoint Foundation 2010 farm, see Scripted deployment reference (SharePoint Foundation 2010).

Installing SharePoint Products by using Windows PowerShell

In SharePoint Foundation 2010, you can use Windows PowerShell cmdlets as an alternative interface to perform several operations that control how the SharePoint products are configured. Additionally, you can streamline deployment by using command-line installations in combination with other administrator tools to automate unattended installations.

You can run the Windows PowerShell cmdlets in the SharePoint 2010 Management Shell, or you can add the snap-in that contains the cmdlets. By using a management shell, you can eliminate the step to register the snap-in that contains the cmdlets by using the **Add-PSSnapin** cmdlet. For more information about how to use Windows PowerShell with Microsoft SharePoint 2010 Products, see SharePoint 2010 Products administration by using Windows PowerShell (*http://technet.microsoft.com/library/ae4901b4-505a-42a9-b8d4-fca778abc12e(Office.14).aspx*).

To use the cmdlets, verify that you meet the following minimum requirements: See **Add-SPShellAdmin**. For information about how to add a user to the **SharePoint_Shell_Access** role for the specified database, see Add-SPShellAdmin (*http://technet.microsoft.com/library/2ddfad84-7ca8-409e-878b-d09cb35ed4aa(Office.14).aspx*).

Note:

When you create a new farm or join a server to a farm for the first time, ignore the following error message that appears: "The local farm is not accessible. Cmdlets with FeatureDependencyId are not registered."

The cmdlets must be run in a specific order to run successfully. If you use SharePoint Products Configuration Wizard to configure the installation, it calls the commands (also known as configuration tasks) in the correct order for you. However, if you use cmdlets, you must ensure that you are performing the tasks in the correct order. The Windows PowerShell cmdlets must be performed in the following order:

1. New-SPConfigurationDatabase
2. Install-SPHelpCollection
3. Initialize-SPResourceSecurity
4. Install-SPService
5. Install-SPFeature
6. New-SPCentralAdministration
7. Install-SPApplicationContent

Note:

Use a fresh Windows PowerShell process to perform operations on a new farm. For example, when you add a server to a new farm that was in a different farm, restart the Windows PowerShell process before you add the server to the new farm.

Windows PowerShell installation cmdlets

You can use the following Windows PowerShell cmdlets to install and configure SharePoint Foundation 2010.

Windows PowerShell cmdlet	Description
New-SPConfigurationDatabase (*http://technet.microsoft.com/library/b04f1577-1985-41b8-b555-2f5145a00241(Office.14).aspx*)	Creates a new configuration database on the specified database server. This is the central database for a new SharePoint farm. This command also creates the administration content database.
Install-SPHelpCollection (*http://technet.microsoft.com/library/489c518b-9d3b-4016-b2a7-5dd4c8ed041a(Office.14).aspx*)	Installs the Help site collection files for SharePoint 2010 Products in the current farm. You must specify the **All** parameter to install all Help Collection CABs under **%Program Files%\Common Files\Microsoft Shared\Web Server Extensions\14\HCCab\<LCID>** in the Help site collection.
Initialize-SPResourceSecurity (*http://technet.microsoft.com/library/2243a930-b4ea-4ec5-9307-96f5d5dec36f(Office.14).aspx*)	Enforces resource security on the local server. This cmdlet enforces security for all resources, including files, folders, and registry keys.

Windows PowerShell cmdlet	Description
Install-SPService (*http://technet.microsoft.com/library/6a7b8a23-85ba-4609-83bf-d8672f5b25b4(Office.14).aspx*)	Installs and optionally provisions services on a farm. This cmdlet installs all services, service instances, and service proxies that are specified in the registry on the local server computer.
Install-SPFeature (*http://technet.microsoft.com/library/a1093d30-68a1-4c84-8454-967bda8d68b9(Office.14).aspx*)	Installs a specific SharePoint feature by using the Feature.xml file. When you create a new farm, you must specify the **AllExistingFeatures** parameter to install all available features.
New-SPCentralAdministration (*http://technet.microsoft.com/library/b51e3b8d-b3de-4c35-bcb7-c0ade288c0e4(Office.14).aspx*)	Creates a new Central Administration Web application and starts the central administration service on the local computer. Central Administration is available only on computers where this service runs.
Install-SPApplicationContent (*http://technet.microsoft.com/library/7d5a75c1-7f1a-43ab-9256-a2c699810d72(Office.14).aspx*)	Copies shared application data to existing Web application folders.

Other Resources

SharePoint 2010 Products administration by using Windows PowerShell (*http://technet.microsoft.com/library/ae4901b4-505a-42a9-b8d4-fca778abc12e(Office.14).aspx*)

Installation and other special directories (SharePoint Foundation 2010)

Published: August 5, 2010

In this article:

This article lists the folders and files that are used by Microsoft SharePoint Foundation 2010.

Installation directory files

The following table lists the files and folders that are created in the installation directory (%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14) when you install SharePoint Foundation 2010.

Folder	Description	Files and purpose
AdmIsapi	The physical directory that hosts the SharePoint Central Administration Web site-specific Web services for the _vti_adm virtual directory within Central Administration.	• Admin.asmx - Web service for Central Administration-specific Web service methods. Accessed by http://*server_name:<admin port>*/_vti_adm/admin.asmx. • AdminDisco.aspx - Web service discovery file that is used for the admin.asmx Web service. Accessed by http://*server_name:<admin port>*/_vti_adm/admin.asmx?disco. • AdminWsdl.aspx - Web Services Description Language file that is used to specify the methods and parameters that are provided by the Admin.asmx Web service. Accessed by http://*server_name:<admin port>*/_vti_adm/admin.asmx?wsdl.

Folder	Description	Files and purpose
		• Web.config - Configuration file for Central Administration
Bin	Contains the core binary files for SharePoint Foundation 2010.	• *.dll - Core binary files • Owstimer.exe - Microsoft SharePoint Timer service • Stsadm.exe - SharePoint Foundation command-line administration tool • Wssadmin - SharePoint Foundation Administration Service • Stscfg.exe - Configuration utility that is used by Setup • Mssearch.exe - Search processes • Wsstracing.exe - Logs events to the SharePoint diagnostic trace log file • Psconfig.exe - SharePoint Products Configuration Wizard • Spwriter.exe - SharePoint Foundation VSS Writer
Bin*LCID*\	Contains the core binary files that were used by specific languages. *LCID* is replaced by the locale ID. For example, 3082 is the locale ID for Spanish. Therefore, the path for Spanish language binary files is \Bin\3082.	• Fpext.msg - Error messages and text strings • Microsoft.Sharepoint.Msg.dll - Microsoft SharePoint Foundation Event messages • Microsoft.Sharepoint.Perfmonmsg.dll • Mssmsg.dll - Microsoft search component • WssSmanifest.man
Config	Contains configuration files and default values for the server.	• *.xml - XML file to map default values • AppwpresWeb.config - Configuration file • AdminWeb.config - Configuration file for the Central Administration Web site • LayoutsWeb.config -

Folder	Description	Files and purpose
		Configuration file for the _layouts directory • Web.config - Configuration file for Web applications • • Wss_mediumtrust.config - Configuration file • Wss_minimaltrust.config - Configuration file • Wss_usercode.config
Config\Adminbin	Contains the core binary files.	*.dll
Config\AdminResources	Contains Central Administration resources.	*.resx
Config\Bin	Contains binary files for the _vti/_bin virtual directory.	Stssoap.dll - Binary file that is used for SOAP code Microsoft.SharePoint.Applicationpages.dll - Core binary file
Config\Browsers	Contains the configuration file for support of mobile access to list data.	Compat.browser
Config\IdentityModel	Contains configuration files for custom claims.	Webconfig.Identitymodel.Add.xml Webconfig.Identitymodel.Remove.xml
Config\Powershell\Format	Contains files that define the default display of objects in the Windows PowerShell console.	SharepointPowershell.Format.ps1xml WssSearchPowershell.Format.ps1xml
Config\Powershell\Help	Information about Windows PowerShell cmdlets for SharePoint 2010 Products.	Microsoft.Sharepoint.Powershell.dll-help.xml Microsoft.Sharepoint.Search.dll-help.xml
Config\Powershell\Help*UILanguage*	The default system language in which to display Help for Windows PowerShell cmdlets.	Microsoft.SharePoint.Powershell.dll-help.xml Microsoft.SharePoint.Search.dll-help.xml Microsoft.SharePoint.TopologyService-help.xml

Folder	Description	Files and purpose
Config\Powershell\Registration	Contains code for the cmdlets and the XML files that register the cmdlets.	Psconsole.psc1 SharePoint.ps1 SPCmdletSchema.xsd WssCmdlet.xml WssSearchCmdlets.xml
Config\Powershell\Types	Contains XML-based text files that let you add properties and methods to the objects that are used in Windows PowerShell.	SharepointPowershell.Types.ps1xml WssSearchPowerShell.Types.ps1xml
Config\Resources	Contains resources for localization.	*.resx
Config\Upgrade	Contains XML files that are used in the upgrade process.	GbwUpgrade.xml GbwUpgradeB2B.xml MpsUpgrade.xml MpsUpgradeB2B.xml WssUpgrade.xml WssUpgradeB2B.xml WssSearchUpgrade.xml
Data	Contains SharePoint Foundation Search index files.	
HCCab*LCID*	Contains Help files and support files. *LCID* is replaced by the locale ID. For example, 3082 is the locale ID for Spanish.	*.cab
Help*LCID*	Contains the .chm Help file for the SharePoint Products Configuration Wizard. *LCID* is replaced by the locale ID. For example, 3082 is the locale ID for Spanish.	*.chm
Isapi	The physical directory that is addressed by the _vti/_bin virtual directory. Contains FrontPage Server Extensions RPC interfaces (Shtml.dll, _vti_aut\Author.dll, _vti_adm\Admin.dll) and Microsoft SharePoint Foundation RPC interfaces	• *.asmx - Web services • Authentication.asmx - Web service for SharePoint Authentication Web service methods • AuthenticationDisco.aspx - Web service discovery file that is used for the Authentication.asmx Web

Folder	Description	Files and purpose
	(Owssvr.dll).	service • AuthenticationWsdl.aspx - Web services description language file that is used to specify the methods and parameters that are provided by the Authentication.asmx Web service • *.xml - XML file for managed code • Web.config - Configuration file
Isapi_Vti_Adm	Contains FrontPage Server Extensions RPC interfaces.	Admin.dll - RPC interface for remote administration for FrontPage Server Extensions and other Microsoft Office client applications and other client applications that implement this protocol.
Isapi_Vti_Aut	Contains FrontPage binary files.	Author.dll - RPC interface for remote authoring for FrontPage Server Extensions and other Office client applications and other client applications that implement this protocol.
Isapi\Anonsvc	Contains a configuration file that is used for anonymous authentication.	Web.config
Isapi\Sts	Contains files that are used by SharePoint Server 2010 security token service.	Spsecuritytokenservice.svc Web.config
Logs	Contains the log files.	
Policy	Contains files that are used for information management policy.	*.dll *.config
Resources	Contains the resource files.	*.resx
Template	Contains templates, features, and core Web site files.	
Template*LCID*Sts	Contains files that are copied to the root of the Web site upon instantiation with the Team Site template (for example, Default.aspx). *LCID* is replaced	This folder contains only the DocTemp folder.

Folder	Description	Files and purpose
	by the locale ID. For example, the path for Spanish is Template\3082\Sts.	
Template*LCID*\Sts\Doctemp\Blankpgs	Contains the default document templates.	Bpstd.aspx _Basicpage.htm
Template*LCID*\Sts\Doctemp\Dcl	Contains document templates for the Data Connection Library.	Template.odc
Template*LCID*\Sts\Doctemp\Fp	Contains document templates for FrontPage and SharePoint Designer.	Fptmpl.htm - Default document templates for FrontPage and SharePoint Designer documents
Template*LCID*\Sts\Doctemp\Onenote	Contains document templates for Microsoft OneNote.	Template.one Template.onepkg
Template*LCID*\Sts\Doctemp\Ppt	Contains document templates for Microsoft PowerPoint.	Filelist.xml Master03.css Master03.htm Master03.xml Pptmpl.htm Pptmpl.pot Pptmpl.pptx Pres.xml Pptml.pptx Preview.wmf Slide001.htm
Template*LCID*\Sts\Doctemp\Smartpgs	Contains document templates for Web Part pages.	*.aspx _Webpartpage.htm
Template*LCID*\Sts\Doctemp\Word	Contains document templates for Microsoft Word.	Wdtmpl.doc Wdtmpl.htm Wdtmpl.dotx
Template*LCID*\Sts\Doctemp\Xl	Contains document templates for Microsoft Excel.	Filelist.xml Sheet001.htm Sheet002.htm Sheet003.htm Style.css Tabstrip.htm

Folder	Description	Files and purpose
		Xltmpl.htm Xltmpl.xls Xltmpl.xlsx
Template*LCID*\Sts\Doctemp\Xmlforms\Blank	Contains document templates for Microsoft InfoPath.	Template.xml - Default document templates for XML documents
Template*LCID*\Workflow	Contains files for workflow activities. *LCID* is replaced by the locale ID. For example, 3082 is the locale ID for Spanish. Therefore, the path for Spanish is Template\3082\Workflow.	Wss.actions Moderationworkflow.xml
Template*LCID*\Xml	Site template files for the specific language. *LCID* is replaced by the locale ID. For example, 3082 is the locale ID for Spanish. Therefore, the path for Spanish is Template\3082\Xml.	Deadweb.xml Rgnlstng.xml Webtemp.xml
Template\Admin	Contains templates and master pages for Central Administration.	*.aspx Admin.master Admin.sitemap
Template\Admin\Bdc	Contains templates and master pages for Microsoft Business Connectivity Services.	*.aspx
Template\ControlTemplates	Contains control templates that determine the layout of list item forms.	*.ascx
Template\DocumentTemplates	Contains the page used for creating document libraries.	Wkpstd.aspx
Template\Features	Contains SharePoint Foundation features.	
Template\Features\AdminLinks	Contains Operations and Application Management pages that use the SharePoint Foundation 2010 features infrastructure to provide link extensibility.	Operations.xml Applications.xml Feature.xml

Folder	Description	Files and purpose
Template\Features\AnnouncementsList	Contains files that are used for the Announcements list.	Feature.xml
Template\Features\AnnouncementsList\Announce	Contains a template description file for the Announcements list.	Schema.xml - Schema file
Template\Features\AnnouncementsList\ListTemplates	Contains a template description file for the Announcements list.	Announcements.xml
Template\Features\BasicWebParts	Contains the feature description and Web Part description files for the built-in SharePoint Foundation Web Parts.	Feature.xml - Feature description Elements.xml - Element manifest *.dwp - Web Part descriptions
Template\Features\ContactsList	Contains the file that is used for the Contacts list.	Feature.xml
Template\Features\ContactsList\Contacts	Contains the template content file for the Contacts list.	Schema.xml - Schema file
Template\Features\ContactsList\ListTemplates	Contains the template description file for the Contacts list.	Contacts.xml
Template\Features\ContentLightup	Contains files that provide several user interface components and links.	Feature.xml
Template\Features\ContentLightup\Controls	Contains template content files for standard user interface items.	SearchArea.xml
Template\Features\ContentTypeSettings	Contains files that are used for content type settings.	Feature.xml ContentTypeSettings.xml
Template\Features\ctypes	Contains files that are used for content types.	Ctypeswss.xml Feature.xml
Template\Features\CustomList	Contains files that are used for Custom lists.	Feature.xml
Template\Features\CustomList\CustList	Contains the template content file for Custom lists.	Schema.xml - Schema file

Folder	Description	Files and purpose
Template\Features\DataSourceLibrary	Contains files that are used for the Data Source Library.	Feature.xml
Template\Features\DataSourceLibrary\DataSrcs	Contains the template content file for the Data Source Library.	Schema.xml - Schema file
Template\Features\DataSourceLibrary\ListTemplates	Contains the template description file for the Data Source Library.	DataSourceLibrary.xml
Template\Features\DiscussionsList	Contains a file that is used for the Discussion Board list.	Feature.xml
Template\Features\DiscussionsList\Discuss	Contains the template content file for the Discussion Board list.	Schema.xml - Schema file
Template\Features\DiscussionsList\ListTemplates	Contains the template description file for the Discussion Board list.	Discussions.xml
Template\Features\DocumentLibrary	Contains the file that is used for the Document Library list type.	Feature.xml
Template\Features\DocumentLibrary\DOCLib	Contains files that are used for document libraries.	*.aspx - Form pages *.htm - Dialog boxes Schema.xml - Schema file
Template\Features\DocumentLibrary\ListTemplates	Contains the template description file for the document libraries.	DocumentLibrary.xml
Template\Features\EventsList	Contains a file that is used for the Events list.	Feature.xml
Template\Features\EventsList\Events	Contains the template content file for the Events list.	Schema.xml - Schema file
Template\Features\EventsList\ListTemplates	Contains the template description file for the Events list.	Events.xml
Template\Features\ExternalList	Contains a file that is used for the External list.	Feature.xml

Folder	Description	Files and purpose
Template\Features\ExternalList\ExtList	Contains the template content file for the External list.	Schema.xml - Schema file
Template\Features\ExternalList\ListTemplates	Contains the template description file for the External list.	ExternalList.xml
Template\Features\FacilityList	Contains a file that is used for the Facility list.	Feature.xml
Template\Features\FacilityList\Facility	Contains the template content file for the Facility list.	Schema.xml - Schema file
Template\Features\FacilityList\ListTemplates	Contains the template description file for the Facility list.	Facilitylist.xml
Template\Features\FCGroupsList	Contains a file that is used for the FCGroups list.	Feature.xml
Template\Features\FCGroupsList\FCGroups	Contains the template content file for the FCGroups list.	Schema.xml - Schema file
Template\Features\FCGroupsList\ListTemplates	Contains the template description file for the FCGroups list.	Fcgroupslist.xml
Template\Features\Fields	Contains files that are used for the fields in a list.	Feature.xml Fieldswss.xml Fieldswss2.xml Fieldswss3.xml
Template\Features\GanttTasksList	Contains a file that is used for the Project Tasks (Gantt Chart) list.	Feature.xml
Template\Features\GanttTasksList\Gantt	Contains the template content file for the Project Tasks (Gantt Chart) list.	Schema.xml
Template\Features\GanttTasksList\ListTemplates	Contains the template description file for the Project Tasks (Gantt Chart) list.	GanttTasksList.xml
Template\Features\GBWProvision	Contains files that are used for the Group Board Workshop.	Feature.xml Listinstance.xml
Template\Features	Contains files that are used for	Elements.xml

Folder	Description	Files and purpose
\GBWWebParts	Group Board Workshop Web Parts.	Feature.xml Timecard.dwp Whatsnew.dwp Whereabouts.dwp
Template\Features\GridList	Contains a file that is used for the Custom list in Datasheet view.	Feature.xml
Template\Features\GridList\GridList	Contains a file that is used for the Custom list in Datasheet view list type.	Schema.xml - Schema file
Template\Features\GridList\ListTemplates	Contains the template description file for the Custom list in Datasheet view.	GridList.xml
Template\Features\GroupWork	Contains files that are used for the Group Board Custom list.	Feature.xml Listinstance.xml
Template\Features\HelpLibrary	Contains a file that is used for the Help collection.	Feature.xml
Template\Features\HelpLibrary\HelpLibrary	Contains a file that is used for the Help collection.	Schema.xml - Schema file
Template\Features\HelpLibrary\ListTemplates	Contains the template description file for the Help collection.	Helplibrary.xml
Template\Features\HolidaysList	Contains a file that is used for the Holidays List.	Feature.xml
Template\Features\HolidaysList\Holidays	Contains a file that is used for the Holidays List.	Schema.xml - Schema file
Template\Features\HolidaysList\ListTemplates	Contains the template description file for the Holidays List.	Holidayslist.xml
Template\Features\IMEDicList	Contains a file that is used for the Medical Dictionary.	Feature.xml
Template\Features\IMEDicList\IMEDic	Contains a file that is used for the Medical Dictionary.	Schema.xml - Schema file
Template\Features	Contains the template	Imediclist.xml

Folder	Description	Files and purpose
\IMEDicList\ListTemplates	description file for the Medical Dictionary.	
Template\Features\IssuesList	Contains a file that is used for the Issue Tracking list.	Feature.xml
Template\Features\IssuesList\Issue	Contains the template content file for the Issue Tracking list.	Schema.xml - Schema file
Template\Features\IssuesList\ListTemplates	Contains the template description file for the Issue Tracking list.	Issues.xml
Template\Features\IssueTrackingWorkflow	Contains files that are used for the Issue Tracking Workflow.	IssueTracking.xml Feature.xml
Template\Features\LinksList	Contains a file that is used for the Links list.	Feature.xml
Template\Features\LinksList\Links	Contains the template content file for the Links list.	Schema.xml - Schema file
Template\Features\LinksList\ListTemplates	Contains the template description file for the Links list.	Links.xml
Template\Features\MobilityRedirect	Contains files that are used for the Mobility Redirection feature for lists.	Feature.xml Default.aspx Elements.xml
Template\Features\MpsWebParts	Contains files that are used for the management pack for Microsoft System Center Operations Manager 2007.	Feature.xml Elements.xml
Template\Features\NoCodeWorkflowLibrary	Contains a file that is used for No-Code Workflows.	Feature.xml
Template\Features\OpenInClient	Contains a file that is used for the OpenInClient feature for opening browser-enabled documents in the Office client applications.	Feature.xml
Template\Features\PictureLibrary	Contains a file that is used for the Picture Library.	Feature.xml
Template\Features	Contains the template content	*.aspx

Folder	Description	Files and purpose
\PictureLibrary\PicLib	files that are used for the Picture Library.	Schema.xml
Template\Features\PictureLibrary\ListTemplates	Contains the template description file for the Picture Library.	PictureLibrary.xml
Template\Features\ScheduleList	Contains a file that is used for the Schedule list.	Feature.xml
Template\Features\ScheduleList\Schedule	Contains the template content file that is used for the Schedule list.	Schema.xml
Template\Features\ScheduleList\ListTemplates	Contains the template description file for the Schedule list.	Schedulelist.xml
Template\Features\SiteHelp	Contains a file that is used for the custom site collection Help.	Feature.xml
Template\Features\SiteSettings	Contains files that are used for site settings.	Features.xml SiteSetting.xml
Template\Features\SPSearchFeature	Contains a file for the SharePoint Foundation Search feature.	Feature.xml
Template\Features\SurveysList	Contains a file for the Survey list.	Feature.xml
Template\Features\SurveysList\Survey	Contains the template content file that is used for the Survey list.	Schema.xml
Template\Features\SurveysList\ListTemplates	Contains the template description file for the Survey list.	Surveys.xml
Template\Features\TasksList	Contains a file for the Tasks list.	Feature.xml
Template\Features\TasksList\ListTemplates	Contains the template description file for the Tasks list.	Tasks.xml
Template\Features\TasksList\Tasks	Contains the template content file that is used for the Tasks list.	Schema.xml - Schema file

Folder	Description	Files and purpose
Template\Features\TeamCollab	Contains a file that provides team collaboration capabilities by making standard lists — such as document libraries and issues — available.	Feature.xml
Template\Features\TenantAdminBDC	Contains files for Tenant Business Data Connectivity Administration.	Default.aspx Feature.xml
Template\Features\TenantAdminBDCStapling	Contains files for Tenant Business Data Connectivity Administration Stapling.	Feature.xml Featurestapling.xml
Template\Features\TenantAdminLinks	Contains files for Tenant Administration Content Deployment Configuration.	Default.aspx Feature.xml
Template\Features\TimecardList	Contains a file for the Timecard list.	Feature.xml
Template\Features\TimecardList\ListTemplates	Contains the template description file for the Timecard list.	Timecardlist.xml
Template\Features\TimecardList\Tasks	Contains the template content file that is used for the Timecard list.	Schema.xml - Schema file
Template\Features\WebPageLibrary	Contains a file that is used for the Web Page Library.	Feature.xml
Template\Features\WebPageLibrary\ListTemplates	Contains the template description file for the Web Page Library.	WebPageLibrary.xml
Template\Features\WebPageLibrary\WebPageLib	Contains the template content file that is used for the Web Page Library.	Schema.xml - Schema file
Template\Features\WhatsNewList	Contains a file for the What's New list.	Feature.xml
Template\Features\WhatsNewList\ListTemplates	Contains the template description file for the What's New list.	Whatsnewlist.xml
Template\Features\WhatsNewList\Tasks	Contains the template content file that is used for the What's New list.	Schema.xml - Schema file

Folder	Description	Files and purpose
Template\Features\WhereaboutsList	Contains a file for the Whereabouts list.	Feature.xml
Template\Features\WhereaboutsList\ListTemplates	Contains the template description file for the Whereabouts list.	Whereaboutslist.xml
Template\Features\WhereaboutsList\Whereabouts	Contains the template content file that is used for the Whereabouts list.	Schema.xml - Schema file
Template\Features\WikiPageHomePage	Contains the file that is used for the Wiki home page.	Feature.xml
Template\Features\WikiWelcome	Contains a file that is used for the Wiki site.	Feature.xml
Template\Features\WorkflowHistoryList	Contains a file that provides support for Workflow History lists for a site.	Feature.xml
Template\Features\WorkflowHistoryList\ListTemplates	Contains the template description file for Workflow History lists for a site.	WorkflowHistory.xml
Template\Features\WorkflowHistoryList\Wrkflhis	Contains the template content file that is used for Workflow History lists for a site.	Schema.xml - Schema file
Template\Features\WorkflowProcessList	Provides the ability to support running custom form actions.	Feature.xml
Template\Features\WorkflowProcessList\WorkflowProcess	Contains the template content file that is used for workflow processes.	Schema.xml - Schema file
Template\Features\WorkflowProcessList\ListTemplates	Contains the template description file for workflow processes.	WorkflowProcess.xml
Template\Features\XmlFormLibrary	Contains a file that is used for form libraries.	Feature.xml
Template\Features\XmlFormLibrary\ListTemplates	Contains the template description file for form libraries.	XmlFormLibrary.xml

Folder	Description	Files and purpose
Template\Features\XmlFormLibrary\XmlForm	Contains the template content file for form libraries.	Schema.xml - Schema file
Template\Global	Contains site definition files that are used for initializing site configurations.	Default.master Minimal.master Mwsdefault.master Mwsdefaultv4.master V4.master
Template\Identity model\\Forms	Contains files that are used for a claims forms page.	Default.aspx Web.config
Template\Identity model\\Login	Contains files that are used for a claims logon page.	Default.aspx Web.config
Template\Identity model\\Trust	Contains files that are used for a trusted provider sign-in page.	Default.aspx Web.config
Template\Identity model\\Windows	Contains files that are used for a Windows sign-in page.	Default.aspx Web.config
Template\Images	Contains images that are shared by all the pages on the server, and that are addressed by the virtual directory _layouts/images.	*.gif, *.jpg, *.png
Template\Layouts	Contains language subdirectories that contain forms such as those for creating lists and site administration pages, and that are addressed by the virtual directory _layouts. All sites share these subdirectories.	*.aspx - Form pages Web.config - Configuration file
Template\Layouts*LCID*	Contains forms for creating lists, site administration pages, and forms for a specific language. *LCID* is replaced by the locale ID. For example, 3082 is the locale ID for Spanish. Therefore, the path for Spanish is \Template\Layouts\3082.	*.htm - Dialog boxes *.htc - Menu control *.js, - JavaScript files *.xml - XML templates *.xsd - XML definitions

Folder	Description	Files and purpose
Template\Layouts*LCID*\Images	Contains images that are used in the default site pages for a specific language.	*.gif
Template\Layouts*LCID*\Styles	Contains style sheets that are shared by all site templates for a particular language, and that are addressable by the virtual directory _layouts/styles.	*.css - Style sheets
Template\Pages	Contains files that are used for master pages.	Form.aspx Viewpage.aspx Webfldr.aspx
Template\Scenarios\AdminConfig	Contains the template description file for a Web site for SharePoint 2010 Products administration and configuration.	Adminconfig.xml
Template\Scenarios\BdcService	Contains the template description file for a Business Data Connectivity administration Web site.	Bdcservice.xml
Template\Scenarios\JoinFarm	Contains the template description file for a Web site where you can join and configure a farm.	Joinfarm.xml
Template\SiteTemplates\Blog	Contains the file that is copied to the root of the Web site upon instantiation of a BLOG by using a BLOG template.	Default.aspx
Template\SiteTemplates\Centraladmin	Contains files that are copied to the root of the Web site upon instantiation of a site by using a CentralAdmin site definition.	*.aspx
Template\SiteTemplates\Centraladmin\Dwp	Contains the file that is used for Central Administration Web Parts.	TopologyView.dwp
Template\SiteTemplates\Centraladmin\Lists\Admintasks	Contains the template content file that is used for the Administrator Tasks list.	Schema.xml
Template\SiteTem	Contains the template content	*.aspx

Folder	Description	Files and purpose
plates\Centraladmin\Lists\Distributionlists	files that are used for distribution lists.	Schema.xml
Template\SiteTemplates\Centraladmin\Lists\Healthreports	Contains the template content file that is used for health reports.	Schema.xml
Template\SiteTemplates\Centraladmin\Lists\Healthrules	Contains the template content file that is used for creating health analyzer rules.	Schema.xml
Template\SiteTemplates\Centraladmin\Xml	Contains the site definition file for Central Administration.	Onet.xml
Template\SiteTemplates\Mps	Contains files that are copied to the root of the Web site upon instantiation with a Meeting Workspace template (for example, Default.aspx).	*.aspx - Form pages
Template\SiteTemplates\Mps\Doctemp\Smartpgs	Contains the file that is used for Web Part pages in Meeting Workspaces.	Spstd1.aspx - Form page
Template\SiteTemplates\Mps\Lists	Contains folders for the categories of the lists that are used in the Meeting Workspace templates, and the schema definition and default views.	
Template\SiteTemplates\Mps\Lists\Agenda	Contains files that are used for the Agenda list.	*.aspx - Form pages Schema.xml - Schema file
Template\SiteTemplates\Mps\Lists\Decision	Contains files that are used for the Decisions list.	*.aspx - Form pages Schema.xml - Schema file
Template\SiteTemplates\Mps\Lists\Meetings	Contains files that are used for the Meeting Workspace templates.	MoveToDt.aspx - Form page Schema.xml - Schema file
Template\SiteTemplates\Mps\Lists\Objectiv	Contains files that are used for the Objectives list.	*.aspx - Form pages Schema.xml - Schema file
Template\SiteTemplates\Mps\Lists\P	Contains files that are used for	*.aspx - Form pages

Folder	Description	Files and purpose
eople	the Attendees list.	Schema.xml - Schema file
Template\SiteTemplates\Mps\Lists\Textbox	Contains files that are used for the Text Box list.	*.aspx - Form pages Schema.xml - Schema file
Template\SiteTemplates\Mps\Lists\Thgbring	Contains files that are used for the Things to Bring list.	*.aspx - Form pages Schema.xml - Schema file
Template\SiteTemplates\Mps\Lists\Wkspglib	Contains files that are used for lists in the Meeting Workspace templates.	Schema.xml - Schema file
Template\SiteTemplates\Mps\Xml	Contains the available lists in the Meeting Workspace templates, base types for fields (Onet.xml), and the standard view template for new views.	Onet.xml
Template\SiteTemplates\Sgs	Contains files that are copied to the root of the Web site upon instantiation with the Group Work Site template (for example, Default.aspx).	Default.aspx - Default home page for sites that are based on sgs templates
	Contains the site definition file.	Onet.xml- Defines navbars, available list types, initial configurations, and modules
Template\SiteTemplates\Sts	Contains files that are copied to the root of the Web site upon instantiation with the Team Site template (for example, Default.aspx).	Default.aspx - Default home page for sites that are based on Team Site templates Defaultdws.aspx
Template\SiteTemplates\Sts\Xml	Contains the site definition file.	Onet.xml- Defines navbars, available list types, initial configurations, and modules
Template\SiteTemplates\TenantAdmin	Contains files that are copied to the root of the Web site upon instantiation with the Tenant Administration template (for example, Default.aspx).	Default.aspx - Default home page for sites that are based on Tenant Administration templates
Template\SiteTemplates\TenantAdmin\Xml	Contains site definition file.	Onet.xml- Defines navbars, available list types, initial configurations and modules

Folder	Description	Files and purpose
Template\SiteTemplates\Wiki\Xml	Contains the site definition file.	Onet.xml
Template\Sql	Contains stored procedures for Microsoft SQL Server.	*.sql - Stored procedures for SQL Server
Template\Themes	Contains the list of themes.	Themes.inf - Themes list
Template\Themes\Theme	Contains files that were used by a specific theme.	*.gif ,*.jpg - Images *.css - Style sheets *.inf - Theme definition file Theme.utf8 - Theme file for UTF8 encoding
Template\Xml	Contains XML files that are used by all site templates in all languages.	*.xmo - Templates that are used across all languages and site types
Template\Xml\Help	Contains XML files that are used by the Help system.	Sts.xml - Context-sensitive Help mapping file
UserCode\	Contains files that are used to load and execute sandboxed solutions.	SpucHostService.exe SpucHostService.exe.config SpucWorkerProcess.exe SpucWorkerProcess.exe.config SpucWorkerProcessProxy.exe SpucWorkerProcessProxy.exe.config
UserCode\assemblies	Contains core binary files for running sandboxed solutions.	Microsoft.SharePoint.dll Microsoft.SharePoint.SubsetProxy.dll Microsoft.SharePoint.UserCode.dll
WebClients\Bdc	Contains a Web client configuration file for a Business Data Connectivity (BDC) Service application.	Client.config
WebClients\SecurityToken	Contains a Web client configuration file for a security token service application.	Client.config
WebClients\SubscriptionSettings	Contains a Web client configuration file for a Subscription Settings Service application.	Client.config

Folder	Description	Files and purpose
WebClients\Topology	Contains a Web client configuration file for a Topology Web Service application.	Client.config
WebServices\Bdc	Contains files that are used to run a Business Data Connectivity (BDC) Service application.	Bdcservice.svc Web.config
WebServices\Root	Contains the Web.config file for the Web application root, which stores ASP.NET configuration options.	Web.config
WebServices\SecurityToken	Contains files that are used to run a security token service application.	Securitytoken.svc Web.config Windowstokencache.svc
WebServices\SubscriptionSettings	Contains files that are used to run a Subscription Settings Service application.	Subscriptionsettings.svc Web.config
WebServices\Topology	Contains files that are used to run a Topology Web Service application.	Topology.svc Web.config
Wpresources	Contains the configuration file for Web Parts.	Web.config

Web Part resource files

In addition to the installation directory, there is a Web Part resources directory that contains the files that are used to support custom Web Parts in SharePoint Foundation 2010. The %COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\Wpresources directory contains a Web.config file that is used to help control the security for ASP.NET files that are used in Web Parts.

For more information about custom Web Parts, see the Microsoft SharePoint 2010 SDK (*http://go.microsoft.com/fwlink/?LinkId=198386*).

Web site content files

The following table lists the files that are added to each top-level Web site or subsite when a SharePoint site is created.

Folder	Description	Files and purpose
Inetpub\Wwwroot\Wss\VirtualDirectories*porthost header*	Contains configuration file.	Web.config
Inetpub*Folder*_vti_pvt	Contains legacy FrontPage Server Extensions files and folders.	Buildversion.cnf Service.cnf Services.cnf
Inetpub*Folder*\Wpresources\	Contains configuration file for Web Parts.	Web.config

All other Web site files are stored in the content and configuration database.

User permissions and permission levels (SharePoint Foundation 2010)

Updated: January 7, 2011

This article describes the default permission levels as well as the user permissions in Microsoft SharePoint Foundation 2010.

In this article:

Default permission levels

Permission levels are collections of permissions that allow users to perform a set of related tasks. SharePoint Foundation 2010 includes five permission levels by default. You can customize the permissions available in these permission levels (except for the Limited Access and Full Control permission levels), or you can create customized permission levels that contain only the permissions you need. For more information about how to customize permission levels, see Configure custom permissions (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/2f1d44be-737a-43a3-bc95-436199eebedb(Office.14).aspx*).

Note:

Although you cannot directly edit the Limited Access and Full Control permission levels, you can make individual permissions unavailable for the entire Web application, which removes those permissions from the Limited Access and Full Control permission levels. For more information about how to manage permissions for a Web application, see Manage permissions for a Web application (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/5cdea29d-d054-414e-9d8a-5d60ff3501c3(Office.14).aspx*).

The following table lists the default permission levels for team sites in SharePoint Foundation 2010.

Permission level	Description	Permissions included by default
Limited Access	Allows access to shared resources in the Web site so that the users can access an item within the site. Designed to be combined with fine-grained permissions to give users	• View Application Pages • Browse User Information • Use Remote Interfaces • Use Client Integration Features • Open

Permission level	Description	Permissions included by default
	access to a specific list, document library, folder, list item, or document, without giving them access to the entire site. Cannot be customized or deleted.	
Read	View pages, list items and download documents.	• Limited Access permissions, plus: • View Items • Open Items • View Versions • Create Alerts • Use Self-Service Site Creation • View Pages
Contribute	View, add, update, and delete items in the existing lists and document libraries.	• Read permissions, plus: • Add Items • Edit Items • Delete Items • Delete Versions • Browse Directories • Edit Personal User Information • Manage Personal Views • Add/Remove Personal Web Parts • Update Personal Web Parts
Design	View, add, update, delete, approve, and customize items or pages in the Web site.	• Approve permissions, plus: • Manage Lists • Add and Customize Pages • Apply Themes and Borders • Apply Style Sheets
Full Control	Allows full control of the scope.	All permissions

User permissions

SharePoint Foundation 2010 includes 33 permissions, which are used in the five default permission levels. You can change which permissions are included in a particular permission level (except for the Limited Access and Full Control permission levels), or you can create a new permission level to contain specific permissions.

Permissions are categorized as list permissions, site permissions, and personal permissions, depending on the objects to which they can be applied. For example, site permissions apply to a particular site, list permissions apply only to lists and libraries, and personal permissions apply only to things such as personal views, private Web Parts, and more. The following tables describe what each permission is used for, the dependent permissions, and the permission levels in which it is included.

List permissions

Permission	Description	Dependent permissions	Included in these permission levels by default
Manage Lists	Create and delete lists, add or remove columns in a list, and add or remove public views of a list.	View Items, View Pages, Open, Manage Personal Views	Design, Full Control
Override Check Out	Discard or check in a document that is checked out to another user without saving the current changes.	View Items, View Pages, Open	Design, Full Control
Add Items	Add items to lists, and add documents to document libraries.	View Items, View Pages, Open	Contribute, Design, Full Control
Edit Items	Edit items in lists, edit documents in document libraries, and customize Web Part Pages in document libraries.	View Items, View Pages, Open	Contribute, Design, Full Control
Delete Items	Delete items from a list, and documents from a document library.	View Items, View Pages, Open	Contribute, Design, Full Control
View Items	View items in lists, and documents in document libraries.	View Pages, Open	Read, Contribute, Design, Full Control
Approve Items	Approve minor versions of list items or documents.	Edit Items, View Items, View Pages, Open	Design, Full Control

Permission	Description	Dependent permissions	Included in these permission levels by default
Open Items	View the source of documents with server-side file handlers.	View Items, View Pages, Open	Read, Contribute, Design, Full Control
View Versions	View past versions of list items or documents.	View Items, Open Items, View Pages, Open	Read, Contribute, Design, Full Control
Delete Versions	Delete past versions of list items or documents.	View Items, View Versions, View Pages, Open	Contribute, Design, Full Control
Create Alerts	Create e-mail alerts.	View Items, View Pages, Open	Read, Contribute, Design, Full Control
View Application Pages	View forms, views, and application pages. Enumerate lists.	Open	All

Site permissions

Permission	Description	Dependent permissions	Included in these permission levels by default
Manage Permissions	Create and change permission levels on the Web site and assign permissions to users and groups.	View Items, Open Items, View Versions, Browse Directories, View Pages, Enumerate Permissions, Browse User Information, Open	Full Control
View Usage Data	View reports on Web site usage.	View Pages, Open	Full Control
Create Subsites	Create subsites such as team sites, Meeting Workspace sites, and Document Workspace sites.	View Pages, Browse User Information, Open	Full Control

Permission	Description	Dependent permissions	Included in these permission levels by default
Manage Web Site	Perform all administration tasks for the Web site, and manage content.	View Items, Add and Customize Pages, Browse Directories, View Pages, Enumerate Permissions, Browse User Information, Open	Full Control
Add and Customize Pages	Add, change, or delete HTML pages or Web Part pages, and edit the Web site by using a Windows SharePoint Services-compatible editor.	View Items, Browse Directories, View Pages, Open	Design, Full Control
Apply Themes and Borders	Apply a theme or borders to the entire Web site.	View Pages, Open	Design, Full Control
Apply Style Sheets	Apply a style sheet (.css file) to the Web site.	View Pages, Open	Design, Full Control
Create Groups	Create a group of users that can be used anywhere within the site collection.	View Pages, Browse User Information, Open	Full Control
Browse Directories	Enumerate files and folders in a Web site by using Microsoft SharePoint Designer 2010 and Web DAV interfaces.	View Pages, Open	Contribute, Design, Full Control
Use Self-Service Site Creation	Create a Web site by using Self-Service Site Creation.	View Pages, Browse User Information, Open	Read, Contribute, Design, Full Control
View Pages	View pages in a Web site.	Open	Read, Contribute, Design, Full Control
Enumerate Permissions	Enumerate permissions on the Web site, list, folder, document, or list item.	Browse Directories, View Pages, Browse User Information, Open	Full Control
Browse User Information	View information about users of the Web site.	Open	All

Permission	Description	Dependent permissions	Included in these permission levels by default
Manage Alerts	Manage alerts for all users of the Web site.	View Items, View Pages, Open	Full Control
Use Remote Interfaces	Use SOAP, Web DAV, or SharePoint Designer 2010 interfaces to access the Web site.	Open	All
Use Client Integration Features	Use features that start client applications. Without this permission, users must work on documents locally and then upload their changes.	Use Remote Interfaces, Open	All
Open	Open a Web site, list, or folder to access items inside that container.	None	All
Edit Personal User Information	Users can change their own user information, such as adding a picture.	Browse User Information, Open	Contribute, Design, Full Control

Personal permissions

Permission	Description	Dependent permissions	Included in these permission levels by default
Manage Personal Views	Create, change, and delete personal views of lists.	View Items, View Pages, Open	Contribute, Design, Full Control
Add/Remove Personal Web Parts	Add or remove personal Web Parts on a Web Part page.	View Items, View Pages, Open	Contribute, Design, Full Control
Update Personal Web Parts	Update Web Parts to display personalized information.	View Items, View Pages. Open	Contribute, Design, Full Control

Other Resources

Configure custom permissions (SharePoint Foundation 2010)
(*http://technet.microsoft.com/library/2f1d44be-737a-43a3-bc95-436199eebedb(Office.14).aspx*)

Database types and descriptions (SharePoint Foundation 2010)

Updated: July 29, 2010

This article describes the databases that are installed for Microsoft SharePoint Foundation 2010. It includes some sizing and placement information.

Databases for SharePoint Foundation 2010 can be hosted in Microsoft SQL Server 2008 R2, SQL Server 2008 with Service Pack 1 (SP1) and Cumulative Update 2, or SQL Server 2005 with SP3 and Cumulative Update 3. Stand-alone installations can also be hosted in the Express Editions of SQL Server 2008 R2 or SQL Server 2008. For more information see Determine hardware and software requirements (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/dcdb7f80-5d48-4b7c-9cb5-affa5f293653(Office.14).aspx*).

Note:

The database names listed in this topic are automatically created when you run the SharePoint Products Configuration Wizard. You do not have to use these naming conventions. You can either specify database names when you create them, or change the database names after they have been created. For more information, see Deploy using DBA-created databases (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/c7647e52-2178-4d3d-9376-84b2c9a35a1e(Office.14).aspx*).

The database sizes listed in this article are based on the following ranges.

Descriptor	Size range
Small	1 gigabyte (GB) or less
Medium	Up to 100 GB.
Large	Up to 1 terabyte
Extra-large	1 terabyte or more

In this article:

For a graphical overview of the databases used by SharePoint Foundation 2010, see Database model (*http://go.microsoft.com/fwlink/?LinkId=187968*).

SharePoint Foundation 2010 databases

The following databases are part of a SharePoint Foundation 2010 deployment. These databases are also part of any other SharePoint 2010 Products deployment.

Configuration

The configuration database contains data about SharePoint databases, Internet Information Services (IIS) Web sites, Web applications, trusted solutions, Web Part packages, site templates, and Web application and farm settings specific to SharePoint 2010 Products, such as default quota settings and blocked file types.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	SharePoint_Config
Location requirements	None
General size information and growth factors	Small. However, transaction log files are likely to become large. For more information, see Additional notes, below.
Read/write characteristics	Read-intensive
Recommended scaling method	Must scale up; that is, the database must grow larger, because only one configuration database is supported per farm. (Significant growth is unlikely.)
Associated health rules	None
Supported backup mechanisms	SharePoint Foundation 2010 backup and recovery, SQL Server, and System Center Data Protection Manager (DPM) 2010. The configuration database is a special case for backup and recovery. For more information, see Additional notes below.
Default recovery model	Full. We recommend that you switch the configuration database to the simple recovery model to restrict growth of the log file.
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

Additional notes

Transaction log files. We recommend that you back up the transaction log for the configuration database regularly to force truncation, or — if you are not mirroring your system — change the database to run in Simple recovery mode. For more information, see Transaction Log Truncation (*http://go.microsoft.com/fwlink/?LinkId=186687*).

Backup and recovery. The configuration database is backed up when you perform a SharePoint farm configuration and content backup, and some configuration settings from the database are exported and stored as XML files. When a farm is restored, the configuration database is not restored. Instead, the saved configuration settings are imported. The configuration database can be successfully backed up and restored by using SQL Server or other tools if the SharePoint farm is first taken offline.

Note:

Many configuration settings are not saved during a farm configuration-only backup or restore, in particular Web application settings, service application settings, and settings that are specific to the local server. These settings are saved during a farm content and configuration backup, but some of them, such as service application proxy settings, cannot be restored during a farm recovery. For information about what is saved during a configuration backup, see Back up a farm configuration (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/6d006882-8dc4-4e28-9a47-9d2d592437dc(Office.14).aspx*). For information about how to document and copy configuration settings that are not backed up, see Copy configurations from one farm to another (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/6635b76f-ad53-4231-9fda-f111f64dcadb(Office.14).aspx*).

Central Administration content

The Central Administration content database is considered to be a configuration database. It stores all site content, including site documents or files in document libraries, list data, and Web Part properties, in addition to user names and rights for the Central Administration site collection.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	SharePoint_AdminContent
Location requirements	None
General size information, and growth factors	Small.
Read/write characteristics	Varies
Recommended scaling method	Must scale up; that is, the database must grow larger, because only one Central Administration database is supported per farm. (Significant growth is unlikely.)

Associated Health rules	None
Supported backup mechanisms	SharePoint Foundation 2010 backup and recovery, SQL Server, and DPM 2010. The Central Administration content database is a special case for backup and recovery. For more information, see Additional notes below.
Default recovery model	Full
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

Additional notes

Backup and recovery. The Central Administration content database is backed up when you perform a SharePoint farm configuration and content backup. When a farm is restored, the Central Administration content database is not restored. The Central Administration content database can be successfully backed up and restored by using SQL Server or other tools if the SharePoint farm is first taken offline.

Content databases

Content databases store all content for a site collection, including site documents or files in document libraries, list data, Web Part properties, audit logs, and sandboxed solutions, in addition to user names and rights.

All the data for a specific site collection resides in one content database on only one server. A content database can be associated with more than one site collection.

Content databases also contain the Microsoft Office Web Apps cache, if Office Web Apps have been deployed. Only one cache is created per Web application. If multiple site collections that are stored in different content databases have Office Web Apps activated, they will all use the same cache. You can configure the size of cache, the expiration period, and the location. For more information about the size of the Office Web Apps cache, see Manage the Office Web Apps cache (*http://technet.microsoft.com/library/9a75a461-6c86-4b61-be98-bcaf9290f2da(Office.14).aspx*).

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	WSS_Content
Location requirements	None

General size information, and growth factors	We strongly recommended limiting the size of content databases to 200 GB to help ensure system performance. For more information, see Additional notes, below. Content database size varies significantly by usage. For more information, see Additional notes, below.
Read/write characteristics	Varies by usage. For example, collaboration environments are write-intensive; document management environments are read-intensive.
Recommended scaling method	The content database that supports a site collection must scale up; that is, the database must be able to grow larger as needed. However, you can create additional site collections that are associated with a Web application and associate the new site collection with a different content database. Also, if a content database is associated with multiple site collections, you can move a site collection to another database.
Associated Health rules	None
Supported backup mechanisms	SharePoint Foundation 2010 backup and recovery, SQL Server, and DPM 2010.
Default recovery model	Full
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	Yes

Additional notes

Recommended content database size limitations

We strongly recommend that you limit the size of content databases to 200 GB to help ensure system performance.

Important:

Content database sizes up to 1 terabyte are supported only for large, single-site repositories and archives in which data remains reasonably static, such as reference document management systems and Records Center sites. Larger database sizes are supported for these scenarios because their I/O patterns and typical data structure formats have been designed for, and tested at, larger scales. For more information about large-scale document repositories, see "Estimate Performance and Capacity Requirements for Large Scale Document Repositories", available from Performance and capacity test results and recommendations (SharePoint Server 2010) (*http://technet.microsoft.com/library/c7f0ba55-d909-4665-85ba-706ef08d3ec8(Office.14).aspx*).

Content database size estimation

Content database size varies substantially with the usage of the site. Growth factors include the number of documents, number of users, use of versioning, use of Recycle Bins, size of quotas, whether the audit log is configured, and how many items are chosen for auditing.

If Office Web Apps are in use, the Office Web Apps cache can significantly affect the size of a content database. For more information about the size of the Office Web Apps cache, see Manage the Office Web Apps cache (*http://technet.microsoft.com/library/9a75a461-6c86-4b61-be98-bcaf9290f2da(Office.14).aspx*).

Usage and Health Data Collection database

The Usage and Health Data Collection service application database stores health monitoring and usage data temporarily, and can be used for reporting and diagnostics.

Note:

The Usage and Health Data Collection database is the only SharePoint Foundation 2010 database that can be directly queried or have its schema modified.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	WSS_UsageApplication
Location requirements	The Usage and Health Data Collection database is very active, and should be put on a separate disk or spindle, if possible.
General size information, and growth factors	Extra large. Database size depends on the retention factor, number of items enabled for logging and external monitoring, how many Web applications are running in the environment, how many users are currently working, and which features are enabled.

Read/write characteristics	The Usage and Health Data Collection database is very write-heavy.
Recommended scaling method	Must scale up; that is, the database must grow larger, because only one logging database is supported per farm.
Associated Health rules	None
Supported backup mechanisms	SharePoint Foundation 2010 backup and recovery, SQL Server, and DPM 2010.
Default recovery model	Simple
Supports mirroring within a farm for availability	Yes. However, although you can mirror the Usage and Health Data Collection database, we do not recommend that you do. It is easily re-created in the event of a failure.
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	Yes. However, although you can asynchronously mirror or log-ship the Usage and Health Data Collection database, we do not recommend that you do. It is easily re-created in the event of a failure.

Business Data Connectivity database

The Business Data Connectivity service application database stores external content types and related objects.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	Bdc_Service_DB_
Location requirements	None
General size information, and growth factors	Small. Size is determined by the number of connections.
Read/write characteristics	The Business Data Connectivity database is very read-heavy.
Recommended scaling method	Must scale up; that is, the database must grow larger, because only one Business Data Connectivity database is supported per farm. (Significant growth is unlikely.)
Associated Health rules	None
Supported backup mechanisms	SharePoint Foundation 2010 backup and recovery, SQL Server, and DPM 2010.

Default recovery model	Full
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

Application Registry database

The Application Registry service application database stores backward-compatible information that is used to connect to information that is used by the Microsoft Office SharePoint Server 2007 Business Data Catalog API.

Note:

When you have finished migrating an application from the Office SharePoint Server 2007 Business Data Catalog, the Application Registry service application can be disabled and the database can be deleted.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	Application_Registry_server_DB_
Location requirements	None
General size information, and growth factors	Small. Size is determined by the number of connections.
Read/write characteristics	Read-heavy.
Recommended scaling method	Must scale up; that is, the database must grow larger, because only one Application Registry service database is supported per farm. (Significant growth is unlikely.)
Associated Health rules	None
Supported backup mechanisms	SharePoint Foundation 2010 backup and recovery, SQL Server, and DPM 2010.
Default recovery model	Full
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

Subscription Settings database

The Microsoft SharePoint Foundation Subscription Settings service application database stores features and settings for hosted customers. The Subscription Settings service application and database are not created by the SharePoint Products Configuration Wizard — they must be created by using Windows PowerShell cmdlets.

For more information, see New-SPSubscriptionSettingsServiceApplication (*http://technet.microsoft.com/library/a0056290-df8b-4167-9a11-59cbb619e194(Office.14).aspx*).

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	SubscriptionSettings_
Location requirements	None
General size information, and growth factors	Small. Size is determined by the number of tenants, farms, and features supported.
Read/write characteristics	The subscription database is read-heavy.
Recommended scaling method	Scale up the database that supports the service application instance. You can scale out by creating additional instances of the service application, however, the decision to create a separate service application is likely to be based on business, rather than scale, requirements.
Associated Health rules	None
Supported backup mechanisms	SharePoint Foundation 2010 backup and recovery, SQL Server, and DPM 2010.
Recommended recovery model	Full
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

SQL Server system databases

SharePoint Foundation 2010 is built on SQL Server, and as a result, makes use of the SQL Server system databases. SQL Server does not support users' directly updating the information in system objects such as system tables, system stored procedures, and catalog views. Instead, SQL Server provides a complete set of administrative tools that let users fully administer their system and manage all users and objects in a database.

For more information about the SQL Server system databases, see System Databases (*http://go.microsoft.com/fwlink/?LinkId=186699*).

master

The master database records all the system-level information for an instance of SQL Server.

Default database name	master
Location requirements	None
General size information, and growth factors	Small
Read/write characteristics	Varies
Recommended scaling method	Scale up. (Significant growth is unlikely.)
Associated Health rules	None
Supported backup mechanisms	SQL Server backup and recovery
Default recovery model	Simple
Supports mirroring within a farm for availability	No
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

model

The **model** database is used as the template for all databases created on the instance of SQL Server. Modifications made to the model database — such as database size, collation, recovery model, and other database options — are applied to any databases created afterward.

Default database name	model
Location requirements	None
General size information, and growth factors	Small
Read/write characteristics	Varies
Recommended scaling method	Scale up. (Significant growth is unlikely.)
Associated Health rules	None
Supported backup mechanisms	SQL Server backup and recovery

Default recovery model	Full
Supports mirroring within a farm for availability	No
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

msdb

The msdb database is used by SQL Server Agent for scheduling alerts and jobs.

Default database name	msdb
Location requirements	None
General size information, and growth factors	Small
Read/write characteristics	Varies
Recommended scaling method	Scale up. (Significant growth is unlikely.)
Associated Health rules	None
Supported backup mechanisms	SQL Server backup and recovery
Default recovery model	Simple
Supports mirroring within a farm for availability	No
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

tempdb

The **tempdb** database is a workspace for holding temporary objects or intermediate result sets. It also fills any other temporary storage needs. The **tempdb** database is re-created every time SQL Server is started.

Default database name	tempdb
Location requirements	Locate on a fast disk, on a separate spindle from other databases. Create as many files as needed to maximize disk bandwidth. Using multiple files reduces tempdb storage contention and yields significantly better scalability. However, do not create too many files because this can reduce performance

	and increase management overhead. As a general guideline, create one data file for each CPU on the server and then adjust the number of files up or down as necessary. Be aware that a dual-core CPU is considered to be two CPUs.
General size information, and growth factors	Small to extra-large. The size of the tempDB database goes both up and down quickly. Size depends on how many users are using the system, in addition to the specific processes that are running; for example, online rebuilds of large indexes, or large sorts cause the database to grow quickly.
Read/write characteristics	Varies
Recommended scaling method	Scale up
Associated Health rules	None
Supported backup mechanisms	SQL Server backup and recovery
Default recovery model	Simple
Supports mirroring within a farm for availability	No
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

User experience on read-only sites (SharePoint Foundation 2010)

Published: May 12, 2010

This article describes how the user interface is modified on a Microsoft SharePoint Foundation 2010 site for which the related content database is set to be read-only (a read-only site).

The user experience of a read-only site is characterized by the following:

- Common tasks that do not require writing to the content database are fully available.
- Most of the common tasks that require writing to the content database are not available, either because they have been disabled in the user interface or because the user is no longer allowed to apply changes.
- Some common tasks that require writing to the content database appear to be available, but return errors.

This article describes the common tasks that are not available and the common tasks that return errors on a read-only site.

Common tasks that are not available on a read-only site, and do not return errors

The user interface is modified so that common tasks that require writing to the database are not available and appear dimmed. The elements of the user interface that are not available are listed in the following table.

Object	Interface elements disabled on a read-only site
Site Actions menu	Edit page New Page New Document Library New Site More Create Options Edit Site in SharePoint Designer Site Workflows
Library tools tab: Documents	New Document Upload Document New Folder Edit Document

Object	Interface elements disabled on a read-only site
	Check Out Check In Discard Check Out Edit Properties Version History Delete Document Mobile Link Manage Copies Go To Source Workflows Publish Unpublish Approve/Reject Cancel Approval
Library tools tab: Library	New Row Refresh Data Create View Modify View Create Column Edit Library Form Web Parts Library Settings Workflows
List tools tab: Items	New Item New Folder Edit Item Delete Item Attach File Workflows Approve/Reject
List tools tab: List	New Row Refresh Data Refresh Data Create View Create Column

Object	Interface elements disabled on a read-only site
	Mobile Link Connect to Outlook Create Visio diagram Open Schedule Edit list Form Web Parts List Settings Customize Form Workflows
Calendar Tools Tab: Events	New Event Edit Event Delete Event Workflows Approve/Reject
Calendar Tools Tab: Calendar	Create View Modify View Alert Me
Site Settings: Users and Permissions People and Groups	New Actions: Remove Users from Group Settings
Site Settings: Users and Permissions: Site Permissions	Grant permissions Create Group User Permissions Remove User Permissions Site Collection Administrators
SiteSettings: Users and Permissions: All People	Actions: Delete Users from Site Settings: List Settings

Some options that are not available on a read-only site appear to be available, but the **OK** button is disabled on subsequent pages. These pages are listed below.

- Users and Permissions
  - Site collection administrators
  - Site permissions: Manage access request
- Look and Feel
  - Title, Description, and Icon

    - Top Link Bar: New Navigation Link
    - Quick Launch
    - New Heading
    - New Navigation Link
    - Tree View
- Galleries
    - Site columns
    - Site content types
- Site Administration: Regional settings
- Site Actions: Reset to site definition

Common tasks that appear to be available in a read-only site, but return errors

Some options that are not available in a read-only database appear to be available in the interface, however users will receive error messages if they attempt to perform these actions. The elements of the user interface that return errors are listed in the following table.

Component or area	Type of operation or action	Behavior or error message
Site Theme	On the Site Theme page, click **Apply**.	SharePoint returns the "Error: Access Denied" message.
Site Libraries and Lists	Click **Create new content**.	SharePoint returns the "An unexpected error has occurred" message.
Sites and workspaces	Click **Create**.	SharePoint returns the "Error: Access Denied" message.
Customize the Quick Launch	Click **Change Order**, reset the order of the links on the Reorder Links page, and then click **OK**.	SharePoint returns the "Error: Access Denied" message.
Site Features	Click **Activate** or **Deactivate.**	SharePoint returns the "Error: Access Denied" message.
Delete this site		SharePoint returns the "Error: Access Denied" message.

Component or area	Type of operation or action	Behavior or error message
Recycle Bin	Click any of the following buttons: • **Restore Selection** • **Delete Selection** • **Empty Recycle Bin**	SharePoint returns the "Error: Access Denied" message.
SharePoint Designer Settings	Change any settings, and then click **OK**.	SharePoint returns the "Error: Access Denied" message.
Help Settings		SharePoint returns the "Error: Access Denied" message.
Custom Commands Ribbon	Click **Customize Form**.	SharePoint returns the Microsoft InfoPath "Enter your credentials to connect to the following Web service" error.
List Tools Ribbon, List tab	Click **Customize Form**.	SharePoint returns the error "Microsoft InfoPath 2010 is required to use this feature."

Language packs (SharePoint Foundation 2010)

Updated: October 14, 2010

This article lists the language packs that are available for Microsoft SharePoint Foundation 2010. Language packs enable you to create sites and site collections in multiple languages without requiring separate installations of SharePoint Foundation 2010 in each language. For more information about language packs, see Deploy language packs (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/bd2a9863-954a-4e44-bafc-af8c9599cb47(Office.14).aspx*). The language packs can be downloaded at Language Packs for SharePoint Foundation 2010 (*http://go.microsoft.com/fwlink/?LinkID=192106&clcid=0x409*).

The following table lists the language packs that are available for SharePoint Foundation 2010:

Language	Language ID
Arabic	1025
Basque	1069
Bulgarian	1026
Catalan	1027
Chinese (Simplified)	2052
Chinese (Traditional)	1028
Croatian	1050
Czech	1029
Danish	1030
Dutch	1043
English	1033
Estonian	1061
Finnish	1035
French	1036
Galician	1110

Language	Language ID
German	1031
Greek	1032
Hebrew	1037
Hindi	1081
Hungarian	1038
Italian	1040
Japanese	1041
Kazakh	1087
Korean	1042
Latvian	1062
Lithuanian	1063
Norwegian (Bokmål)	1044
Polish	1045
Portuguese (Brazil)	1046
Portuguese (Portugal)	2070
Romanian	1048
Russian	1049
Serbian (Latin)	2074
Slovak	1051
Slovenian	1060
Spanish	3082
Swedish	1053
Thai	1054
Turkish	1055
Ukrainian	1058

Languages for word breakers and stemmers (SharePoint Foundation 2010)

Published: May 12, 2010

This article lists the languages for which Microsoft SharePoint Foundation 2010 provides word breakers and stemmers. For information about using word breakers and stemmers with multilingual sites, see Plan for multilingual sites (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/95dc3f61-13da-4447-926a-ddae0326393e(Office.14).aspx*).

The following table lists the languages for which SharePoint Foundation 2010 provides word breakers and stemmers:

Language	Language	Language
Arabic*	Hindi	Punjabi
Bengali	Hungarian*	Romanian
Bulgarian	Icelandic	Russian
Catalan	Indonesian	Serbian (Cyrillic)
Chinese (Simplified)*	Italian	Serbian (Latin)
Chinese (Traditional)*	Japanese*	Slovak
Croatian	Kannada	Slovenian
Czech	Korean	Spanish (Spain)
Danish	Latvian	Spanish (Mexico)
Dutch	Lithuanian	Swedish
English	Malay	Tamil
Finnish*	Malayalam	Telugu
French	Marathi	Thai*
German	Norwegian	Turkish*
Greek	Polish	Ukrainian
Gujarati	Portuguese (Brazil)	Urdu
Hebrew*	Portuguese (Portugal)	Vietnamese*

These languages have only word breakers. There are no stemmers available for these languages.

Scripted deployment reference (SharePoint Foundation 2010)

Published: May 12, 2010

This article describes the commands and syntax that is used in scripted deployment of a Microsoft SharePoint Foundation 2010 farm. It also contains a table of common templates used in Installing SharePoint Foundation 2010 by using Windows PowerShell (*http://technet.microsoft.com/library/8528643d-27bc-4592-8a21-0c5b1cea466d(Office.14).aspx*).

Important:

The Install-SharePoint, New-SharePointFarm, and Join-SharePointFarm commands should only be used in the context of the SPModule.zip file.

For information about using these commands to install SharePoint Foundation 2010, see Installing SharePoint Foundation 2010 by using Windows PowerShell (*http://technet.microsoft.com/library/8528643d-27bc-4592-8a21-0c5b1cea466d(Office.14).aspx*).

In this article:

Install-SharePoint

The Install-SharePoint command installs SharePoint Foundation 2010 on all servers.

There are two ways—defined by a parameter set—to run the **Install-SharePoint** command. In the first case, you specify a path for the install files, and many other values to deviate from the default. The second way is to specify the path for the install files, and then the path to a Config.xml file. During Setup, the PIDKey and other settings are parsed in the config.xml file..

The syntax for the Install-SharePoint command is listed below. Note that the result is determined by which parameter set is specified. For the first parameter set, the **SetupExePath** is required. All other parameters are optional. If no value is specified for the optional **LogPath** parameter, the default value is *%Temp%*.

Note:

In SharePoint Foundation, the PIDKey is not required.

Install-SharePoint -SetupExePath <String> -PIDKey <String> [-LoggingType < Verbose | Off | Standard | Debug>] [-LogPath <String>] [-LogTemplate <String>] [-DisplayLevel <None | Basic | Full>] [-ShowCompletionNotice <SwitchParameter>] [-UseIInstallMode <SwitchParameter>] [-AcceptEula <SwitchParameter>] [-ShowModalDialog <SwitchParameter>] [-AllowCancel <SwitchParameter>] [-ServerRole <APPLICATION | WFE | SINGLESERVER>] [-SetupType <CLEAN_INSTALL | V2V_INPLACE_UPGRADE | B2B_UPGRADE | SKU2SKU_UPGRADE>] [-InstallDirectory <String>] [-DataDirectory <String>] [-RunsWorkaround <SwitchParameter>] [-PhysicalSKU <OfficeServer | SharePoint | SearchServer | SearchServerExpress | WCServer | ProjectServer | SharePointLanguagePack | ServerLanguagePack>]

For the second parameter set, there are two required parameters, **SetupExePath** and **ConfigXMLPath**.

Install-SharePoint -SetupExePath <String> -ConfigXMLPath <String> [-PIDKey <String>] [-PhysicalSKU <OfficeServer | SharePoint | SearchServer | SearchServerExpress | WCServer | ProjectServer | SharePointLanguagePack | ServerLanguagePack>]

New-SharePointFarm

The New-SharePointFarm command creates the farm on the server that will be running the Central Administration Web site.

The command performs the following actions:

1. Creates the configuration database.
2. Creates the administration content database.
3. Installs the Help collection.
4. Creates the Central Administration Web application.
5. Copies shared application data to existing Web application folders.

The syntax for the New-SharePointFarm command is listed below and there are two required parameters, **DatabaseAccessAccount** and **DatabaseServer**. All other parameters are optional.

New-SharePointFarm -DatabaseAccessAccount <PSCredential> -DatabaseServer <String> [-Passphrase <SecureString>] [-Port <Int>] [-AdminAuthMethod <NTLM | Kerberos>] [-FarmName <String>]

Example: **New-SharePointFarm -DatabaseAccessAccount (Get-Credential DOMAIN\username) -DatabaseServer "SQL01" -FarmName "TestFarm"**

Join-SharePointFarm

You run the Join-SharePointFarm command on servers to connect them to the farm.

The syntax for the Join-SharePointFarm command is listed below and there are two required parameters, **DatabaseServer** and **ConfigurationDatabaseName**. All other parameters are optional.

Join-SharePointFarm -DatabaseServer <String> -ConfigurationDatabaseName <String> [-Passphrase <SecureString>]

Note:

To stop the user from being prompted for the password, you can use the **Passphrase** parameter. The value for the **Passphrase** parameter is the password of the user.

Common site collection templates

The following table describes common templates used in Installing SharePoint Foundation 2010 by using Windows PowerShell (*http://technet.microsoft.com/library/8528643d-27bc-4592-8a21-0c5b1cea466d(Office.14).aspx*).

Parameter value	Description
GLOBAL#0	Global template
STS#0	Team Site
STS#1	Blank Site
STS#2	Document Workspace
MPS#0	Basic Meeting Workspace
MPS#1	Blank Meeting Workspace
MPS#2	Decision Meeting Workspace
MPS#3	Social Meeting Workspace
MPS#4	Multipage Meeting Workspace
CENTRALADMIN#0	Central Admin Site
WIKI#0	Wiki Site
BLOG#0	Blog
SGS#0	Group Work Site
TENANTADMIN#0	Tenant Admin Site

ACCSRV#0	Access Services Site
ACCSRV#1	Assets Web Database
ACCSRV#3	Charitable Contributions Web Database
ACCSRV#4	Contacts Web Database
ACCSRV#6	Issues Web Database
ACCSRV#5	Projects Web Database
BDR#0	Document Center
OFFILE#0	(obsolete) Records Center
OFFILE#1	Records Center
OSRV#0	Shared Services Administration Site
PPSMASite#0	PerformancePoint
BICenterSite#0	Business Intelligence Center
PWA#0	Project Web App Site
PWS#0	Microsoft Project Site
SPS#0	SharePoint Portal Server Site
SPSPERS#0	SharePoint Portal Server Personal Space
SPSMSITE#0	Personalization Site
SPSTOC#0	Contents area Template
SPSTOPIC#0	Topic area template
SPSNEWS#0	News Site
CMSPUBLISHING#0	Publishing Site
BLANKINTERNET#0	Publishing Site
BLANKINTERNET#1	Press Releases Site
BLANKINTERNET#2	Publishing Site with Workflow
SPSNHOME#0	News Site
SPSSITES#0	Site Directory
SPSCOMMU#0	Community area template
SPSREPORTCENTER#0	Report Center
SPSPORTAL#0	Collaboration Portal

SRCHCEN#0	Enterprise Search Center
PROFILES#0	Profiles
BLANKINTERNETCONT	Publishing Portal
SPSMSITEHOST#0	My Site Host
ENTERWIKI#0	Enterprise Wiki
SRCHCENTERLITE#0	Basic Search Center
SRCHCENTERLITE#1	Basic Search Center
SRCHCENTERFAST#0	FAST Search Center
visprus#0	Visio Process Repository

Timer job reference (SharePoint Foundation 2010)

Published: July 8, 2010

This article describes the default timer jobs for SharePoint Foundation 2010. A timer job runs in a specific Windows service for SharePoint Foundation. Timer jobs also perform infrastructure tasks for the Timer service, such as clearing the timer job history and recycling the Timer service; and tasks for Web applications, such as sending e-mail alerts. A timer job contains a definition of the service to run and specifies how frequently the service is started. The SharePoint 2010 Timer service (SPTimerv4) runs timer jobs. Many features in SharePoint Foundation rely on timer jobs to run services according to a schedule.

In this article:

Manage timer jobs

You can check the status of a timer job and edit the timer job definition.

For the general administration of all jobs, the SharePoint Central Administration Web site has a Timer Job Status page and a Job Definitions page. You can find these pages in Central Administration, on the Monitoring page, in the **Timer Jobs** section.

From the **View** menu, you can filter the timer jobs at the following levels:

- **All** Displays all timer jobs for the farm.
- **Service** Displays all the timer jobs for a particular service. If you select this command, use the **Service** menu to select the service by which you want to filter the listed jobs.
- **Web Application** Displays all the timer jobs for a Web application. If you select this option, use the **Web Application** menu to select the Web application by which you want to filter the listed jobs.
- **Server** Displays all the timer jobs for the specified server. If you select this command, use the **Server** menu to select the server by which you want to filter the listed jobs.
- **Job Definition** Displays all the timer jobs for the specified job definition. On the Timer Job Status page, use the **Job Definition** menu to select the job definition by which you want to filter the listed jobs.
- **Failed Jobs** Displays all the timer jobs on the farm that have failed to finish.

The SharePoint 2010 Timer service (SPTimerv4) is based on the Gregorian calendar for scheduling. For every job that you schedule, you specify when the timer job will run, specified in a 24-hour time format. You must specify the time in local time instead of as an offset from Coordinated Universal Time (UTC). The time is stored in that format. Daily, weekly, and monthly schedules also include a window of execution. The timer service will select a random time within this interval to start executing the job on each applicable server. This feature is appropriate for high-load jobs that run on multiple servers on the farm. Running this kind of job on all the servers at the same time might place an unreasonable load on the farm. Timer job schedules can be specified by using Windows PowerShell. For more information, see Timer jobs cmdlets (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/cc4edde1-9406-4571-a96b-e85151e4b2b1(Office.14).aspx*).

Default timer jobs

The following table lists the default timer jobs for SharePoint Foundation 2010.

Timer job title	Description	Schedule type
Application Addresses Refresh Job	Synchronizes connection information for remote service applications.	15 minutes
Audit Log Trimming	Trims audit trail entries from site collections.	Monthly
CEIP Data Collection	Gathers farm data for the Customer Experience Improvement Program.	Daily
Cell Storage Data Cleanup Timer Job	Deletes temporary cell storage data and frees SQL Server disk space.	Weekly
Cell Storage User Data Deletion Job	Deletes user data that is stored as cell storage. This job should only be run only if the SQL Server database server is running out of disk space. **Important:** This job can cause user data loss and does not run automatically by default.	Monthly

Timer job title	Description	Schedule type
Change Log	Documents changes to sites and pages in the Web application since the last time that the timer job was run.	Daily
Config Refresh	Checks the configuration database for configuration changes.	15 seconds
Content Organizer Processing	Processes documents in the drop-off library that match organizing rules.	Daily
Dead Site Delete	When auto site cleanup is enabled, sites that have not been used in a certain period of time are deleted.	Daily
Delete Job History	Deletes old entries from the timer job history.	Weekly
Diagnostic Data Provider: Event Log	Collects Windows Event Log entries and stores the data in the logging database.	10 minutes
Diagnostic Data Provider: Performance Counters – Database Servers	Collects Performance Monitor Counters data on database servers. **Important:** The timer service account must have sufficient permission to collect counters on the database server. The account should be a member of the Performance Monitor Users (PMU) group.	5 minutes
Diagnostic Data Provider: Performance Counters – Web Front Ends	Collects Performance Monitor Counters data on front-end Web servers.	5 minutes
Diagnostic Data Provider: SQL Blocking Queries	Collects data associated with blocked SQL queries.	15 seconds
Diagnostic Data Provider:	Collects SQL Dynamic	30 minutes

Timer job title	Description	Schedule type
SQL DMV	Management Views (DMV) data.	
Diagnostic Data Provider: Trace Log	Collects Trace Log entries and stores the usage data in the logging database.	10 minutes
Disk Quota Warning	Looks for sites that have exceeded the storage quota.	Daily
Gradual Site Delete	Deletes all the data from the host content database for all deleted site collections.	Daily
Health Analysis Job (Daily, Central Administration, All Servers)	Runs SharePoint Health Analyzer jobs on all servers in the farm that run the Central Administration Web application and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Daily, Central Administration, Any Server)	Runs SharePoint Health Analyzer jobs on all servers in the farm that run the Central Administration Web application and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Daily, Microsoft SharePoint Foundation Timer, All Servers)	Runs SharePoint Health Analyzer jobs on all servers in the farm that run the SharePoint Timer Service and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Daily, Microsoft SharePoint Foundation Timer, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs the SharePoint Timer Service and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Daily, Microsoft SharePoint Foundation Web Application, All Servers)	Runs SharePoint Health Analyzer jobs on all servers in the farm that run SharePoint Web applications and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Daily, Microsoft SharePoint	Runs SharePoint Health Analyzer jobs on the first server	Daily

Timer job title	Description	Schedule type
Foundation Web Application, Any Server)	found in the farm that runs SharePoint Web applications and the Usage and Health Data Collection Service application.	
Health Analysis Job (Hourly, Claims Based Authentication, All Servers)	Runs SharePoint Health Analyzer jobs on all servers in the farm that run the Security Token Service (STS) and the Usage and Health Data Collection Service application.	Hourly
Health Analysis Job (Hourly, Microsoft SharePoint Foundation Timer, All Servers)	Runs SharePoint Health Analyzer jobs on all servers in the farm that run the SharePoint Timer Service and the Usage and Health Data Collection Service application.	Hourly
Health Analysis Job (Hourly, Microsoft SharePoint Foundation Timer, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs the SharePoint Timer Service and the Usage and Health Data Collection Service application.	Hourly
Health Analysis Job (Hourly, User Profile Service, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs Profile Services and the Usage and Health Data Collection Service application.	Hourly
Health Analysis Job (Monthly, Microsoft SharePoint Foundation Timer, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs the SharePoint Timer Service and the Usage and Health Data Collection Service application.	Monthly
Health Analysis Job (Weekly, Central Administration, All Servers)	Runs SharePoint Health Analyzer jobs on all servers in the farm that run the Central Administration Web site and the Usage and Health Data Collection Service application.	Weekly
Health Analysis Job (Weekly, Microsoft	Runs SharePoint Health Analyzer jobs on all servers in	Weekly

Timer job title	Description	Schedule type
SharePoint Foundation Timer, All Servers)	the farm that run the SharePoint Timer Service and the Usage and Health Data Collection Service application.	
Health Analysis Job (Weekly, Microsoft SharePoint Foundation Timer, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs the SharePoint Timer Service and the Usage and Health Data Collection Service application.	Weekly
Health Analysis Job (Weekly, Microsoft SharePoint Foundation Web Application, All Servers)	Runs SharePoint Health Analyzer jobs on all servers in the farm that run SharePoint Web applications and the Usage and Health Data Collection Service application.	Weekly
Health Analysis Job (Weekly, User Profile Service, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs Profile Services and the Usage and Health Data Collection Service application.	Weekly
Immediate Alerts	Sends out immediate and scheduled alerts.	5 Minutes
Microsoft SharePoint Foundation Site Inventory Usage Collection	Collects site inventory information for each site collection in the farm.	Daily
Microsoft SharePoint Foundation Usage Data Import	Imports usage log files into the logging database.	30 minutes
Microsoft SharePoint Foundation Usage Data Processing	Checks for expired usage data at the farm level and deletes the data. Expired usage data consists of records in the central usage data collection database that are older than 30 days. If the Web Analytics Service application is also installed, this timer job moves the data to a Web Analytics Reporting database. You can run this timer job manually to force a check on	Daily

Timer job title	Description	Schedule type
	expired data, or to force a usage data import to a Web Analytics application database.	
Password Management	Sends e-mail and logs events for expiring passwords and password changes. This timer job helps ensure that managed passwords are changed before they expire.	Daily
Product Version Job	Checks the installation status of the computer and adds that data to the database.	Daily
Recycle Bin	Looks for content in the Recycle Bins and moves it to the next stage or deletes it.	Daily
Solution Daily Resource Usage Update	Marks the daily boundary for sandboxed solution resource quota monitoring.	Daily
Solution Resource Usage Log Processing	Aggregates resource usage data from sandboxed solution execution.	5 minutes
Solution Resource Usage Update	Records resource usage data from sandboxed solution execution, and sends e-mail to owners of site collections that are exceeding their allocated resource quota.	15 minutes
Timer Service Lock Management	Manages the content database locks that are used by the Timer Service to determine which server will run timer jobs for a content database.	1 minute
Timer Service Recycle	Recycles the Timer Service to free resources.	Daily
Upgrade Work Item Job	Processes the logs and aggregates usage data for each site.	Daily
Workflow	Processes workflow events that are in the scheduled items table, such as delays.	5 Minutes

Timer job title	Description	Schedule type
Workflow Auto Cleanup	Deletes tasks and instances in the workflow instance table for workflows that have been marked completed more than *n* days in the past, where *n* is specified in the workflow association. Crawls through tasks and the workflow instance table.	Daily
Workflow Failover	Processes events for workflows that have failed and are marked to be retried.	15 Minutes

SharePoint 2010 Administration Toolkit (SharePoint Foundation 2010)

Published: July 15, 2010

This article provides information for farm administrators about the July 2010 release of the SharePoint Administration Toolkit version 1.0, which includes the following features:

- The Load Testing Kit, which generates a Visual Studio Team System 2008 (VSTS) load test based on Windows SharePoint Services 3.0 IIS logs. The VSTS load test can be used to generate synthetic load against Microsoft SharePoint Foundation 2010 as part of a capacity planning exercise or a pre-upgrade stress test.
- The Security Configuration Wizard (SCW) manifest, which add roles for SharePoint 2010 Products to Windows Server 2008 with Service Pack 2 or to Windows Server 2008 R2.
- The User Profile Replication Engine, which provides a shared services administrator the ability to replicate user profiles and social data between shared services providers (SSP) in Office SharePoint Server 2007 and User Profile service applications in SharePoint Server 2010.

  Note:

  This tool is not supported for SharePoint Foundation 2010.

- The Content Management Interoperability Services (CMIS) connector for Microsoft SharePoint Server 2010, which enables SharePoint users to interact with content stored in any repository that has implemented the CMIS standard, as well as making SharePoint 2010 content available to any application that has implemented the CMIS standard.

  Note:

  This is not supported for SharePoint Foundation 2010.

When you plan to install the entire toolkit, the SharePoint Administration Toolkit installer supports the use of a quiet installation using the **/quiet** switch. However, to script partial installations, the following command must be used to extract the Spat.msi from the SharePoint2010AdministrationToolkit.exe file:

SharePoint2010AdministrationToolkit.exe /extract:<path>

where *path* is the location of where the extracted files will reside.

The installation package is customizable and selectable, meaning that a user can control which tools are installed or uninstalled and can specify a custom installation folder for any tool.

The toolkit can be downloaded from the Microsoft SharePoint 2010 Administration Toolkit page (*http://go.microsoft.com/fwlink/?LinkId=196866*).

In this section:

- Installing the SharePoint 2010 Administration Toolkit (SharePoint Foundation 2010)
- Uninstalling the SharePoint 2010 Administration Toolkit (SharePoint Foundation 2010)
- Load Testing Kit (SharePoint Foundation 2010)
- Security Configuration Wizard manifest for SharePoint Foundation 2010

Installing the SharePoint 2010 Administration Toolkit (SharePoint Foundation 2010)

Published: July 15, 2010

This article describes how to install the SharePoint 2010 Administration Toolkit.

The SharePoint Administration Toolkit requires Microsoft SharePoint Foundation 2010 to be installed. Membership in the following groups is required to install each tool:

- Load Testing Kit, Security Configuration Wizard (SCW) manifest, Content Management Interoperability Services (CMIS) connector: Farm administrator and local administrator
- User Profile Replication Engine: Local administrator only

  Note:

  The User Profile Replication Engine tool is only available by using Windows PowerShell cmdlets. Verify that you meet the following minimum requirements: See **Add-SPShellAdmin**. Also, on a Windows Server 2008-based computer, if User Access Control (UAC) is enabled, you must elevate the permission of this tool to Run as Administrator. For additional information about User Access Control, see User Account Control Step-by-Step Guide (*http://technet.microsoft.com/en-us/library/cc709691.aspx*).

  The User Profile Replication Engine and the Content Management Interoperability Services connector are not supported for Microsoft SharePoint Foundation 2010.

To install the SharePoint 2010 Administration Toolkit

1. From the Microsoft SharePoint 2010 Administration Toolkit page (*http://go.microsoft.com/fwlink/?LinkId=196866*), download the **SharePoint2010AdministrationToolkit.exe** file by clicking the **Download** button, and then save the file to your hard disk.
2. Double-click the **SharePoint2010AdministrationToolkit.exe** program file on your hard disk to start the Setup program.
3. After the License Terms for Microsoft Software is accepted, click **Next**.
4. Select which tool or tools are to be installed by choosing the appropriate icon and select the top-level feature (“This feature will be installed on local hard drive”).
5. Click **Browse** to change the location of this folder. After a location is selected, click **OK**, and then click **Next**.

The default folder location is %ProgramFiles%\Microsoft\SharePoint 2010 Administration Toolkit.

6. To complete installation, click **Finish**.

Concepts

Uninstalling the SharePoint 2010 Administration Toolkit (SharePoint Foundation 2010)

Uninstalling the SharePoint 2010 Administration Toolkit (SharePoint Foundation 2010)

Published: July 15, 2010

This article describes how to uninstall the entire SharePoint 2010 Administration Toolkit or how to uninstall a specific tool.

To uninstall the SharePoint 2010 Administration Toolkit

1. From **Programs and Features**, select the Microsoft SharePoint 2010 Administration Toolkit and click **Uninstall**.

   Note:

   The same dialog box is displayed if you run the **SharePoint2010AdministrationToolkit.exe** file instead of using **Programs and Features**.

2. Click **Finish**.

To uninstall a specific tool from the SharePoint 2010 Administration Toolkit

1. From **Programs and Features**, select the Microsoft SharePoint 2010 Administration Toolkit and click **Change**.

   Note:

   The same dialog box is displayed if you run the **SharePoint2010AdministrationToolkit.exe** file instead of using **Programs and Features**.

2. Select the tool you want to remove.
3. Click **Next**, and then click **Finish**.

Security Configuration Wizard manifest for SharePoint Foundation 2010

Published: July 15, 2010

This article provides information about how to register the Security Configuration Wizard (SCW) manifest that is included in the Microsoft SharePoint 2010 Administration Toolkit. The SCW manifest adds roles for Microsoft SharePoint Foundation 2010 to Windows Server 2008 Service Pack 2 or to Windows Server 2008 R2.

Note:

These roles are specific roles that you create in SCW after you have installed the SharePoint Foundation SCW manifest, and not the server roles to configure Windows features in Server Manager.

SCW is an attack surface reduction tool introduced with Windows Server 2003 Service Pack 1. SCW uses a roles-based metaphor to solicit the functionality required for a server and disables the functionality that is not required. By automating this security best practice, SCW helps to create Windows environments that are less susceptible, on the whole, to security vulnerabilities that have been exploited.

For more information about SCW in Windows Server 2008, see Security Configuration Wizard (*http://go.microsoft.com/fwlink/?LinkId=185511*).

The SCW manifest for Microsoft SharePoint Foundation 2010 is included in the SharePoint 2010 Administration Toolkit. Different versions of the manifest are included for Windows Server 2008 Service Pack 2 and Windows Server 2008 R2.

Before you perform these procedures, confirm that:

- You have installed the SharePoint 2010 Administrator Toolkit.
- You are running Windows Server 2008 with Service Pack 2 or Windows Server 2008 R2.
- You have administrator permission for the Command Prompt window.

Register the SCW manifest

Perform the following procedure to register the SCW manifest.

To register the Microsoft SharePoint Foundation 2010 SCW manifest

1. Open a Command Prompt window.

   Note:

   If you have User Account Control (UAC) turned on in Windows, you might be prompted to run as administrator.

2. At the command prompt, type **cd C:\Program Files\Microsoft\SharePoint 2010 Administration Toolkit\SCWManifests**, or type the location where you installed the SharePoint 2010 Administration Toolkit.
3. Register the Microsoft SharePoint Foundation 2010 SCW manifest:
   - If you are using Windows Server 2008 Service Pack 2, type **scwcmd register /kbname:SPF2010 /kbfile:SPF2010W2K8.xml** and press ENTER.
   - If you are using Windows Server 2008 R2, type **scwcmd register /kbname:SPF2010 /kbfile:SPF2010W2K8R2.xml** and press ENTER.

You can now run the SCW to create a security policy that incorporate the roles for SharePoint Foundation 2010.

Concepts

SharePoint 2010 Administration Toolkit (SharePoint Foundation 2010)

Other Resources

Security Configuration Wizard Documentation
(*http://go.microsoft.com/fwlink/?LinkId=162647*)

Load Testing Kit (SharePoint Foundation 2010)

Published: July 15, 2010

This article provides a basic overview of and how-to steps for the Load Testing Kit (LTK) of the Microsoft SharePoint 2010 Administration Toolkit.

Overview

The Load Testing Kit (LTK) lets an administrator simulate a synthetic load test against a Microsoft SharePoint Foundation 2010 farm. The goal of the tool is to assist an administrator to certify that an existing Windows SharePoint Services 3.0 topology running on specific hardware can sustain an upgrade to a Microsoft SharePoint Foundation 2010 farm, with the same load.

The Load Testing Kit is a command-line tool that will use information from a Windows SharePoint Services 3.0 production farm as a baseline. There are three steps to perform a load test:

1. Collect logs.
2. Prepare data for analysis.
3. Use the project file to generate a synthetic load.

To install the Load Testing Kit, you must be a local administrator on the any x64-based computer. The files for the Load Testing Kit are installed in the following folder: %ProgramFiles%\Microsoft\SharePoint 2010 Administration Toolkit\Load Testing Kit. The Load Testing Kit includes the following files: Prerequisitecollector.exe, Prerequisitecollector.exe.config, Ltk.exe, and Microsoft.Office.Server.AdministrationToolkit.LoadTestingKitIntl.dll. These files must be copied from the installation folder to any server on the Windows SharePoint Services 3.0 farm.

To use the tool, you need to be a member of the Farm Administrators SharePoint group on both the Windows SharePoint Services 3.0 (original production) and SharePoint Foundation 2010 (upgraded) farms. Also, the LTK.exe file must be run on a computer where SharePoint 2010 Products is installed.

Collect logs

The first step is to gather all the Internet Information Services (IIS) logs on the Windows SharePoint Services 3.0 computer and to determine the Web application-to-ID mapping. This is performed by running the Prerequisitecollector.exe file.

The administrator needs to choose a server in the farm to act as a baseline, and then install the Prerequisitecollector.exe file onto that server.

Note:

The Prerequisitecollector.exe file must be copied to the physical computer in the Windows SharePoint Services 3.0 farm; otherwise, an error message is displayed.

The Prerequisitecollector.exe file contains one parameter, **TargetFolder**. The **TargetFolder** parameter specifies the location where the IIS logs of Windows SharePoint Services 3.0 will be stored.

The Prerequisitecollector tool will copy all the IIS logs available in the default source locations. The size of the IIS log files can be very large, so we recommend to check for log file sizes and plan accordingly. If the sizes of the IIS logs are too large, the size can be reduced by using the LogParser.exe or any comparable tool before or after they are being copied.

Typically, the time period needed to collect a complete set of IIS logs is 24 hours.

Prepare data for analysis

Once the IIS log files are captured, use the Load Testing Kit application (Ltk.exe) to prepare the data for analysis.

Note:

The Visual Studio Team System (VSTS) product and Microsoft Visual Studio 2008 Service Pack 1 must be installed before the Ltk.exe is run. Also, some knowledge of how to use VSTS is required. To install the Visual Studio Team System (VSTS), see Visual Studio Team System 2008 Team Suite (*http://go.microsoft.com/fwlink/?LinkID=101641*).

To install Service Pack1, see Microsoft Visual Studio 2008 Service Pack 1 (*http://go.microsoft.com/fwlink/?LinkID=116488*).

The Ltk.exe file generates a VSTS-ready project file, which includes default Web Tests (*.WebTest) and comma-separated value (*.csv) parameter files.

To analyze log files, type the following syntax:

ltk.exe -source LTKSource -output VSSolution -userlist users.csv

Ltk.exe syntax

ltk.exe -source <source directory>

-output <output directory>

-userlist <userlist file>

[-userrolefixup]

[-debugmatchrules <rule1;rule2;rule3>]

Parameters

Parameter name	Value	Required?	Description
source	A valid directory, for example, IISLogs	Yes	Specifies the folder containing the IIS log files that were collected from the Windows SharePoint Services 3.0-based computer using the Prerequisitecollector.exe file.
output	A valid directory, for example, VSSolution	Yes	Specifies the folder for the Load Testing Kit output file, which is a project file that contains all Visual Studio files and .csv files.
userlist	A valid location where the .csv file is stored, for example, C:\users.csv	Yes	Specifies a .csv file that has at least three columns: Username, Password, and Permission. The .csv file contains all the users that you created in the test domain and the permissions that they are supposed to represent. There should be at least one user for each permission. Valid permission values are FullRead and FullControlWithoutAdmin.
userrolefixup	<none>	No	Grants permissions specified in the **userlist** parameter by adding the users to the target Web application's permission policy.
debugmatchrules	A valid rule that is used for querying log files.	No	Generates a verbose log that maps which IIS logs entries matched each rule. These match rules are contained in the MatchRules section of the WebTestsConfiguration.xml file located in the %ProgramFiles%\Microsoft\SharePoint 2010 Administration Toolkit\Load Testing Kit directory. This parameter is only for advanced debugging purposes.

For example, to use **userlist** parameter to add a user name "testacct" with the FullControlWithoutAdmin permission, use the following values:

Username	Password	Permission
Domain\testacct	Password	FullControlWithoutAdmin

For example, to use **userlist** parameter to add a user name "testacct" with the FullRead permission, use the following values:

Username	Password	Permissioin
Domain\testacct	Password	FullRead

Use the project file to generate a synthetic load

Once the project file has been generated, the final step is to use VSTS to open and use the project file. For more information about how to use a VSTS project file, see Getting Started with Load and Web Performance Test Walkthroughs (*http://go.microsoft.com/fwlink/?LinkId=196791*).

Conformance statement A-level (SharePoint Foundation 2010)

Published: July 22, 2010

Conformance statement for Microsoft SharePoint Foundation 2010 in regards to Web Content Accessibility Guidelines 2.0 (*http://www.w3.org/TR/WCAG20/*).

Conformance statement for configuration and administration experience at A-level

Claim	Details
Date of the claim	May 12th, 2010
Guidelines title, version, and URI	Web Content Accessibility Guidelines 2.0 (*http://www.w3.org/TR/2008/REC-WCAG20-20081211/*)
Conformance level satisfied: (Level A, AA or AAA)	A
A concise description of the Web pages, such as a list of URIs for which the claim is made, including whether subdomains are included in the claim.	Default content included with SharePoint Foundation 2010 and Administration and Configuration features of SharePoint Foundation 2010. For other product features, see Conformance statement AA-level (SharePoint Foundation 2010).
A list of the Web content technologies relied upon.	HTML JavaScript CSS
Additional Web content technologies used, but not relied upon.	ARIA Silverlight RSS PNG GIF JPEG
A list of success criteria beyond the level of conformance claimed that have been met. This information should be provided	Conforms to 1.4.9 Images of Text (No Exception) - AAA. Conforms to 2.1.3 Keyboard (No Exception)

Claim	Details
in a form that users can use, preferably machine-readable metadata.	- AAA. Conforms to 2.2.3 No Timing (No Exception) - AAA. Conforms to 2.3.2 Three Flashes - AAA. Conforms to 2.4.8 Location - AAA. Conforms to 3.3.6 Error Prevention (All) - AAA.

This conformance statement pertains to SharePoint Foundation 2010.

Customization of the product voids this conformance statement from Microsoft. Customers may make independent conformance statements if they have conducted due diligence to meet all relevant requirements for their customization.

Please consult with Assistive Technology (AT) vendors for compatibility specifications of specific AT products. AT products that are compatible with all the rely-upon-technologies are expected to be functional with the product.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Revised 07/22/2010.

Microsoft regularly updates its websites and provides new information about the accessibility of products as that information becomes available.

Conformance statement AA-level (SharePoint Foundation 2010)

Published: July 22, 2010

Conformance statement for Microsoft SharePoint Foundation 2010 in regards to Web Content Accessibility Guidelines 2.0 (*http://www.w3.org/TR/WCAG20/*).

Conformance statement for core reader, author, and contributor experience at AA-level

Claim	Details
Date of the claim	May 12th, 2010
Guidelines title, version, and URI	Web Content Accessibility Guidelines 2.0 (*http://www.w3.org/TR/2008/REC-WCAG20-20081211/*)
Conformance level satisfied: (Level A, AA or AAA)	AA
A concise description of the Web pages, such as a list of URIs for which the claim is made, including whether subdomains are included in the claim.	All default content included with SharePoint Foundation 2010 and Web application features of SharePoint Foundation 2010 except where limited by Conformance statement A-level (SharePoint Foundation 2010).
A list of the Web content technologies relied upon.	HTML JavaScript CSS
Additional Web content technologies used, but not relied upon.	ARIA Silverlight RSS PNG GIF JPEG
A list of success criteria beyond the level of conformance claimed that have been met. This information should be provided	Conforms to 1.4.9 Images of Text (No Exception) - AAA. Conforms to 2.1.3 Keyboard (No Exception)

Claim	Details
in a form that users can use, preferably machine-readable metadata.	- AAA. Conforms to 2.2.3 No Timing (No Exception) - AAA. Conforms to 2.3.2 Three Flashes - AAA. Conforms to 2.4.8 Location - AAA. Conforms to 3.3.6 Error Prevention (All) - AAA.

This conformance statement pertains to SharePoint Foundation 2010.

Customization of the product voids this conformance statement from Microsoft. Customers may make independent conformance statements if they have conducted due diligence to meet all relevant requirements for their customization.

Please consult with Assistive Technology (AT) vendors for compatibility specifications of specific AT products. AT products that are compatible with all the rely-upon-technologies are expected to be functional with the product.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Revised 07/22/2010.

Microsoft regularly updates its websites and provides new information about the accessibility of products as that information becomes available.

Settings and features backed up from a farm configuration (SharePoint Foundation 2010)

Published: August 12, 2010

This article describes the settings and features that are included in a backup of a server farm configuration. For more information about how to back up a farm configuration, see Back up a farm configuration (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/6d006882-8dc4-4e28-9a47-9d2d592437dc(Office.14).aspx*).

Settings and features backed up

The following table lists the settings and features that are included in a backup of the configuration of a server farm, and the pages on the SharePoint Central Administration Web site where you can access these settings and features.

Setting or feature	Description
Managed account password settings	_Admin/PasswordSettings.aspx
Outgoing e-mail settings	_Admin/globalemailconfig.aspx **Note:** Outgoing e-mail settings are restored only when content and settings are restored to their original locations on the same farm they were backed up from. • When you use Central Administration to restore a farm, on the Restore from Backup — Step 2 of 3: Select Restore Options page, in the **Restore Options** section, select the **Type of Restore** option, and use the **Same configuration** setting. • When you use the Windows PowerShell **Restore-SPFarm** cmdlet to restore a farm, use the *RestoreMethod*

Setting or feature	Description
	parameter to specify **overwrite**. **Note:** Outgoing e-mail settings are restored only when content and settings are restored to their original server location in the same farm. If you are restoring the configuration and content to a different farm, you are prompted to specify new configuration settings.
Solutions deployed to the farm (trusted solutions)	_Admin/Solutions.aspx Solutions that are deployed to the farm.
InfoPath Forms Services	_Admin/IpfsConfig.aspx The list of user agents that are added to a farm.
Web application service	Settings that are shared by all content Web applications. • Active Directory Domain Services (AD DS) account creation mode settings • Antivirus settings _Admin/AVAdmin.aspx • Quota templates _Admin/ManageQuotaTemplate.aspx • Information Rights Management (IRM) settings _Admin/IrmAdmin.aspx • Managed paths for host-named site collections
Sandboxed solutions service	Solution restrictions and load balancing settings.
Diagnostic logging settings	_Admin/Metrics.aspx All diagnostic logging settings are backed up except the trace log location.

Other Resources

Restore a farm configuration (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/25cffd9e-d1d5-43ef-86c2-e2d966a1f1e8(Office.14).aspx*)

Change passwords used for administration accounts (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/91746936-a420-4b6c-bfd3-7f42f5e4e2ac(Office.14).aspx*)

Configure outgoing e-mail (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/ebb924d4-b9a2-4e40-bcb3-0ee582cc5a21(Office.14).aspx*)

Restore-SPFarm (*http://technet.microsoft.com/library/8e18ea80-0830-4ffa-b6b6-ad18a5a7ab3e(Office.14).aspx*)

Get-SPInfoPathUserAgent (*http://technet.microsoft.com/library/fef7e923-ac38-4054-aa7b-cd1f143d487e(Office.14).aspx*)

Create, edit, and delete quota templates (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/6d984258-158b-40d5-b4a5-cdb2cfe8e5f3(Office.14).aspx*)

Define managed paths (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/e325f0a3-02c3-4d39-b468-a51b2fe7d3a2(Office.14).aspx*)

Configure load balancing for sandboxed solutions (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/203d66a8-90e2-4001-8d56-830eb57a9824(Office.14).aspx*)

Block or unblock a sandboxed solution (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/6687e357-8531-4904-9c17-faa6908a793d(Office.14).aspx*)

Configure diagnostic logging (SharePoint Foundation 2010) (*http://technet.microsoft.com/library/a5641210-8224-4e11-9d93-4f96fa4c327c(Office.14).aspx*)

Peoplepicker-peopleeditoronlyresolvewithinsitecollection: Stsadm property (SharePoint Foundation 2010)

Published: February 3, 2011

Checks the user against the existing site collection users.

Note:

This operation was added in Microsoft SharePoint Foundation 2010.

Syntax

The syntax for the **setproperty** operation is:

stsadm -o setproperty
-propertyname peoplepicker-peopleeditoronlyresolvewithinsitecollection
-propertyvalue {Yes | No}
[-url] <*URL*>

The syntax for the **getproperty** operation is:

stsadm -o getproperty
propertyname peoplepicker-peopleeditoronlyresolvewithinsitecollection
[-url] <*URL*>

Note:

You can substitute **-pn** for **-propertyname** and **-pv** for **-propertyvalue**.

Parameters

Name	Value
propertyname	Gets or sets the name of the property.
propertyvalue	**Yes**: Resolves only against the existing site collection users. **No**: Resolves users against the existing site collection users and users from other identity providers, for example, Active Directory Domain Services.

Name	Value
url	Typically a path to the URL of the Web application, in the form http://*server_name*.

Examples

Display users within a site collection

If you want to display users only from a specific site collection, use the following syntax:

stsadm -o setproperty –url http://<server> –pn peoplepicker- peoplepicker-peopleeditoronlyresolvewithinsitecollection –pv yes

If you want to display any user from an existing site collection, use the following syntax:

stsadm -o setproperty –url http://<server_name> –pn peoplepicker-peopleeditoronlyresolvewithinsitecollection –pv no

To view the current setting for the **peopleeditoronlyresolvewithinsitecollection** property, use the following syntax:

stsadm -o getproperty -pn peoplepicker-peopleeditoronlyresolvewithinsitecollection