Technical reference for Microsoft SharePoint Server 2010

Microsoft Corporation
Published: May 2011
Author: Microsoft Office System and Servers Team (itspdocs@microsoft.com)

Abstract
This book contains technical information about the Microsoft SharePoint Server 2010 provider for Windows PowerShell and other helpful reference information about general settings, security, and tools. The audiences for this book include application specialists, line-of-business application specialists, and IT administrators who work with SharePoint Server 2010.
The content in this book is a copy of selected content in the SharePoint Server 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

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.
Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.
This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.
© 2011 Microsoft Corporation. All rights reserved.
Microsoft, Access, Active Directory, Backstage, Excel, Groove, Hotmail, InfoPath, Internet Explorer, Outlook, PerformancePoint, PowerPoint, SharePoint, Silverlight, Windows, Windows Live, Windows Mobile, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

Table of Contents

Getting help xiii

Technical reference for SharePoint Server 2010 1

System Center Operations Manager knowledge articles (SharePoint Server 2010) ... 2

Access Services in SharePoint Server 2010 knowledge articles 5

Access Services - configuration database access failed - Event 1 (SharePoint Server 2010) 6

Access Services cannot create session cache - Event 11 (SharePoint Server 2010) . 9

Access Services out of memory - Event 16 (SharePoint Server 2010) 10

Access Services failed to load calculation library - Event 17 (SharePoint Server 2010) 11

Access Services template input output error - Event 21 (SharePoint Server 2010) .. 12

Access failed to contact Access Services - Events 24 25 26 (SharePoint Server 2010) 13

Access Data Services no longer available - Event 28 (SharePoint Server 2010) 14

Access Services server is not available - Event 29 (SharePoint Server 2010) 15

Excel Services Application in SharePoint Server 2010 knowledge articles 16

Excel unauthorized attempt to access a session - Event 2011 (SharePoint Server 2010) 17

Excel Services Application internal error - Event 2026 (SharePoint Server 2010) 18

Excel Services Application save failed - Event 3348 (SharePoint Server 2010) 19

Excel Services Application unexpected workbook failure - Event 5225 (SharePoint Server 2010) 20

Excel workbook disk cache cannot be created - Event 5226 (SharePoint Server 2010) 21

Unable to establish connection with Excel Services Application - Events 5231 5233 (SharePoint Server 2010) 23

Error communicating with Excel Services Application - Events 5231 5239 5240 (SharePoint Server 2010) 24

Excel Services Application not available - Event 5234 (SharePoint Server 2010) 25

Excel Services Application configuration database access failed - Event 5244 (SharePoint Server 2010) 26

Max memory configured for Excel Services Application exceeded - Event 5255 (SharePoint Server 2010) 28

Excel Services Application memory allocation failed - Event 5256 (SharePoint Server 2010) 29

Excel Services Application not running locally - Event 5271 (SharePoint Server 2010) 30

Excel invalid file access method configured - Event 5557 (SharePoint Server 2010)31

Excel Services Application user-defined function exception - Event 6467 (SharePoint Server 2010)..... 32

Excel Services Application localized template file not found - Event 7924 (SharePoint Server 2010)..... 33

Excel Services Application template file missing - Event 7925 (SharePoint Server 2010) 34

Excel Services Application null access violation - Event 7926 (SharePoint Server 2010) 35

Excel Services Application non-null access violation - Event 7927 (SharePoint Server 2010) 36

Excel Services Application array out of bounds - Event 7928 (SharePoint Server 2010) 37

Excel workbook disk cache full (SharePoint Server 2010)..... 38

InfoPath Forms Services in SharePoint Server 2010 knowledge articles 39

InfoPath Forms Services business logic failed - Event 5337 (SharePoint Server 2010) 40

InfoPath Forms Services business logic exceeded re-entrant count - Event 5340 (SharePoint Server 2010) 41

InfoPath Forms Services business logic is out of memory - Event 5342 (SharePoint Server 2010)..... 42

InfoPath Forms Services business logic load exception - Event 5343 (SharePoint Server 2010)..... 43

InfoPath Forms Services Web files list load failed - Event 5369 (SharePoint Server 2010) 44

InfoPath Forms Services postback failure - Event 5374 (SharePoint Server 2010) .. 45

InfoPath Forms Services conflicting assembly identities found - Event 5733 (SharePoint Server 2010) 46

InfoPath Forms Services business logic cannot be serialized - Event 5734 (SharePoint Server 2010) 47

InfoPath Forms Services DoS postbacks per session - Event 5736 (SharePoint Server 2010)..... 48

InfoPath Forms Services DoS actions per postback - Event 5737 (SharePoint Server 2010) 50

InfoPath Forms Services data adapter security error submit - Event 5758 (SharePoint Server 2010) 52

InfoPath Forms Services solution cache churning - Event 5759 (SharePoint Server 2010) 53

InfoPath Forms Services data adapter security error query - Event 6932 (SharePoint Server 2010) 54

InfoPath Forms Services solution load failure - Event 7056 (SharePoint Server 2010) 55

InfoPath Forms Services not working due to invalid State Service configuration - Event 7898 (SharePoint Server 2010) 56

Managed Metadata services in SharePoint Server 2010 knowledge articles 58

Disk-based cache misconfigured - Event 5787 (SharePoint Server 2010) 59

Metadata Service is unavailable - Event 8088 (SharePoint Server 2010) 60

Disk-based cache at critical capacity (SharePoint Server 2010) 61

Disk-based cache flushing (SharePoint Server 2010) 62

Disk-based cache is compacting (SharePoint Server 2010) 63

PerformancePoint Services in SharePoint Server 2010 knowledge articles 64

PerformancePoint Services - login failed - Events 5 6 37 45 (SharePoint Server 2010) 65

PerformancePoint Services - Service unavailable - Events 33 39 (SharePoint Server 2010) 66

PerformancePoint Services - Database Connection Failed - Event 34 (SharePoint Server 2010) 68

Search services in SharePoint Server 2010 knowledge articles 71

Search gatherer disk is full - Event 23 (SharePoint Server 2010) 72

Search database out of space - Event 52 (SharePoint Server 2010) 73

Search relegate query component - Event 58 (SharePoint Server 2010) 74

Search query critical error - Event 60 (SharePoint Server 2010) 75

Search indexer initialization index failed - Event 71 (SharePoint Server 2010) 76

Search index corrupted - Events 74 93 (SharePoint Server 2010) 77

Search indexer low disk space - Event 80 (SharePoint Server 2010) 79

Search propagation communication error - Event 92 (SharePoint Server 2010) 81

Search gatherer host unavailable - Event 114 (SharePoint Server 2010) 82

Search administration component failed - Event 121 (SharePoint Server 2010) 83

Search crawl component index path error - Events 2588 2589 (SharePoint Server 2010) 84

Search Query and Site Settings Service is not running (SharePoint Server 2010) ... 85

SharePoint Server 2010 search is not running (SharePoint Server 2010) 87

Word Services in SharePoint Server 2010 knowledge articles 88

Word Services timer job failed - Events 1022 8077 (SharePoint Server 2010) 89

Word services - PDF file converter failing - Event 8004 (SharePoint Server 2010)... 90

Word services - XPS file converter failing - Event 8005 (SharePoint Server 2010)... 91

Word services must be updated - Event 8010 (SharePoint Server 2010) 92

Word services - language pack not installed - Event 8012 (SharePoint Server 2010) 93

Visio Services in SharePoint Server 2010 knowledge articles 94

Visio Services data refresh failed - Events 8037 8038 8063 8062 (SharePoint Server 2010)..... 95

Visio configuration database not found - Event 8040 (SharePoint Server 2010)..... 96

Visio Services untrusted data provider request - Event 8041 (SharePoint Server 2010) 97

Visio Services failed to generate diagram - Events 8042 8043 8060 (SharePoint Server 2010)..... 98

Visio proxy initialization failed - Event 8044 (SharePoint Server 2010) 99

Visio application proxy has invalid endpoint - Event 8049 (SharePoint Server 2010) 101

Visio Services data provider not found - Event 8050 (SharePoint Server 2010) 103

Visio Services file loading error - Events 8051 8061 (SharePoint Server 2010)..... 104

User Profile Synchronization Configuration Service cannot connect to SQL Server - Event 4 (SharePoint Server 2010) 105

ULS not enough storage for log directory - Event 2150 (SharePoint 2010 Products) 107

Event log flooding - Events 2158 2159 (SharePoint 2010 Products) 108

SQL Server database login failed - Event 3351 (SharePoint 2010 Products) 109

Backup failed due to insufficient permissions - Event 3353 (SharePoint 2010 Products) 111

Cannot connect to SQL Server - Event 3355 (SharePoint 2010 Products) 112

The application pool account cannot add user accounts to Active Directory - Event 3359 (SharePoint 2010 Products)..... 114

Active Directory organization unit unregistered - Event 3360 (SharePoint 2010 Products) 116

SQL Server database is full - Event 3758 (SharePoint 2010 Products) 117

Database could not be accessed - Event 3760 (SharePoint 2010 Products) 119

Content deployment job failed - Events 4958 5323 5325 5335 (SharePoint 2010 Products) 121

Content database is Read-Only - Event 4971 (SharePoint 2010 Products) 122

Cannot create My Sites - Event 5187 (SharePoint Server 2010) 123

User Profile changes cannot be committed - Event 5188 (SharePoint Server 2010) 124

Insufficient SQL Server database permissions - Event 5214 (SharePoint 2010 Products) 125

Unable to write to trace log - Event 5401 (SharePoint 2010 Products) 127

Could not schedule synchronization jobs - Event 5556 (SharePoint Server 2010) . 128

Unknown SQL exceptions - Event 5586 (SharePoint 2010 Products) 129

Audience compilation failed - Event 5693 (SharePoint Server 2010) 132

Synchronizing data between SharePoint Server and directory failed - Events 6000-6099 (SharePoint Server 2010) 133

SharePoint Foundation failed to create a site - Event 6141 (SharePoint 2010 Products) 134

Unable to load authentication provider - Event 6143 (SharePoint 2010 Products).. 135

User Profile Synchronization Service unexpected failure - Events 6300-6309 (SharePoint Server 2010) 137

Insufficient permissions to write to the configuration data cache - Event 6395 (SharePoint 2010 Products) 138

Alternate access mapping update failed - Event 6397 (SharePoint 2010 Products)139

Service Instance timer execution failed - Event 6398 (SharePoint 2010 Products). 140

ULS not enough free disk space - Event 6457 (SharePoint 2010 Products) 143

Access denied for writing to registry - Event 6588 (SharePoint 2010 Products) 144

Access denied for writing to disk - Event 6589 (SharePoint 2010 Products) 146

Application pool account must be registered as Kerberos - Event 6590 (SharePoint 2010 Products) 148

SMTP service not running - Event 6599 (SharePoint 2010 Products) 150

Event handler failed to load - Event 6644 (SharePoint 2010 Products) 151

Product Help Library Permission - Event 6769 (SharePoint 2010 Products) 152

Cannot resolve name of the outbound SMTP server - Event 6856 (SharePoint 2010 Products) 153

Cannot connect to SMTP host - Event 6857 (SharePoint 2010 Products) 155

Error occurred while communicating with SMTP server - Event 6858 (SharePoint 2010 Products) 156

SharePoint lists cannot receive e-mail - Event 6872 (SharePoint 2010 Products) .. 158

E-mail service cannot deliver e-mail - Event 6873 (SharePoint 2010 Products) 159

Event receiver failed - Event 6875 (SharePoint 2010 Products) 160

Service instance provisioning failed - Event 7034 (SharePoint Server 2010) 161

Backup timer job could not be created - Event 7035 (SharePoint 2010 Products) .. 162

Central Administration update failed - Event 7037 (SharePoint 2010 Products) 163

Secure Store reencrypt credentials failed - Event 7510 (SharePoint Server 2010) . 165

Secure Store could not retrieve master encryption key - Event 7535 (SharePoint Server 2010) 166

Secure Store SQL exception - Event 7551 (SharePoint Server 2010) 169

Secure Store proxy unexpected exception - Event 7557 (SharePoint Server 2010) 170

Throttling starts alert- Events 8032 8062 (SharePoint 2010 Products) 171

Cannot retrieve end point - Event 8070 (SharePoint 2010 Products) 173

Cannot retrieve list of service applications from remote farm - Event 8071 (SharePoint Server 2010) 174

Log folder does not exist - Event 8074 (SharePoint 2010 Products) 175

Usage timer job failed - Event 8075 (SharePoint 2010 Products) 176

Business Data Connectivity Service - BDC database adapter connection exception - Event 8080 (SharePoint 2010 Products) 178

Business Data Connectivity Service - BDC Web service proxy generations exception - Event 8082 (SharePoint 2010 Products) 179

Business Data Connectivity Service - BDC Proxy - unexpected exception - Event 8085 (SharePoint 2010 Products) 180

Business Data Connectivity Service - SQL exception - Event 8086 (SharePoint 2010 Products) 181

ULS trace log reaching maximum size - Event 8094 (SharePoint 2010 Products) .. 182

ULS usage log reaching maximum size - Event 8095 (SharePoint 2010 Products) 183

STS signing certificate missing - Event 8303 (SharePoint 2010 Products) 184

STS cannot sign credentials - Event 8304 (SharePoint 2010 Products) 185

Claims cannot establish endpoint - Event 8305 (SharePoint 2010 Products) 186

STS claims provider error - Event 8307 (SharePoint 2010 Products)..... 187

Administration service is not running (SharePoint 2010 Products) 188

Backend server not reachable (SharePoint Server 2010)..... 189

Document conversion failures high (SharePoint Server 2010) 190

Document conversion launcher unavailable (SharePoint 2010 Products)..... 191

Document conversion load balancer unavailable (SharePoint 2010 Products) 192

Knowledge article is not yet available (SharePoint 2010 Products)..... 194

Sandboxed code is running (SharePoint 2010 Products) 195

SharePoint Administration service is disabled (SharePoint 2010 Products)..... 196

SharePoint Foundation 2010 search is not running (SharePoint 2010 Products) ... 197

SharePoint Health Analyzer has detected an error or warning (SharePoint 2010 Products) 198

SharePoint Timer service could not start (SharePoint 2010 Products)..... 199

SharePoint Timer service is not running (SharePoint 2010 Products)..... 200

SQL Server remote access is disabled (SharePoint 2010 Products)..... 201

Tracing service is not running (SharePoint 2010 Products)..... 202

Unacceptable rendering response time (SharePoint Server 2010)..... 203

User Profile Configuration service not started (SharePoint Server 2010)..... 204

User Profile Synchronization service not started (SharePoint Server 2010) 205

Web application taking too long to render a page (SharePoint 2010 Products) 206

Web application unavailable (SharePoint 2010 Products) 207

Web site unavailable (SharePoint 2010 Products)..... 208

SharePoint Health Analyzer rules reference (SharePoint Server 2010) 209

Web Applications using Claims authentication require an update (SharePoint Server 2010) 213

Automatic update setting inconsistent across farm servers (SharePoint Foundation 2010) 214

Diagnostic logging is set to verbose (SharePoint Foundation 2010) 215

The server farm account should not be used for other services (SharePoint Foundation 2010) 216

One or more services have started or stopped unexpectedly (SharePoint Foundation 2010) 217

Databases used by SharePoint have fragmented indices (SharePoint Foundation 2010) 218

Content databases contain orphaned items (SharePoint Foundation 2010) 219

Outbound e-mail has not been configured (SharePoint Foundation 2010) 220

Some health analyzer rules do not have associated timer jobs (SharePoint Foundation 2010) 221

Drives are running out of free space (SharePoint Foundation 2010) 222

The paging file size should exceed the amount of physical RAM in the system (SharePoint Foundation 2010) 223

Built-in accounts are used as application pool or service identities (SharePoint Foundation 2010) 224

Web Analytics: Monitors the health of the Report Consolidator component (SharePoint Foundation 2010) 225

Web Analytics: Verifies that when the Web Analytics is installed and running, usage logging is enabled in the farm (SharePoint Foundation 2010) 226

Web Analytics: Verifies that a web application is serviced by at most one Web Analytics service application proxy (SharePoint Foundation 2010) 227

Web Analytics: Verifies that the SQL Server Service Broker is enabled for the Web Analytics staging databases (SharePoint Foundation 2010) 228

InfoPath Forms Services Maintenance Timer Job not enabled (SharePoint Server 2010) 229

Validate the My Site Host and individual My Sites are on a dedicated Web application and separate URL domain (SharePoint Server 2010) 230

Search scopes not defined for My Sites (SharePoint Server 2010) 231

Verify each User Profile service application has a My Site host configured (SharePoint Server 2010) 232

Visio Graphics Service has a maximum cache age setting that will adversely impact performance (SharePoint Server 2010) 233

The Visio Graphics Service has a Maximum Web Drawing Size setting that will adversely impact performance (SharePoint Server 2010) 234

Visio Graphics Service has a maximum recalculation duration setting that will adversely impact performance (SharePoint Server 2010) 235

The Visio Graphics Service has a minimum cache age setting that may cause a security issue (SharePoint Server 2010) 236

The Visio Graphics Service has a minimum cache age setting that will adversely impact performance (SharePoint Server 2010) 237

All State Service databases are paused for a State Service Application (SharePoint Server 2010) 238

A State Service Application has no database defined (SharePoint Server 2010) ... 239

InfoPath Forms Services forms cannot be filled out in a Web browser because no State Service connection is configured (SharePoint Server 2010) ... 240

Expired sessions are not being deleted from the ASP.NET Session State database (SharePoint Server 2010) ... 241

The State Service Delete Expired Sessions timer job is not enabled (SharePoint Server 2010) ... 242

One or more Search crawl databases have fragmented indices (SharePoint Server 2010) ... 243

One or more Search property databases have fragmented indices (SharePoint Server 2010) ... 245

InfoPath Forms Services forms cannot be filled out in a Web browser (SharePoint Server 2010) ... 247

Word Automation Service timer job is not running (SharePoint Server 2010) ... 248

Installation reference (SharePoint Server 2010) ... 249

Setup command-line reference (SharePoint Server 2010) ... 250

Psconfig command-line reference (SharePoint Server 2010) ... 254

Config.xml reference (SharePoint Server 2010) ... 261

Windows PowerShell commands (SharePoint Server 2010) ... 274

Enterprise search technical reference (SharePoint Server 2010) ... 277

Default connectors (SharePoint Server 2010) ... 278

File types and IFilters reference (SharePoint Server 2010) ... 280

Languages for word breakers and stemmers (SharePoint Server 2010) ... 283

Managing privacy (SharePoint Server 2010) ... 284

User permissions and permission levels (SharePoint Server 2010) ... 289

Database types and descriptions (SharePoint Server 2010) ... 295

Language packs (SharePoint Server 2010) ... 320

Regional settings (SharePoint Server 2010) ... 322

Managed metadata input file format (SharePoint Server 2010) ... 334

User experience on read-only sites (SharePoint Server 2010) ... 337

Scripted deployment reference (SharePoint Server 2010) ... 341

Account permissions and security settings (SharePoint Server 2010) ... 345

PerformancePoint Services glossary ... 360

Word Automation Services Troubleshooting (SharePoint Server 2010) ... 371

Timer job reference (SharePoint Server 2010) 379

SharePoint 2010 Administration Toolkit (SharePoint Server 2010) 389

Installing the SharePoint 2010 Administration Toolkit (SharePoint Server 2010) 391

Uninstalling the SharePoint 2010 Administration Toolkit (SharePoint Server 2010) 392

Security Configuration Wizard manifest for SharePoint Server 2010 393

Load Testing Kit (SharePoint Server 2010) 395

User Profile Replication Engine overview (SharePoint Server 2010) 398

Content Management Interoperability Services (CMIS) connector overview (SharePoint Server 2010) 402

SharePoint Diagnostic Studio 2010 (SPDiag 3.0) (SharePoint Server 2010) 409

Conformance statement A-level (SharePoint Server 2010) 425

Conformance statement AA-level (SharePoint Server 2010) 427

Settings and features backed up from a farm configuration (SharePoint Server 2010) 429

Peoplepicker-peopleeditoronlyresolvewithinsitecollection: Stsadm property (SharePoint Server 2010) 432

Default user profile properties (SharePoint Server 2010) 434

Default user profile property mappings (SharePoint Server 2010) 436

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.coms
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 Server 2010

Published: May 12, 2010

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

In this section:

- Windows PowerShell for SharePoint Server 2010 (Available on TechNet at *http://technet.microsoft.com/library/93ca2966-8000-498d-8539-83c59ddad4d8(Office.14).aspx*)
- System Center Operations Manager knowledge articles (SharePoint Server 2010)
- Managing privacy (SharePoint Server 2010)
- User permissions and permission levels (SharePoint Server 2010)
- Database types and descriptions (SharePoint Server 2010)
- Managed metadata input file format (SharePoint Server 2010)
- User experience on read-only sites (SharePoint Server 2010)
- Language packs (SharePoint Server 2010)
- Scripted deployment reference (SharePoint Server 2010)
- Account permissions and security settings (SharePoint Server 2010)
- SharePoint 2010 Administration Toolkit (SharePoint Server 2010)
- Peoplepicker-peopleeditoronlyresolvewithinsitecollection: Stsadm property (SharePoint Server 2010)
- Default user profile properties (SharePoint Server 2010)
- Default user profile property mappings (SharePoint Server 2010)

Other Resources

Stsadm command-line tool (Office SharePoint Server) (*http://technet.microsoft.com/en-us/library/cc261956(office.12).aspx*)

System Center Operations Manager knowledge articles (SharePoint Server 2010)

Published: May 12, 2010

The articles in this section are knowledge articles for the Microsoft SharePoint Server 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 Server 2010.

Relevant System Center Operations Manager knowledge articles for Project Server 2010 are available in the Project Server document library at System Center Operations Manager knowledge articles (Project Server 2010) (*http://technet.microsoft.com/library/d95bc95a-1ffc-41f8-8039-33a8d68810d1(Office.14).aspx*)

In this section:

- Access Services in SharePoint Server 2010 knowledge articles
- Excel Services Application in SharePoint Server 2010 knowledge articles
- InfoPath Forms Services in SharePoint Server 2010 knowledge articles
- Managed Metadata services in SharePoint Server 2010 knowledge articles
- PerformancePoint Services in SharePoint Server 2010 knowledge articles
- Search services in SharePoint Server 2010 knowledge articles
- Visio Services in SharePoint Server 2010 knowledge articles
- User Profile Synchronization Configuration Service cannot connect to SQL Server - Event 4 (SharePoint Server 2010)
- ULS not enough storage for log directory - Event 2150 (SharePoint 2010 Products)
- Event log flooding - Events 2158_2159 (SharePoint 2010 Products)
- SQL Server database login failed - Event 3351 (SharePoint 2010 Products)
- Backup failed due to insufficient permissions - Event 3353 (SharePoint 2010 Products)
- Cannot connect to SQL Server - Event 3355 (SharePoint 2010 Products)
- The application pool account cannot add user accounts to Active Directory - Event 3359 (SharePoint 2010 Products)
- Active Directory organization unit unregistered - Event 3360 (SharePoint 2010 Products)
- SQL Server database is full - Event 3758 (SharePoint 2010 Products)
- Database could not be accessed - Event 3760 (SharePoint 2010 Products)
- Content deployment job failed - Events 4958_5323_5325_5335 (SharePoint 2010 Products)
- Content database is Read-Only - Event 4971 (SharePoint 2010 Products)
- Cannot create My Sites - Event 5187 (SharePoint Server 2010)
- User Profile changes cannot be committed - Event 5188 (SharePoint Server 2010)
- Insufficient SQL Server database permissions - Event 5214 (SharePoint 2010 Products)
- Unable to write to trace log - Event 5401 (SharePoint 2010 Products)
- Could not schedule synchronization jobs - Event 5556 (SharePoint Server 2010)
- Unknown SQL exceptions - Event 5586 (SharePoint 2010 Products)
- Audience compilation failed - Event 5693 (SharePoint Server 2010)
- Synchronizing data between SharePoint Server and directory failed - Events 6000-6099 (SharePoint Server 2010)

- SharePoint Foundation failed to create a site - Event 6141 (SharePoint 2010 Products)
- Unable to load authentication provider - Event 6143 (SharePoint 2010 Products)
- User Profile Synchronization Service unexpected failure - Events 6300-6309 (SharePoint Server 2010)
- Insufficient permissions to write to the configuration data cache - Event 6395 (SharePoint 2010 Products)
- Alternate access mapping update failed - Event 6397 (SharePoint 2010 Products)
- Service Instance timer execution failed - Event 6398 (SharePoint 2010 Products)
- 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)
- Service instance provisioning failed - Event 7034 (SharePoint Server 2010)
- Backup timer job could not be created - Event 7035 (SharePoint 2010 Products)
- Central Administration update failed - Event 7037 (SharePoint 2010 Products)
- Secure Store reencrypt credentials failed - Event 7510 (SharePoint Server 2010)
- Secure Store could not retrieve master encryption key - Event 7535 (SharePoint Server 2010)
- Secure Store SQL exception - Event 7551 (SharePoint Server 2010)
- Secure Store proxy unexpected exception - Event 7557 (SharePoint Server 2010)
- Throttling starts alert- Events 8032 8062 (SharePoint 2010 Products)
- Cannot retrieve end point - Event 8070 (SharePoint 2010 Products)
- Cannot retrieve list of service applications from remote farm - Event 8071 (SharePoint Server 2010)
- 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 - 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)
- Backend server not reachable (SharePoint Server 2010)
- Document conversion failures high (SharePoint Server 2010)
- 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)
- Unacceptable rendering response time (SharePoint Server 2010)
- User Profile Configuration service not started (SharePoint Server 2010)
- User Profile Synchronization service not started (SharePoint Server 2010)
- Web application taking too long to render a page (SharePoint 2010 Products)
- Web application unavailable (SharePoint 2010 Products)
- Web site unavailable (SharePoint 2010 Products)

Access Services in SharePoint Server 2010 knowledge articles

Published: May 12, 2010

The articles in this section are knowledge articles for Access Services in Microsoft SharePoint Server 2010. 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 Access Services.

In this section:

- Access Services - configuration database access failed - Event 1 (SharePoint Server 2010)
- Access Services cannot create session cache - Event 11 (SharePoint Server 2010)
- Access Services out of memory - Event 16 (SharePoint Server 2010)
- Access Services failed to load calculation library - Event 17 (SharePoint Server 2010)
- Access Services template input output error - Event 21 (SharePoint Server 2010)
- Access failed to contact Access Services - Events 24 25 26 (SharePoint Server 2010)
- Access Data Services no longer available - Event 28 (SharePoint Server 2010)
- Access Services server is not available - Event 29 (SharePoint Server 2010)

Access Services - configuration database access failed - Event 1 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Configuration database access failed

Event ID: 1

Summary: Access Services in Microsoft SharePoint Server 2010 stores its settings in the Microsoft SharePoint Server 2010 configuration database. Either a web front end or a back end server component of Access Services was unable to read its settings from the configuration database.

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

- Access Services in SharePoint might not start.
- Access Services might fail to create Access Services applications.
- Users might not be able to view applications in their browsers, or the service might be otherwise unavailable.
- This event appears in the event log: Event ID: 1 Description: Access Services: Unexpected exception while trying to access <configuration database name>. Error = <exception message>
- This event appears in the event log: Event ID: 32 Description: Unable to obtain configuration information.
- This event appears in the event log: Event ID: 33 Description: Unable to obtain AccessWebServiceInstance.
- This event appears in the event log: Event ID: 34 Description: There is no application associated with proxy <name of Access Services proxy>.
- This event appears in the event log: Event ID: 35 Description: There is no SharePoint service context.
- This event appears in the event log: Event ID: 36 Description: There is no default Access Services Application Proxy.

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

- The configuration database might be experiencing a failure.
- Permissions might have changed for the account that runs the application pool that Access Services is running, so Access Services no longer has access to the SharePoint Server 2010 configuration database.
- The front end proxy for Access Services may have been deleted.
- No front end proxy for Access Services is designated as the default.
- An unexpected failure occurred during provisioning of the service.

Resolution for event ID 1 and 32: Grant correct permissions to the database access account

- Resolve this issue by finding the name of the database access account, adding the database access account in Microsoft SQL Server 2008 , and then verifying that the account has correct permissions in SQL Server 2008.

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

To find the database access account:

1. On the SharePoint Central Administration Web site, in the **Security** section click **Configure service accounts**.
2. On the Service Accounts page, in the **Credential Management** section, in the upper drop-down list, select the application pool that is running Access Services. When the application pool is selected, the name of the Access Services application is listed in the text box; for example, AccessDataService-Type.
3. Note the account that is selected in the **Select an account for this component** drop-down list.

To add the database account in SQL Server 2008:

1. Connect to the computer that runs SQL Server 2008 by using an account that has 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, expand the **Databases** node, expand the configuration database node, expand the **Security** node, and then expand the **Roles** node.
4. Expand the **Database Roles** node and double-click the **db_reader** role.
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 this account has correct permissions in SQL Server:

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 Windows PowerShell command **Get-SPAccessServiceApplication"<name of your access service>" | format-table**.
3. This command retrieves the Access Services application and displays the values for some settings. These values are read from the configuration database.

Ensure there is a default proxy for Access Services

1. On the Central Administration home page, click **Application Management**.
2. On the Application Management page, under **Service Applications**, click **Configure service application associations**.
3. On the Service Application Associations page, clock on proxy listed in the **Application Proxy Group** column for the Web application.
4. In the **Configure Service Application Associations** dialog, ensure that the **AccessDataServiceInstance - Access Services Web Service Application Proxy** box is checked and click **OK**.
5. If the **AccessDataServiceInstance - Access Services Web Service Application Proxy** box does not exist, you must re-provision Access Services on the server.

Re-provision Access Services

1. If you only have one Access Services application in your farm, you will want to remove it before provisioning a new one. This will ensure that any proxies are correctly cleaned up. To remove an existing Access Services application:
    a) On the Central Administration home page, click **Application Management**.
    b) On the Application Management page, under **Service Applications**, click **Manage service applications**.

c) On the Manage service applications page, highlight the **Access Services Web Service Application** and click **Delete** on the ribbon.

Important:

Do not check the **Delete data associated with the Service Applications** checkbox. On the **Delete Service Application** dialog, click **OK**.

2. Add a new Access Services application to the server:
   a) On the Central Administration home page, click **Application Management**.
   b) On the Application Management page, under **Service Applications**, click **Manage service applications**.
   c) On the Manage service applications page, click **New** on the ribbon and select **Access Services**.
   d) In the **Create New Access Services Application** dialog, under **Name**, type in the name for the Access Services application. The name must be unique among all Access Services applications.
   e) Under **Application Pool**, choose to reuse an existing application pool, or create a new one and choose an account to run the application pool as.
   f) Click **OK**.

Access Services cannot create session cache - Event 11 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Access Services cannot create cession cache

Event ID: 11

Summary: Access Services in Microsoft SharePoint Server 2010 maintains query results in a session on the Access Services back-end server computer. The issue in this case is that the Access Services server computer failed to create a session for caching query results.

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

- Access Services applications that run on the server might not be able to display data in forms, reports, or the table view.
- This event appears in the event log: Event ID: 11 Description: Access Services: Unable to create a cache for the session for application <application name>. Exception message: <exception message>

Cause: The Access Services in SharePoint server computer is in an unstable state.

Resolution: **Restart the Access Services computer**

- Restart the Access Services computer to free up memory and return to a known good state.

Access Services out of memory - Event 16 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Access Services out of memory

Event ID: 16

Summary: The Access Services in Microsoft SharePoint Server 2010 computer maintains sessions that hold query cache results, and performs other operations that use a lot of memory. The Access Services server computer is low on memory or is out of memory.

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

- Access applications in the Web browser time out or respond very slowly.
- Users cannot load or view their Access Services applications in the browser.
- This event appears in the event log: Event ID: 16 The ADS box <machine name> has run out of memory.

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

1. The amount of memory consumed by Access Services in SharePoint on the back-end server computer has grown too large.
2. There is excessive traffic to the Access Services server computer and the computer cannot serve that many users.

Resolution: Restart Access Services

1. Consider whether you have enough Access Services server computers in the farm to support the number of users of your deployment. The addition of Access Services computers in your farm reduces the amount of traffic and memory requirements on any single Access Services computer.
2. Use the SharePoint Central Administration Web site to change the Maximum Session Memory setting for Access Services to a lower value.
    a) On the SharePoint Central Administration Web site, on the Quick Launch, click **Application Management**, and in the **Service Applications** section, click **Manage service applications**. In the Type column, note that **Access Services Web Service Application** appears for Access Services applications.
    b) In the **Name** column, click the Access Services application that is out of memory.
    c) On the Manage Access Services page, in the **Session Management** section, type a lower value for **Maximum Session Memory**, and then click **OK**.
3. Restart the Access Services computer to free up memory and return the Access Services computer to a known good state.

Access Services failed to load calculation library - Event 17 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Access Services failed to load calculation library

Event ID: 17

Summary: Access Services in Microsoft SharePoint Server 2010 depends on a critical DLL file, ascalc.dll, to enable caching of session information and queries.

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

- Access Services fails to start or fails to create Access Services applications.
- This event appears in the event log: Event ID: 17 Description: Failed to load ASCalc.dll <path to file>.

Cause: The ascalc.dll file became corrupt or is not present on disk.

Resolution: **Repair the installation**

1. Run setup for Microsoft SharePoint Server 2010 , and select the option to repair the installation.
2. Complete any required setup wizard processes.

Access Services template input output error - Event 21 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Access Services template input output error

Event ID: 21

Summary: Access Services in Microsoft SharePoint Server 2010 creates Web sites, which are a representation of Access Services in SharePoint applications on the server. Access Services tried to create an Access Services application on the Web, but encountered an error when it read the template file that was used to create that site.

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

- Users cannot create a new site from a specified Access Services template.
- This event appears in the event log: Event ID: 21 Description: Access Services: A file read error has occurred during site creation. File the error occurred on: <path to the file>.

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

1. The Access Services template file is corrupt.
2. The Access Services template file is missing.

Resolution: Reinstall the user-defined template

- Install the custom Access Services templates on the Microsoft SharePoint Server 2010 server computer where Access Services is installed.

Resolution: Reinstall templates included with Access Services

- Run setup for SharePoint Server 2010 and repair the Access Services installation.

Access failed to contact Access Services - Events 24 25 26 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Failed to contact Access Services

Event ID: 24 25 26

Summary: The front-end Web application made a request to a specific Access Services in Microsoft SharePoint Server 2010 back-end server computer and encountered an unexpected exception. This can indicate an intermittent problem or a problem with a specific server computer. In these cases, the front-end Web application attempts to load balance to a different back-end server computer. The Access Services server computer is required to run queries and maintain cache state for those queries.

Symptoms:

- The following message may appear in the event log: Event ID: 24 Description: There was an error in communicating with Access Data Services exception: <exception description> [Session: <session ID> User: <username>].
- The following message may appear in the event log: Event ID: 25. Description: There was an error in communicating with Access Data Services exception: <exception description> [Session: <session ID> User: <username>].
- The following message may appear in the event log: Event ID: 26. Description: Unable to reach Access Data Services. [Session: <session ID> User: <username>].

Cause: The Access Services in SharePoint server computer is in an unstable state and might need to be restarted.

- The web front end encountered an intermittent failure when trying to contact the Access Data Services server.
- The specific Access Data Services server is in an invalid state and may need to be restarted.

Restart the Access Data Services server

1. Before restarting, verify that this is a problem that occurs often. It may be an intermittent problem that is automatically recovered from.
2. Restart the Access Data Services server.
3. If the problem continues to often, and restarting the server does not correct the problem, ensure that the hardware of the server is functioning correctly. If this is not the problem, reinstall Access Services on the server and re-add the server to the farm.

Access Data Services no longer available - Event 28 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Access Services is no longer available

Event ID: 28

Summary: The front end Access application sent a request to a specific Access Services server computer and encountered an unexpected exception. This can indicate an intermittent problem or a problem with the server computer. In these cases, the front end Access application attempts to load-balance to a different server computer. The Access Services server computer is required to query data that is typically used in Access Services reports.

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

- Access Services applications fail to refresh data.
- Access Services applications fail to load or be displayed correctly.
- This event appears in the event log: Event ID: 28 Description: The Access Data Services is no longer available. [Session: <session ID> User: <username>].

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

- The front end Access application encountered an intermittent failure when it sent a request to the Access Services server computer.
- The specific Access Services server computer is in an invalid state and must be restarted.
- There are network related failures that are preventing the server that is running the front-end Access application from contacting the Access Services server computer.

Resolution: Restart the server

1. Before restarting the Access Services server computer, refer to the System Center Operations Manager reports to learn how often this problem occurs. If the problem occurs intermittently and Access Services automatically recovers from it, do not restart the server computer unless the symptoms noted above persist.
2. Restart the Access Services server computer.
3. If the problem occurs often, and restarting the server computer does not correct the issue, verify that the server computer is functioning correctly. You may need to reinstall Microsoft SharePoint Server on the server computer and join it to the SharePoint farm.

Access Services server is not available - Event 29 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Access Services server computer is not available

Event ID: 29

Summary: A front-end Access application computer cannot locate or send requests to any server computer that is running Access Services. The Access Services server computer is required to query data that is typically used in Access Services reports.

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

- Access Services does not render any data in forms, reports, or any other view of an Access application in the browser.
- This event appears in the event log: Event ID: 29 Description: No Access Data Services is available in the farm.[User: <username>].

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

- The Access Services server computer is not running.
- Access Services was not started on the server computer.
- The proxy that the front-end Access application is not the default member of the default proxy group for Access Services.

Resolution: Verify that Access Services runs on the server

1. On the Central Administration Home page, in the **System Settings** section, click **Manage servers in this farm**.
2. Select the server computer that hosts the Access Database Service.
3. On the Services on Server page, check whether **Started** is indicated for **Access Services** in the **Status** column. If it is not, click **Start** in the **Action** column.

Resolution: Verify that the proxy for the service application is the default member for Access Services

1. On the SharePoint Central Administration Home page, on the Quick Launch, click **Application Management**. In the **Service Applications** section, click **Configure service application associations**.
2. On the Service Application Associations page, in the **Application Proxy Group** column, click the name of the proxy group for your front-end Access application. The default name for the proxy group is **default**.
3. In the **Configure Service Application Associations** dialog box, make sure that the check box for the Access Services proxy is selected. If there is more than one Access Services application proxy and the word **[default]** does not appear after the name of the proxy you want to use, select the check box, and then click **[set as default]**.
4. Click **OK**.

Excel Services Application in SharePoint Server 2010 knowledge articles

Published: May 12, 2010

The articles in this section are knowledge articles for the Excel Services Application. 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 Excel Services Application.

In this section:

- Excel unauthorized attempt to access a session - Event 2011 (SharePoint Server 2010)
- Excel Services Application internal error - Event 2026 (SharePoint Server 2010)
- Excel Services Application save failed - Event 3348 (SharePoint Server 2010)
- Excel Services Application unexpected workbook failure - Event 5225 (SharePoint Server 2010)
- Excel workbook disk cache cannot be created - Event 5226 (SharePoint Server 2010)
- Unable to establish connection with Excel Services Application - Events 5231_5233 (SharePoint Server 2010)
- Error communicating with Excel Services Application - Events 5231_5239_5240 (SharePoint Server 2010)
- Excel Services Application not available - Event 5234 (SharePoint Server 2010)
- Excel Unable To Delegate Credentials - Event 5243 (*http://technet.microsoft.com/library/dfa6bafd-7ea9-4542-8222-84285a52079c(Office.14).aspx*)
- Excel Services Application configuration database access failed - Event 5244 (SharePoint Server 2010)
- Max memory configured for Excel Services Application exceeded - Event 5255 (SharePoint Server 2010)
- Excel Services Application memory allocation failed - Event 5256 (SharePoint Server 2010)
- Excel Services Application not running locally - Event 5271 (SharePoint Server 2010)
- Excel invalid file access method configured - Event 5557 (SharePoint Server 2010)
- Excel Services Application user-defined function exception - Event 6467 (SharePoint Server 2010)
- Excel Services Application localized template file not found - Event 7924 (SharePoint Server 2010)
- Excel Services Application template file missing - Event 7925 (SharePoint Server 2010)
- Excel Services Application null access violation - Event 7926 (SharePoint Server 2010)
- Excel Services Application non-null access violation - Event 7927 (SharePoint Server 2010)
- Excel Services Application array out of bounds - Event 7928 (SharePoint Server 2010)
- Excel workbook disk cache full (SharePoint Server 2010)

Excel unauthorized attempt to access a session - Event 2011 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel unauthorized attempt to access a session

Event ID: 2011

Summary: Excel Services Application maintains individual user sessions. Sessions maintain state related to workbook calculations, parameters that a user sets, interactions that a user has with a live workbook, and data returned from a data source as a result of a data refresh operation. Sessions are maintained per user per workbook, and can contain private data and information. Sessions are available only to the user that started the session. The issue in this case is that a user who did not start a session attempted to access data from that session.

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

- The user that attempted to access a session that the user did not start cannot view the workbook.
- This event appears in the event log: Event ID: 2011 Description: Unauthorized attempt to access session by user <username>. Session belonged to user <username of user that started the session>. [Session: <session id> User: <username>].

Cause: A user that did not start the session attempted to request data from the session.

Excel Services Application internal error - Event 2026 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application internal error

Event ID: 2026

Summary: The server for Excel Services Application is responsible for loading, refreshing, and recalculating workbooks, and maintaining user session state. An unexpected internal error was encountered by the server for Excel Services Application.

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

- Some user sessions are interrupted and workbooks in the browser might stop responding.
- This event appears in the event log: Event ID: 2026 Description: An internal error occurred. <error message>.

Cause: The Excel Services Application server experienced an unexpected failure.

Resolution: **Restart the server computer**

- Excel Services Application will try to recover automatically from this event by restarting the service. If the System Center Operations Manager (SCOM) monitor for this event is triggered, the event has occurred repeatedly. To resolve the problem, restart the server that runs Excel Services Application.

Excel Services Application save failed - Event 3348 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application save failed

Event ID: 3348

Summary: The server for Excel Services Application is responsible for loading, refreshing, and recalculating workbooks, and maintaining user session state. The server for Excel Services Application failed to save a workbook file. Users may be unable to save their workbook changes.

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

- Users may receive an error message that informs them that their changes cannot be saved while editing workbooks in their browser.
- This event appears in the event log: Event ID: 3348 Description: Saving <URL of workbook> failed mid-save. [Session: <session ID> User: <username>].

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

- The user's permissions to edit or save files were revoked at the same time that the workbook was being saved.
- The content database is unavailable and could not be accessed.

Excel Services Application unexpected workbook failure - Event 5225 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application unexpected workbook failure
Event ID: 5225
Summary: The server for Excel Services Application is responsible for loading, refreshing, and recalculating workbooks, and maintaining user session state. An unexpected failure occurred on the server for Excel Services Application and a workbook session was terminated.
Symptoms: One or more of the following symptoms might appear:

- User sessions are dropped on Excel Services Application. This causes a workbook in the browser to stop responding or causes an error message to appear; for example, An error has occurred.
- This event appears in the event log: Event ID: 5225 Description: An unexpected serious error occurred when executing <URL to workbook>. The workbook will be unloaded by the server for Excel Services Application. If this error continues to occur, an administrator should look at the file and verify its contents.

Cause: A workbook file that is in a corrupted state was loaded on the Excel Services Application server.

Note:
Administrator permissions are required to perform these steps.

Resolution: Remove the affected file

1. From the event log, note the path to the file for event ID 5225.
2. Use the path to locate the file on the disk, or in the list of workbook files in SharePoint.
3. Delete the file.

Resolution: Restart the Excel Services Application server computer

- If the problem persists or occurs for numerous files or for files that were previously loading correctly, restart the Excel Services Application server computer.

Excel workbook disk cache cannot be created - Event 5226 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel workbook disk cache cannot be created
Event ID: 5226
Summary: Excel Services Application saves the workbooks it loads to a temporary cache on disk. In this case, a workbook disk cache cannot be created on the Excel Services Application server computer.
Symptoms: One or more of the following symptoms might appear:

- Excel Services Application fails to start.
- The provisioning of the service fails.
- Workbooks fail to load.
- This event appears in the event log: Event ID: 5226 Description: Unable to create or access workbook cache at <disk location of cache>. Excel Services Application cannot function without a workbook cache.

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

1. The account that runs the application pool in which Excel Services Application runs might not have permissions to create a directory on the Excel Services Application server computer.
2. The Excel Services Application server computer might have hard disk problems or the hard disk might be full.

Resolution: Verify that the server computer is functioning and has sufficient disk space

- Verify that the computer that runs the Excel Services Application server functions correctly and contains enough disk space. The event log message for ID 5226 identifies the disk that the Excel Services Application server uses.

Resolution: Verify that the account that runs Excel Services Application can create a Temp folder

- Verify that the account that runs Excel Services Application has permissions to create a Temp folder on the server computer. Delete the existing Temp folder so that the service can create a new Temp folder. Use the following procedure to identify the account that runs the application pool in which Excel Services Application runs.

To identify the application pool account:

1. Click **Start**, click **All Programs**, click **Microsoft SharePoint 2010 Products**, and then click **SharePoint Management Shell**.
2. At the command prompt, type the name of the **Get-SPExcelServiceApplication**Windows PowerShell cmdlet to obtain the name of the application pool. Note the value of the **ApplicationPool** property that this cmdlet returns.
3. Click the **Start** button, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
4. In the **Connections** pane, expand the server node and then click **Application Pools**.

5. In the reading pane, in Features View, in the **Identity** column, note the account for the application pool that you identified.

Resolution: Verify permissions on the workbook cache location

- Verify that the account that runs the application pool in which Excel Services Application runs has permissions to create a directory on the Excel Services Application server computer. Start by indentifying the location of the workbook cache.
  To identify the workbook cache location:
  1. On the SharePoint Central Administration Web site, in the **Application Management** section, click **Manage service applications** and in the **Name** column click the name of the Excel Services Application application that is affected by the problem.
  2. On the Manage Excel Services Application page, click **Global Settings** and in the **Workbook Cache** section note the location of the workbook cache in the **Workbook Cache Location** text box.
  3. If the **Workbook Cache Location** box is empty, Excel Services Application is using the default location, %windir%\temp.
     To verify permissions on the workbook cache location
  1. Navigate to the parent directory for the workbook cache location. The default location is <OS drive>:\windows\temp.
  2. Right-click the folder and click **Properties**. The **Properties** dialog box appears.
  3. On the **Security** tab, in the **Group or user names** list, verify that the account appears that runs the application pool in which Excel Services Application runs. Note that the account might be a member of a group in this list.
  4. If the application pool account is not included in the list, click **Edit**, and then click **Add**.
  5. Type the name of the account and click **OK**.
  6. In the **Properties** dialog box, on the **Security** tab, click **Advanced**.
  7. In the **Advanced Security Settings** dialog box, select the name of the account, and then click **Edit**.
  8. In the **Advanced Security Settings for <folder name>** dialog box, verify that the account is selected, and then click **Edit**.
  9. In the **Permission Entry for <folder name>** dialog box, verify that all permission check boxes are selected for **Allow**, and that all permission check boxes are cleared for **Deny**.
  10. Click **OK** to close all dialog boxes.

Resolution: Delete old Excel Services Application folders in the workbook cache directory, so that the cache can be recreated

1. Navigate to the parent directory of the workbook cache. The default location is <OS drive>:\windows\temp.
2. If the directory includes an Excel Services Application folder, delete the folder.

Resolution: Perform an iisreset operation to restart the service

- On the computer, click **Start**, click **Run**, and in the **Open** text box, type **iisreset** and click **OK**.

Unable to establish connection with Excel Services Application - Events 5231 5233 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Unable to establish a connection with Excel Services Application

Event ID: 5231 and 5233

Summary: The front-end Web application sent a request to a specific server for Excel Services Application and could not contact the server computer. In this case, the Web front end attempts to load balance to a different Excel Services Application server if another server is available.

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

- Workbooks fail to load.
- Longer load times for workbooks that succeed to load.
- This event appears in the event log: Event ID: 5231 Description: The Excel Calculation Server <URL to server> is no longer available. Session: <session ID> User: <username>]
- The following message may be shown in the event log: Event ID: 5233 Description: The Excel Calculation Server <URL to server> is no longer available. Session: <session ID> User: <username>].

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

- The Excel Services Application server computer is turned off or is off the network.
- The Excel Services Application server computer is having difficulty and is unavailable.

Ensure the server is started and can connect to the network

1. Ensure that the server running Excel Services Application is turned on and running.
2. Ensure that the server running Excel Services Application is able to connect to the network and that you can connect to the server form another computer on the network.
3. If the server is started and it can connect to the network and the problem is not fixed, re-install Excel Services Application and re-add the server to the farm.

Error communicating with Excel Services Application - Events 5231 5239 5240 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Error communicating with Excel Services Application

Event ID: 5231, 5239, and 5240

Summary: The front-end Web application made a request to a specific server for Excel Services Application and encountered an unexpected exception. This could indicate an intermittent problem or a problem with the specific server computer. In such a case, the Web front end attempts to load balance to a server computer. The Excel Services Application server is required to load workbooks and maintain session state for those workbooks.

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

- Delayed load times for workbooks.
- Workbooks fail to load.
- This event appears in the event log: Event ID: 5231 Description: Unable to reach Excel Calculation Server <URL of machine> [Session: <session ID> User: <username>].
- This event appears in the event log: Event ID: 5239 Description: There was an error in communicating with Excel Calculation Server <URL of machine> exception: <exception message> [Session: <session ID> User: <username>].
- This event appears in the event log: Event ID: 5240 Description: There was an error in communicating with Excel Calculation Server <URL of machine> exception: <exception message> [Session: <session ID> User: <username>].

Cause: The Excel Services Application server computer is in a non-valid state and may need to be restarted.

Restart the server

1. Before restarting, verify that this problem occurs often. It may be an intermittent problem that is automatically corrected and does not require you to restart the server.
2. If the problem occurs often, restart the server running Excel Services Application.
3. If the problem continues to occur often, and restarting the server did not correct the problem, confirm that the hardware of the server is functioning correctly, or reinstall Excel Services Application and re-add the server to the server farm.

Excel Services Application not available - Event 5234 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application not available

Event ID: 5234

Summary: A front-end Web application computer cannot locate and send requests to the server for Excel Services Application. The Excel Services Application server computer is required to load workbooks.

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

- Workbooks do not load on Excel Services Application server.
- This event appears in the event log: Event ID: 5234 Description: No Excel Calculation Server is available in the farm. [User: <username>].

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

- The Excel Services Application server computer might not be running.
- Excel Services Application might not be started on the server computer.
- The proxy that the front-end Web server is using might not be the default member of the default proxy group for Excel Services Application.

Resolution: Verify that the service application instance runs on the machine

1. On the SharePoint Central Administration Web site, click **System Settings**.
2. Click **Manage servers in this farm**.
3. For each server that you want to run Excel Services Application, select the name of the server.
4. On the Services on Server page, if **Started** is not indicated for **Excel Calculation Services** in the **Status** column, click **Start** in the **Action** column.

Resolution: Restart the Excel Services Application server

- Restart the Excel Services Application server computer.

Resolution: Verify that the proxy for the service application is the default member for Excel Services Application

1. On the SharePoint Central Administration Web site, on the Quick Launch click **Application Management**, and in the **Service Applications** section click **Configure service application associations**.
2. On the Service Application Associations page, in the **Application Proxy Group** column, for your Web application, click the name of the proxy group. The default name for the proxy group is **default**.
3. In the **Configure Service Application Associations** dialog box, if the check box for the Excel Services Application proxy is not selected select it. If there is more than one Excel Services Application proxy and the word **[default]** does not appear after the name of the proxy you want to use, select the check box, and then click **[set as default]**.
4. Click **OK**.

Excel Services Application configuration database access failed - Event 5244 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application configuration database access failed
Event ID: 5244
Summary: The application server for Excel Services Application failed to access the configuration database and might not be able to read or save any settings. All settings for Excel Services Application are stored in the configuration database.
Symptoms: One or more of the following symptoms might appear:

- Excel Services Application might fail to provision.
- Excel Services Application might not start.
- Excel Services Application might be interrupted and user workbooks might fail to load.
- This event appears in the event log: Event ID: 5244 Description: Unexpected error when trying to access service settings in the SharePoint configuration database. Make sure the proxy for this service application is a member of the default proxy group for the active web application. Error =<error returned from SharePoint>.

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

1. Configuration database might be offline or unavailable.
2. Permissions on the configuration database have changed, or permissions for the application pool account in which Excel Services Application runs have changed, and Excel Services Application no longer has access to the configuration database.

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

Resolution: Grant correct permissions to the database access account

- To find the database access account:
  1. On the Central Administration page, on the Quick Launch, click **Security**, and in the **General Security** section click **Configure service accounts**.
  2. On the Service Accounts page, in the **Credential Management** section, from the drop-down list select the **Service Application Pool** option for the application pool that runs Excel Services Application. When this option is selected, the name of the Excel Services Application appears in the list box below the drop-down list; for example, Excel Service Application.
  3. Note the account that is selected in the **Select an account for this component** list, and click **OK**.
- To 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, 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 logon account ; for example, ##MS_PolicyTsqlExecutionLogin##.

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 then 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 Excel Services Application can read from the configuration database
  1. On the computer, click **Start**, click **All Programs**, click **Microsoft SharePoint 2010 Products**, and then click **SharePoint Management Shell**.
  2. At the command prompt, type the Windows PowerShell cmdlet name **Get-SPExcelServiceApplication** to obtain the settings of the specified Excel Services Application. These settings are read from the configuration database.

Max memory configured for Excel Services Application exceeded - Event 5255 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Maximum memory configured for Excel Services Application has been exceeded
Event ID: 5255
Summary: Administrators of Excel Services Application can determine how much memory the service should use on each physical computer that runs Excel Services Application. This is an important setting because Excel Services Application is calculation-intensive and maintains state, and can require a large amount of memory. The amount of memory that the server for Excel Services Application can consume is specified with the **MaxPrivateBytes** property. This problem occurs when the server consumes more memory than is allocated in this property setting.
Symptoms: One or more of the following symptoms might appear:

- Workbooks fail to load.
- Users experience miscellaneous error messages; for example, An error has occurred.
- Performance of workbooks is poor.
- This event appears in the event log: Event ID: 5255 Description: Maximum Private Bytes size exceeded. Unable to complete the operation.[Session: <session ID> User: <username>].

Cause: Excel Services Application has exceeded its **MaxPrivateBytes** setting value, and requests to the server are being denied as a result.

Ensure your servers have enough RAM memory to serve the number of users

1. Ensure that your servers have enough RAM memory and that your Excel Services Application deployment is large enough to support your user base. For more information, see Determine resource requirements to support Excel Services Application.

Increase the MaxPrivateBytes setting

1. On Central Administration home page, click **Application Management**.
2. On the Application Management page, under **Service Applications**, click **Manage service applications**.
3. Click on the Excel Services Application. By default this has the name “Excel Service Application”.
4. On the Manage Excel Services Application page, click **Global Settings**.
5. On the Excel Services Application Settings page, under **Memory Utilization**, type the number of megabytes (MB) of RAM memory that you want Excel Services Application to use.
6. Click **OK**.

Excel Services Application memory allocation failed - Event 5256 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application memory allocation failed

Event ID: 5256

Summary: The server for Excel Services Application is responsible for loading, refreshing, and recalculating workbooks, and maintaining user session state. The server for Excel Services Application failed to allocate memory.

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

- Users cannot create sessions and so cannot view workbooks in their browser.
- Existing user sessions may stop responding and cause open workbooks in the browser to stop responding.
- This event appears in the event log: Event ID: 5256 Description: Access Memory Allocation failed. [Session: <session ID> User: user name]

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

- The server for Excel Services Application has reached capacity and the server cannot allocate more memory resources.
- The server for Excel Services Application has experienced an unexpected failure and cannot allocate new memory.

Resolution: Evaluate whether servers are sufficient to support user load

- Before you perform any corrective steps, evaluate whether you have enough Excel Services Application server computers to support the user load.

Resolution: Restart the Server Machine

- Restart the Excel Services Application server computer.

Excel Services Application not running locally - Event 5271 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application is not running locally

Event ID: 5271

Summary: Excel Services Application supports the defining of load balancing between the Web application front end and the server for Excel Services Application. An option for load balancing is Local. However, this is a valid setting only if the Web front end and the server for Excel Services Application run on the same physical computer.

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

- Delay in workbook load times.
- This event appears in the event log: Event ID: 5271 Description: Load Balancing scheme is configured as Local; however local Excel Calculation Server is not running. Using default round robin load balancing scheme [User: <username>]

Cause: The load-balancing scheme is set to Local but Excel Services Application is not running on that Web front end computer.

Resolution: **Change the load balancing scheme**

1. On Central Administration home page, click **Application Management**.
2. On the Application Management page, under **Service Applications**, click **Manage service applications**.
3. Click on the Excel Services Application. By default this has the name “Excel Service Application”.
4. On the Manage Excel Services Application page, click **Global Settings**.
5. On the Excel Services Application Settings page, under **Load Balancing**, select either **Workbook URL** or **Round Robin with Health Check**.
6. Click **OK**.

Excel invalid file access method configured - Event 5557 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel invalid file access method configured

Event ID: 5557

Summary: Excel Services Application supports two types of communication between its front-end Web application and back-end server components: Trusted Subsystem and Delegation. The communication type is controlled with the Access Model setting. An Excel Services Application administrator can also specify how the server component retrieves files: Use the process account the service runs as, or impersonate the user, requesting the workbook and delegate the user's credentials. This error occurs when the Access Model is set to Trusted Subsystem and the file access method is set to Impersonation. In this configuration, the server component is unable to obtain or delegate the end user's credentials because they were not delegated from the front-end Web application.

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

- Failure to load workbooks.
- This event appears in the event log: Event ID: 5557 Description: Failed to load <workbook URL> with error: 'The server is configured to use Impersonation to access workbooks but impersonation cannot be used when the communication between the Excel Calculation Server and Excel Web Access is set to use a Trusted Subsystem.' [Session: <session ID> User: <username>]

Cause: The AccessModel setting and the FileAccessMethod setting conflict.

Excel Services Application user-defined function exception - Event 6467 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application user-defined function exception

Event ID: 6467

Summary: A user-defined function has thrown an exception. User-defined functions are custom code assemblies that are deployed to the back-end server for Excel Services Application and are called from an Excel Services Application front-end application. Workbooks that require this user-defined function might not calculate properly. The user-defined function might have to be fixed and redeployed to the server.

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

- Workbooks that use this user-defined function do not calculate correctly and might display errors in the spreadsheet.
- This event appears in the event log: Event ID: 6467 Description: An exception occurred in a user-defined function. Assembly=<name and path of the assembly>, class= <class that threw exception>, function name=< name of function>, exception text=<exception message>

Cause: The user-defined function code has encountered an error condition from which it cannot recover.

Resolution: Correct the user-defined function code

- This error occurs when a user-defined function often throws exceptions. User-defined functions are not Excel Services Application product code. Use the following steps to find the location of the deployed assembly.

  To correct the user-defined function:

  1. Consult with the developer of the user-defined function about deployment of more robust error handling for the function.
  2. Deploy the updated user-defined function. Ask the developer of the user-defined function to save the new user-defined function assembly to the server global assembly cache (GAC) or file share, depending on how the assembly was deployed initially.

  To find the location of the assembly:

  1. On the SharePoint Central Administration Web site, in the **Application Management** section, click **Manage service applications**.
  2. In the **Name** column, click the name of the Excel Services Application application. In the **Type** column Excel Services Application applications are of type **Excel Services Application Web Service Application**.
  3. On the Manage Excel Services Application page, click **User Defined Function Assemblies**.
  4. In the **Assembly** column, click the user-defined function that you plan to redeploy.
  5. In the **Assembly details** section, the **Assembly** text box shows the path to the assembly, or only its strong name if the user-defined function is installed to the global assembly cache (GAC), under **<root>\windows\assembly**. Note that the **Assembly Location** option indicates whether the assembly is in the global assembly cache or is a file path.

Excel Services Application localized template file not found - Event 7924 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application localized template file not found

Event ID: 7924

Summary: The localized template file that Excel Services Application uses to create new workbooks was not found. The server might be in the process of creating new workbooks by using a template file of a different locale. Users that create workbooks by using Excel Services Application might see a workbook with the incorrect language.

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

- Buttons with text and other UI elements in workbooks displayed by Excel Services Application might be in the incorrect language.
- This event appears in the event log: Event ID: 7924 Description: The locale <name of locale> could not be found. As a result, a new workbook was created using the <path of workbook template> workbook template. To enable workbooks to be created for <desired locale>, you must install the <language pack> language pack. [Session: <session ID> User: <username>]

Cause: A localized template workbook file was not found. The localized template file was not correctly installed on the computer, or is corrupt. The file must be reinstalled. The easiest method for reinstalling the template is to repair the installation.

Resolution: Repair the installation

- Run setup for Excel Services Application, select the repair installation option, and follow the steps in the wizard.

Excel Services Application template file missing - Event 7925 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application template file missing

Event ID: 7925

Summary: The template file that is used to create new workbooks by Excel Services Application was not found. Users might be unable to create new workbooks on the server for Excel Services Application until this problem is corrected.

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

- Users are unable to create new workbooks.
- This event appears in the event log: Event ID: 7925 Description: The new workbook template for Excel Services Application could not be found. As a result, a user was unable to create a new workbook. You may need to repair your installation. [Session: <session ID> User:<username>]

Cause: The new workbook template file cannot be found or read from disk. The file should be reinstalled. The easiest method for reinstalling the template is to repair the installation.

Resolution: **Repair the Excel Services Application installation**

- Run setup for Excel Services Application, choose the repair installation option, and follow the steps in the wizard.

Excel Services Application null access violation - Event 7926 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application null access violation

Event ID: 7926

Summary: The server for Excel Services Application is responsible for loading, refreshing, and recalculating workbooks, and maintaining user session state. A workbook loaded on Excel Services Application caused a null access violation.

Symptoms: This event appears in the event log: Event ID: 7926 Description: Excel Calculation Server process tried to access a null virtual address for which it does not have access to. Access Type: <type of access>, Workbook Url: <URL to workbook>, Site Id: <site id> [Session: <session id> User:<username>]

Cause: A workbook with malformed input was loaded on the server.

Excel Services Application non-null access violation - Event 7927 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application non-null access violation

Event ID: 7927

Summary: The server for Excel Services Application is responsible for loading, refreshing, and recalculating workbooks, and maintaining user session state. A workbook that was loaded on Excel Services Application caused an access violation that was not null. These access violations are potential security concerns as they might cause the server to read data to which a user does not have access or might cause the server to execute malicious code.

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

- A user might lose an existing workbook session. This causes a user's view of the workbook in the browser to stop responding or causes an error message to appear; for example, an error has occurred.
- This event appears in the event log: Event ID: 7927 Description: Excel Calculation Server process tried to access a virtual address for which it does not have access to. Access Type: <type of access>, Workbook Url: <URL of workbook>, Site Id: <ID of site>. [Session: <session ID> User: <username>]

Cause: A workbook with malformed input was loaded on the server.

Excel Services Application array out of bounds - Event 7928 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Services Application array out of bounds

Event ID: 7928

Summary: A workbook loaded on Excel Services Application attempted to overrun the boundary of a memory structure and illegally access data. Multiple, different, workbooks that are loaded by the same user and cause this problem can indicate a security violation by that user.

Symptoms: This event appears in the event log: Event ID: 7928 Description: Excel Services Application process tried to access an array element that is out of bounds. Workbook Url: <URL of workbook file>, Site Id: <site>. [Session: <Id of session> User: <username>]

Cause: A workbook file contains invalid input and caused a memory overrun.

Excel workbook disk cache full (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Excel Workbook disk cache is full

Event ID: No event ID

Summary: Excel Services Application saves workbooks it loads to a temporary cache on disk. The hard disk on the Excel Services Application server computer is full and Excel Services Application cannot save additional workbooks to that cache.

Symptoms: Intermittent workbook load failure.

- The following event may appear in event log: Event ID: 2015 Description: Failed to load <workbook URL> with error: 'The workbook cache is full, or does not contain enough free space to load the workbook. (workbook cache size is <size in MB> MB)'. [Session: <session ID> User: <username>].
- The following event may appear in event log: Event ID: 2016 Description: Failed to load '<workbook URL> with error: 'The disk containing the workbook cache is full, or does not contain enough space to load the workbook'. [Session: <session ID> User: <username>].

Cause:

- The hard disk on the server for Excel Services Application is full.
- The hard disk is not full, but the workbook cache size is set to too low a value.

Ensure there is enough disk space on the server

- Ensure there is enough disk space on the server.
- If disk space is running low, delete unused files or add disk space to the server.

Increase the Maximum Size of Workbook Cache setting

- On Central Administration home page, click **Application Management**.
- On the Application Management page, under **Service Applications**, click **Manage service applications**.
- Click the Excel Services Application. By default this has the name “Excel Service Application”.
- On the Manage Excel Services Application page, click **Global Settings**.
- On the Excel Services Application Settings page, under **Workbook Cache**, type the number of megabytes (MB) of disk space that you want Excel Services Application to use for the workbook cache files in the **Maximum Size of Workbook Cache** box.
- Click **OK**.

InfoPath Forms Services in SharePoint Server 2010 knowledge articles

Published: May 12, 2010

The articles in this section are knowledge articles for the InfoPath Forms Services in Microsoft SharePoint Server 2010. 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 InfoPath Forms Services.

In this section:

- InfoPath Forms Services business logic failed - Event 5337 (SharePoint Server 2010)
- InfoPath Forms Services business logic exceeded re-entrant count - Event 5340 (SharePoint Server 2010)
- InfoPath Forms Services business logic is out of memory - Event 5342 (SharePoint Server 2010)
- InfoPath Forms Services business logic load exception - Event 5343 (SharePoint Server 2010)
- InfoPath Forms Services Web files list load failed - Event 5369 (SharePoint Server 2010)
- InfoPath Forms Services postback failure - Event 5374 (SharePoint Server 2010)
- InfoPath Forms Services conflicting assembly identities found - Event 5733 (SharePoint Server 2010)
- InfoPath Forms Services business logic cannot be serialized - Event 5734 (SharePoint Server 2010)
- InfoPath Forms Services DoS postbacks per session - Event 5736 (SharePoint Server 2010)
- InfoPath Forms Services DoS actions per postback - Event 5737 (SharePoint Server 2010)
- InfoPath Forms Services data adapter security error submit - Event 5758 (SharePoint Server 2010)
- InfoPath Forms Services solution cache churning - Event 5759 (SharePoint Server 2010)
- InfoPath Forms Services data adapter security error query - Event 6932 (SharePoint Server 2010)
- InfoPath Forms Services solution load failure - Event 7056 (SharePoint Server 2010)
- InfoPath Forms Services not working due to invalid State Service configuration - Event 7898 (SharePoint Server 2010)

InfoPath Forms Services business logic failed - Event 5337 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services business logic failed

Event ID: 5337

Summary: Users who design InfoPath form templates for InfoPath Forms Services in Microsoft SharePoint Server 2010 can add managed code to their forms. Errors can occur when this custom code is executed.

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

- An error message appears when opening or filling out the form.
- This event appears in the event log: Event ID: 5337 Description: Business logic failed due to an exception. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>, Type: <ExceptionType>, Exception Message: <ExceptionMessage>).

Cause: The form code has thrown an unhandled business logic exception.

InfoPath Forms Services business logic exceeded re-entrant count - Event 5340 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services business logic exceeded re-entrant count

Event ID: 5340

Summary: Users who design InfoPath form templates can add managed code to their forms. Errors can occur when this custom code is executed.

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

- An error message appears when opening or filling out the form in the browser.
- This event appears in the event log: Event ID: 5340 Description: Business logic object model reentrance count limit was exceeded. The business logic may be in an infinite event recursion. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>)

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

- The business logic is running in an infinite loop.
- The number of business logic calls for a single update in the data exceeded the maximum limit.

InfoPath Forms Services business logic is out of memory - Event 5342 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services business logic is out of memory
Event ID: 5342
Summary: Users who design InfoPath form templates can add managed code to their forms. Errors can occur when this custom code is executed.
Symptoms: One or more of the following symptoms might appear:

- An error message appears when opening or filling out the form.
- This event appears in the event log: Event ID: 5342 Description: A memory allocation made by business logic could not be satisfied. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>, Type: <ExceptionType>, Exception Message: <ExceptionMessage>)

Cause: An out-of-memory exception has been generated by the custom code in an InfoPath form template.

InfoPath Forms Services business logic load exception - Event 5343 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services business logic load exception
Event ID: 5343
Summary: Users who design InfoPath form templates can add managed code to their forms. Errors can occur when this custom code is executed.
Symptoms: One or more of the following symptoms might appear:

- An error message appears when a form is loaded.
- This event appears in the event log: Event ID: 5342 Description: An exception occurred during loading of business logic. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>, Type: <ExceptionType>, Exception Message: <ExceptionMessage>)

Cause: Unhandled business logic exception occurred during form load time.

InfoPath Forms Services Web files list load failed - Event 5369 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services Web files list load failed

Event ID: 5369

Summary: InfoPath Forms Services includes a file named ifsFileNames.xml. This file contains pointers to downloadable files, such as scripts and images for forms.

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

- IfsFileNames.xml cannot be found.
- InfoPath forms cannot be opened in a Web browser.
- This event appears in the event log: Event ID: 5369 Description: Failed to load product component ifsFileNames.xml. Web virtual root may be installed improperly. (User: <Username>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Type: <Exception Type>, Exception Message: <Exception Message>)

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

- The ifsFileNames.xml file is missing or is not valid on one or more front-end Web servers in the farm.
- Internet Information Services (IIS) is not configured correctly.

Resolution: Run Office Server Setup

- On the affected servers, run the Microsoft SharePoint Server Setup Wizard and select the **Repair** option.

Resolution: Check the Internet Information Services configuration

- If the problem persists, Internet Information Services (IIS) might not be configured correctly. In this case, start IIS Manager and undo any changes to the virtual directory that were made after Microsoft SharePoint Server was installed.

InfoPath Forms Services postback failure - Event 5374 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services postback failure

Event ID: 5374

Summary: Some form actions, such as running business logic, switching views, or submitting the form, require a postback to the server. An error occurred when this postback was processed by InfoPath Forms Services in Microsoft SharePoint Server 2010.

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

- An error message appears when filling out the form.
- This event appears in the event log: Event ID: 5374 Description: There was a form postback error. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>, Type: <ExceptionType>, Exception Message: <ExceptionMessage>)

Cause: An internal server error occurred.

InfoPath Forms Services conflicting assembly identities found - Event 5733 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services conflicting assembly identities found

Event ID: 5733

Summary: InfoPath form templates can contain managed code that is stored in a business logic assembly. When a form template that contains managed code is deployed to a server on which InfoPath Forms Services runs, the business logic assembly must have a unique, strong name.

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

- An error message appears during deployment of the form template on the Microsoft SharePoint Foundation server.
- This event appears in the event log: Event ID: 5733 Description: Two business logic assemblies with the same identity, <AssemblyName>, exist. The following forms are associated with the assemblies: <FormName1>, <FormName2>. The server should never be in this state since each business logic assembly must have a unique identity. One of the forms and its associated assembly should immediately be removed. (User: <UserName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>)

Cause: A form template was deployed that contains a managed code assembly that conflicts with another managed code assembly that has been deployed.

InfoPath Forms Services business logic cannot be serialized - Event 5734 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services business logic cannot be serialized

Event ID: 5734

Summary: In InfoPath Forms Services in Microsoft SharePoint Server 2010, the FormState property bag provides a way to maintain business logic state across multiple server postbacks. For example, in a particular method in business logic, local variables can be persisted in the FormState property bag for multiple postbacks. All objects stored in the property bag must be capable of being serialized.

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

- An error occurs when executing custom code in the form.
- This event appears in the event log: Event ID: 5734 Description: Cannot persist business logic type <ObjectType> because it is not serializable. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>)

Cause: Business logic in a form template attempted to store a non-serializable type in the FormState property bag.

InfoPath Forms Services DoS postbacks per session - Event 5736 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services DoS postbacks per session

Event ID: 5736

Summary: Some InfoPath form controls, actions, and features require the browser to communicate with the server during a form session. This exchange of data during the session is called a postback, and usually occurs when a form feature has to send data to the server for processing. Unnecessary postbacks impose an additional load on both the browser and the server. To protect the server, a threshold is set for the maximum number of postbacks per session. This limits the number of postbacks that can be executed during a single session when a user is filling out a form, and prevents malicious users from trying to bring down the server.
A user has exceeded the threshold that was set for the number of postbacks allowed per form session. When this condition occurs, the user session is stopped to protect the server.

Symptoms: The following message may appear in the event log: Event ID: 5736 DescriptionNumber of postbacks, <integer>, has exceeded <integer>, the maximum allowable value per session. This value is configurable and can be changed by the administrator. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>)

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

- A user has tried a denial of service (DoS) attack against a server on which InfoPath Forms Services in Microsoft SharePoint Server 2010 runs.
- The number of postbacks allowed per InfoPath form session state is too low.

Resolution: **Check the server logs for signs of a DoS attack**

- Search the Windows event log and the Internet Information Services (IIS) logs for indications of a DoS attack. If this is a DoS attack and if an administrator-approved form template is affected, remove the form template from the site collection or deactivate the form template.
  To check the Windows event log:
  1. Open the Windows Event Viewer.
  2. Search for event ID 5736 in the Windows application event log.
  3. In the event description, check the Form ID. If there are multiple events for the same form ID, this might indicate that a malicious user has deployed a form that is causing many postbacks in an attempt to bring down the server.
     To check the IIS logs:
  1. Go to \inetpub\logs to review the IIS logs.
  2. The Internet Information Services (IIS) log entries can be correlated to the event log information. If many GET requests for a specific form are in the IIS log and if this form is also causing many postbacks, which are being logged, a DoS attack might be in progress.
  3. The IIS log entries also contain the IP address of the machine that sent the request.
     To deactivate a form template from a site collection:

1. On the SharePoint Central Administration Web site, on the Quick Launch click **General Application Settings**, and in the **InfoPath Forms Services** section click **Manage form templates**.
2. In the list of form templates click the form template that you want to deactivate, and in the drop-down list click **Deactivate from a Site Collection**.
3. On the Deactivate Form Template: <template> page, in the **Deactivation Location** section, select the site collection and then click **OK**.

   To remove a form template completely:

1. On the Central Administration page, on the Quick Launch, click **General Application Settings** and in the **InfoPath Forms Services** section click **Manage form templates**.
2. In the list of form templates click the form template that you want, and in the drop-down list click **Remove Form**.

Resolution: Increase the number of postbacks allowed per session

1. On the Central Administration page, on the Quick Launch, click **General Application Settings** and in the **InfoPath Forms Services** section click **Configure InfoPath Forms Services**.
2. In the **Thresholds** section, increase the value for number of postbacks allowed per session.

   Note:

   Increasing the value of this setting can adversely affect server performance and increase the risk of DoS attacks on the server.

InfoPath Forms Services DoS actions per postback - Event 5737 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services DoS actions per postback
Event ID: 5737
Summary: InfoPath Forms Services forms record every action in a temporary event log that is stored in the browser client. When a server postback is necessary, the recorded log data is sent and the actions are replayed on the server. A postback is triggered when a user updates a form or performs an action that requires a postback, such as running business logic or submitting the form. To prevent InfoPath Forms Services from dedicating too much time to a single postback, a threshold setting for the maximum number of actions per postback is defined on the server. This setting limits the number of actions that can be replayed on the server in a single postback and prevents malicious users from creating their own event logs and bringing down the server.
A user has exceeded the threshold set for the number of form actions allowed per postback. When this occurs, InfoPath Forms Services terminates the user session in order to protect the server.
Symptoms: The following message may appear in the event log: Event ID: 5737 Description: Number of form actions, <integer>, has exceeded <integer>, the maximum allowable value per request. This value is configurable and can be changed by the administrator. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>)
Cause: One or more of the following might be the cause:

- A user has attempted a denial of service (DoS) attack against a server on which InfoPath Forms Services runs.
- The number of actions allowed per postback is too low.

Resolution: Check the Windows event log for signs of a DoS attack

- Search the Windows event log for signs of a DoS attack. If this is a DoS attack and if an administrator-approved form template is affected, remove the form template from the site collection or deactivate the form template.
  To check the Windows event log:
  1. Open the Windows Event Viewer.
  2. Search for event ID 5737 in the Windows application event log.
  3. In the event description, check the Form ID. If there are multiple events for the same form ID, this might indicate that a malicious user has deployed a form that has many actions per postback in an attempt to bring down the server.
     To deactivate a form template from a site collection:
  1. On the SharePoint Central Administration Web site, on the Quick Launch, click **General Application Settings** and in the **InfoPath Forms Services** section click **Manage form templates**.
  2. In the list of form templates click the form template that you want to deactivate, and in the drop-down list click **Deactivate from a Site Collection**.

3. On the Deactivate Form Template: <template> page, in the **Deactivation Location** section, select the site collection and click **OK**.

To remove a form template completely:

1. On the Central Administration page, on the Quick Launch, click **General Application Settings** and in the **InfoPath Forms Services** section click **Manage form templates**.
2. In the list of form templates click the form template that you want, and in the drop-down list click **Remove Form**.

Resolution: Increase the number of actions allowed per postback

1. On the Central Administration page, on the Quick Launch, click **General Application Settings** and in the **InfoPath Forms Services** section click **Configure InfoPath Forms Services**.
2. In the **Thresholds** section, increase the value for number of postbacks allowed per session.

   Note:

   Increasing the value of this setting can adversely affect server performance and increase the risk of DoS attacks on the server.

InfoPath Forms Services data adapter security error submit - Event 5758 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services data adapter security error submit
Event ID: 5758
Summary: InfoPath form templates can contain connections to external data sources. An error occurs if the security settings are not configured to allow connections to data sources on different domains.
Symptoms: One or more of the following symptoms might appear:

- An error message appears stating that the form cannot be submitted.
- This event appears in the event log: Event ID: 5758 Description: The form could not be submitted to <DataSource> because this action would violate cross-domain security restrictions. To allow this data connection for administrator-approved forms, enable full trust for the form template, or add the connection to a data connection library. For user forms, cross-domain connections must be enabled in SharePoint Central Administration, and all connections must be in a data connection library. For more information, please see the security documentation for InfoPath Forms Services. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>, Type: <ExceptionType>, Exception Message: <ExceptionMessage>)

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

- The form template security level is not set to full trust.
- The form template data connections are not defined in a data connection file.
- Cross-domain data access for user form templates is disabled in Central Administration.

InfoPath Forms Services solution cache churning - Event 5759 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services solution cache churning

Event ID: 5759

Summary: InfoPath Forms Services uses the ASP.NET cache to cache form templates when the form templates are first loaded on a front-end Web server. When the in-memory cache is full, the ASP page releases system memory and form templates are reloaded. This churning could indicate high memory pressure and performance that is less than optimal.

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

- InfoPath forms take longer than usual to open in the Web browser.
- This event appears in the event log: Event ID: 5759 Description: Form templates in the InfoPath Forms Services in-memory cache are being reloaded frequently. This could indicate high memory pressure and suboptimal performance.

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

- Low-memory conditions exist or a form is consuming a large amount of memory.
- Microsoft SQL Server is running on a front-end Web server.

Resolution: Restart Internet Information Services

- In a Command Prompt window, type **iisreset /noforce <computername>**.

Resolution: Install product updates

- Check Windows Update for updates and install the available product updates.

Resolution: Check SQL Server installation

- If you run SQL Server on a SharePoint Server front-end Web server — for example, in a single-server evaluation deployment — the ASP.NET cache releases system memory at a lower threshold than SQL Server, which could result in InfoPath Forms Services memory starvation.
- To mitigate this issue, configure SQL Server memory limits manually when SQL Server is installed on the same computer as SharePoint Server 2010. For more information, see Server memory options(*http://go.microsoft.com/fwlink/?LinkId=160542*).

Resolution: Upgrade hardware

- If all previous resolutions do not result in improved form performance, the problem might be hardware-related. Verify that the current server has adequate memory. Upgrade the memory if necessary.

InfoPath Forms Services data adapter security error query - Event 6932 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services data adapter security error query
Event ID: 6932
Summary: InfoPath Forms Services in Microsoft SharePoint Server 2010 form templates can contain connections to external data sources. An error can occur if the security settings are not configured to allow connections to data sources on different domains.
Symptoms: One or more of the following symptoms might appear:

- An error message stating that the form could not retrieve data from a data source.
- This event appears in the event log: Event ID: 6932 Description: The form could not retrieve data from <DataSource> because it would violate cross-domain restrictions. To allow this connection for administrator-approved form templates, enable full trust for the form template, or add the connection to a data connection library. For user form templates, cross-domain connections must be enabled in SharePoint Central Administration, and all connections must be in a data connection library. For more information, please see the security documentation for InfoPath Forms Services. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>, Type: <ExceptionType>, Exception Message: <ExceptionMessage>)

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

- The form template security level is not set to full trust.
- The form template data connections are not defined in a data connection file.
- Cross-domain data access for user form templates is disabled in SharePoint Central Administration.

InfoPath Forms Services solution load failure - Event 7056 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: InfoPath Forms Services solution load failure

Event ID: 7056

Summary: Users can open and fill out InfoPath forms in a Web browser. A form template could not be loaded by InfoPath Forms Services in Microsoft SharePoint Server 2010.

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

- An error message appears when opening an InfoPath form in a Web browser.
- This event appears in the event log: Event ID: 7056 Description: The form template failed to load. (User: <UserName>, Form Name: <FormName>, Request: <http://servername/_layouts/Postback.Formserver.aspx>, Form ID: <FormID>, Type: <ExceptionType>, Exception Message: <ExceptionMessage>)

Cause: An internal server error occurred when the form template was loaded.

InfoPath Forms Services not working due to invalid State Service configuration - Event 7898 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: State Service not configured for InfoPath Forms Service

Event ID: 7898

Summary: InfoPath Forms Services is not functional because the Microsoft SharePoint Server State Service configuration is not valid.

Symptoms: One or more of the following symptoms appears:

- InfoPath forms cannot be opened in a Web browser.
- Workflow forms cannot be opened in a Web browser.
- An error message appears when a form is loaded that states that the form cannot be rendered.
- This event appears in the event log: Event ID: 7898 Description: Microsoft SharePoint State Service is not configured correctly and cannot respond to requests. InfoPath Forms Services relies on Microsoft SharePoint State Service to function correctly. Check the SharePoint Maintenance Engine rules in SharePoint Central Administration for issues with Microsoft SharePoint State Service configuration.

Cause: The State Service, an InfoPath Forms Services dependency, is not configured correctly or is not associated with the Web application that hosts InfoPath forms.

Resolution: Create a State Service application 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 (PS C:\>), type the following command, and then press ENTER:
   ```
   $serviceApp = New-SPStateServiceApplication -Name "State Service"
   ```
   To create a State Service database and associate it with the service application, type the following command, and then press ENTER:
   ```
   New-SPStateServiceDatabase -Name "StateServiceDatabase" -ServiceApplication
   $serviceApp
   ```
   To create a State Service application proxy in the farm's default proxy group, and associate it with the service application, type the following command, and then press ENTER:
   ```
   New-SPStateServiceApplicationProxy -Name "State Service" -ServiceApplication
   $serviceApp -DefaultProxyGroup
   ```

For more information, see New-SPStateServiceApplication (*http://technet.microsoft.com/library/d9fe0940-2f01-45be-be77-905b8589e1a4(Office.14).aspx*), New-SPStateServiceDatabase (*http://technet.microsoft.com/library/221e439c-c501-4d4c-9d8a-171a01e67e25(Office.14).aspx*) and New-SPStateServiceApplicationProxy (*http://technet.microsoft.com/library/f20db78d-5f88-4ac1-85d8-5a2809bacefb(Office.14).aspx*).

Resolution: Associate a State Service proxy with the Web application

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 Web Applications**.
4. On the Manage Web Applications page, click the name of the Web application, and then click **Service Connections**.
5. Select the **State Service Proxy** check box.
   If a State Service Proxy is not listed, create a State Service application, a State Service database, and a State Service proxy.

Resolution: Create a State Service application by using the Farm Configuration Wizard

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 **Configuration Wizards**.
3. On the Configuration Wizards page, click **Launch the Farm Configuration Wizard**.
4. Ensure that **State Service** check box is selected, and then finish the Farm Configuration Wizard.

Managed Metadata services in SharePoint Server 2010 knowledge articles

Published: May 12, 2010

The articles in this section are knowledge articles for the Managed Metadata service. 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 with the Managed Metadata service in Microsoft SharePoint Server 2010.

In this section:

- Disk-based cache misconfigured - Event 5787 (SharePoint Server 2010)
- Metadata Service is unavailable - Event 8088 (SharePoint Server 2010)
- Disk-based cache at critical capacity (SharePoint Server 2010)
- Disk-based cache flushing (SharePoint Server 2010)
- Disk-based cache is compacting (SharePoint Server 2010)

Disk-based cache misconfigured - Event 5787 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Disk-based cache misconfigured

Event ID: 5787

Summary: To save time accessing frequently used static files, Microsoft SharePoint Server 2010 uses the disk-based cache to store these files on the disk of the front-end Web server instead of accessing these files directly from the database server. Farm administrators can configure settings for the cache by modifying the Web.config file on each front-end Web server. This alert indicates that the configuration settings of the disk-based cache are not valid.

Symptoms: The following event appears in the event log: Event ID: 5787 Description: Unable to connect publishing blob caching. Web.Config is not set up correctly. Cache is not valid. WebId is '<webid>', Url is '<url>'.

Cause: The configuration settings of the disk-based cache are not valid.

Resolution: **Correct the configuration settings in the Web.config file**

1. For information about how to configure the Web.config file, see Configure cache settings for a Web application (SharePoint Server 2010) (*http://technet.microsoft.com/library/478be4b7-1480-4f97-87c5-b18cd2436bce(Office.14).aspx*).

Metadata Service is unavailable - Event 8088 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Metadata Service is unavailable
Event ID: 8088
Summary: The managed metadata service provides access to one term store and the term sets that it contains, or it provides content types from a content type syndication hub.
Symptoms: One or more of the following symptoms might appear:

- The term store management tool displays an error that indicates that the term store is not available.
- Managed metadata controls and enterprise keyword controls may appear disabled.
- This event might appear in the event log: Event ID: 8088 Description: The Managed Metadata Service '<Service>' is inaccessible.

Cause: This can occur if the server is offline or the managed metadata service is not started or has been disabled. The service might not start if the application pool account does not have sufficient permissions to the term store.
Resolution: **Verify the application pool account permissions**

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, in the **Type** column, click the managed metadata service application, and then click **Properties**.
5. In the **Create New Managed Metadata Service** dialog box, in the **Application Pool** section, record the name of the application pool and the application pool account name.
6. Click **Cancel**.
7. Log on as a member of the local Administrators group.
8. In Central Administration, on the Service Applications page, in the **Type** column, click the managed metadata service application, and then click **Permissions**.
9. Confirm that the account that you recorded in step 5 has one of the following permissions:
    - Read Access to Term Store
    - Read and Restricted Write Access to Term Store
    - Full Access to Term Store

Other Resources

Grant permission to access the managed metadata service (*http://technet.microsoft.com/library/631ccca6-a1c9-4999-b0c0-2025610e7f4c(Office.14).aspx*)
Managed metadata overview (*http://technet.microsoft.com/library/e580fcae-b768-4b81-afda-c037fbd7bd6d(Office.14).aspx*)

Disk-based cache at critical capacity (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Disk-based cache at critical capacity

Event ID: None

Summary: To save time accessing frequently used static files, Microsoft SharePoint Server 2010 uses the disk-based cache to store these files on the disk of the front-end Web server instead of accessing these files directly from the database server. Farm administrators can configure settings for the cache by modifying the Web.config file on each front-end Web server. This alert indicates that the disk-based cache is too full to serve files efficiently. When the disk-based cache is full, it will start *compacting* — that is, removing files from the cache to free up space. Compacting is a resource-intensive process that might affect the performance of the front-end Web server.

Symptoms: The **Blob Cache fill ratio** performance counter threshold has been exceeded.

Cause: The configured size for the disk-based cache is smaller than the total size of frequently accessed files for the Web application.

Resolution: Increase the size of the disk-based cache

1. For information about how to configure the Web.config file, see Configure cache settings for a Web application (SharePoint Server 2010) (*http://technet.microsoft.com/library/478be4b7-1480-4f97-87c5-b18cd2436bce(Office.14).aspx*).

Resolution: Manually flush the disk-based cache 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:

```
Add-PSSnapin Microsoft.SharePoint.Powershell
Write-Host "Flush the Blob Cache for the application containing the specified site collection"
$site = Get-SPSite -Identity <URL>
[System.Reflection.Assembly]::LoadWithPartialName("Microsoft.SharePoint.Publishing")
Write-Host "Flushing..."
[Microsoft.SharePoint.Publishing.PublishingCache]::FlushBlobCache($site.WebApplication)
Write-Host "Flushed Cache for:" $site.WebApplication
```

   Where:

   - *<URL>* is the URL in the event details.

Resolution: Change the file types to be stored by the disk-based cache

1. For information about how to configure the Web.config file, see Configure cache settings for a Web application (SharePoint Server 2010) (*http://technet.microsoft.com/library/478be4b7-1480-4f97-87c5-b18cd2436bce(Office.14).aspx*)

Disk-based cache flushing (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Disk-based cache flushing

Event ID: None

Summary: To save time accessing frequently used static files, Microsoft SharePoint Server 2010 uses the disk-based cache to store these files on the disk of the front-end Web server instead of accessing these files directly from the database server. Farm administrators can configure settings for the cache by modifying the Web.config file on each front-end Web server. This alert indicates that a user or administrator has made a change that caused some of the disk-based cache contents to become invalid. This will initiate the process of cache *flushing*, which is removing a large set of items from the cache. Flushing is a resource-intensive process that can affect the performance of the front-end Web server. When the flushing process is finished, the performance of the front-end Web server will return to normal.

Tip:
If you want to reduce the frequency of the flushing processes, you can perform one or more of the resolutions in this article. You can also ensure that users or administrators are not making changes that might invoke a cache flush process during peak usage hours.

Symptoms: The **Blob cache flushes / second** performance counter threshold has been exceeded.

Cause: A user or administrator made a change that caused the cached contents to become invalid. Examples include modifying content types of cached items, updated the schema of lists, or changing permissions on a list or library.

Resolution: Change the file types to be stored by the disk-based cache

1. For information about how to configure the Web.config file, see Configure cache settings for a Web application (SharePoint Server 2010) (*http://technet.microsoft.com/library/478be4b7-1480-4f97-87c5-b18cd2436bce(Office.14).aspx*)

Disk-based cache is compacting (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Disk-based cache is compacting

Event ID: None

Summary: To save time accessing frequently used static files, Microsoft SharePoint Server 2010 uses the disk-based cache to store these files on the disk of the front-end Web server instead of accessing these files directly from the database server. Farm administrators can configure settings for the cache by modifying the Web.config file on each front-end Web server. This alert indicates that the disk-based cache is too full to serve files efficiently and is currently in the process of *compacting* — that is, removing files from the cache to free up space. Compacting is a resource-intensive process that can affect the performance of the front-end Web server. When the compacting process is finished, the performance of the front-end Web server will return to normal.

Tip:
If you want to reduce the frequency of the compacting processes, you can perform one or more of the resolutions in this article.

Symptoms: The **Total number of cache compactions** performance counter threshold has been exceeded.

Cause: The disk-based cache has reached its maximum size.

Resolution: Increase the size of the disk-based cache

1. For information about how to configure the Web.config file, see Configure cache settings for a Web application (SharePoint Server 2010) (*http://technet.microsoft.com/library/478be4b7-1480-4f97-87c5-b18cd2436bce(Office.14).aspx*).

Resolution: Manually flush the disk-based cache 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:

```
Add-PSSnapin Microsoft.SharePoint.Powershell
Write-Host "Flush the Blob Cache for the application containing the specified site collection"
$site = Get-SPSite -Identity <URL>
[System.Reflection.Assembly]::LoadWithPartialName("Microsoft.SharePoint.Publishing")
Write-Host "Flushing..."
[Microsoft.SharePoint.Publishing.PublishingCache]::FlushBlobCache($site.WebApplication)
Write-Host "Flushed Cache for:" $site.WebApplication
```

   Where:
   - *<URL>* is the URL in the event details.

Resolution: Change the file types to be stored by the disk-based cache

1. For information about how to configure the Web.config file, see Configure cache settings for a Web application (SharePoint Server 2010) (*http://technet.microsoft.com/library/478be4b7-1480-4f97-87c5-b18cd2436bce(Office.14).aspx*).

PerformancePoint Services in SharePoint Server 2010 knowledge articles

Published: May 12, 2010

The articles in this section are knowledge articles for PerformancePoint Services in Microsoft SharePoint Server 2010. 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 PerformancePoint Services.

In this section:

- PerformancePoint Services - login failed - Events 5_6_37_45 (SharePoint Server 2010)
- PerformancePoint Services - Service unavailable - Events 33_39 (SharePoint Server 2010)
- PerformancePoint Services - Database Connection Failed - Event 34 (SharePoint Server 2010)

PerformancePoint Services - login failed - Events 5 6 37 45 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Performance Point-login failed

Event ID: 5, 6, 37, and 45

Summary: PerformancePoint Services in Microsoft SharePoint Server 2010 uses an unattended service account for data connectivity integration. PerformancePoint Services uses this account to access data sources on behalf of the user who is running or creating a dashboard. When the user creates a data source and does not select **Per-user Identity** for authentication, the data source connection will run as the unattended service account.

Symptoms: One or more of the following events appears in the event log:

- Event ID: 5 Description: Shared account is misconfigured.
- Event ID: 6 Description: Data source shared account is misconfigured.
- Event ID: 37 Description: Data Source cannot get Windows identity.
- Event ID: 45 Description: Get unattended service account password failed.

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

- The unattended service account is set to an account that is not valid or is configured incorrectly.
- The Secure Store is not accessible. For more information about resolving this problem, see Secure Store could not retrieve master encryption key - Event 7535 (SharePoint Server 2010).

Resolution: Confirm the unattended service account settings

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 Manage Service Applications page, click the name of the PerformancePoint Services service application.
5. On the Manage PerformancePoint Services page, click **PerformancePoint Service Application Settings**.
6. On the PerformancePoint Service Application Settings page, verify that the user account is correct by typing a domain user name and password in the **Secure Store and Unattended Service Account** section, and then clicking **OK**.

Resolution: Confirm the application pool account

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 Manage Service Applications page, select the name of the PerformancePoint Services service application, and then click **Properties** in the ribbon.
5. On the Edit PerformancePoint Service Application page, in the **Application Pool** section, verify that the application pool account is correct.

PerformancePoint Services - Service unavailable - Events 33 39 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: PerformancePoint Services service unavailable

Event ID: 33 and 39

Summary: The PerformancePoint Services in Microsoft SharePoint Server 2010 service is unavailable.

Symptoms: One or more of the following symptoms appears:

- Users receive error messages saying that PerformancePoint Services is unavailable or cannot be found.
- The application pool appears as stopped in Internet Information Services (IIS) Manager.
- This event appears in the event log: Event ID: 33 Description: Service application is not configured for Web Application.
- This event appears in the event log: Event ID: 39 Description: Service application is unavailable.

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

- The application pool has not been started.
- The password for the application pool service account has changed.
- There is an internal service error.

Resolution: Start the application pool

1. In IIS Manager, connect to the application server.
2. Expand the server node, and then click **Application Pools**.
3. Ensure that the PerformancePoint Services application pool is started. If it is not, right-click the name of the application pool, and then click **Start**.
   If the application pool is started, right-click the name of the application pool, and then click **Recycle**.
4. If the application pool does not start, follow the steps in "Resolution: Verify the application pool account," later in this article, and then repeat these steps to start the application pool.

Resolution: Verify the application pool account

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 Manage Service Applications page, select the name of the PerformancePoint Services service application, and then click **Properties** in the ribbon.
5. On the Edit PerformancePoint Service Application page, in the **Application Pool** section, make a note of the name of the application pool. This information will be used later in this procedure.
6. In IIS Manager, connect to the application server.
7. Expand the server node, and then click **Application Pools**.

8. Right-click the name of the application pool that you recorded in step 5, and then click **Advanced Settings**.
9. In the **Advanced Settings** dialog box, under **Process Model**, click the ellipsis next to the **Identity** account.
10. In the **Application Pool Identity** dialog box, click **Set**.
11. In the **Set Credentials** dialog box, type the domain account name and password, confirm the password, and then click **OK**.
12. In the **Application Pool Identity** dialog box, click **OK**.
13. In the **Advanced Properties** dialog box, click **OK**.

PerformancePoint Services - Database Connection Failed - Event 34 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: PerformancePoint Services database connection failed
Event ID: 34
Summary: The PerformancePoint Services in Microsoft SharePoint Server 2010 service requires access to a database to store annotations, temporary information, and filters.
Symptoms: One or more of the following symptoms appears:

- Users cannot navigate reports, render scorecards, or navigate OLAP views.
- The application pool appears as stopped in Internet Information Services (IIS) Manager.
- This event might appear in the event log: Event ID: 34 Description: Store cannot connect to database.

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

- The password for the application pool service account was changed, or the account is not the correct one.
- The PerformancePoint Services database is corrupted, or it was deleted and restored from a backup database.

Resolution: Ensure that the application pool identity has the correct SQL Server permissions

1. Verify that the user account that is performing this procedure is a member of the SQL Server **db_owner** fixed database role for the PerformancePoint Services database.
2. Open SQL Server Management Studio and connect to the database server.
3. In Object Explorer, expand **Databases**.
4. Expand the PerformancePoint Services database node. Expand **Security**, and then expand **Users**.
   Note:
   To determine the name of the PerformancePoint Services database, follow the steps in "To identify the PerformancePoint database by using Windows PowerShell," later in this article.
5. Ensure that the application pool account is listed as a SQL login.
   Note:
   To determine which application pool the service uses, follow the steps in "To identify the application pool," later in this article.
6. If the account is not listed, add the account as a SQL Server login with the **db_owner** fixed database role for the PerformancePoint Services database by following these steps:
   a) Right-click the **Users** node, and then click **New User**.
   b) On the **General** tab, select the **Login name** option, and then click the ellipsis.
   c) In the **Select Login** dialog box, type the login name, or click **Browse** and select the login from the list.
   If the application pool account does not appear in the list, it must be added to the database server as a SQL Server login.
   d) In the **Select Login** dialog box, click **OK**.

e) In the **Database User** dialog box, on the **General** tab, under **Database role membership**, ensure that the **db_owner** check box is selected, and then click **OK**.

7. If the account is listed, verify that it has the **db_owner** fixed database role for the PerformancePoint Services database by doing the following:
   a) Right-click the login, and then click **Properties**.
   b) In the **Database User** dialog box, under **Database role membership**, ensure that the **db_owner** check box is selected, and then click **OK**.

To identify the PerformancePoint database 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 (PS C:\>), type the following command, and then press ENTER:
   Get-SPPerformancePointServiceApplication
   Record the name of the database from the `SettingsDatabase` property.

For more information, see Get-SPPerformancePointServiceApplication (*http://technet.microsoft.com/library/ba040c45-9636-4ac4-a80b-2d3c9e0b71d1(Office.14).aspx*).

Resolution: Verify the application pool account by using Central Administration

1. In IIS Manager, connect to the server that is running Central Administration.
2. Expand the server node, and then click **Application Pools**.
3. Right-click the application pool, and then click **Advanced Properties**.
   Note:
   To determine which application pool the service uses, follow the steps in "To idenitfy the application pool," later in this article.
4. In the **Advanced Properties** dialog box, under **Process Model**, click the ellipsis next to the **Identity** account.
5. In the **Application Pool Identity** dialog box, click **Set**.
6. In the **Set Credentials** dialog box, type the domain account name and password, confirm the password, and then click **OK**.
7. In the **Application Pool Identity** dialog box, click **OK**.
8. In the **Advanced Properties** dialog click **OK**.
   Note:
   You do not have to restart the application pool for the changes to take effect.

Resolution: Restore the database from a backup 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 (PS C:\>), type the following command, and then press ENTER:
   Restore-SPFarm -Directory <Backup folder name> -RestoreMethod {New | Overwrite} -Item <Content database name> [-BackupId <GUID>] [-Verbose]
6. To reattach the restored database to the farm, type the following command, and then press ENTER:
   Set-SPPerformancePointServiceApplication -SettingsDatabase <Database name>

For more information, see Restore-SPFarm (*http://technet.microsoft.com/library/8e18ea80-0830-4ffa-b6b6-ad18a5a7ab3e(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.

To identify the application pool

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 (PS C:\>), type the following command, and then press ENTER:
   Get-SPPerformancePointServiceApplication
   Record the name listed after `Name=`
   under `ApplicationPool`
   .
6. At the Windows PowerShell command prompt (PS C:\>), type the following command, and then press ENTER:
   Get-SPServiceApplicationPool | Where-Object {&_.Name -eq " <ApplicationPool name from previous step>" | Format-Table -Property Name,DisplayName,Id
   The application pool name is the GUID listed as `Id`
   .

For more information, see Get-SPServiceApplicationPool (*http://technet.microsoft.com/library/079fd20b-2542-4d03-8b45-2da83cebe0ff(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.

Search services in SharePoint Server 2010 knowledge articles

Published: May 12, 2010

The articles in this section are knowledge articles for Microsoft Search Server 2010 services in Microsoft SharePoint Server 2010. 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 Search Server 2010.

In this section:

- Search gatherer disk is full - Event 23 (SharePoint Server 2010)
- Search database out of space - Event 52 (SharePoint Server 2010)
- Search relegate query component - Event 58 (SharePoint Server 2010)
- Search query critical error - Event 60 (SharePoint Server 2010)
- Search indexer initialization index failed - Event 71 (SharePoint Server 2010)
- Search index corrupted - Events 74 93 (SharePoint Server 2010)
- Search indexer low disk space - Event 80 (SharePoint Server 2010)
- Search propagation communication error - Event 92 (SharePoint Server 2010)
- Search gatherer host unavailable - Event 114 (SharePoint Server 2010)
- Search administration component failed - Event 121 (SharePoint Server 2010)
- Search crawl component index path error - Events 2588 2589 (SharePoint Server 2010)
- Search Query and Site Settings Service is not running (SharePoint Server 2010)
- SharePoint Server 2010 search is not running (SharePoint Server 2010)

Search gatherer disk is full - Event 23 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search gatherer disk is full

Event ID: 23

Summary: As the crawler searches content to create an index, it creates files in a temporary location. This temporary location can grow in size over time. The disk where the temporary location is located is running out of space.

Symptoms: Microsoft SharePoint Server 2010 experiences the following symptoms when it crawls content:

- The crawl does not progress and seems to stall.
- The crawl logs show no new crawled documents.
- This event appears in the event log: Event ID: 23 Description: The crawl has been delayed because a disk is full.

Cause: The disk on which the search crawler creates temporary files is running out of space.

Resolution: **Free up disk space**

- Free up space on the disk on which the crawler creates an index as it searches content.
  To free up disk space:
  1. Use Disk Cleanup to delete temporary files on the drive where the index files are stored. Use the procedure following this one to determine the location of the index files.
     Note:
     If the temporary files are located on a drive other than the operating system drive (drive C), you must restart the Microsoft Search Server 2010 service (OSearch) to test the performance of the crawler after you delete the temporary files.
  2. After Disk Cleanup is complete, test the performance of the crawler. If the crawler is not searching content, delete unnecessary files and folders on the selected drive.
  3. If you cannot clear any disk space, restart the Search Server 2010 service (OSearch). Restarting the Search Server 2010 service (OSearch) recreates the Temp directory for index files. In a Command Prompt window, run the command **net stop osearch14** to stop the search service. Run the command **net start osearch14** to restart the search service.
     To determine the location of the index files:
  1. Run **regedit**.
  2. If the following registry flag is set, the system Temp directory is used for the index files:**HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\Search\Global\Gathering Manager\UseSystemTemp**
  3. If the system Temp directory is not used for the index files, the location of the index files is indicated by the following registry key:**HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\Search\Global\Gathering Manager\TempPath**

Search database out of space - Event 52 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search database out of space

Event ID: 52

Summary: Each search application depends on the following sets of databases for storing a specific type of content:

- One or more search property databases store metadata about the crawled items.
- One or more search crawl databases store information about when and where items were crawled.
- A search administration database stores information that is specific to managing the search application.

Symptoms: As more items are crawled, the size of the property and crawl database increases over time. At some point, Microsoft SharePoint Server 2010 might display the following symptoms:

- The crawl does not progress and seems to stall.
- The crawl logs show no new crawled documents.
- This event appears in the event log: Event ID: 52 Description: The database is out of space. Source:<data> Code:<data> occurred <data> time(s) Description: <data>

Cause: One or more search databases are out of disk space.

Resolution: Check storage space

1. Check the detailed error message for the location and name of the database. Use the following procedure on the server on which the instance of Microsoft SQL Server is running to determine whether the search database has adequate storage space available:
2. Start SQL Server Management Studio.
3. Log on and expand the Databases container.
4. Right-click the name of the database with the issue, and then click **Properties**.
5. On the **General** tab, click **Size** to determine the current file size.

Resolution: Move the search database

- After you create a larger storage space, move the search database to the new location by using the Detach and Attach functions of SQL Server, as described in KB 220071.

Search relegate query component - Event 58 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search relegate query component

Event ID: 58

Summary: To support high availability, we recommend that multiple query components be created in the same query group. If a query component fails, the Microsoft Search Server 2010 service (OSearch) relegates the operations of the failed component to another query component to continue to serve queries.

Symptoms: Microsoft SharePoint Server 2010 experiences the following symptoms when serving queries:

- Under high query load there may be a decrease in query throughput.
- This event appears in the event log: Event ID: 58 Description: Query component <data> has been taken out of rotation due to this error: <data>. It will be retried in <data> seconds. <data>

  Note:

  The event details identifies the query component as <GUID>-<Query Component number>, for example "baebc6d3-4a2e-4584-9ff7-ad8866debe92-query-30". To identify the query component, use the second part, "query-30".

Cause: A query component was taken out of rotation for the reason presented in the event error message.

Resolution: Restart the search service

1. Propagation to the affected query component will be automatically retried in the time period given in the event. If the retry attempt fails, stop and restart the Microsoft Search Server 2010 service (OSearch) by opening a Command Prompt window and type **net stop osearch14** to stop the search service. Type **net start osearch14** to restart the search service.

If failure persists, add a new query component as a mirror in the same query group as the failed query component.

Resolution: Add a new query component

1. On the SharePoint Central Administration Web site, click **General Application Settings** and in the **Search** section click **Farm-wide Search Dashboard**.
2. In the **Search Application Topology** section find the search application that generated the event, and then click **Modify Topology**.
3. On the Topology for Search Application: <searchappname> page, select the failed query component from the topology list, and then click **Add Mirror**.
4. In the **Add query component** dialog box, select the query server and associated metadata database for the new query component, and then click **OK**.
5. Click **Apply Topology Changes**. The changes are processed for the search application and the index is copied from the failed query component to the new query component.
6. Click the failed query component and click **Delete**.
7. The topology removes the index from the failed query component and deletes the index.

Search query critical error - Event 60 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search query critical error

Event ID: 60

Summary: In scenarios where a query component has no mirror and lacks high-availability, or all query components in a query group fail, it is possible that query results will not be served for a portion of the index.

Symptoms: Microsoft SharePoint Server 2010 experiences the following symptoms when serving queries:

- Query latency increases or queries fail.
- This event appears in the event log: Event ID: 60 Description: Cannot take the last query component out of rotation. Check previous event logs to determine cause. Propagation may be necessary. <data>

  Note:

  The event details identifies the query component as <GUID>-<Query Component number>, for example “baebc6d3-4a2e-4584-9ff7-ad8866debe92-query-30”. To identify the query component, use the second part, “query-30”.

Cause: A query component has been taken out of rotation due to the reason present in the previous search event's error message.

Resolution: Restart the search service

1. Stop and restart the Microsoft Search Server 2010 service (OSearch).
2. Open a Command Prompt window and type **net stop osearch14** to stop the search service. Type **net start osearch14** to restart the search service.

If failure persists, add a new query component as a mirror in the same query group as the failed query component.

Resolution: Add a new query component

1. On the SharePoint Central Administration Web site, click **General Application Settings** and in the **Search** section click **Farm-wide Search Dashboard**.
2. In the **Search Service Applications** section, from the drop-down list select the search application that generated the event, and then click **Modify Topology**.
3. On the Topology for Search Service Application page, click the failed query component in the topology list, and then select **Add Mirror** from the component’s drop-list.
4. In the **Add mirror query component** dialog box, select the query server and associated metadata database for the new query component, and then click **OK**.
5. Click **Apply Topology Changes**. The changes are processed for the search application and the index is copied from the failed query component to the new query component.
6. Click the failed query component and click **Delete**.
7. The topology removes the index from the failed query component and deletes the component.

Search indexer initialization index failed - Event 71 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search indexer initialization index failed

Event ID: 71

Summary: The key process that drives crawls and queries is mssearch.exe. This process hosts the crawl and query components for search. During search initialization, Microsoft SharePoint Foundation 2010 displays the symptoms described while initializing the mssearch.exe process or a crawl or query component.

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

- Crawl or query search activities that involve the component stall.
- The system automatically retries every minute silently. If two events are thrown within 30 minutes, action should be taken.
- This event appears in the event log: Event ID: 71 Description: Content index on <data> could not be initialized. Error <data>. <data>

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

- Could not access index files on disk
- Lack of available memory
- Index corruption

Resolution: Correct resources on the server

- Resolve any issues with accessing index files. The location of the index file is provided in the **Edit Query Component** dialog. Ensure that the WSS_ADMIN_WPG security group account has Full Control access to the index files folder.
  To see the location of an index file:
  1. On the SharePoint Central Administration Web site, on the Quick Launch click **General Application Settings**.
  2. On the General Application Settings page, under **Search**, click **Farm-wide Search Dashboard**.
  3. On the Farm-Wide Search Dashboard page, under **Search Service Applications**, click **Modify Topology** next to the search service you need to configure.
  4. On the Topology for Search Service Application page, under **Index Partition**, click the query component that needs to be configured.
  5. Click **Index Component** and click **Edit Properties**. The location of the index file appears in the **Indexing Directory** section.
  6. Click **Edit Properties**.
  7. In **Edit Query Component** dialog the location of the index files is displayed in the **Location of Index** box under **Location of Index**.
- Ensure that the WSS_ADMIN_WPG security group account has Full Control access to this location.

Resolution: Restart the search server service

- If low memory is the issue, stop and restart the Microsoft Search Server 2010 service (OSearch). In a Command Prompt window, run the command **net stop osearch14** to stop the search service. Run the command **net start osearch14** to restart the search service.

Resolution: Fix the index corruption

- If an index corruption event ID 74 or 93 accompanies this event, correct the issue by using the resolutions for the specified type of index corruption event.

Search index corrupted - Events 74 93 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search index corrupted

Event ID: 74 and 93

Summary: The key process that drives search crawls and queries is Mssearch.exe. This process hosts the crawl and query components for search.

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

- Search activities (crawl or query) that involve the query component are stalled.
- One or more of these events might appear in the event log:
  - Event ID: 74 Description: <data> An index corruption of type <data> was detected in catalog <data>. Stack trace is <data>.

    Warning:
    The system will not re-run the crawl after it raises this error.
  - Event ID: 93 Description: An index corruption was encountered while attempting to restart an aborted merge. A catalog reset of search application <data> may be necessary.

    Warning:
    The system will automatically silently retry to restart the merge. If two events are raised within 30 minutes, you should resolve the problem.

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

- Disk failures are affecting the index files.
- The index is corrupt.

Resolution: Check the disk for corruption

1. On the server listed in the event details, run the **Chkdsk** command to check the disk for errors.

Resolution: Create a new crawl component

1. On the SharePoint Central Administration Home page, click **General Application Settings**.
2. On the General Application Settings page, in the **Search** section, click **Farm Search Administration**.
3. On the Farm Search Administration page, in the **Search Service Applications** section, click **Modify Topology** for the correct Search service application.
4. On the Manage Search Topology page, click **New**, and then select **Crawl Component** from the context menu.
5. In the **Add Crawl Component** dialog box, select the correct farm server and crawl database, and type the location for the index if it is different from the location shown. Click **OK**.
6. On the Manage Search Topology page, click **Apply Topology Changes**.

Resolution: Recover the query component from a mirror database

1. If this component is part of a mirror database, follow these steps to enumerate a list of query components, and — from that list — use the correct query component ID to restore the component by using the **RequestRecover** method.
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:
```
$app = Get-SPEnterpriseSearchServiceApplication "<Name>"

$qt = Get-SPEnterpriseSearchQueryTopology -SearchApplication $app -Active
$querycomponents = Get-SPEnterpriseSearchQueryComponent -QueryTopology $qt

foreach ($qc in $querycomponents) {"Name: " +  $qc.Name + "  Index Location: " +
$qc.IndexLocation + "  ID: " + $qc.ID + "   State: " + $qc.State}
```
   Where:
   - *<Name>* is the name of the Search service application given in the event details. This command produces a list of query components. Find the identity ($qc.ID) of the query component that has the issue. Check the component's **State** value. You will use this identity in the next step.
7. Using the identity that you found in step 6, use Windows PowerShell to restore the component.
   At the Windows PowerShell command prompt, type the following command:
```
$qc = Get-SPEnterpriSesearchQueryComponent -Identity "<ID>" -QueryTopology $qt

$qc.RequestRecover()
```
   Where:
   - *<ID>* is the identity of the query component that you obtained from the list in step 6.

Search indexer low disk space - Event 80 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search indexer low disk space

Event ID: 80

Summary: As the crawler searches content to create an index, it creates index files to use for retrieving search results. As more items are indexed, the index files grow in size:

Symptoms: Microsoft SharePoint Server 2010 displays the following symptoms while the crawler searches content:

- The crawl does not progress and appears to stall.
- The crawl logs show no new crawled documents.
- This event appears in the event log: Event ID: 80 Description: <data> Very low disk space was detected for catalog <data>. Please free up some disk space so that crawling can continue.

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

- If the error was reported against a crawl component, the storage location associated with the crawl component is running out of space. Remove unnecessary files and folders on that drive to gain more disk space.
- The storage location associated with the index of the query component is running out of space.
  - If the error was reported against a query component, the search application likely has outgrown the storage capacity. In this case, move the index that is associated with the query component to a larger storage device.
  - If the search application index contains more than 10 million items per query component, add another query group to the application, on a new server.

Resolution: Reclaim disk space for a crawl component

1. Use Disk Cleanup to delete temporary files on the drive where the index files are stored.
2. After Disk Cleanup is complete, test the performance of the crawler. If the crawler is not searching content, delete unnecessary files and folders on the selected drive.

Resolution: Gain disk space by moving the query component index

1. On the SharePoint Central Administration Web page, click **General Application Settings** and in the **Search** section, click **Farm-wide Search Dashboard**.
2. In the **Search Service Application** section, select the search application that generated the event, and then click **Modify Topology**.
3. On the Topology for Search Service Application page, click **Query Component**, and then click **Edit Properties**.
4. In the **Location of Index** box, specify the new storage path for the query component index.
5. Click **OK**, and then click **Apply Topology Changes**.

   Note:

   This operation could take several minutes or longer depending upon the size of the indexes.
6. The topology will move the index to new storage path and delete the previous index

Resolution: Gain disk space by adding an another index partition on a new application server

1. On the Central Administration page, click **General Application Settings** and in the **Search** section click **Farm-wide Search Dashboard**.
2. In the **Search Service Application** section, from the drop-down list select the search application that generated the event, and then click **Modify Topology**.
3. On the Topology for Search Service Application page, click **New**, and then click **Index Partition and Query Component**.
4. In the **Add query component** dialog box, in the **Query Server** box, select the new application server and then click **OK**.
5. Click **Apply Topology Changes**. The changes are processed for the search application.
6. The topology splits the existing index partition into the new set of index partitions equally.

Search propagation communication error - Event 92 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search propagation communication error

Event ID: 92

Summary: As the crawler searches content to create an index, it creates index files to use for retrieving search results. These files are created by the crawl component in its storage area, and then propagated to the appropriate query components.

Symptoms: When Microsoft SharePoint Server 2010 is crawling content, and the crawl component cannot propagate to the query server, SharePoint Server 2010 displays the following symptoms:

- The crawl does not progress and appears to stall.
- The crawl logs show no new crawled documents.
- Users might not be able to view applications in their browsers, or the service may otherwise be unavailable
- This event appears in the event log: Event ID: 92 Description: A Crawl Component for search application '<data>' could not communicate with the query server '<data>'.

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

- The crawl component might have stale, or expired, credentials.
- Network issues might prevent the communication.
- The query server might be unresponsive.

Resolution: Authorization failure

- Make sure that search service credentials are up to date by rebooting the servers that had the problem.

Resolution: Correct Network connection issue

- Verify the network connection between the server that hosts the crawl component and the query server. If the network connection is working, examine the query component on the query server and make sure that the share exists and is writable from the crawler.

Resolution: Create a new query component

- If a file cannot be copied from the crawl component to the query server after rebooting servers, create a new query component in the same query group:
  1. On the SharePoint Central Administration Web site, click **General Application Settings** and in the **Search** section click **Farm-wide Search Dashboard**.
  2. On the Farm-wide Search Dashboard page, modify the search application that generated the event: Add a new query component in the same query group as the affected query component, and then remove the affected query component.
  3. In the topology, the index migrates from the affected query component to the new query component.

Search gatherer host unavailable - Event 114 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search gatherer host unavailable

Event ID: 114

Summary: As part of a search crawl, the servers that contain the crawl components communicate with content servers to retrieve the items for the crawl. Network communication problems between crawl server and content server will inhibit this crawl.

Symptoms: When Microsoft SharePoint Server 2010 is crawling content from a specific content server and network communication problems exist, Microsoft SharePoint Server might display the following symptoms:

- The crawl of the specific content server does not progress and appears to stall.
- The crawl logs show no new crawled documents for the specific content server.
- This event appears in the event log: Event ID: 114 Description: The server <data> is unavailable and could not be accessed. The server is probably disconnected from the network. Items from this server will be skipped by the crawl for the next 10 minutes <data>.

Cause: Network issues might be preventing the communication. Check that the content server is online and can connect to the crawl server.

Resolution: **Check the status of the content server**

1. On the SharePoint Central Administration Home page, click **Application Management**.
2. In the **Service Applications** section, click **Mangage service applications**.
3. On the Manage Service Applications page, click **Search Service Application**.
4. On the Search Administration page, in the **System Status** section, record the user account listed as the **Default content access account**.
5. On the left menu, in the **Crawling** section, click **Content Sources**.
6. On the Manage Content Sources page, click one of the content sources.
7. On the Edit Content Source page, in the **Start Address** section, record the URL from the textbox.
8. Open a Web browser as the user account you recorded in step 4 above and navigate to the URL you recorded in step 7 above. The page should load successfully.
9. If the content server is online and serves content to the crawl account, there is likely a network connection issue. For information to determine and repair the problem, see How to Troubleshoot Basic TCP/IP Problems (*http://go.microsoft.com/fwlink/?LinkId=157440*).

Search administration component failed - Event 121 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search administration component failed
Event ID: 121
Summary: A search administration component is created for each search service application. The search administration component modifies search application settings.
Symptoms: When the search service application is being modified and the administration component fails, one or more of the following symptoms might appear:

- The action of modifying the search application setting is not completed.
- This event appears in the event log: Event ID: 121 Description: The administration component for application '<data>' failed with exception '<data>' .

Cause: The search administration component is not correctly configured, or it cannot connect to the search application administration database.
Resolution: Verify that the search service application server can write to the database

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
2. From the search service application server, ping the database server to confirm that the servers can communicate over the network.
3. On the Central Administration Home page, click **Application Management**.
4. On the Application Management page, in the **Service Applications** section, click **Manage service applications**.
5. On the Service Applications page, select the search service application.
6. In the **Edit Properties** dialog box, note the Search Service Account name for the appropriate search service application.
7. Connect to the database server that hosts the search administration database for the given search service application by using the Search Service Account and password. Ensure the account has read/write permissions for the database.

Resolution: Create a new search administration component

1. If the problem persists, move the search administration component to a different server by using the **Set-SPEnterpriseSearchAdministrationComponent**Windows PowerShell cmdlet. For more information, see Set-SPEnterpriseSearchAdministrationComponent (*http://technet.microsoft.com/library/45a38f5b-92ee-4fbf-bd35-54b83f535b82(Office.14).aspx*).

Search crawl component index path error - Events 2588 2589 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search crawl component index path error

Event ID: 2588 2589

Summary: When each search crawl component is created, it creates a folder to use for storing index files that are used as part of the crawling process.

Symptoms: These events might appear in the event log:

- Event ID: 2588 Description: The index location for component <data> for application <data> is invalid: <data>.
- Event ID: 2589 Description: The index location for component <data> for application <data> is invalid: unauthorized access to <data>.

Cause: The location provided for the index did not exist, or the application did not have rights to create a folder for the index at the location.

Resolution: Verify that the service account has sufficient permissions to the index folder

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, click the Search service application.
5. On the Search Administration page, in the **Search Application Topology** section, click **Modify**.
6. On the Manage Search Application Topology page, click the index partition query component, and then click **Edit Properties**.
7. In the **Edit Query Component** dialog box, in the **Location of Index**, record the path for the index folder. Click **Cancel**.
8. Navigate to that location and verify that the location exists.
9. Verify that the service account that you recorded earlier in this procedure has Read and Write permissions on this folder.

Resolution: Refresh service credentials

1. Verify that you meet the following minimum requirements: See **Add-SPShellAdmin**. Perform the following steps on each server in the farm:
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:
   `Repair-SPManagedAccountDeployment`

For more information, see Repair-SPManagedAccountDeployment (*http://technet.microsoft.com/library/42ea7573-8b34-49da-9d7f-ec7b8211a138(Office.14).aspx*).

Search Query and Site Settings Service is not running (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Search Query and Site Settings Service is not running

Event ID: No event ID

Summary: The Search Query and Site Settings service is an Internet Information Services (IIS) service. By default, this service runs on each server that includes a search query component. The service manages the query processing tasks, which include sending queries to one or more of the appropriate query components and building the results set. At least one instance of the service must be running to serve queries.

Symptoms: All search queries fail.

Cause: The location provided for the index does not exist, or the application does not have rights to create a directory for the index at the location.

Resolution: Start the service on the server

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, next to **Search Query and Site Settings Service**, click **Start** if the service is not started.

Find servers that include query components

1. On the SharePoint Central Administration Home page, under **Application Management**, click **Manage service applications**.
2. On the Manage Service Applications page, click the name of the Search service application.
3. On the Search Administration page, in the **Search Application Topology** section, under **Index Partition**, record the names of the servers that include query components.

Resolution: Start the service on servers that include query components

1. Verify that you meet the following minimum requirements: See **Add-SPShellAdmin**.
2. On each server that includes a query component, 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-SPEnterpriseSearchQueryAndSiteSettingsServiceInstance -Local | Start-SPEnterpriseSearchQueryAndSiteSettingsServiceInstance
   ```
   For more information, see Get-SPEnterpriseSearchQueryAndSiteSettingsServiceInstance (*http://technet.microsoft.com/library/f1438a74-92fb-498d-aac1-66743403f3bc(Office.14).aspx*).

Resolution: Verify that the service account has sufficient permissions to the index folder

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, click the Search service application.

5. On the Search Administration page, in the **System Status** section, record the name of the **Default content access account**.
6. On the Search Administration page, in the **Search Application Topology** section, click **Modify**.
7. On the Manage Search Application Topology page, click the index partition query component, and then click **Edit Properties**.
8. In the **Edit Query Component** dialog box, in the **Location of Index**, record the path to the index folder. Click **Cancel**.
9. Navigate to that location and verify that the location exists.
10. Verify that the service account that you recorded in step 5 has read and write permissions on this folder.

Resolution: Refresh service credentials

1. Verify that you meet the following minimum requirements: See **Add-SPShellAdmin**.
2. Perform this procedure on each server in the farm.
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:
   `Repair-SPManagedAccountDeployment`

For more information, see Repair-SPManagedAccountDeployment (*http://technet.microsoft.com/library/42ea7573-8b34-49da-9d7f-ec7b8211a138(Office.14).aspx*).

SharePoint Server 2010 search is not running (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: SPServiceInstance search server is not running

Event ID:

Summary: The Microsoft Search Server 2010 service (OSearch) 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:

- Microsoft Search Server 2010 service (OSearch) 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 Search Server 2010 service (OSearch) is not running.

Resolution: **Start the service on the server**

- You can restart the Microsoft Search Server 2010 service (OSearch) on a specific server by opening a Command Prompt window and enter the following command at an elevated command prompt:
  net start osearch14

Word Services in SharePoint Server 2010 knowledge articles

Published: July 22, 2010

The articles in this section are knowledge articles for Word Services in Microsoft SharePoint Server 2010. 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 Word Services.

In this section:

- Word Automation Service - SQL Server exception event - Event 1001 (SharePoint Server 2010) (*http://technet.microsoft.com/library/7d017c66-a07e-4d8a-a2bf-bbfcef10a627(Office.14).aspx*)
- Word Services timer job failed - Events 1022 8077 (SharePoint Server 2010)
- Word services - PDF file converter failing - Event 8004 (SharePoint Server 2010)
- Word services - XPS file converter failing - Event 8005 (SharePoint Server 2010)
- Word services must be updated - Event 8010 (SharePoint Server 2010)
- Word services - language pack not installed - Event 8012 (SharePoint Server 2010)

Word Services timer job failed - Events 1022 8077 (SharePoint Server 2010)

Published: July 22, 2010

Alert Name: Word Automation Service timer job failed

Event ID: 1002 and 8077

Summary: Word Automation Services uses a custom timer job to pull items to be converted from the Word Automation Services database and then assign those items to be converted to individual application servers. If the custom timer job does not run, items to be converted cannot begin to be converted.

Symptoms: If the Word Automation Services timer job is not running, Word Automation Services will fail and one or more of the following symptoms might appear:

- New jobs are successfully added to the database, but the items to be converted for that job never start.
- Existing jobs do not finish: Any items to be converted that are already assigned to application servers may still succeed, but items to be converted that are not assigned to application servers do not start, leaving the job perpetually incomplete.
- This event appears in the event log: Event ID: 1002 Description: Conversion jobs may not execute because the timer job '%1' for service application '%2' does not appear to be active.
- This event appears in the event log: Event ID: 8077 Description: SharedServices_NoOnlineServiceInstancesInLocalFarm with "Word Automation Services Timer Job" indicated as the instance not started.

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

- An administrator has disabled the Word Automation Services timer job.
- There was an error in provisioning the Word Automation Services timer job.

Resolution: Verify that the Word Automation Services timer job is enabled in SharePoint Central Administration

- For the steps to perform this task, see Word Automation Services Troubleshooting (SharePoint Server 2010).

Resolution: Verify that the Word Automation Services timer job was provisioned successfully

- For the steps to perform this task, see Word Automation Services Troubleshooting (SharePoint Server 2010).

Word services - PDF file converter failing - Event 8004 (SharePoint Server 2010)

Published: July 22, 2010

Alert Name: Word services - PDF file converter failing

Event ID: 8004

Summary: Word Automation Services includes a default converter for converting files to the PDF file format. In addition to this default converter, third-party converters can be used with Word Automation Services. When third-party converters cause file conversions to fail, Word Automation Services raises this event. Files cannot be successfully converted to PDF until the converter is made functional or until it is removed.

Symptoms: If the Word Automation Services third-party PDF converter is not working correctly, PDF conversion will fail and one or more of the following symptoms might appear:

- Conversions to PDF fail with this message ID: 131183
- This event appears in the event log: Event ID: 8004 Description: The PDF converter '[file path & name]' failed during file conversion.

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

- The third-party converter is out of date.
- The third-party converter is corrupted.
- The third-party converter is otherwise non-functional.

Resolution: Verify that the latest version of the converter is installed

- Ensure that the latest third-party converter is installed.
- Try to reinstall the third-party converter.
- If this does not work, uninstall the third-party converter. This will cause Word Automation Services to use its default PDF converter.

Resolution: Update Word Automation Services

- For the steps to perform this task, see Word Automation Services Troubleshooting (SharePoint Server 2010).

Word services - XPS file converter failing - Event 8005 (SharePoint Server 2010)

Published: July 22, 2010

Alert Name: Word services - XPS file converter failing

Event ID: 8005

Summary: Word Automation Services includes a default converter for converting files to the XPS file format. In addition to this default converter, third-party converters can be used with Word Automation Services. When third-party converters cause file conversions to fail, Word Automation Services raises this event. Files cannot be successfully converted to XPS until the converter is made functional or until it is removed.

Symptoms: If the Word Automation Services third-party XPS converter is not working correctly, XPS conversion will fail and one or more of the following symptoms might appear:

- Conversions to XPS fail with this message ID: 131184
- This event appears in the event log: Event ID: 8005 Description: The XPS converter '[file path & name]' failed during file conversion.

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

- The third-party converter is out of date.
- The third-party converter is corrupted.
- The third-party converter is otherwise non-functional.

Resolution: Verify that the latest version of the converter is installed

- Ensure that the latest version of the third-party converter is installed.
- Try to reinstall the third-party converter.
- If this does not work, uninstall the third-party converter. This will cause Word Automation Services to use its default XPS converter.

Resolution: Update Word Automation Services

- For the steps to perform this task, see Word Automation Services Troubleshooting (SharePoint Server 2010).

Word services must be updated - Event 8010 (SharePoint Server 2010)

Published: July 22, 2010

Alert Name: Word services must be updated

Event ID: 8010

Summary: Periodically, Microsoft releases updates for Word Automation Services. These updates help ensure that Word Automation Services can convert newly created files with the best possible quality.

Symptoms: Conversions may fail, but it is more likely that output files will only have some fidelity loss for some features.

Cause: A file submitted for conversion was created with a newer version of Microsoft Word than the current Word Automation Services converter.

Resolution: **Update Word Automation Services**

- For the steps to perform this task, see Word Automation Services Troubleshooting (SharePoint Server 2010).

Word services - language pack not installed - Event 8012 (SharePoint Server 2010)

Published: July 22, 2010

Alert Name: Word services - language pack not installed

Event ID: 8012

Summary: Word Automation Services requires that the appropriate language packs be installed on all application servers on which Word Automation Services runs. If the correct language packs are not installed, documents created in the corresponding languages cannot be converted.

Symptoms: This event appears in the event log: Event ID: 8012 Description: One or more localized components could not be loaded for the specified language. Please check that the required language pack is installed and properly configured.

Cause: A file submitted for conversion requires a language pack that is not currently installed on the server that is processing the conversion.

Resolution: **Install the language pack**

- Install the correct language pack on all application servers that run Word Automation Services.
- For the steps to perform this task, see Word Automation Services Troubleshooting (SharePoint Server 2010).

Visio Services in SharePoint Server 2010 knowledge articles

Published: May 12, 2010

The articles in this section are knowledge articles for Visio Services in Microsoft SharePoint Server 2010. 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 Visio Services.

In this section:

- Visio Services data refresh failed - Events 8037_8038_8063_8062 (SharePoint Server 2010)
- Visio configuration database not found - Event 8040 (SharePoint Server 2010)
- Visio Services untrusted data provider request - Event 8041 (SharePoint Server 2010)
- Visio Services failed to generate diagram - Events 8042_8043_8060 (SharePoint Server 2010)
- Visio proxy initialization failed - Event 8044 (SharePoint Server 2010)
- Visio application proxy has invalid endpoint - Event 8049 (SharePoint Server 2010)
- Visio Services data provider not found - Event 8050 (SharePoint Server 2010)
- Visio Services file loading error - Events 8051_8061 (SharePoint Server 2010)

Visio Services data refresh failed - Events 8037 8038 8063 8062 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Visio Services data refresh failed

Event ID: 8037, 8038, 8062, and 8063

Summary: Users can connect published Microsoft Visio diagrams to external data sources, such as Excel Services in Microsoft SharePoint Server 2010. This error might occur because the schema of the data in a file changes in such a way that the expected primary key is invalid.

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

- This event appears in the event log: Event ID: 8037 Description: Invalid data type found in Published File cache for file <FileName> Exception : <ExceptionCode>.
- This event appears in the event log: Event ID: 8038 Description: Invalid data type found in Rendered File cache for file <FileName> Exception : <ExceptionCode>.
- This event appears in the event log: Event ID: 8063 Description: Invalid data type found in ODC cache for file %1.
- This event appears in the event log: Event ID: 8062 Description: Primary key column deleted.

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

- A user might connect to an external data source, such as an Microsoft Excel workbook that no longer exists or is inaccessible.
- A user might connect to an external data source whose primary key column is changed, and Visio Services in Microsoft SharePoint Server 2010 cannot update the external data in the Visio diagram.
- A user might connect to a data source that is not a valid data provider type.

Visio configuration database not found - Event 8040 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Visio configuration database not found

Event ID: 8040

Summary: Visio Services in Microsoft SharePoint Server 2010 stores its application settings in the configuration-a12-n database. Access to this database is critical for the service to function.

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

- Visio Services might fail to render diagrams.
- This event appears in the event log: Event ID: 8040 Description: Can't find configuration manager.

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

- The configuration database is inaccessible.
- The configuration database is responding slowly due to heavy network activity or load on the Microsoft SQL Server computer.

Resolution: Verify the status of the SQL Server configuration database

1. On the SharePoint Central Administration Web site, in the **System Settings** section in the reading pane, click **Manage Servers in this farm**.
2. In the **Farm Information** section, note the **Configuration database server** and the name and the version of the configuration database.
3. Start SQL Server Management Studio and connect to the configuration database server.
4. If the configuration database does not exist, run the SharePoint Products and Technologies Configuration Wizard.

Resolution: Verify the SQL Server network connection

1. On the Central Administration page, in the **System Settings** section in the reading pane, click **Manage Servers in this farm**.
2. In the **Farm Information** section, note the **Configuration database server** and the name and the version of the configuration database information.
3. Open a Command Prompt window and type **ping <serverAddress>** to confirm the server connection.
4. Failure to contact the server indicates a problem with the network connection or another problem that prevents a response from the server.
5. Log on to the server computer and troubleshoot the issue.

Visio Services untrusted data provider request - Event 8041 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Visio Services untrusted data provider request

Event ID: 8041

Summary: An error occurred because Visio Services in Microsoft SharePoint Server 2010 requested data from a data provider that was not in the list of trusted providers. Administrators can specify the data sources to which users can connect in their published Microsoft Visio diagrams.

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

- A diagram or diagrams might not refresh data.
- This event appears in the event log: Event ID: 8041 Description: Trusted data provider error. <error name>.

Cause: A user might have linked to a data provider in a user's published Visio diagram that was not specified as a trusted data provider by the service administrator.

Visio Services failed to generate diagram - Events 8042 8043 8060 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Visio Services failed to generate diagram
Event ID: 8060, 8042, 8043
Summary: An error occurred that caused Visio Services in Microsoft SharePoint Server 2010 to fail to generate a diagram. This rule is triggered when the service does not generate a diagram, and can be triggered together with any of the other rules for Visio Services. If the rule is triggered alone without a corresponding rule, an unknown error occurred that caused the service to fail to generate a diagram.
Symptoms: One or more of the following symptoms might appear:

- This event appears in the event log: Event ID: 8060 Description: Rasterization failed.
- This event appears in the event log: Event ID: 8042 Description: Failed to generate Raster diagram for file <file name>.
- This event appears in the event log: Event ID: 8043 Description: Failed to generate Vector diagram for file <file name>. Some diagram or diagrams may not render.

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

- If this rule is triggered together with another rule, the diagram might fail to render due to the causes specified in the corresponding rule that is triggered.
- If only this rule is triggered, Visio Services in SharePoint might have failed to generate a diagram for an unknown reason.
- Visio Services might be configured incorrectly.

Visio proxy initialization failed - Event 8044 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Visio proxy initialization failed

Event ID: 8044

Summary: Visio Services in Microsoft SharePoint Server 2010 application and its corresponding Web Parts use a proxy to connect to the back-end service. For the service to function, you must configure this proxy correctly.

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

- Visio Services might fail to render diagrams.
- This event appears in the event log: Event ID: 8044 Description: Unable to initialize Visio service proxy.

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

- The service application proxy for the Visio Services in SharePoint application is not running or has not been provisioned.
- The service application proxy for the Visio Services application is not configured correctly.

Resolution: Verify the Visio Services application proxy

1. On the SharePoint Central Administration Web site, on the Quick Launch click **Application Management**, and in the **Service Applications** section, click **Manage service applications**.
2. Note the name of the Visio Services application. In the Type column, **Visio Graphics Service Application** appears for Visio Services applications.
3. Verify that a service application proxy is associated with each Visio Services application. In the Type column **Visio Graphics Service Application Proxy** appears for Visio Services application proxies.

If no service application proxy corresponds to the Visio Services application that fails, create a new one by using Windows PowerShell 2.0.

Resolution: Create a new service application proxy

1. On the computer, click **Start**, click **All Programs**, click **Microsoft SharePoint 2010 Products**, and then click **SharePoint Management Shell**.
2. Create a new Visio Services application proxy by entering the Windows PowerShell cmdlet **New-SPVisioServiceApplicationProxy** at the command prompt in the SharePoint Management Shell. For more information about the syntax of this cmdlet, type **Get-Help New-SPVisioServiceApplicationProxy**.

If there is a service application proxy for the failing service application, create a new service application.

Resolution: Create a new service application

1. On the Central Administration page, on the Quick Launch, click **Application Management**, and then click **Manage service applications**.
2. In the **Name** column, select the Visio Services application proxy that is failing, and then on the Ribbon click the **Delete** option.
3. Select the parent Visio Services application of the application proxy that you deleted, and then on the Ribbon click the **Delete** option.

4. Create a new Visio Services application. On the **Service Applications** tab of the Ribbon, click **New**, and then click **Visio Graphics Service**. Make sure that the **Create Service Application Proxy** check box is selected.
5. In a Command Prompt window, type the command **ping <serverAddress>** to confirm the server connection.

Visio application proxy has invalid endpoint - Event 8049 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Visio application proxy has invalid endpoint

Event ID: 8049

Summary: The application for Visio Services in Microsoft SharePoint Server 2010 uses a proxy to abstract communication between the front-end service and back-end service. This proxy also provides a load-balancing mechanism between servers. For Visio Services to function, the front-end service must be connected to the application server that is returned by the application proxy.

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

- Visio Services in SharePoint might fail to render diagrams.
- This event appears in the event log: Event ID: 8049 Description: Application proxy invalid endpoint for <descriptive text>.

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

- The specified SharePoint Server application server is inaccessible.
- The specified application server is responding slowly due to heavy network activity or load on the specific server.

Resolution: Check the error logs

1. Open the Windows Event Viewer.
2. Search for event ID 8049 in the Windows Application Event log.
3. In the event description, note the application server that is failing.

Resolution: Verify the application server connection

1. From the failing application server, open the SharePoint Central Administration Web site.
2. If you cannot access the Central Administration site from the failing server, check that the network settings are correct and that the server has appropriate permissions to join the SharePoint farm.

Resolution: Verify that Visio Services runs on the failing server

1. On the Central Administration page, in the reading pane, in the **System Settings** section, click **Manage servers in this farm.**
2. Verify that Visio Services runs on the failing application server.

If there is a service application proxy for the failing service application, create a new service application.

Resolution: Restart Visio Services

1. On the Central Administration page, in the reading pane, in the **System Settings** section, click **Manage servers in this farm**.
2. In the **Server** column, click the name of the failing application server. The Services on Server page opens.
3. In the **Service** column, locate **Visio Graphics Service**, click **Stop**, and then click **Start**.

Resolution: Create a new Visio Services application

1. On the Central Administration page, in the reading pane, in the **Application Management** section, click **Manage service applications**.

2. In the **Type** column, click the name of the Visio Services application that has the failing service instance.
3. On the ribbon, click **Delete**.
4. In the **Delete Service Application** dialog box, click **OK**.
5. Create a new Visio Services application.

Visio Services data provider not found - Event 8050 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Visio Services data provider not found

Event ID: 8050

Summary: Users can connect published Microsoft Visio diagrams to external data sources, such as Excel Services in Microsoft SharePoint Server 2010.

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

- A diagram or diagrams might not refresh data.
- This event appears in the event log: Event ID: 8050 Description: Data provider connection failed with connection string <descriptive text>.

Cause: Visio Services in Microsoft SharePoint Server 2010 cannot connect to a data provider that was referenced by a user in a Visio diagram.

Visio Services file loading error - Events 8051 8061 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Visio Services file loading error

Event ID: 8061, 8051

Summary: Users can upload published Microsoft Visio diagrams to a document library, and some users can embed Visio diagrams in a page by using the Visio Web Access Web Part. This error might occur because a requested file is not found, or the service is unable to parse the requested file.

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

- A file or files might not load.
- This event appears in the event log: Event ID: 8061 Description: File not found at this location: <file location>.
- This event appears in the event log: Event ID: 8051 Description: Unable to parse file at location: <file location>.

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

- A user might try to load a page that contains a Web Part that references a file that no longer exists or is invalid.
- A user might try to view a Visio diagram that is corrupted.
- A user might try to view an invalid Visio diagram.

User Profile Synchronization Configuration Service cannot connect to SQL Server - Event 4 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: User Profile Synchronization Configuration Windows Service cannot connect to SQL Server

Event ID: 4

Summary: The User Profile Synchronization service cannot connect to the instance of SQL Server. If the service cannot connect to the instance of SQL Server, user profile synchronization will fail to function.

Symptoms: This event appears in the event log: Event ID: 4 Description: The Forefront Identity Manager Service cannot connect to the SQL Database Server. The SQL Server could not be contacted. The connection failure may be due to a network failure, firewall misconfiguration, or other connection issue. Additionally, the SQL Server connection information could be configured incorrectly. Verify that the SQL Server is reachable from the Forefront Identity Manager Service computer. Ensure that SQL Server is running, that the network connection is active, and that the firewall is configured properly. Last, verify the connection information has been configured properly. This configuration is stored in the Windows Registry.

Cause: The database for the instance of SQL Server is not accessible from the User Profile Synchronization Configuration Service, because of network connectivity issues or a wrong or changed password in the instance of SQL Server.

Resolution: Verify that the database server is running and available

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

Resolution: Verify connectivity between the database server and the farm

1. Log on to Microsoft SQL Server Management Studio as the account provided in the error details, click **Connect**, and then click **Database Engine**.
2. Type the server name provided in the error details, and then click **Connect**.

Resolution: Verify the User Profile Synchronization service credentials

1. On the Central Administration Home page, click **Application Management**, and in the **Service Applications** section, click **Manage service applications**.
2. On the Service Applications page, click the User Profile service application.
3. On the User Profile Service page, in the **Synchronization** section, click **Configure Synchronization Connections**.
4. Right click the connection, and then click **Edit Connection**.
5. Verify that the credentials and rights containers are provided in the connection. Verify that the credentials have sufficient permissions to read and write data in the directory, and also ensure that the User Profile Synchronization service is targeting the correct organizational units in the directory. Verify that the credentials have the **db_owner** fixed database role in the databases on the database server.

Resolution: Verify the database access credentials

1. On the Central Administration Home page, click **Security**, and then click **Service Applications**.
2. On the Security page, in the General Security section, click **Configure service accounts**.
3. On the Service Accounts page, in the service account drop-down list, click **Farm Account**.
4. Verify that this account has sufficient permissions on the database server.

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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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**.

Cannot create My Sites - Event 5187 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Cannot create My Sites

Event ID: 5187

Summary: If a Microsoft SharePoint Server 2010 user tries to open their My Site for the first time, and the My Site does not exist, SharePoint Server 2010 provisions the My Site collection for the user. This event is logged if SharePoint Server 2010 could not create the My Site.

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

- Users receive an error message that their My Site could not be created.
- This event appears in the event log: Event ID: 5187 Description: My Site creation failure for user '<User ID>' for site url '<User URL>'. The exception was: <Exception>.

Cause: There is a naming conflict caused by the Site Naming Format setting.

Resolution: **Change the Site Naming Format setting 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 **Application Management**.
3. On the Application Management page, in the **Service Applications** section, click **Manage service applications**.
4. On the Service Applications page, click the User Profile service.
5. On the User Profile Service page, in the **My Site Settings** section, click **Setup My Sites**.
6. On the My Site Settings page, in the **Site Naming Format** section, click either **User name (resolve conflicts by using domain_username)** or **Domain and user name (will not have conflicts)**.
7. Click **OK**.

User Profile changes cannot be committed - Event 5188 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: User Profile changes cannot be committed

Event ID: 5188

Summary: Users can edit properties in their own profiles, as allowed by the administrator. This event is logged when these changes made by the user (or by another process that has authority to update the profile) cannot be committed to the database.

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

- Users get an error that their changes cannot be applied.
- The following event appears in the event log: Event ID: 5188 Event Description: There was an error saving the user profile for user '<User ID>'. The exception was: <Exception>.

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

- The database server is unreachable because of network connectivity issues.
- The database server is not responding because network connections are overloaded, or memory — and, hence, the commit request — is encountering a time out.
- The database server is down because of additional issues with the server, such as disk failure.

Resolution: Verify that the database server is running and available

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

Resolution: Verify connectivity between the database server and the farm

1. Log on to Microsoft SQL Server Management Studio as the account provided in the error details, click **Connect**, and then click **Database Engine**.
2. Type the server name provided in the error details, and then click **Connect**.

Resolution: Verify that the database server is not low on resources

1. On the database server, verify that the server has sufficient RAM memory and disk space.

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.

Could not schedule synchronization jobs - Event 5556 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Could not schedule synchronization jobs

Event ID: 5556

Summary: A Microsoft SharePoint Server 2010 timer job creates and schedules the two synchronization jobs that synchronize user profile information between the user profile store and user tables. The two synchronization jobs are as follows:

- **User Profile to SharePoint Full Synchronization** - Performs full synchronization for all users
- **User Profile to SharePoint Quick Synchronization** - Performs synchronization for any newly added users

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

- None of the additional information stored in the user profile store is propagated to tables.
- This event appears in the event log: Event ID: 5556 Description: Failure trying to schedule synchronization jobs. Exception message is <Exception>.

Cause: The SharePoint Server 2010 timer service does not have sufficient permissions to start the other two timer jobs it schedules or these timer jobs do not exist.

Resolution: **Verify the timer jobs by using 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 **Monitoring**.
3. On the Monitoring page, in the **Timer Jobs** section, click **Review job definitions**.
4. On Job Definitions page, find the **User Profile to SharePoint Full Synchronization** and **User Profile to SharePoint Quick Synchronization** timer jobs. To page through the timer job status data rows, click the paging arrows at the bottom of these groups.
5. If the timer jobs do not exist, you must create them by manually running the **User Profile to SharePoint Synchronization Scheduler** timer job. To do this, follow these steps:
    a) On Job Definitions page, click the **User Profile to SharePoint Synchronization Scheduler** timer job. To page through the timer job status data rows, click the paging arrows at the bottom of these groups.
    b) On the edit Timer Job page, click **Run Now**.
    c) Wait a few minutes, and then check for the **User Profile to SharePoint Full Synchronization** and **User Profile to SharePoint Quick Synchronization** timer jobs again.

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:

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. 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.
4. 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.

Audience compilation failed - Event 5693 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Audience compilation failed

Event ID: 5693

Summary: To make it easier to target specific information to specific users, Microsoft SharePoint Server 2010 administrators can define rules that dynamically compile users into *audiences*. For example, all salespeople in the company can be compiled into an audience named Sales. If the audience compilation process fails, this event is logged.

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

- Users see more information than administrators intended for them to see.
- This event appears in the event log: Event ID: 5693 Description: Failed to compile audience. Exception was: '<Exception>'.

Cause: One or more of the audience rules is not correctly defined or the User Profile service cannot access the parameter values for the rule — for example, the information for a particular user is not accessible.

Resolution: **Manually compile the audience rule**

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, click the User Profile Service.
5. On the User Profile Service page, in the **People** section, click **Manage Audiences**.
6. On the View Audiences page, click the audience, and, from the context menu, click **Compile**.

Synchronizing data between SharePoint Server and directory failed - Events 6000-6099 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Synchronizing data between SharePoint Server and directory failed
Event ID: 6000-6099
Summary: Synchronizing data between Microsoft SharePoint Server and the directory failed.
Symptoms: One or more of the following events appear in the event log: Event ID: 6000-6099. For the description, see the event details.
Cause: These failures indicate that the User Profile Synchronization service was configured incorrectly or that corrupted data is being synchronized from SharePoint Server 2010 — for example, a required attribute such as an account name is missing.
Resolution: **Verify the User Profile Synchronization service credentials**

1. On the Central Administration Home page, click **Application Management**, and in the **Service Applications** section, click **Manage service applications**.
2. On the Service Applications page, click the User Profile service application.
3. On the User Profile Service page, in the **Synchronization** section, click **Configure Synchronization Connections**.
4. Right click the connection, and then click **Edit Connection**.
5. Verify that the credentials and rights containers are provided in the connection. Verify that the credentials have sufficient permissions to read and write data in the directory, and also ensure that the User Profile Synchronization service is targeting the correct organizational units in the directory.

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.

User Profile Synchronization Service unexpected failure - Events 6300-6309 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: User Profile Synchronization Service unexpected failure
Event ID: 6300-6309
Summary: The User Profile Synchronization service has experienced a generic, unexpected failure.
Symptoms: One or more of the following events appear in the event log: Event ID: 6300-6309 For the description, see the event details.
Cause: There can be multiple causes, but primarily these events indicate connectivity failures with the User Profile Synchronization service — for example, the SharePoint farm failed to connect to the database for the instance of SQL Server.
Resolution: Verify that the database server is running and available

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

Resolution: Verify connectivity between the database server and the farm

1. Log on to Microsoft SQL Server Management Studio as the account provided in the error details, click **Connect**, and then click **Database Engine**.
2. Type the server name provided in the error details, and then click **Connect**.

Resolution: Verify the database access credentials

1. On the Central Administration Home page, click **Security**, and then click **Service Applications**.
2. On the Security page, in the General Security section, click **Configure service accounts**.
3. On the Service Accounts page, in the service account drop-down list, click **Farm Account**.
4. Verify that this account has sufficient permissions on the database server.

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 Server 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 Server 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 Server 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 Server 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 Server 2010 installation:

   a) In Control Panel, open **Programs and Features**.
   b) Select your installation of SharePoint Server 2010 from the list, and then click **Change**.
   c) In the SharePoint Products Configuration Wizard, select **Repair**, and then click **Continue**.
   d) 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.
   e) 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

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** text 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.

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 Server 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 Server 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 Server 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 Server 2010 installation:

   a) In Control Panel, open **Programs and Features**.
   b) Select your installation of SharePoint Server 2010 from the list, and then click **Change**.
   c) In the SharePoint Products Configuration Wizard, select **Repair**, and then click **Continue**.
   d) 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.
   e) Retry the operation that triggered the event handler. These events should not continue to appear in the Windows event log.

Service instance provisioning failed - Event 7034 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Service instance provisioning failed
Event ID: 7034
Summary: An attempt to start or stop a service instance failed on a server in your farm because the service instance provisioning failed.
Symptoms: This event might appear in the event log: Event ID: 7034 Description: An attempt to start/stop instance of service <service type> on server <server name> did not succeed. Re-run the action via UI or command line on the specified server. Additional information is below:<more details>.
Cause: The failure can have several causes. For more details, see the event details.
Resolution: **Start the service**

- Ensure that you are a member of the Farm Administrators SharePoint group before performing this task.
- On the Central Administration Home page, in the **System Settings** section, click **Manage services on sever**.
- On the Services on Server page, select the server from the **Server** drop-down list.
- On the Services on Server page, click **Start** in the **Action** column next to the service.

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:
    a) The SharePoint Timer V4 service must be started on all front-end Web servers and application servers in the farm.
    b) 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 Server 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.

Secure Store reencrypt credentials failed - Event 7510 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Secure Store reencrypt credentials failed

Event ID: 7510

Summary: The credentials stored in the secure store credential database are encrypted by using a master key. When the master key is changed, the system decrypts the data in the database by using the old master key and re-encrypts it by using the new master key.

If the old master key is not valid or is not available, the re-encryption process will fail. The credentials stored in the database will not be usable, and all client applications that rely on the Secure Store service application for authentication will fail.

Symptoms: The following event appears in the event log: Event ID: 7510 Description: The Secure Store service application %name% errored out. The credentials encryption process failed. "n" credentials were not encrypted correctly.

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

- The master encryption key is not valid.
- The secure store database failed while it was being encrypted.
- The secure store database is corrupted.

Resolution: Create a new encryption key

1. Verify that you have the following administrative credentials:
   - You must be a service application administrator for the Secure Store service.
2. On the Central Administration Home page, under **Application Management**, click **Mange service applications**.
3. Click the Secure Store service application.
4. In the Key Management group, click **Generate New Key**.
5. On the **Generate New Key** page, type a pass phrase string in the **Pass Phrase** box, and type the same string in the **Confirm Pass Phrase** box.

   Important:

   A passphrase string must consist of at least eight characters and must include at least three of the following four elements:
   - Uppercase characters
   - Lowercase characters
   - Numerals
   - Any of the following special characters “! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

   Tip:

   The passphrase that you enter will not be stored. Make sure you write it down and store it in a safe place. At times you will need it to refresh the key, such as when you add a new application server to the server farm.
6. Click **OK**.

Resolution: Restore the secure store database

- Use the SharePoint Central Administration Web site or Windows PowerShell to restore the Secure Store service. For more information, see Restore the Secure Store service (SharePoint Server 2010) (*http://technet.microsoft.com/library/237d399e-b50b-42e6-90ff-e659a94d8099(Office.14).aspx*).

Secure Store could not retrieve master encryption key - Event 7535 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Secure Store could not retrieve the master encryption key
Event ID: 7535
Summary: The Secure Store Service application cannot retrieve the master encryption key. The service uses the master key to encrypt user identity and password data before storing it in the secure store database, and to decrypt the data when a client application requests it.
If the master encryption key cannot be retrieved, the credentials in the secure store database cannot be decrypted and will be unusable. Any client application that relies on the secure store database will be unable to authenticate users.
Symptoms: This event appears in the event log: Event ID: 7535 Description: The Secure Store service application %name% errored out because of a database exception.
Cause: One or more of the following might be the cause:

- The master encryption key was not generated after the Secure Store Service application was created.
- The master encryption key was deleted.
- The secure store database is corrupted.

Resolution: Create the master encryption key

- Create the master encryption key if it was not generated or it was deleted.
  To verify that the master encryption key was created:
  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 Service Applications page, click the Secure Store Service application.
  5. If you see an error page, no master encryption key was created. You can create the key by following the steps in "To create the master encryption key," later in this article.
     If you see another error page, try to refresh the key by following the steps in "To refresh the master encryption key," later in this article.
     To create the master encryption key:
  1. Verify that the user account that is performing this procedure is a Service Application Administrator for the instance of the Secure Store Service.
  2. Click the instance of the Secure Store Service application.
  3. On the ribbon, click **Generate New Key**.
  4. On the **Generate New Key** page, type a passphrase string in the **Pass Phrase** box, and type the same string in the **Confirm Pass Phrase** box.

Important:
A passphrase string must consist of at least eight characters and must contain at least three of the following four elements:
- Uppercase characters
- Lowercase characters
- Numerals
- Any of the following special characters:“! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Tip:
The passphrase that you enter will not be stored. Make sure that you write it down and store it in a safe location. You must use this passphrase any time you refresh the key, such as when you add a new application server to the server farm.

- Click **OK**.

To refresh the master encryption key:

- Verify that the user account that is performing this procedure is a Service Application Administrator for the instance of the Secure Store Service.
- Click the instance of the Secure Store Service application.
- On the ribbon, click **Refresh key**.
- On the **Refresh Key** page, type a passphrase string in the **Pass Phrase** box, and then click **OK**.

  Important:
  A passphrase string must consist of at least eight characters and must contain at least three of the following four elements:
  - Uppercase characters
  - Lowercase characters
  - Numerals
  - Any of the following special characters:“! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

  Tip:
  The passphrase that you enter will not be stored. Make sure that you write it down and store it in a safe location. You must use this passphrase any time you refresh the key, such as when you add a new application server to the server farm.
- Click **OK**.

To restore the Secure Store Service by using Central Administration

- If the secure store database is corrupted, restore the database from a backup. After the restore operation is successfully completed, you must refresh the passphrase.

  Note:
  You cannot use a configuration-only backup to restore the Secure Store Service.
  To restore the secure store database:
  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, in the **Backup and Restore** section, click **Restore from a backup**.
  3. On the Restore from Backup — Step 1 of 3: Select Backup to Restore page, select the backup job that contains the most recent farm-level backup, and then click **Next**. You can view more details about each backup by clicking the plus sign (+) next to the backup.

Note:
If the backup job that you want does not appear, in the **Backup Directory Location** text box, type the path of the folder that contains the correct backup, and then click **Refresh**.

4. On the Restore from Backup — Step 2 of 3: Select Component to Restore page, expand **Shared Services Applications**, select the check box that is next to the Secure Store Service application backup group, and then click **Next**.
5. On the Restore from Backup — Step 3 of 3: Select Restore Options page, in the **Restore Component** section, make sure that **Farm\Shared Services\Shared Services Applications\<Secure Store Service name>** appears in the **Restore the following component** list.
6. In the **Restore Options** section, under **Type of restore**, click **Same configuration**.
7. In the dialog box that asks you to confirm the operation, click **OK**.
8. Click **Start Restore**.
   You can view the general status of all recovery jobs at the top of the Backup and Restore Job Status page in the **Readiness** section. You can view the status for the current recovery job in the lower part of the page in the **Restore** section. The status page is automatically updated every 30 seconds. You can manually update the status details by clicking **Refresh**. Backup and recovery are timer service jobs. Therefore, it may take several seconds for the recovery to start.
   If you receive any errors, you can review them in the **Failure Message** column of the Backup and Restore Job Status page. You can also find more details in the Sprestore.log file at the path that you specified in step 3.

To refresh the passphrase:

1. On the Central Administration Home page, in the **Application Management** section, click **Manage service applications**.
2. On the Service Applications page, click the instance of the Secure Store Service. You might receive an error that says "Unable to obtain master key."
3. On the Secure Store Service page, on the ribbon, click **Refresh Key**.
4. In the **Refresh Key** dialog box, type the passphrase in the **Pass Phrase** box, and then click **OK**.

Secure Store SQL exception - Event 7551 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Secure Store SQL exception

Event ID: 7551

Summary: The Secure Store service application connects to the credential database for reading or writing credentials. This event is logged when the service application fails to connect to the database. The SQL Server exceptions are not logged immediately; the system tries to connect the service application to the database three times before it logs the errors. This is because some unexpected, but temporary, system failures can also cause the SQL Server exceptions.

Symptoms: The following event appears in the event log: Event ID: 7551 Description: The Secure Store service application %name% errored out because of a database exception.

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

- The database server is down or not accessible because of network issues.
- The Secure Store service application database connection information is incorrect.
- The Secure Store service application metadata database was not provisioned correctly.

Resolution: Verify that the Secure Store service application server is available

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, under **System Settings**, click **Manage services on server**.
3. On the Services on Server page, under **Services**, if the Secure Store service is not started, click **Start**.
4. On the Central Administration Home page, click **Application Management**.
5. On the Application Management page, in the **Service Applications** section, click **Manage service applications**.
6. On the Service Applications page, ensure that the Secure Store service application is started, and then click **Secure Store**.
7. On the Secure Store Service Application page, ensure that at least one target application appears in the list.
8. If the Secure Store service application is not started, do the following:
    a) On the Service Applications page, select the Secure Store service application name, and then click **Properties** on the ribbon.
    b) In the **Edit Properties** dialog box, in the **Database** section, ensure that the authentication method used is correct and that the account (if listed) has read and write permissions to the database.
    c) In the **Application Pool** section, ensure that the application pool account (if listed) has sufficient permissions to run the application pool.
9. On the Application Management page, in the **Service Applications** section, click **Manage service applications**.
10. On Service Applications page, select the **Secure Store Service Application**.
11. On the ribbon, click **Properties**.
12. Verify that the database server name and other connection properties are correct.

Secure Store proxy unexpected exception - Event 7557 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Secure Store proxy unexpected exception

Event ID: 7557

Summary: When a front-end Web server receives a request from a client computer, it routes the request to a Microsoft SharePoint Server 2010 application server through a load balancer. The load balancer maintains a list of available servers for a given service application. If the Secure Store service application on one or more application servers does not respond, the load balancer will remove the application server from the list of available servers and will raise this event.

If the Secure Store service application is enabled on more than one Microsoft SharePoint Server 2010 application server, the client computers will not be affected. If the service is not enabled on more than one application server, the client computers that rely on the secure store credential database to authenticate users will fail to authenticate.

Symptoms: The following event appears in the event log: Event ID: 7557 Description: The Secure Store service application %name% is not accessible.

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

- The application server is down or is not accessible due to network issues.
- The Secure Store service application is not provisioned correctly.

Resolution: **Verify that the Secure Store application server is available**

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, under **System Settings**, click **Manage services on server**.
3. On the Services on Server page, under **Services**, if the Secure Store service is not started, click **Start**.
4. On the Central Administration Home page, click **Application Management**.
5. On the Application Management page, in the **Service Applications** section, click **Manage service applications**.
6. On the Service Applications page, click **Secure Store**.
7. On the Secure Store Service Application page, ensure that at least one target application appears in the list.
8. If the Secure Store service application is not started, do the following:
    a) On the Service Applications page, select the Secure Store service application name, and then click **Properties** on the ribbon.
    b) In the **Edit Properties** dialog box, in the **Database** section, ensure that the authentication method used is correct and that the account (if listed) has read and write permissions to the database.
    c) In the **Application Pool** section, ensure that the application pool account (if listed) has sufficient permissions to run the application pool.

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.

Cannot retrieve list of service applications from remote farm - Event 8071 (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Cannot retrieve list of service applications from remote farm
Event ID: 8071
Summary: The application load balancer and topology service is unable to retrieve the list of published service applications from the remote farm.
Symptoms: This event appears in the event log: Event ID: 8071 Description: An exception occurred when trying to call EnumerateSharedServiceApplications: <exception>.
Cause: One or more of the following might be the cause:

- The farm service account on this farm does not have permissions to connect to the remote farm.
- Network errors or connectivity issues are preventing this operation from succeeding.

Resolution: Verify that the farm has sufficient permissions on the remote farm

- Contact the administrator of the remote farm and verify the following:
  - 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.
  - The remote farm has been added as a trusted farm on this farm.

    Tip:
    To establish the trust between two server farms, the administrator of both farms must add the other farm's public root certificate to the list of trusted root authorities by using the **New-SPTrustedRootAuthority**Windows PowerShell cmdlet.

Resolution: Verify that there are no networking issues

1. Ping the servers in the remote farm to ensure that they are available. Ask the administrator of the remote farm to ping the servers in your farm.

   Note:
   Contact the remote farm administrator and verify 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 Server 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 Server 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

1. On the Central Administration Home page, click **Monitoring**, and in the **Reporting** section, click **Configure usage and health data collection**.
2. 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.
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.

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 Server 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 Server 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 Server 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 Server 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.

Backend server not reachable (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Backend server not reachable

Event ID: None

Summary: The Word Viewing service application takes a Microsoft Office document as an input and produces a Portable Network Graphics (PNG) file, Microsoft Silverlight application, or a PDF file as output — the kind of output depends on the client application that requested the conversion.

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

- Users get an error every time they try to view a Word document that has not been viewed before.
- Users open a file and cannot convert it to a different format — for example, they open a .doc file and cannot save it as a .docx file.
- The Word Viewing service application writes errors to the event log.

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

- The Application Manager on the application server has unexpectedly stopped.
- The Word Viewing service application stopped working.
- The file conversion service stopped working.

Resolution: Restart Internet Information Services

1. Verify that the user account that is performing this procedure is a member of the local Administrators group.
2. Open a Command Prompt window and type the following at the command prompt:
   iisreset -force

Document conversion failures high (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Document conversion failures high

Event ID: None

Summary: A high rate of conversion failures may mean something is wrong with the application server, or a configuration setting is incorrect.

Symptoms: A large number of users' documents fail to be rendered and displayed after conversion.

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

- Users are attempting to view a large number of corrupted documents.
- The Microsoft SharePoint Server 2010 application server is malfunctioning.

Resolution: Verify availability of the application server

1. Verify that the application servers are consistently available.

Resolution: Restart Internet Information Services

1. Verify that the user account that is performing this procedure is a member of the local Administrators group.
2. Open a Command Prompt window and type the following at the command prompt:
   iisreset -force

Resolution: Add another server to the farm

1. If this failure keeps occurring, you should add a server to the farm to help load-balance the workload.

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 Server 2010. System Center Operations Manager raised an alert because of a problem in SharePoint Server 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 Server 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 Server 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 Server 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 Server 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://support.microsoft.com/kb/914277*).

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

Unacceptable rendering response time (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Unacceptable response time

Event ID: No event ID

Summary: In typical Microsoft SharePoint Server 2010 deployments, pages should be rendered in less than a second to provide the best experience for users.

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

- Response time to render content is consistently more than 1 second.
- The Executing Time/Page Request performance counter exceeds its threshold.

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

- A high volume of traffic that causes a high server load.
- Slow network connections among servers in the SharePoint farm.
- Poorly designed pages that contain a large number of Web Parts or a Web Part that sends a large number of server requests.

Resolution: Diagnose specific pages that are rendered slowly

1. If this is a performance issue for only specific pages in your sites, identify the page and diagnose the issue.
    a) Verify that the user account that is performing this procedure is a member of the Farm Administrators group.
    b) On the Central Administration the Home page, click **Monitoring**.
    c) On the Monitoring page, in the **Reporting** section, click **View health reports**.
    d) On the Review problems and solutions page, click **Slowest pages**, and then click **Go**.
    e) The pages that are being rendered the most slowly have the highest values in the **average duration** column.
    f) Contact the owner or developer of the page and request modifications needed for faster rendering.

Resolution: Diagnose servers and network connections

- If the performance issue is more general and affects many pages in a SharePoint farm, make sure that the servers in your SharePoint farm are located either on the same network or on networks that have high bandwidth and low latency connections.

Resolution: Diagnose server hardware and software configuration

1. Use Windows Task Manager and the resource monitor tools to inspect the hardware performance of the servers in your SharePoint farm.
2. If the CPU usage of the servers is consistently high, consider adding hardware to reduce the load on individual servers.
3. If disk usage on the servers is high or memory consumption is high, consider adding more memory to the servers in your SharePoint farm.
4. Click **OK**.

User Profile Configuration service not started (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: User Profile Configuration service not started

Event ID: None

Summary: The Forefront Identity Manager Configuration service has not been started. This Windows service enables Microsoft SharePoint Server 2010 to synchronize profile information with the directory. If the service is not started, user profile configuration will not function.

Symptoms: User profile configuration does not function.

Cause: A common cause for this issue can be that the Forefront Identity Manager service tried to start prior to SQL Server after a server restart.

Resolution: **Start the service**

1. Open a Command Prompt window and type the following at the command prompt:
   ```
   net start FIMService
   net start FIMSynchronizationService
   ```
2. If starting the service does not work, verify that the instance of SQL Server is running on the farm database server and try to start the services again.
3. If starting the service does not work, review the Windows application log for additional errors.

User Profile Synchronization service not started (SharePoint Server 2010)

Published: May 12, 2010

Alert Name: Identity Manager Synchronization service not started

Event ID: None

Summary: The Forefront Identity Manager Synchronization service enables Microsoft SharePoint Server 2010 to synchronize profile information with the directory. If the service is not started, user profile synchronization will not function.

Symptoms: User profile synchronization does not function.

Cause: A common cause for this issue can be that the Forefront Identity Manager Synchronization service tried to start prior to SQL Server after a server restart.

Resolution: **Start the service**

1. Open a Command Prompt window and type the following at the command prompt:
   ```
   net start FIMService
   net start FIMSynchronizationService
   ```
2. If starting the service does not work, verify that the instance of SQL server is running on the farm database server and try to start the services again.
3. If starting the service does not work, review the Windows application log for additional errors.

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 Server 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 Server 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 Server 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 Server 2010.

In this section:

- Web Applications using Claims authentication require an update (SharePoint Server 2010)
  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.
- InfoPath Forms Services Maintenance Timer Job not enabled (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "InfoPath Forms Services Maintenance Timer Job not enabled", and describes how to enable the timer job.
- Validate the My Site Host and individual My Sites are on a dedicated Web application and separate URL domain (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "Validate the My Site Host and individual My Sites are on a dedicated Web application and separate URL domain", and describes how to configure a dedicated Web application.
- Search scopes not defined for My Sites (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "Search scopes not defined for My Sites", and describes how to define search scopes.
- Verify each User Profile service application has a My Site host configured (SharePoint Server 2010)

This article provides information about the SharePoint Health Analyzer rule "Verify each User Profile service application has a My Site host configured", and describes how to configure a My Site.

- The Visio Graphics Service has a Maximum Web Drawing Size setting that will adversely impact performance (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "The Visio Graphics Service has a Maximum Web Drawing Size setting that will adversely impact performance", and describes how to change the Maximum Web Drawing Size setting for better performance.
- Visio Graphics Service has a maximum recalculation duration setting that will adversely impact performance (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "The Visio Graphics Service has a maximum recalculation duration setting that will adversely impact performance", and describes how to change the maximum recalculation duration setting for better performance.
- The Visio Graphics Service has a minimum cache age setting that will adversely impact performance (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "The Visio Graphics Service has a minimum cache age setting that will adversely impact performance", and describes how to change the minimum cache age setting for better performance.
- All State Service databases are paused for a State Service Application (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "All State Service databases are paused for a State Service Application", and describes how to resume the databases.
- A State Service Application has no database defined (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "A State Service Application has no database defined", and describes how to define a database for the State Service Application.
- InfoPath Forms Services forms cannot be filled out in a Web browser because no State Service connection is configured (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "InfoPath Forms Services forms cannot be filled out in a Web browser because no State Service connection is configured", and describes how to configure a State Service connection.
- Expired sessions are not being deleted from the ASP.NET Session State database (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "Expired sessions are not being deleted from the ASP.NET Session State database", and describes how to start the SQL Server Agent so that expired sessions will be deleted.
- The State Service Delete Expired Sessions timer job is not enabled (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "The State Service Delete Expired Sessions timer job is not enabled", and describes how to configure the timer job so that expired sessions will be deleted.
- One or more Search crawl databases have fragmented indices (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "One or more Search crawl databases have fragmented indices", and describes how to defragment the indexes.
- One or more Search property databases have fragmented indices (SharePoint Server 2010)

This article provides information about the SharePoint Health Analyzer rule "One or more Search property databases have fragmented indices", and describes how to a health rule that will defragment the indexes.

- InfoPath Forms Services forms cannot be filled out in a Web browser (SharePoint Server 2010)
  This article provides information about the SharePoint Health Analyzer rule "InfoPath Forms Services forms cannot be filled out in a Web browser", and describes how to enable browser rendering of forms.

Web Applications using Claims authentication require an update (SharePoint Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server. 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 Server deployment. With no SMPT server configured for outgoing e-mail, SharePoint Server 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 Server 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 Server 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:
   a) Page Requests
   b) Search Query Usage
   c) Site Inventory Usage
   d) 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.
4. 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**.

InfoPath Forms Services Maintenance Timer Job not enabled (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: The InfoPath Forms Services Maintenance timer job is not enabled

Summary: The InfoPath Forms Services Maintenance timer job is not enabled.

The InfoPath Forms Services Maintenance timer job is used by InfoPath Forms Services to improve performance by caching form template data on each front-end Web server.

Cause: The timer job may have been disabled on the Job Definitions page on the Central Administration Web site or the Windows PowerShell cmdlet **Disable-SPTimerJob** was used.

Resolution: Enable the timer job by using the Central Administration Web site

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators SharePoint group.
2. On the home page of the Central Administration Web site, click **Monitoring**.
3. Click **Review Job definitions**.
4. Click **InfoPath Forms Services Maintenance**.
5. Click **Enable**.

Resolution: Enable the timer job 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:
   `Enable-SPTimerJob "<FormsMaintenanceJobDefinition>"`
   Where:
   - *<FormsMaintenanceJobDefintion>* is the actual name of the timer job to enable.

For more information, see Enable-SPTimerJob (*http://technet.microsoft.com/library/ca2ce54c-1a9a-46d5-8055-a1f87c30a99a(Office.14).aspx*).

Validate the My Site Host and individual My Sites are on a dedicated Web application and separate URL domain (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: Validate the My Site Host and individual My Sites are on a dedicated Web application and separate URL domain

Summary: For performance and manageability reasons, we recommend that the My Site host and individual My Sites be deployed in a dedicated Web application. The owner of each individual My Site is the site collection administrator for that My Site. Having a dedicated Web application for the My Site host and individual My Sites reduces the security risk that a My Site owner can introduce same-domain scripting attacks on other sites that are hosted on the same Web application.

Cause: The My Site host and individual My Sites are deployed in the same Web application as the root site collection. If the User Profile Service was configured by using the Farm Configuration Wizard, this is how My Sites are set up.

Resolution: Set up a dedicated Web application

- We recommend that you have a separate, dedicated Web application to host the My Site host and individual My Sites.
  For more information, see Create a Web application (SharePoint Server 2010) (*http://technet.microsoft.com/library/121c8d83-a508-4437-978b-303096aa59df(Office.14).aspx*).

Search scopes not defined for My Sites (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: Search scopes not defined for My Sites

Summary: When you create a My Site host, it is important to make sure that search scopes are defined for the My Site host and My Sites. Otherwise, performance can be degraded on My Site pages, causing very high latencies, low throughput, and high CPU utilization on the Web server.

Cause: The administrator did not define search scopes for My Sites and the My Site host.

Resolution: **Define search scopes for My Sites and the My Site host**

1. Verify that the user account that is performing this procedure is an administrator for the User Profile Service service application.
2. On the Central Administration Home page, in the **Application Management** section, click **Manage service applications**.
3. On the Manage Service Applications page, click the User Profile Service service application.
4. On the User Profile Service page, in the **My Site Settings** section, click **Setup My Sites**.
5. On the My Site Settings page, in the **Preferred Search Center** section, select the correct search scopes from the **Search scope for finding people** and **Search scope for finding documents** lists.
   Typically, the setting for the **Search scope for finding people** list is **People** and the **Search scope for finding documents** list is **All Sites**.
6. Click **OK**.

Verify each User Profile service application has a My Site host configured (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: Verify each User Profile service application has a My Site Host configured

Summary: Without a My Site host, end-users are not able to use personal sites or people profiles. Therefore, we recommend that if you create a User Profile Service service application, you also create a My Site host for the User Profile Service.

Symptoms: My Sites and other people profile features are not available to users.

Cause: The administrator who created the User Profile Service service application did not also create a My Site host.

Resolution: Verify that a My Site site collection has been created

- For information about setting up a My Site site collection, see Set up My Site (SharePoint Server 2010) (*http://technet.microsoft.com/library/e6600dfa-7f96-4c6f-a1be-b7ad348ac30f(Office.14).aspx*).

Resolution: Associate the My Site host with a User Profile Service service application 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:
   `Set-SPProfileServiceApplication [-Name` *`<UserProfileServiceApplicationName>`*`] -MySiteHostLocation` *`<URL>`*
   Where:
   - *<UserProfileServiceApplicationName>* is the friendly name of the User Profile Service service application. If you only have one User Profile Service service application, you do not need to specify the name.
   - *<URL>* is URL of an empty site collection that has no templates associated with it.

Visio Graphics Service has a maximum cache age setting that will adversely impact performance (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: The Visio Graphics Service has a maximum cache age setting that will adversely impact performance

Summary: The Visio Graphics Service has a maximum cache age setting that will adversely impact performance. If the **Maximum Cache Age** setting is longer than 60 minutes it might result in a large memory load of the Visio Graphics Service.

Cause: The **Maximum Cache Age** setting was set greater than 60 minutes.

Resolution: **Reduce the value of the Maximum Cache Age setting**

1. Verify that the user account that is performing this procedure is an administrator of the Visio Graphics Service service application.
2. In Central Administration, on the Home page, in the **Application Management** section, click **Manage service applications**.
3. On the Service Applications page, click the Visio Graphics service application.
4. On the Manage the Visio Graphics Service page, click **Global Settings**.
5. Ensure that the settings have the values that are listed in the following table. If they do not, type the value in the corresponding text box.

Setting	Value
Maximum Web Drawing Size	< 5 (Megabytes)
Minimum Cache Age	> 4 (Minutes)
Maximum Cache Age	< 60 (Minutes)
Maximum Recalc Duration	< 60 (Seconds)

6. Click **OK**.

The Visio Graphics Service has a Maximum Web Drawing Size setting that will adversely impact performance (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: The Visio Graphics Service has a Maximum Web Drawing Size setting that will adversely impact performance

Summary: The Visio Graphics Service has a maximum Web drawing size setting that will adversely affect performance. If the **Maximum Web Drawing Size** setting is larger than 5 MB, it might result in increased bandwidth usage, decreasing the expected performance of the Visio Graphics Service.

A Web drawing size increases performance by downloading smaller images which, minimizes bandwidth usage.

Cause: The **Maximum Web Drawing Size** setting was set greater than 5 MB.

Resolution: **Decrease the value of the Maximum Web Drawing Size setting**

1. Verify that the user account that is performing this procedure is an administrator of the Visio Graphics Service service application.
2. In Central Administration, on the Home page, in the **Application Management** section, click **Manage service applications**.
3. On the Service Applications page, click the Visio Graphics service application.
4. On the Manage the Visio Graphics Service page, click **Global Settings**.
5. Ensure that the settings have the values that are listed in the following table. If they do not, type the value in the corresponding text box.

Setting	Value
Maximum Web Drawing Size	< 5 (Megabytes)
Minimum Cache Age	> 4 (Minutes)
Maximum Cache Age	< 60 (Minutes)
Maximum Recalc Duration	< 60 (Seconds)

6. Click **OK**.

Visio Graphics Service has a maximum recalculation duration setting that will adversely impact performance (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: The Visio Graphics Service has a maximum recalc duration setting that will adversely impact user perceived performance

Summary: The Visio Graphics Service has a maximum recalculation duration setting that will adversely affect performance. If the **Maximum Recalc Duration** setting is longer than 60 seconds, it might result in large processor load of the Visio Graphics Service and Microsoft SharePoint Server 2010, decreasing the expected performance of both.

A shorter duration increases performance by only allowing simple data-connected diagrams to be recalculated by the server, minimizing CPU and memory usage. A longer duration allows the recalculation of more complex data-connected diagrams while using more CPU cycles and memory. The default duration is 60 seconds.

Cause: The **Maximum Recalc Duration** setting was set longer than 60 seconds.

Resolution: **Decrease the value of the Maximum Recalc Duration setting**

1. Verify that the user account that is performing this procedure is an administrator of the Visio Graphics Service service application.
2. In Central Administration, on the Home page, in the **Application Management** section, click **Manage service applications**.
3. On the Service Applications page, click the Visio Graphics service application.
4. On the Manage the Visio Graphics Service page, click **Global Settings**.
5. Ensure that the settings have the values that are listed in the following table. If they do not, type the value in the corresponding text box.

Setting	Value
Maximum Web Drawing Size	< 5 (Megabytes)
Minimum Cache Age	> 4 (Minutes)
Maximum Cache Age	< 60 (Minutes)
Maximum Recalc Duration	< 60 (Seconds)

6. Click **OK**.

The Visio Graphics Service has a minimum cache age setting that may cause a security issue (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: The Visio Graphics Service has a minimum cache age setting that may cause a security issue

Summary: Setting **Minimum Cache Age** to 0 minutes may leave the Visio Graphics Service open to a denial of service (DoS) attack. A value of 0 for this setting might lead to large processor and network load of the Visio Graphics Service and Microsoft SharePoint Server 2010, decreasing the expected performance of both. However, increasing this value means that users will not see their data-connected diagrams refreshing as frequently.

Cause: The **Minimum Cache Age** setting was set to 0 minutes.

Resolution: **Increase the value of the Minimum Cache Age setting**

1. Verify that the user account that is performing this procedure is an administrator of the Visio Graphics Service service application.
2. In Central Administration, on the Home page, in the **Application Management** section, click **Manage service applications**.
3. On the Service Applications page, click the Visio Graphics service application.
4. On the Manage the Visio Graphics Service page, click **Global Settings**.
5. Ensure that the settings have the values that are listed in the following table. If they do not, type the value in the corresponding text box.

Setting	Value
Maximum Web Drawing Size	< 5 (Megabytes)
Minimum Cache Age	> 4 (Minutes)
Maximum Cache Age	< 60 (Minutes)
Maximum Recalc Duration	< 60 (Seconds)

6. Click **OK**.

The Visio Graphics Service has a minimum cache age setting that will adversely impact performance (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: The Visio Graphics Service has a minimum cache age setting that will adversely impact performance

Summary: The Visio Graphics Service has a minimum cache age setting that will adversely affect performance. If the **Minimum Cache Age** setting is shorter than 4 minutes, it might result in large processor and network load of the Visio Graphics Service and Microsoft SharePoint Server 2010, decreasing the expected performance of both. However, increasing this value means that users will not see their data-connected diagrams refreshing as frequently.

Cause: The **Minimum Cache Age** setting was set shorter than 4 minutes.

Resolution: **Increase the value of the Minimum Cache Age setting**

1. Verify that the user account that is performing this procedure is an administrator of the Visio Graphics Service service application.
2. In Central Administration, on the Home page, in the **Application Management** section, click **Manage service applications**.
3. On the Service Applications page, click the Visio Graphics service application.
4. On the Manage the Visio Graphics Service page, click **Global Settings**.
5. Ensure that the settings have the values listed in the following table. If they do not, type the values in the corresponding text boxes, and then click **OK**.

Setting	Value
Maximum Web Drawing Size	< 5 (Megabytes)
Minimum Cache Age	> 4 (Minutes)
Maximum Cache Age	< 60 (Minutes)
Maximum Recalc Duration	< 60 (Seconds)

6. Click **OK**.

All State Service databases are paused for a State Service Application (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: All State Service databases are paused for a State Service Application

Summary: All of the databases associated with a State Service service application are paused. This may result in errors when using some Microsoft SharePoint Server 2010 components such as InfoPath Web browser forms and the Microsoft SharePoint Chart Web Part.

Cause: This might be caused by the administrator pausing all databases for the service application.

Resolution: Resume the State Service service application databases 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. To identify the paused database, type the following command at the Windows PowerShell command prompt:
   ```
   Get-SPStateServiceDatabase
   ```
6. If you want to resume a paused database, type the following command at the Windows PowerShell command prompt:
   ```
   Resume-SPStateServiceDatabase -Identity <DatabaseID>
   ```
   Where:
   - *<DatabaseID>* is the identifier for the State Service service application database as a GUID.
7. If you want to create a new database instead of using an existing database, type the following command at the Windows PowerShell command prompt:
   ```
   New-SPStateServiceDatabase -Name <DatabaseName> -ServiceApplication <ID> -
   DatabaseServer <ServerName> [-DatabaseCredentials <Credential>]
   ```
   Where:
   - *<DatabaseName>* is name of the database as a string.
   - *<ID>* is the identifier for the affected State Service service application as a string or a GUID. If there is only one State Service service application, you do not have to specify this parameter.
   - *<ServerName>* is name of the database server.
   - *<Credential>* is SQL Server authentication credentials for the database server. If this parameter is not specified, Windows authentication will be used.

For more information, see Resume-SPStateServiceDatabase (*http://technet.microsoft.com/library/5a608d7b-80e3-482b-832a-e2033d403249(Office.14).aspx*) or New-SPStateServiceDatabase (*http://technet.microsoft.com/library/221e439c-c501-4d4c-9d8a-171a01e67e25(Office.14).aspx*).

A State Service Application has no database defined (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: A State Service Application has no database defined

Summary: A State Service service application has no State Service database defined. This may result in errors when using some SharePoint components such as InfoPath Web browser forms and the Microsoft SharePoint Server Chart Web Part.

Cause: One or more of the following might be causing this:

- The farm administrator deleted all databases associated with the State Service service application.
- The farm administrator never created or associated a database with the State Service service application.

Resolution: Create a new database or use an existing database for the State Service service application 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. If no database already exists that you can use, type the following command at the Windows PowerShell command prompt:
   `New-SPStateServiceDatabase -Name <DatabaseName> -DatabaseServer <ServerName> [-DatabaseCredentials <Credential>] [-ServiceApplication <ID>]`
   Where:
   - *<DatabaseName>* is name of the database as a String.
   - *<ServerName>* is name of the database server.
   - *<Credential>* is SQL Server authentication credentials for the database. If this parameter is not used, Windows authentication will be used.
   - *<ID>* is the identifier for the State Service service application as a string or a GUID. If there is only one State Service service application, you do not have to specify this parameter.
6. In some environments, you must connect to an existing, empty SQL database. In this case, type the following command at the Windows PowerShell command prompt:
   `Mount-SPStateServiceDatabase -Name <DatabaseName> -DatabaseServer <ServerName> [-DatabaseCredentials <Credential>] [-ServiceApplication <ID>]`
   Where:
   - *<DatabaseNname>* is name of the database as a String.
   - *<ServerName>* is name of the database server.
   - *<Credential>* is the SQL Server authentication credentials for the database. If this parameter is not used, Windows authentication will be used.
   - *<ID>* is the identifier for the State Service service application as a string or a GUID. If there is only one State Service service application, you do not have to specify this parameter.

For more information, see Mount-SPStateServiceDatabase (*http://technet.microsoft.com/library/bd559347-c8f9-4ecf-9fbc-17821ae0afc4(Office.14).aspx*) or New-SPStateServiceDatabase (*http://technet.microsoft.com/library/221e439c-c501-4d4c-9d8a-171a01e67e25(Office.14).aspx*).

InfoPath Forms Services forms cannot be filled out in a Web browser because no State Service connection is configured (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: InfoPath Forms Services forms cannot be filled out in a Web browser because no State Service connection is configured

Summary: InfoPath Forms Services depends on the Web application having a service connection to a State Service Proxy to store data across HTTP requests. Without a service connection, users cannot successfully open or fill browser-enabled InfoPath forms.

Cause: No service connection for the State Service is configured for the Web application that is in the Health Analyzer alert.

Resolution: **Configure a service connection by using Central Administration**

1. Verify that the user account performing this procedure is a member of the Farm Administrators group.
2. If a State Service already exists, you can proceed to step 7.
3. If a State Service does not exist, you must create one. To do this, in Central Administration, on the home page, click **Configuration Wizards**.
4. On the Configuration Wizards page, under **Farm Configuration**, click **Launch Farm Configuration Wizard**.
5. On the Configure your Farm page, click **Start the Wizard**.
6. On the next page, ensure that the **State Service** check box is selected, and then click **OK** at the bottom of the page.
7. Complete the wizard to create the State Service.
8. Associate the State Service with the Web application mentioned in the health analyzer rule. To do this in Central Administration, on the home page, under **Application Management**, click **Manage web applications**.
9. On the Web Applications page, click the Web application for which you want to configure a service connection, and then click **Service Connections** on the ribbon.
10. In the **Configure Service Application Associations** dialog box, ensure that the **State Service** check box is selected, and then click **OK**.

Expired sessions are not being deleted from the ASP.NET Session State database (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: Expired sessions are not being deleted from the ASP.NET Session State database

Summary: If expired sessions are not deleted, the server that hosts the ASP.NET Session State database may run out of disk space and the SharePoint farm may cease to function.

Cause: One or more of the following might be causing this:

- The SQL Server Agent service was stopped.
- SQL Server Express is installed.

  Important:

  You cannot run the SQL Server Agent service on an instance of SQL Server Express.

Resolution: **Start the SQL Server Agent service**

1. Verify that the user account that is performing this procedure is a member of the Administrators group on the database server that is hosting the ASP.NET Session State database.
2. In the Services snap-in, start the SQL Server Agent service.

The State Service Delete Expired Sessions timer job is not enabled (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: The State Service Delete Expired Sessions timer job is not enabled

Summary: The State Service uses a timer job to delete data for expired sessions from the State Service databases. If this timer job is not enabled, the server that hosts the State Service database will run out of disk space and the SharePoint farm will cease to function

Cause: The State Service Delete Expired Sessions timer job is not enabled.

Resolution: Enable the timer job by using Central Administration

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

   Note:

   The timer job 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 **Timer Jobs** section, click **Review job definitions**.
4. On the Job Definitions page, click the State Service Delete Expired Sessions timer job.
5. On the Edit Timer Job page, specify the schedule that you want, and then click **Enable**.

Resolution: Enable the timer job 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:

   ```
   Enable-SPTimerJob StateServiceExpiredSessionJobDefinition
   ```

For more information, see Enable-SPTimerJob (*http://technet.microsoft.com/library/ca2ce54c-1a9a-46d5-8055-a1f87c30a99a(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.

One or more Search crawl databases have fragmented indices (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: Search - One or more crawl databases may have fragmented indices

Summary: This article describes the SharePoint Health Analyzer rule for Search service application crawl database defragmentation. The fragmentation of crawl data indexes occurs on a different level than regular disk fragmentation. It occurs in each crawl database as data is created, updated, or deleted during normal crawl activity. When you run the health rule, the system makes used storage contiguous, eliminates unused storage, and compacts the database.

We recommend that you run the crawl database rule under the following circumstances:

- If you are using Microsoft SQL Server 2008 Enterprise. Running the crawl database rule automatically enables the Page Compression feature to optimize I/O and disk storage usage.
- If significant performance degradation is determined to be caused by crawl database fragmentation. This should be a rare occurrence because crawl databases will usually have some level of fragmentation.

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

- Crawl rate may decrease as more time is spent writing crawl history to the crawl database.
- The crawl database defragmentation health rule is run and attempts to correct the fragmentation. Note: when this rule is correcting the fragmentation, the crawl rate is affected. Crawl rate may decrease as more time is spent writing metadata to the property database.

Cause: Fragmentation exists when indexes have pages in which the logical ordering, based on the key value, does not match the physical ordering inside the data file. All leaf pages of an index contain pointers to the next and the previous pages in the index. This forms a doubly linked list of all index/data pages. Ideally, the physical order of the pages in the data file should match the logical ordering. Overall disk throughput is increased when the physical ordering matches the logical ordering of the data.

For more information about database fragmentation, including how to manually detect and repair fragmented indexes, see the Microsoft SQL Server documentation.

Resolution: Enable and run the crawl database defragmentation health rule

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 Analyzer** section, click **Review rule definitions**.
4. On the All Rules page, in the **Performance** section, click **Search - One or more crawl databases may have fragmented indices**.
5. If the rule is not enabled, in the **Health Analyzer Rule Definitions** dialog, click **Edit Item** on the ribbon. Ensure that the **Enabled** check box is selected, and then click **Save** on the ribbon.
6. On the ribbon, click **Run Now**.
7. Click **Close**.

The rule iterates over all crawl databases in all Search service applications. When it runs, it attempts to perform an online defragmentation first, and then it switches to offline defragmentation where required. In online defragmentation, only the SQL Server leaf pages are defragmented, not the SQL Server locked pages. In offline defragmentation, the locked pages and all the leaf pages are defragmented.

Note:
In SQL Server 2008 Enterprise, the health rule automatically enables the Page Compression feature to optimize I/O and disk usage.

One or more Search property databases have fragmented indices (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: Search - One or more property databases have fragmented indices

Summary: This article gives more information about the SharePoint Health Analyzer rule for Search service application property database defragmentation. The fragmentation of property data indexes occurs on a different level than regular disk fragmentation; it occurs within each property database as data is created, updated, or deleted during normal crawl activity. Running the property database health rule makes used storage contiguous, eliminates unused storage, and compacts the database.

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

- Query latency might increase.
- Crawl rate may decrease as more time is spent writing metadata to the property database.
- The property database defragmentation health rule detects that one or more property databases have fragmented indexes and attempts to correct the fragmentation. Note: when this rule is correcting the fragmentation, query latency and crawl rate are affected.

Cause: Fragmentation exists when indexes have pages in which the logical ordering, based on the key value, does not match the physical ordering inside the data file. All leaf pages of an index contain pointers to the next and the previous pages in the index. This forms a doubly linked list of all index/data pages. Ideally, the physical order of the pages in the data file should match the logical ordering. Overall disk throughput is significantly increased when the physical ordering matches the logical ordering of the data.

Refer to Microsoft SQL Server documentation for more details about database fragmentation, including how to manually detect and repair fragmented indexes.

Resolution: Enable and run the property database defragmentation health rule

1. In Central Administration, on the home page, click **Monitoring**.
2. On the Monitoring page, in the **Health Analyzer** section, click **Review rule definitions**.
3. On the All Rules page, in the **Performance** section, click the **Search - One or more property databases have fragmented indices** rule.
4. If the rule is not enabled, in the **Health Analyzer Rule Definitions** dialog box, click **Edit Item** on the ribbon. Ensure that the **Enabled** check box is selected, and then click **Save** on the ribbon.
5. Click **Run Now** on the ribbon.
6. Click **Close**.

By default, the property database defragmentation rule is enabled to run once a week over all property databases in all Search service applications. When the rule runs, it determines whether a given property database exceeds the preset fragmentation percentage. If a property database exceeds the preset fragmentation percentage, the health rule attempts to perform an online defragmentation first. Then it switches to offline defragmentation where required. In online defragmentation, only the Microsoft SQL Server leaf pages are defragmented, not the SQL

Server locked pages. In offline defragmentation, the locked pages and all the leaf pages are defragmented.

Note:
On Microsoft SQL Server 2008 Enterprise, the health rule automatically enables the Page Compression feature to optimize I/O and disk usage.

InfoPath Forms Services forms cannot be filled out in a Web browser (SharePoint Server 2010)

Published: July 8, 2010

Rule Name: InfoPath form library forms cannot be filled out in a Web browser

Summary: InfoPath Forms Services users can publish browser-enabled form templates to a Microsoft SharePoint Server 2010 form library but cannot open the forms in a Web browser.

Note:
This issue only applies to forms published to form libraries. It does not apply to list forms or to forms that have been uploaded by farm administrators.

Cause: One or more of the following might be causing this:

- The **Render form templates that are browser-enabled by users** check box in Central Administration is cleared.
- The following Windows PowerShell command has been run: `Set-SPInfoPathFormsService -AllowUserFormBrowserRendering $false`
.

Resolution: Enable browser rendering of user forms by using Central Administration

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, click **General Application Settings**.
3. On the General Application Settings page, in the **InfoPath Forms Services** section, click **Configure InfoPath Forms Services**.
4. On the Configure InfoPath Forms Services page, in the **User Browser-enabled Form Templates** section, select the **Render form templates that are browser-enabled by users** check box.
5. Click **OK** at the bottom of the page.

Resolution: Enable browser rendering of user forms 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:
```
Set-SPInfoPathFormsService -AllowUserFormBrowserRendering $true
```

For more information, see Set-SPInfoPathFormsService (*http://technet.microsoft.com/library/ac13cd00-c372-4159-943d-98c016c7e96a(Office.14).aspx*).

Word Automation Service timer job is not running (SharePoint Server 2010)

Published: August 5, 2010

Rule Name: A Word Automation Services timer job is not running

Summary: Critical state of this SPHA rule indicates that the Word Automation Services Timer Job is not running when it should be running.

Cause: Word Automation Services uses a custom Timer Job to pull conversion items from the Word Automation Services database and then assign those conversion items to individual application servers. If the custom Timer Job does not run then conversion items cannot begin to convert.

Resolution: Enable the timer job by using the Central Administration Web site

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators SharePoint group.
2. On the home page of the Central Administration Web site, click **Monitoring**.
3. Click **Review Job definitions**.
4. Click **Word Automation Services Timer Job**.
5. Click **Enable**.

Resolution: Enable the timer job 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:
   `Enable-SPTimerJob "Word Automation Services"`

For more information, see Enable-SPTimerJob (*http://technet.microsoft.com/library/ca2ce54c-1a9a-46d5-8055-a1f87c30a99a(Office.14).aspx*).

Resolution Verify that the Word Automation Services service is provisioned correctly

1. To verify that the Word Automation Services service is provisioned correctly, see Configuring Word Automation Services for Development (*http://msdn.microsoft.com/en-us/library/ee557330.aspx*).

Resolution See other troubleshooting information

1. For additional trouble shooting steps, see Word Automation Services Troubleshooting (SharePoint Server 2010).

Installation reference (SharePoint Server 2010)

Published: July 8, 2010

In this section:

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

Setup command-line reference (SharePoint Server 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
- Available switches and parameters

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

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.
	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

Switch or parameter	Description
	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 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 Server 2010 product DVD, or customize your own configuration file.
3. Press ENTER.

For more information, see Install SharePoint Server 2010 using Windows PowerShell (*http://technet.microsoft.com/library/7443092a-87a6-4063-a7d0-8d10d9d23682(Office.14).aspx*).

Psconfig command-line reference (SharePoint Server 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
- Available commands and parameters

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 Server 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
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

Command	Description, parameters, and examples

	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 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]*

Command	Description, parameters, and examples

	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>]
	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

Command	Description, parameters, and examples
	Server 2010 Web site during installation. If not specified, the site is not deleted. **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.
	
	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

Command	Description, parameters, and examples
	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]* 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]*

Command	Description, parameters, and examples
	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 Server 2010)

Updated: November 4, 2010

When you want to control how Microsoft SharePoint Server 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 Server 2010.
- Install SharePoint Server 2010 by using a common configuration across multiple servers.
- Perform an automated or scripted installation of SharePoint Server 2010.

In this article:

- Customizing Config.xml
- Config.xml element quick reference
- How it works
- Config.xml file format
- Config.xml element reference

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 for a single server (stand-alone, with SQL Express).
- **SetupFarm** Contains a Config.xml file for use in setting up a clean installation for a server farm.
- **SetupFarmSilent** Contains a Config.xml file for use in setting up a server farm in silent mode.
- **SetupFarmUpgrade** Contains a Config.xml file for use in upgrading an existing server farm in place.
- **SetupSilent** Contains a Config.xml file for use in setting up a clean installation for a single server (stand-alone, with SQL Express) in silent mode.
- **SetupSingleUpgrade** Contains a Config.xml file for use in upgrading an existing single server (stand-alone) in place.

For more information about the differences among the various upgrade scenarios, see Determine upgrade approach (SharePoint Server 2010) (*http://technet.microsoft.com/library/f11e6c4f-dc2a-4d17-a2c8-9455792b4b9b(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.
INSTALLLOCATION Element	The fully qualified path of the folder on the user's computer in which the product is installed.
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.
PIDKEY Element	The 25-character volume license key.
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 Server 2010 is **spswfe**. Because SharePoint Server 2010 is based on the platform technology in SharePoint Foundation 2010, you must also install the **sts** (SharePoint Foundation 2010) package or the installation will not succeed.
Use the **sts** and **spswfe** Package IDs in Config.xml to specify SharePoint Foundation 2010 and SharePoint Server 2010 by entering the following:

```
<Configuration>
   <Package Id="sts">
   ...
   </Package>
   ...
   <Package Id="spswfe">
   ...
   </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 Office Servers\14.0\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 Product Key (PIDKEY) page (if it is needed), 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.
If the **Level** attribute is set to *Basic* or *None* and you supply a product key by using the PIDKEY Element element, Setup assumes that you also accept the license terms on behalf of the user. In this case, regardless of how you set the **AcceptEULA** attribute, the user is not prompted for the license terms during 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"
/>
```

INSTALLLOCATION Element
Specifies the fully qualified path of the folder on the user's computer in which the product is installed.
Syntax
<INSTALLLOCATION Value="*path***" />**
Attributes

Attribute	Value	Description
Value	path	The fully qualified path of the folder on the user's computer in which the product is installed.

Remarks
You can use system environment variables in the path. If this element is not specified, the product is installed in the following path:
%PROGRAMFILES%\Microsoft Office Servers\14.0\
Note that the SharePoint Foundation 2010 technology is not affected by this element; it is installed into the following path:
%COMMONPROGRAMFILES%\Common Files\Microsoft Shared\Web Server Extensions\14
Example

```
<INSTALLLOCATION VALUE="%ProgramFiles%\MyApps" />
```

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 Server 2010 is **spswfe**. Because SharePoint Server 2010 is based on the platform technology in SharePoint Foundation 2010, you must also install the **sts** (SharePoint Foundation 2010) package or the installation will not succeed.
PIDKEY Element
The 25-character volume license key.
Syntax
<PIDKEY Value="*25-character-key***" />**
Attributes

Attribute	Value	Description

Value	*25-character-key*	The 25-character volume license key.

Remarks
When the **PIDKEY** value is set, users are not required to enter a product key when they run Setup.
Example

```
<PIDKEY Value="12345123451234512345123 45" />
```

Note:
If the **Level** attribute of the Display Element element is set to *Basic* or *None* and you supply a product key by using the **PIDKEY** element, Setup assumes that you also accept the license terms on behalf of the user. In this case, regardless of how you set the **AcceptEULA** attribute of the Display Element element, the user is not prompted for the license terms during installation.

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
LAUNCHEDFROMSETUPSTS	Yes | No	Use as part of the Package Id attribute. The default is Yes.
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,	Specifies whether to install a

	V2V_INPLACE_UPGRADE, SKU2SKU_UPGRADE	new copy of the product or technology (CLEAN_INSTALL), install the new version and upgrade the previous version in place (V2V_INPLACE_UPGRADE), or upgrade from one product to another (such as from SharePoint Foundation 2010 to SharePoint Server 2010. 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. For a complete list of Windows Installer properties, including an explanation of supported and blocked properties, see Setup properties in Office 2010 (*http://technet.microsoft.com/library/41f07f9b-f0d0-489d-a185-d7b96f21f561(Office.14).aspx*).

Example

```
<Setting Id="REBOOT" Value="ReallySuppress" />
```

Windows PowerShell commands (SharePoint Server 2010)

Published: July 8, 2010

This article discusses the Windows PowerShell cmdlets that are needed to install Microsoft SharePoint Server 2010 on a stand-alone server or on a server farm.

In this article:

- Installing SharePoint Products by using Windows PowerShell
- Windows PowerShell installation cmdlets

For information about the commands and syntax that are used in scripted deployment of a SharePoint Server 2010 farm, see Scripted deployment reference (SharePoint Server 2010).

Installing SharePoint Products by using Windows PowerShell

In SharePoint Server 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 Server 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.
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

Windows PowerShell cmdlet	Description
	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*)

Enterprise search technical reference (SharePoint Server 2010)

Published: September 23, 2010

The articles in this section include information about enterprise search in Microsoft SharePoint Server 2010.

In this section:

- Default connectors (SharePoint Server 2010)
- File types and IFilters reference (SharePoint Server 2010)
- Languages for word breakers and stemmers (SharePoint Server 2010)

Default connectors (SharePoint Server 2010)

Published: September 23, 2010

This article lists the connectors, which were called *protocol handlers* in previous versions, that are installed by default in Microsoft SharePoint Server 2010. SharePoint Server 2010 uses connectors to connect to different content repositories so that the content in that repository can be crawled. You can install additional connectors to crawl content created by other Microsoft products or third-party software. For more information, see Install connectors (SharePoint Server 2010) (*http://technet.microsoft.com/library/77104730-7036-466c-8b79-0f89fcbe7b08(Office.14).aspx*). You can also develop additional connectors by using the SharePoint Server search connector framework. For more information, see SharePoint Server Search Connector Framework (*http://msdn.microsoft.com/en-us/library/ee556429.aspx*).
The following table shows the connectors that are installed by default in SharePoint Server 2010.

This connector	Is used to connect to this type of content repository
Bcs	Business Connectivity Services (internal protocol)
Bcs2	Business Connectivity Services URLs (internal protocol)
File	File shares
http	Web sites
https	Web sites over Secure Sockets Layer (SSL)
Notes	Lotus Notes databases
Rb	Exchange public folders for versions prior to Microsoft Exchange Server 2003
Rbs	Exchange public folders over SSL for versions prior to Exchange Server 2003
Sps	People profiles in Microsoft Office SharePoint Portal Server 2003
Sps3	People profiles in Microsoft Office SharePoint Server 2007
Sps3s	People profiles in Office SharePoint Server 2007 over SSL
Spss	People profiles in SharePoint Portal Server 2003 over SSL
Sts	SharePoint Team Services 1.0 sites (internal protocol)
Sts2	Windows SharePoint Services 2.0 and SharePoint Portal Server 2003 sites
Sts2s	Windows SharePoint Services 2.0 and SharePoint Portal Server 2003 sites over SSL
Sts3	Windows SharePoint Services 3.0 and Office

This connector	Is used to connect to this type of content repository
	SharePoint Server 2007 sites
Sts3s	Windows SharePoint Services 3.0 and Office SharePoint Server 2007 sites over SSL
Sts4	Microsoft SharePoint Foundation 2010 and SharePoint Server 2010 sites
Sts4s	SharePoint Foundation 2010 and SharePoint Server 2010 sites over SSL

File types and IFilters reference (SharePoint Server 2010)

Published: November 11, 2010

When crawling content, the crawler uses an IFilter to read individual file types. Some IFilters read only one file type, whereas others can read several file types. If you have to crawl a file type that is not supported by an IFilter that is provided with Microsoft SharePoint Server 2010, you must install and register the appropriate IFilter on the crawl server. The procedures used to install and register IFilters vary among different IFilters. If you want to use an IFilter that is not listed here, contact the manufacturer for instructions for installing third-party IFilters. If you add a file type without registering an IFilter, only the file properties are included in the index.

The following table lists the file types that appear by default on the **Manage File Types** page in Central Administration and describes whether their corresponding IFilters are registered by default. The table also lists file types that do not appear on the **Manage File Types** page by default but are supported by default IFilters. You can add these file types without having to register a new IFilter.

File name extension	IFilter supported by default?	File type included by default?
.ascx	Yes	Yes
.asm	Yes	No
.asp	Yes	Yes
.aspx	Yes	Yes
.bat	Yes	No
.c	Yes	No
.cmd	Yes	No
.cpp	Yes	No
.css	Yes	No
.csv	Yes	Yes
.cxx	Yes	No
.def	Yes	No
.dic	Yes	No
.doc	Yes	Yes
.docm	Yes	Yes
.docx	Yes	Yes
.dot	Yes	Yes
.dotx	Yes	Yes
.eml	Yes	Yes
.exch	No	Yes
.h	Yes	No
.hhc	Yes	No
.hht	Yes	No
.hpp	Yes	No

File name extension	IFilter supported by default?	File type included by default?
.hta	Yes	No
.htm	Yes	Yes
.html	Yes	Yes
.htw	Yes	No
.htx	Yes	No
.jhtml	No	Yes
.jsp	No	Yes
.lnk	Yes	No
.mht	Yes	Yes
.mhtml	Yes	Yes
.mpx	Yes	No
.msg	Yes	Yes
.mspx	No	Yes
.nsf	No	Yes
.odc	Yes	Yes
.odp	Yes	Yes
.ods	Yes	Yes
.odt	Yes	Yes
.one	No	No
.php	No	Yes
.pot	Yes	No
.pps	Yes	No
.ppt	Yes	Yes
.pptm	Yes	Yes
.pptx	Yes	Yes
.pub	No	Yes
.stm	Yes	No
.tif	Yes	Yes
.tiff	No	Yes
.trf	Yes	No
.txt	Yes	Yes
.url	No	Yes
.vdw	Yes	Yes
.vdx	Yes	Yes
.vsd	Yes	Yes
.vss	Yes	Yes
.vst	Yes	Yes
.vsx	Yes	Yes
.vtx	Yes	Yes
.xlc	Yes	No
.xls	Yes	Yes
.xlsb	Yes	Yes
.xlsm	Yes	Yes

File name extension	IFilter supported by default?	File type included by default?
.xlsx	Yes	Yes
.xlt	Yes	No
.xml	Yes	Yes
.zip	Yes	Yes

Languages for word breakers and stemmers (SharePoint Server 2010)

Published: May 12, 2010

This article lists the languages for which Microsoft SharePoint Server 2010 provides word breakers and stemmers. For information about using word breakers and stemmers with multilingual sites, see Plan for multilingual sites (SharePoint Server 2010) (*http://technet.microsoft.com/library/22d5dc9c-66bd-40d7-8c60-2a2a066db224(Office.14).aspx*). The following table lists the languages for which SharePoint Server 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.

Managing privacy (SharePoint Server 2010)

Published: May 12, 2010

Several features in Microsoft SharePoint Server 2010 interact with personally identifiable information. This document lists the features that store or use personally identifiable information and describes how that information is used. The article also tells you how to control the behavior of the features — or turn off the features — to help protect the privacy of the information.

In this article:

- Web Analytics
- SharePoint social tagging and Note Boards
- SharePoint ratings
- My Sites and user profiles
- Support for SharePoint Server Colleague add-in
- Activity feed
- SharePoint Search Federation
- SharePoint query logging
- Managed metadata and enterprise keywords

Web Analytics

The Web Analytics services enable SharePoint Server 2010 customers to understand more about visits to their SharePoint sites. The Web Analytics services collect data about how end-users access SharePoint pages. Data that is collected by the Web Analytics services can include but is not limited to the following information:

- The site from which the end-user starts
- The keywords that the end-user uses to find the SharePoint site
- The pages viewed on the site
- The searches run on the site
- The browser type

Important:
None of this information is sent to Microsoft unless Microsoft hosts the SharePoint site.

A member of the Farm Administrators group can decide not to use the Web Analytics services. The administrator either does not create a Web Analytics Service Application or stops the Web Analytics services by using the following procedure.

1. On the Central Administration Web site, on the Quick Launch, click **Monitoring** and in the **Reporting** section click **Configure usage and health data collection**.
   The Configure web analytics and health data collection page opens.
2. In the **Event Selection** section, clear the **Events to log** check boxes to stop logging these data points.

A member of the Farm Administrators group can disable the reporting of Web Analytics services data for a specific site collection.

1. On the top-level page of a site collection, on the **Site Actions** menu, click **Site Settings**.

2. In the **Site Collection Administration** section, click **Site collection features** and, next to **Advanced Web Analytics**, click **Deactivate**.

If a member of the Farm Administrators group stops the Web Analytics services or decides not to log certain data, subsequent logging is stopped, but information that is already logged will not immediately be deleted or removed from Web Analytics reports.

Members of the SharePoint Farm Administrators group can also set the limit on the period that the data is retained in the Web Analytics warehouse database. After the limit is reached, the data does not show in Web Analytics reports because the data is no longer in the database. For example, if the administrator sets the data retention period to one month, only data of the past month will appear in reports.

To set the limit on the data retention period:

1. On the Central Administration Web site, in the **Application Management** section, click **Manage service applications**.
2. Click the **Web Analytics Service Application** row to select it and in the **Operations** group of the ribbon click **Properties**.
3. In the dialog box, in the **Data Retention Period** section, set the data retention period, which can range from 1 month to 25 months.

SharePoint social tagging and Note Boards

The SharePoint Social Tagging and Note Boards features enable users to tag or add notes to SharePoint pages and Internet pages. By default, the SharePoint Social Tagging and Note Boards features are turned on. Social tagging can be turned off by a member of the Farm Administrators group, an administrator who has been assigned to a User Profile Service Application, or anyone who has the Manage Social Data permission. To turn off social tagging, remove the Use Social Features permission from a user or group.

When a user adds tags or notes, the user’s user name is stored with the tag or note. Tags and notes that users create appear in the activity feeds of both the users' Colleagues and any users who have the tag listed as an interest in their user profile.

Users can decide to have their tags marked as private — so that the tags' URLs are not visible to other users — by selecting the **Private** check box on the **Tag Entry** dialog box or by marking their items private from their Tags and Notes pages. Notes cannot be marked as private.

SharePoint ratings

SharePoint lets users add ratings to SharePoint list items and document library items. These ratings are also displayed on the activity feeds of users. User names are not displayed next to the ratings on SharePoint list items, document library items, or activity feeds. Microsoft SharePoint Server does store user names, and user names can be accessed through the SharePoint object model. By default, the SharePoint ratings feature is turned on. The ratings feature can be turned off by a member of the Farm Administrators group, an administrator who has been assigned to a User Profile Service Application, or anyone who has the Manage Social Data permission. To turn off ratings, remove the Use Social Features permission from a user or group. A SharePoint administrator can also disable the ratings control on SharePoint pages for a site collection so that users can no longer see the control on Web pages. The following is the Windows PowerShell command to disable the ratings control:

Disable-spfeature -id "915c240e-a6cc-49b8-8b2c-0bff8b553ed3" -url Site Collection Url -force -Confirm:$false

A SharePoint administrator must have both site collection administrator permissions and the Shell_Access and WSS_WPG Windows PowerShell permissions to perform this action.
This command disables the controls on the Web pages but does not delete existing ratings or associated user names from the SharePoint database. Ratings and associated user name data can be deleted permanently by using the SharePoint object model.

My Sites and user profiles

My Sites let users store and display personal information that other SharePoint users and applications can access. Users can personalize the appearance, behavior, and content of their My Site pages. Users can also update their SharePoint user profiles from their My Site pages. By default, some user information, such as name, account name, e-mail address, telephone number, and manager's name, is included in the My Site and SharePoint profiles. A User Profile service administrator who has Manage Profile permissions can configure user profiles to include specific data in a user's My Site and SharePoint profiles.

1. On the Central Administration Web site, in the **Application Management** section, click **Manage service applications**.
2. Click **User Profile Service**, and in the **People** section, click **Manage User Profiles**.

Each profile property has an associated privacy level. Microsoft SharePoint Server supports the following privacy levels:

Only Me	My Manager	My Team	My Colleagues	Everyone

Users can choose privacy levels that help ensure that data that is stored in their profiles is visible only to intended people. A User Profile Service administrator with Manage Profile permissions can configure a default privacy level for a profile property and enable users to override it. A SharePoint administrator can also enforce a privacy level on a particular profile property so that users cannot override it.

1. On the Central Administration Web site, click **Manage service applications**.
2. Click **User Profile Service**, and then click **Profile services policies**.

Except for the My Team and My Colleagues privacy levels, profile privacy levels are automatically computed by SharePoint Server. Users decide which people are at the My Team and My Colleagues privacy levels. My Colleagues refers to Colleague relationships that a user has identified. My Team is a subset of Colleagues who are specified by a user.
User Profile service administrators with Manage Profile permissions who manage the databases for profile data have access to all data regardless of privacy levels that users set.

Support for SharePoint Server Colleague add-in

The SharePoint Server Colleague Add-in feature in Microsoft Outlook 2010 scans a user's sent e-mail folder to look for specific names and keywords and the frequency of those names and keywords. A list of suggested keywords is available on the Edit profile page of the user profile. The list is updated periodically and stored in the user's profile on his or her local computer. The list of possible colleagues is accessed by the Add Colleagues page on the My Site, where users can choose the colleagues they want to add to their trusted My Site. A user must approve or reject each contact name or keyword before it is added to the user profile. Members of the SharePoint Farm Administrators group can turn off this functionality and prevent My Sites from accessing this information by setting the following Group Policy setting registry key.

HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Portal\ColleagueImport\Enabled
Values = DWORD 0 to turn it off and 1 to turn it on.
An end user can turn off both or either the analysis of content in the Sent Items e-mail folder and the uploading of contact names and keywords to My Site by following these steps:
1. On the **File** menu of Outlook 2010, click **Options**.
2. In the Outlook Options dialog box, click **Advanced**.
3. In the **Other** section, clear the option that allows analysis of sent e-mails and subjects.

Activity feed

Activity Feed lets users add feeds of events to their My Sites. Feeds might give information about activities of their Colleagues, such as updates to profile properties and creation of social tags and notes. Activity Feed does not enable tracking of activities that a user does not have permissions to see.
Activity Feed is off by default in a User Profile Service Application. To turn on this feature, a member of the Farm Administrators group must configure the User Profile service Activity Feed timer job.
1. On the Central Administration Web site, on the Quick Launch, click **Monitoring**.
2. In the **Timer Jobs** section, click **Review job definitions**.
3. Click **User Profile Service – Activity Feed Job** in the list of timer jobs.
4. On the **Edit Timer Job** page, click **Enable**.

Users choose their Colleagues for their My Site by selecting names of other users and setting them as Colleagues. When a user is selected as a Colleague, a notification e-mail message is sent to the new Colleague.

SharePoint Search Federation

SharePoint Search Federation allows an administrator for a Search Service Application to provide results from multiple search providers for user queries. By default, SharePoint Search Federation searches only local SharePoint content. An administrator for a Search Service Application can add search providers, such as any third-party remote or online search engine. If an administrator for a Search Service Application adds a search provider, user queries are sent to that search provider, and the results returned by the search provider are displayed. Information about the privacy practices of the Microsoft Bing search engine is at http://go.microsoft.com/fwlink/?LinkID=147849. Microsoft does not control the data collection and use practices of third-party search providers.

SharePoint query logging

SharePoint search collects information about user search queries and about the search results that users select on their computers. SharePoint uses this information to improve the relevancy of search results and to improve query suggestions. Members of the Farm Administrators group or an administrator of the Search Service Application can also create reports, depending on this information.
Query logging can be turned off as follows:
1. On the Central Administration Web site, in the **Application Management** section, click **Manage service applications**.

2. Click **Search Service Application** and in the **System Status** section of the Search Service Application page, click the **Disable** link next to **Query logging**.

Managed metadata and enterprise keywords

Enterprise keywords are managed metadata values from a term store that are stored in a special column type. Instead of being bound to a single term set, this column type is validated against all available terms in all accessible term sets. However, this column type is not validated against term sets that are specific to a site collection and does not participate in enterprise keyword validation.

Default behavior

By default, both managed metadata and enterprise keyword columns are available in SharePoint Server 2010. These columns can be applied to a content type or list. After either the managed metadata or enterprise keywords column is applied to a content type, the data that users enter in these fields is stored in a term store database.

Enterprise keywords and managed metadata should generally be considered public and readable by all users. If an enterprise keyword column or a managed metadata column is bound to a globally available term set, all metadata that users create will be accessible to other enterprise users who are viewing or validating terms.

After managed metadata and enterprise keyword columns are used, and user data is stored in and shared from the term store database, a SharePoint list can be configured to share its managed metadata and enterprise keyword data with the social tagging database that the User Profile service maintains. Doing so expands the visibility of a user's data to all users of any features that rely on the social tagging database, with the exception of user data in columns that are bound to term sets. Metadata values that are stored in site collectionspecific term sets will not be shared with the social tagging database regardless of whether the list setting is enabled to share with the social tagging database or not.

User interface text for managing the feature

The UI displays the following descriptive text:

- When you add enterprise keywords to either a list or content type, you see the following descriptive text:
  Enterprise Keywords are shared with other users to allow for ease of search and filtering, as well as metadata consistency and reuse.
- The list settings UI gives list owners a shortcut for adding the enterprise keywords column. The UI displays the following text:
  Add Enterprise Keywords
  An Enterprise Keyword column allows users to enter one or more text values that will be shared with other users and application to allow for ease of search and filtering, as well as metadata consistency and reuse.
  Adding an Enterprise Keywords column also provides synchronization between existing legacy keyword fields and the managed metadata infrastructure. (Document tags will be copied into the Enterprise Keywords on upload.)
- The same list settings page displays the following descriptive text for metadata promotion:
  Values added to columns of types Managed Metadata and Enterprise Keywords can be shared with the Social service in order for metadata and keyword tags on items in this list to appear in tag clouds.

User permissions and permission levels (SharePoint Server 2010)

Updated: January 7, 2011

This article describes the default permission levels as well as the user permissions in Microsoft SharePoint Server 2010.

In this article:

- Default permission levels
- User permissions

Default permission levels

Permission levels are collections of permissions that allow users to perform a set of related tasks. SharePoint Server 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 specific permissions you need. For more information about how to customize permission levels, see Configure custom permissions (SharePoint Server 2010)(*http://technet.microsoft.com/library/c5dd8b7e-202d-4d33-8535-5c03f88ea1ff(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 Server 2010) (*http://technet.microsoft.com/library/28a53440-2adc-4957-84bd-99ed97f0c430(Office.14).aspx*).

The following table lists the default permission levels for team sites in SharePoint Server 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 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.	• View Application Pages • Browse User Information • Use Remote Interfaces • Use Client Integration Features • Open
Read	View pages, list items and	• Limited Access

Permission level	Description	Permissions included by default
	download documents.	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

If you use a site template other than the team site template, you will see a different list of default SharePoint groups. For example, the following table shows additional permission levels provided with the publishing template.

Permission level	Description	Permissions included by default
Restricted Read	View pages and documents. For publishing sites only.	• View Items • Open Items • View Pages • Open
Approve	Edit and approve pages, list items, and documents. For publishing sites only.	• Contribute permissions, plus: • Override Checkout • Approve Items
Manage Hierarchy	Create sites; edit pages, list items, and documents. For Publishing sites only.	• Design permissions minus the Approve Items, Apply Themes and Borders, and Apply Style Sheets permissions, plus:

Permission level	Description	Permissions included by default
		• Manage permissions • View Web Analytics Data • Create Subsites • Manage Alerts • Enumerate Permissions • Manage Web Site

User permissions

SharePoint Server 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	View Pages, Open	Read,

Permission	Description	Dependent permissions	Included in these permission levels by default
	documents in document libraries.		Contribute, Design, Full Control
Approve Items	Approve minor versions of list items or documents.	Edit Items, View Items, View Pages, Open	Design, Full Control
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
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	Use features that start	Use Remote Interfaces,	All

Permission	Description	Dependent permissions	Included in these permission levels by default
Features	client applications. Without this permission, users must work on documents locally and then upload their changes.	Open	
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 Server 2010)
(*http://technet.microsoft.com/library/c5dd8b7e-202d-4d33-8535-5c03f88ea1ff(Office.14).aspx*)

Database types and descriptions (SharePoint Server 2010)

Updated: July 29, 2010

This article describes the databases that are installed for Microsoft SharePoint Server 2010. It includes some sizing and placement information. For more information about where to locate databases, see Plan for SQL Server, storage and BLOB configuration (SharePoint Server 2010) (*http://technet.microsoft.com/library/a96075c6-d315-40a8-a739-49b91c61978f(Office.14).aspx*). Databases for SharePoint Server 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 Server 2010) (*http://technet.microsoft.com/library/4d88c402-24f2-449b-86a6-6e7afcfec0cd(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 Server 2010) (*http://technet.microsoft.com/library/798aa915-7025-4adc-a210-4f6ff14c43fc(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:

- SharePoint Foundation 2010 databases (*http://technet.microsoft.com/library/c852ebba-48b4-433c-83c3-e774e88d6680(Office.14).aspx#Section1*)
- SharePoint Server 2010, Standard Edition databases (*http://technet.microsoft.com/library/c852ebba-48b4-433c-83c3-e774e88d6680(Office.14).aspx#Section2*)
- SharePoint Server 2010, Enterprise Edition databases (*http://technet.microsoft.com/library/c852ebba-48b4-433c-83c3-e774e88d6680(Office.14).aspx#Section3*)
- Project Server 2010 databases (*http://technet.microsoft.com/library/c852ebba-48b4-433c-83c3-e774e88d6680(Office.14).aspx#Section4*)

If you are running SharePoint Server 2010, you may also have Microsoft Project Server 2010 in the environment.

- FAST Search Server for SharePoint 2010 databases (*http://technet.microsoft.com/library/c852ebba-48b4-433c-83c3-e774e88d6680(Office.14).aspx#Section5*)
  If you are running SharePoint Server 2010, you may also have Microsoft FAST Search Server 2010 for SharePoint in the environment.
- SQL Server system databases (*http://technet.microsoft.com/library/c852ebba-48b4-433c-83c3-e774e88d6680(Office.14).aspx#Section6*)
- SQL Server Reporting Services databases (*http://technet.microsoft.com/library/c852ebba-48b4-433c-83c3-e774e88d6680(Office.14).aspx#Section7*)

For a graphical overview of the databases used by SharePoint Server 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 Server 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 Server 2010) (*http://technet.microsoft.com/library/a6d383c0-3817-4acd-afa9-ad7a9b7e6b5a(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 Server 2010) (*http://technet.microsoft.com/library/8404adef-6bfb-4795-be16-15739e1212f5(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. If Microsoft SQL Server PowerPivot for Microsoft SharePoint is installed, the Central Administration content database also stores the Excel worksheets and PowerPivot data files used in the PowerPivot Management Dashboard.

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. If you are using PowerPivot, the Central Administration content will grow over the span of one year, assuming that you use default settings that keep usage data collection and data refresh history for 365 days. For more information about PowerPivot for SharePoint, see Plan a PowerPivot Deployment in a SharePoint Farm (*http://go.microsoft.com/fwlink/?LinkID=186698*).
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 Server 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*).

Content databases also store user data for PowerPivot for SharePoint, if it has been installed in the environment.

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. For specific guidance about how to size content databases, see Plan for SQL Server, storage and BLOB configuration (SharePoint Server 2010) (*http://technet.microsoft.com/library/a96075c6-d315-40a8-a739-49b91c61978f(Office.14).aspx*).
Associated Health rules	None
Supported backup mechanisms	SharePoint Server 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*).

If PowerPivot for SharePoint is in use, the Excel files stored in SharePoint Server grow larger, which increases the size of the content database. For more information, see Plan a PowerPivot Deployment in a SharePoint Farm (*http://go.microsoft.com/fwlink/?LinkID=186698*).

For detailed recommendations about how to calculate the size of a content database, see Storage and SQL Server capacity planning (SharePoint Server 2010) (*http://technet.microsoft.com/library/a96075c6-d315-40a8-a739-49b91c61978f(Office.14).aspx*).

Usage and Health Data Collection database

The Usage and Health Data Collection database is used by the Usage and Health Data Collection service application. It 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 Server 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 Server 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	Bdc_Service_DB_

by using the SharePoint Products Configuration Wizard	
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 Server 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 Server 2010 backup and recovery, SQL Server, and DPM 2010.
Default recovery model	Full
Supports mirroring within a farm for	Yes

availability	
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 Server 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

SharePoint Server 2010, Standard Edition databases

The following databases are part of a SharePoint Server 2010, Standard Edition deployment.
Secure Store database
The Secure Store service application database stores and maps credentials, such as account names and passwords.

Default database name prefix when installed	Secure_Store_Service_DB_

by using the SharePoint Products Configuration Wizard	
Location requirements	For secure credential storage, we recommend that the secure store database be hosted on a separate database instance or database server that has access limited to one administrator. By default, if the database is hosted on the default SharePoint database server and instance, all database administrators will have access to the secure store database.
General size information, and growth factors	Medium. Size and growth are determined by the number of target applications, number of credential fields per target application, and the number of users stored in each target application.If auditing is turned on, the number of read/write operations performed against a given target application also affects size.
Read/write characteristics	Equal read/write ratio
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 Server 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

State database
The State service application database stores temporary state information for InfoPath Forms Services, the chart Web Part, and Visio Services.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	StateService
Location requirements	None
General size information, and growth factors	Medium-large. Size is determined by the use of InfoPath Forms services and Visio Services.
Read/write characteristics	Varies
Recommended scaling method	Scale out; add another state database to the service application by using Windows PowerShell cmdlets. For

	more information, see Manage the State Service (SharePoint Server 2010) (*http://technet.microsoft.com/library/5765c57c-372b-4974-a60a-2277996550aa(Office.14).aspx*).
Associated Health rules	None
Supported backup mechanisms	SharePoint Server 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

Web Analytics Staging database
The Staging database temporarily stores un-aggregated fact data, asset metadata, and queued batch data for the Web Analytics service application.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	WebAnalyticsServiceApplication_StagingDB_
Location requirements	None
General size information, and growth factors	Medium. Size varies based on the number of reports being generated
Read/write characteristics	Varies
Recommended scaling method	Scale out; associate another Web Analytics Staging database with the service application instance.
Associated SharePoint health rules	A rule checks whether the service broker queue is enabled for the Web Analytics databases.
Supported backup mechanisms	SharePoint Server 2010 backup and recovery, SQL Server, and DPM 2010.
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

Web Analytics Reporting database
The Reporting database stores aggregated standard report tables, fact data aggregated by groups of sites, date and asset metadata, and diagnostics information for the Web Analytics service application.

Important:
For large-scale environments, we recommend that you run the Web Analytics service application Reporting database on a server that is running SQL Server 2008 Enterprise Edition so that the Web Analytics service application can take advantage of table partitioning.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	WebAnalyticsServiceApplication_ReportingDB_
Location requirements	None
General size information, and growth factors	Extra-large. Size varies based on retention policy.
Read/write characteristics	Varies
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	A rule checks whether the service broker queue is enabled for the Web Analytics databases.
Supported backup mechanisms	SharePoint Server 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

Search service application Administration database
The Administration database hosts the Search service application configuration and access control list (ACL), and best bets for the crawl component. This database is accessed for every user and administrative action.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	Search_Service_Application_DB_
Location requirements	The Administration database should fit into RAM on the server so that the server can handle the end-user query load most efficiently. Because of this requirement, it is usually best not to have the Administration and Crawl databases located on the same server.
General size information, and growth factors	Small to medium. The factors that influence growth include the number of best bets, the number of content sources and crawl rules, the

	security descriptions for the corpus, and the amount of traffic.
Read/write characteristics	Approximately equal read/write ratio
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 Server 2010 backup and recovery.
Default recovery model	Simple
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

Search service application Crawl database
The Crawl database stores the state of the crawled data and the crawl history.

Important:
For large-scale environments, we recommend that you run the Crawl database on a server that is running SQL Server 2008 Enterprise Edition so that the service application can take advantage of data compression.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	Search_Service_Application_CrawlStoreDB_
Location requirements	The Crawl database is very I/O intensive, and causes the SQL Server cache to be flushed regularly. In large-scale environments, we recommend that you locate this database on a server that does not contain the Property database or other databases involved in end-user tasks.
General size information, and growth factors	Medium to large. Generally, the Crawl database starts medium-sized and grows over time, without shrinking. The factors that influence growth are the number of items in the corpus.
Read/write characteristics	Read-heavy. The read/write ratio is 3:1.
Recommended scaling method	Scale out; associate another Crawl database with the service application instance. Multiple Crawl databases can be placed on the same server, if the server can handle the I/O per second required.
Associated Health rules	The **Search - One or more crawl databases may have fragmented indices on-demand health rule**

	defragments indices health rule rebuilds statistics, and — if the system is running SQL Server Enterprise Edition — turns on data compression at the page level.
Supported backup mechanisms	SharePoint Server 2010 backup and recovery.
Default recovery model	Simple
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No

Search service application Property database
The Property database stores information that is associated with the crawled data, including properties, history, and crawl queues.

Important:
For large-scale environments, we recommend that you run the Property database on a server that is running SQL Server 2008 Enterprise Edition so that the service application can take advantage of data compression.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	Search_Service_Application_PropertyStoreDB_
Location requirements	At least one-third of the Property database should fit into RAM on the server. In large-scale environments, we recommend that you put this database on its own server to achieve faster query results.
General size information, and growth factors	Large to extra-large. Factors that influence growth are the number of managed properties and the number of documents.
Read/write characteristics	Write-heavy. The read/write ratio is 1:2.
Recommended scaling method	Scale out; associate another Property database with the service application instance. We recommend that you locate each additional Property database on a different server.
Associated Health rules	The **Search - One or more property databases have fragmented indices** health rule runs once a week by default. It defragments indices, rebuilds statistics, and — if the system is running SQL Server Enterprise Edition — turns on data compression.
Supported backup mechanisms	SharePoint Server 2010 backup and recovery.
Default recovery model	Simple
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring	No

or log-shipping to another farm for disaster recovery	

User Profile service application Profile database
The Profile database stores and manages users and associated information. It also stores information about a user's social network in addition to memberships in distribution lists and sites.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	User Profile Service Application_ProfileDB_
Location requirements	None
General size information, and growth factors	Medium to large. Growth factors include additional users and the use of news feeds. News feeds grow with user activities. The default is to maintain the last two weeks of activity, after which a timer job deletes the news feed items older than two weeks.
Read/write characteristics	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 Server 2010 backup and recovery.
Default recovery model	Simple
Supports mirroring within a farm for availability	Yes
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	No, however, an administrator can use the User Profile Replication Engine, part of the SharePoint Administration Toolkit, to replicate user profiles and social data, such as social tags, notes, and ratings, between User Profile Service applications. This replication can be one-way or bidirectional. For more information, see User Profile Replication Engine overview (SharePoint Server 2010).

User Profile service application Synchronization database
The Synchronization database stores configuration and staging data for use when profile data is being synchronized with directory services such as Active Directory.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	User Profile Service Application_SyncDB_

Location requirements	
General size information, and growth factors	Medium to large. Growth factors include the number of users and groups, and the ratio of users to groups.
Read/write characteristics	Approximately equal read/write ratio.
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 Server 2010 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, however, an administrator can use the User Profile Replication Engine, part of the SharePoint Administration Toolkit, to replicate user profiles and social data, such as social tags, notes, and ratings, between User Profile Service applications. This replication can be one-way or bidirectional. For more information, see User Profile Replication Engine overview (SharePoint Server 2010).

User Profile service application Social Tagging database
The Social Tagging database stores social tags and notes created by users, along with their respective URLs.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	User Profile Service Application_SocialDB_
Location requirements	None
General size information, and growth factors	Small to extra large. Growth factors include the number of tags, ratings and notes that have been created and used.
Read/write characteristics	Read-heavy. The read/write ratio is approximately 50:1.
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 Server 2010 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, however, an administrator can use the User Profile Replication Engine, part of the SharePoint Administration Toolkit, to replicate user profiles and social data, such as social tags, notes, and ratings, between User Profile Service applications. This replication can be one-way or bidirectional. For more information, see User Profile Replication Engine overview (SharePoint Server 2010).

Managed Metadata database
The Managed Metadata service application database stores managed metadata and syndicated content types.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	Managed Metadata Service_
Location requirements	None
General size information, and growth factors	Medium. Growth factors include the amount of managed metadata.
Read/write characteristics	Read-heavy. The read/write ratio is approximately 1,000:1.
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 Server 2010 backup and recovery.
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

Word Automation Services database
The Word Automation Services database stores information about pending and completed document conversions.

Default database name prefix when installed by using the SharePoint Products	WordAutomationServices_

Configuration Wizard	
Location requirements	None
General size information, and growth factors	Small
Read/write characteristics	Varies
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 Server 2010 backup and recovery.
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

SharePoint Server 2010, Enterprise Edition databases

The following databases are part of a SharePoint Server 2010, Enterprise Edition deployment, in addition to the databases that ship with the Standard Edition.

PerformancePoint service application database

The PerformancePoint service application database stores temporary objects, persisted filter values, and user comments.

Note:

Microsoft SQL Server 2008 Analysis Services (SSAS) is also recommended as a data source for the PerformancePoint service application. If you have configured SQL Server Analysis Services and created cubes, additional functionality, such as drill-down analytics from published dashboards, becomes available.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	PerformancePoint Service Application_
Location requirements	None
General size information, and growth factors	Small. User comments and annotations are persisted indefinitely and increase based on the number of application users. Temporary items are removed once per day.
Read/write characteristics	Varies
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	The **Database not available** health rule verifies that the PerformancePoint database is available.
Supported backup mechanisms	SharePoint Server 2010 backup and recovery.
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

Project Server 2010 databases

Project Server 2010 requires SharePoint Server 2010, Enterprise Edition.

Draft database

The Draft database contains data for editing projects. This database also hosts the tables used by the Project Queue. Data in the Draft database is not directly accessible by end users.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	ProjectServer_Draft
Location requirements	Must be located on the same database instance as the Published and Archive databases.
General size information, and growth factors	Medium
Read/write characteristics	Equal read/write ratio.
Recommended scaling method	Scale up the database that supports the service application instance.
Associated Health rules	None
Supported backup mechanisms	SharePoint Server 2010 and SQL Server backup and recovery.
Default recovery model	Full
Supports mirroring within a farm for availability	Yes, but you must follow additional steps.
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	Yes, but you must synchronize the logs of all of the databases.

Published database

The Published database contains a copy of all of the projects that have been published. The Published database also contains tables that are specific to Project Server (timesheets, resources, custom fields, security definitions, and other metadata). This database also hosts the

tables used by the Timesheet Queue. Data in the Published database is not directly accessible by end users.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	ProjectServer_Published
Location requirements	Must be located on the same database server as the Draft and Archive databases.
General size information, and growth factors	Medium
Read/write characteristics	Equal read/write ratio
Recommended scaling method	Scale up the database that supports the service application instance.
Associated Health rules	None
Supported backup mechanisms	SharePoint Server 2010 and SQL Server backup and recovery.
Default recovery model	Full
Supports mirroring within a farm for availability	Yes, but you must follow additional steps.
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	Yes, but you must synchronize the logs of all of the databases.

Archive database
The Archive database stores the backup data of projects, resources, calendars, enterprise custom fields, the enterprise global Project Web Access view definitions, Project Web Access system settings, and category and group security settings as set up by the Project Web Access administrator. Data in the Archive database is not directly accessible by end users.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	ProjectServer_Archive_
Location requirements	Must be located on the same database server as the Draft and Published databases.
General size information, and growth factors	Small, but can grow to extra large. If your system is using archiving functionality, this database will be at least as large as the Draft database, but is likely to be much larger. You can set a limit for the size of the Archive database to be no larger than a specified multiplier of the Draft database.
Read/write characteristics	Equal read/write ratio.
Recommended scaling method	Scale up the database that supports the service application instance.
Associated Health rules	None
Supported backup mechanisms	SharePoint Server 2010 and SQL Server backup and recovery.
Default recovery model	Full
Supports mirroring within a farm for	Yes, but you must follow additional steps.

availability	
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	Yes, but you must synchronize the logs of all of the databases.

Reporting database
The Reporting database is the repository for the entire portfolio of projects in Project Server. These tables present stable snapshots of each project plan based on the last time a project was published to Project Server and include de-normalized time phased data, allowing for advanced reporting capabilities outside of the Project client. Data in the Reporting database is accessible by end users.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	ProjectServer_Reporting
Location requirements	None
General size information, and growth factors	Large
Read/write characteristics	Read-heavy
Recommended scaling method	Scale up the database that supports the service application instance.
Associated Health rules	None
Supported backup mechanisms	SharePoint Server 2010 and SQL Server backup and recovery.
Default recovery model	Full
Supports mirroring within a farm for availability	Yes, but you must follow additional steps to ensure that the Project databases and logs are fully synchronized.
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	Yes, but you must follow additional steps to ensure that the Project databases and logs are fully synchronized.

FAST Search Server for SharePoint 2010 databases

FAST Search Server 2010 for SharePoint requires SharePoint Server 2010, Enterprise Edition.
Search Administration database
The Search Administration database stores and manages data related to administration of FAST Search Server 2010 for SharePoint. This includes search setting groups, keywords, synonyms, document and site promotions and demotions, term entity extractor inclusions and exclusions, spell check exclusions, best bets, visual best bets, and search schema metadata.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	FASTSearchAdminDatabase
Location requirements	None
General size information, and growth factors	Small. Growth and size are affected by the

	number of keywords, synonyms, document promotions and demotions, site promotions and demotions, term entity extractor inclusions, term entity extractor exclusions, spell checking exclusions, best bets, and visual best bets.
Read/write characteristics	Read-heavy
Recommended scaling method	Scale up the database. (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

PowerPivot for SharePoint

PowerPivot for SharePoint extends SharePoint Server 2010 and Excel Services to add server-side processing, collaboration, and document management support for the PowerPivot workbooks that you publish to SharePoint Server 2010.
PowerPivot for SharePoint requires that SQL Server 2008 R2 Enterprise Edition Analysis Services be installed in the environment.

Note:
The use of PowerPivot for SharePoint also influences the size of the Central Administration content database and the content databases in which the Excel workbooks are stored. For more information, see Plan a PowerPivot Deployment in a SharePoint Farm (*http://go.microsoft.com/fwlink/?LinkID=186698*).

PowerPivot Application database
The PowerPivot Application database stores the location of cached or loaded PowerPivot data files, data refresh schedules, and PowerPivot usage data that is copied from the central usage data collection database.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	DefaultPowerPivotServiceApplicationDB
Location requirements	None
General size information, and growth factors	Small
Read/write characteristics	
Recommended scaling method	Scale up the database that supports the service application instance.
Associated Health rules	None. Rely on SQL Server health rules.
Supported backup mechanisms	SQL Server backup and recovery.

Default recovery model	Full
Supports mirroring within a farm for availability	Yes, but mirroring is managed solely through SQL Server: SharePoint Server 2010 is not aware of the PowerPivot database.
Supports asynchronous mirroring or log-shipping to another farm for disaster recovery	Yes

SQL Server system databases

SharePoint Server 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

SQL Server Reporting Services databases

The following SQL Server Reporting Services databases can be used as part of a SharePoint Server 2010 deployment.

Note:
If your deployment requires the use of Access Services, then the requirements for Reporting Services depend on the mode in which you are running, as follows:

- Local mode requires only SharePoint Server 2010 and the SQL Server 2008 R2 Reporting Services (SSRS) Add-in.
- Connected mode requires SharePoint Server 2010, the SSRS Add-in, and a SQL Server 2008 R2 Report Server, available in Standard or Enterprise Edition.

For more information about how to manage SQL Server Reporting Services databases, see Report Server Catalog Best Practices (*http://go.microsoft.com/fwlink/?LinkID=185486*).

ReportServer database

The SQL Server Reporting Services ReportServer database stores all report metadata including report definitions, report history and snapshots, and scheduling information.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	RSDB
Location requirements	Must be located on the same database server as the ReportServerTempDb database.
General size information, and growth factors	Small
Read/write characteristics	Read-heavy
Recommended scaling method	Scale up the database
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

ReportServerTempDB database

The SQL Server Reporting Services ReportServerTempDB database stores all the temporary snapshots while reports are running.

Default database name prefix when installed by using the SharePoint Products Configuration Wizard	RSTempDB
Location requirements	Must be located on the same database server as the ReportServer database.
General size information, and growth factors	Small to extra large. The size of the ReportServerTempDB database goes both up and down quickly, depending on the number of concurrent interactive users, and the number of report snapshots.
Read/write characteristics	Read-heavy
Recommended scaling method	Scale up the database
Associated Health rules	None
Supported backup mechanisms	SQL Server backup and recovery, but we do not recommend that you back up this database.
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

Language packs (SharePoint Server 2010)

Updated: September 16, 2010

This article lists the language packs that are available for Microsoft SharePoint Server 2010. Language packs enable you to create sites and site collections in multiple languages without requiring separate installations of SharePoint Server 2010 in each language. For more information about language packs, see Deploy language packs (SharePoint Server 2010) (*http://technet.microsoft.com/library/26c07867-0150-463d-b21a-a6d42aecf05a(Office.14).aspx*). The language packs can be downloaded at 2010 Server Language Packs for SharePoint Server 2010, Project Server 2010, Search Server 2010, and Office Web Apps 2010 (*http://go.microsoft.com/fwlink/?LinkID=192105&clcid=0x409*).

The following table lists the language packs that are available for SharePoint Server 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
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

Language	Language ID
Portuguese (Portugal)	2070
Romanian	1048
Russian	1049
Serbian (Latin)	2074
Slovak	1051
Slovenian	1060
Spanish	3082
Swedish	1053
Thai	1054
Turkish	1055
Ukrainian	1058

Regional settings (SharePoint Server 2010)

Published: April 28, 2011

This article lists the regional settings for Microsoft SharePoint Server 2010.

In this article:

- Locale
- Sort order
- Time zone
- Calendar
- Currency

SharePoint Server 2010 uses the following types of regional settings: locale, time zone, sort order, calendar, and currency. Although currency is not a regional setting per se, the default value of the currency is determined by the locale you specified in your regional settings. You specify the locale, sort order, time zone, and calendar settings on the Regional Settings page, and you specify the currency settings on the Create Column page when you work with lists.

For more information about how to access and modify regional settings, see Regional Settings Schema (*http://go.microsoft.com/fwlink/?LinkId=217116*).

Locale

The locale setting controls numbering, sorting, calendar, and date and time formatting for the Web site. You can change the locale for a Web site by using the Regional Settings page. You can set the locales for your SharePoint sites to the locales shown in the following table.

ID	Locale	ID	Locale
1078	Afrikaans	1089	Kiswahili
1052	Albanian	1111	Konkani
1156	Alsatian	1042	Korean
1118	Amharic	1088	Kyrgyz
5121	Arabic (Algeria)	1108	Lao
15361	Arabic (Bahrain)	1062	Latvian
3073	Arabic (Egypt)	1063	Lithuanian
2049	Arabic (Iraq)	2094	Lower Sorbian
11265	Arabic (Jordan)	4155	Lule Sami (Norway)
13313	Arabic (Kuwait)	5179	Lule Sami (Sweden)
12289	Arabic (Lebanon)	1134	Luxembourgish
4097	Arabic (Libya)	1071	Macedonian
6145	Arabic (Morocco)	1086	Malay (Malaysia)
8193	Arabic (Oman)	2110	Malay (Brunei Darussalam)
16385	Arabic (Qatar)	1100	Malayalam

ID	Locale	ID	Locale
1025	Arabic (Saudi Arabia)	1082	Maltese
10241	Arabic (Syria)	1153	Maori
7169	Arabic (Tunisia)	1146	Mapudungun
14337	Arabic (U.A.E.)	1102	Marathi
9217	Arabic (Yemen)	1148	Mohawk
1067	Armenian	1104	Mongolian (Cyrillic)
1101	Assamese	2128	Mongolian (Mongolian)
2092	Azeri (Cyrillic)	1121	Nepali
1068	Azeri (Latin)	3131	Northern Sami (Finland)
1133	Bashkir	1083	Northern Sami (Norway)
1069	Basque	2107	Northern Sami (Sweden)
1059	Belarusian	1044	Norwegian (Bokmal)
1093	Bengali (India)	2068	Norwegian (Nynorsk)
2117	Bengali (Bangladesh)	1154	Occitan
5146	Bosnian (Latin)	1096	Oriya
8218	Bosnian (Cyrillic)	1123	Pashto
1150	Breton	1065	Persian
1026	Bulgarian	1045	Polish
1027	Catalan	1046	Portuguese (Brazil)
3076	Chinese (Hong Kong S.A.R.)	2070	Portuguese (Portugal)
5124	Chinese (Macau SAR)	1094	Punjabi
2052	Chinese (PRC)	3179	Quechua (Peru)
4100	Chinese (Singapore)	2155	Quechua (Ecuador)
1028	Chinese (Taiwan)	1131	Quechua (Bolivia)
1155	Corsican	1048	Romanian
1050	Croatian (Croatia)	1047	Romansh
4122	Croatian (Bosnia and Herzegovina)	1049	Russian
1029	Czech	1157	Sakha
1030	Danish	1103	Sanskrit
1164	Dari	2074	Serbian (Latin)
1125	Divehi	3098	Serbian (Cyrillic)
2067	Dutch (Belgium)	6170	Serbian (Bosnia and Herzegovina)
1043	Dutch (Netherlands)	7194	Serbian (Bosnia

ID	Locale	ID	Locale
			and Herzegovina)
3081	English (Australia)	1132	Sesotho sa Leboa
10249	English (Belize)	1074	Setswana
4105	English (Canada)	1115	Sinhala
9225	English (Caribbean)	8251	Skolt Sami
6153	English (Ireland)	1051	Slovak
16393	English (India)	1060	Slovenian
8201	English (Jamaica)	6203	Southern Sami (Norway)
17417	English (Malaysia)	7227	Southern Sami (Sweden)
5129	English (New Zealand)	21514	Spanish (United States)
13321	English (Philippines)	2058	Spanish (Mexico)
18441	English (Singapore)	3082	Spanish (Spain)
7177	English (South Africa)	19466	Spanish (Nicaragua)
11273	English (Trinidad and Tobago)	6154	Spanish (Panama)
2057	English (United Kingdom)	15370	Spanish (Paraguay)
1033	English (United States)	10250	Spanish (Peru)
12297	English (Zimbabwe)	20490	Spanish (Puerto Rico)
1061	Estonian	1034	Spanish (Traditional Sort)
1080	Faeroese	4106	Spanish (Guatemala)
1124	Filipino	14346	Spanish (Uruguay)
1035	Finnish	8202	Spanish (Venezuela)
2060	French (Belgium)	5130	Spanish (Costa Rica)
3084	French (Canada)	7178	Spanish (Dominican Republic)
1036	French (France)	9226	Spanish (Colombia)
5132	French (Luxembourg)	11274	Spanish (Argentina)
6156	French (Monaco)	12298	Spanish (Ecuador)
4108	French (Switzerland)	13322	Spanish (Chile)
1122	Frisian	16394	Spanish (Bolivia)

ID	Locale	ID	Locale
1110	Galician	17418	Spanish (El Salvador)
1079	Georgian	18442	Spanish (Honduras)
3079	German (Austria)	2077	Swedish (Finland)
1031	German (Germany)	1053	Swedish (Sweden)
5127	German (Liechtenstein)	1114	Syriac
4103	German (Luxembourg)	1089	Swahili
2055	German (Switzerland)	1064	Tajik
1032	Greek	2143	Tamazight
1135	Greenlandic	1097	Tamil
1095	Gujarati	1092	Tatar
1128	Hausa	1098	Telugu
1037	Hebrew	1054	Thai
1081	Hindi	1105	Tibetan
1038	Hungarian	1055	Turkish
1039	Icelandic	1090	Turkmen
1136	Igbo	1058	Ukrainian
9275	Inari Sami	1070	Upper Sorbian
1057	Indonesian	1056	Urdu
1117	Inuktitut (Syllabics)	1152	Uyghur
2141	Inuktitut (Latin)	1091	Uzbek (Latin)
2108	Irish	2115	Uzbek (Cyrillic)
1040	Italian (Italy)	1066	Vietnamese
2064	Italian (Switzerland)	1106	Welsh
1041	Japanese	1160	Wolof
1099	Kannada	1076	Xhosa
1087	Kazakh	1144	Yi
1107	Khmer	1130	Yoruba
1158	K'iche	1077	Zulu
1159	Kinyarwanda		

Sort order

This setting controls the sort order for lists and libraries. You can specify the sort order that you want to use for your SharePoint sites. You can change the sort order for a site by using the Regional Settings page. The following list shows the sort orders available in SharePoint Server 2010:

- General
- Albanian
- Arabic
- Azeri (Cyrillic)
- Azeri (Latin)

- Chinese (Traditional) Bopomofo
- Chinese (Traditional) Stroke Count
- Chinese Pronunciation
- Chinese Stroke Count
- Croatian
- Cyrillic
- Czech
- Danish/Norwegian
- Divehi
- Estonian
- Finnish/Swedish
- French
- Georgian Modern
- German Phone Book
- Greek
- Hebrew
- Hindi
- Hong Kong Stroke Order
- Hungarian
- Hungarian Technical
- Icelandic
- Indic (General)
- Japanese
- Japanese Unicode
- Kazakh
- Korean
- Korean Unicode
- Latvian
- Lithuanian
- Lithuanian Classic
- Macedonian (FYROM)
- Polish
- Romanian
- Slovak
- Slovenian
- Spanish (Modern Sort)
- Spanish (Traditional Sort)
- Syriac
- Tatar
- Thai
- Turkish
- Ukrainian
- Uzbek (Latin)
- Vietnamese

Time zone

You can set the time zone for your SharePoint sites to one of the time zones shown in the following table. You can change the time zone for a Web site by using the Regional Settings page. For more information about how to set time zones, see Configure settings for a Web application (SharePoint Server 2010) (*http://technet.microsoft.com/library/2687d49f-b114-4f16-a4c0-5f2bfe496c92(Office.14).aspx*).

Note:
In the following table, time zones are based on their offset from Coordinated Universal Time, or UTC (Greenwich Mean Time).

Code	Time zones
39	(UTC-12:00) International Date Line West
95	(UTC-11:00) Coordinated Universal Time-11
16	(UTC-11:00) Samoa
15	(UTC-10:00) Hawaii
14	(UTC-09:00) Alaska
13	(UTC-08:00) Pacific Time (US and Canada)
78	(UTC-08:00) Baja California
38	(UTC-07:00) Arizona
77	(UTC-07:00) Chihuahua, La Paz, Mazatlan
12	(UTC-07:00) Mountain Time (US and Canada)
55	(UTC-06:00) Central America
11	(UTC-06:00) Central Time (US and Canada)
37	(UTC-06:00) Guadalajara, Mexico City, Monterrey
36	(UTC-06:00) Saskatchewan
35	(UTC-05:00) Bogota, Lima, Quito
10	(UTC-05:00) Eastern Time (US and Canada)
34	(UTC-05:00) Indiana (East)
88	(UTC-04:30) Caracas
91	(UTC-04:00) Asuncion
9	(UTC-04:00) Atlantic Time (Canada)
33	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
81	(UTC-04:00) Cuiaba
65	(UTC-04:00) Santiago
28	(UTC-03:30) Newfoundland
8	(UTC-03:00) Brasilia
85	(UTC-03:00) Buenos Aires
32	(UTC-03:00) Cayenne, Fortaleza
60	(UTC-03:00) Greenland
90	(UTC-03:00) Montevideo
96	(UTC-02:00) Coordinated Universal Time-02
30	(UTC-02:00) Mid-Atlantic

Code	Time zones
29	(UTC-01:00) Azores
53	(UTC-01:00) Cape Verde Is.
86	(UTC) Casablanca
93	(UTC) Coordinated Universal Time
2	(UTC) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
31	(UTC) Monrovia, Reykjavik
4	(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
6	(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
3	(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
57	(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb
69	(UTC+01:00) West Central Africa
83	(UTC+01:00) Windhoek
79	(UTC+02:00) Amman
5	(UTC+02:00) Athens, Bucharest, Istanbul
80	(UTC+02:00) Beirut
49	(UTC+02:00) Cairo
98	(UTC+02:00) Damascus
50	(UTC+02:00) Harare, Pretoria
59	(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
27	(UTC+02:00) Jerusalem
7	(UTC+02:00) Minsk
26	(UTC+03:00) Baghdad
74	(UTC+03:00) Kuwait, Riyadh
51	(UTC+03:00) Moscow, St. Petersburg, Volgograd
56	(UTC+03:00) Nairobi
25	(UTC+03:30) Tehran
24	(UTC+04:00) Abu Dhabi, Muscat
54	(UTC+04:00) Baku
89	(UTC+04:00) Port Louis
82	(UTC+04:00) Tbilisi
84	(UTC+04:00) Yerevan
48	(UTC+04:30) Kabul
58	(UTC+05:00) Ekaterinburg
87	(UTC+05:00) Islamabad, Karachi
47	(UTC+05:00) Tashkent
23	(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Code	Time zones
66	(UTC+05:30) Sri Jayawardenepura
62	(UTC+05:45) Kathmandu
46	(UTC+06:00) Novosibirsk
71	(UTC+06:00) Astana, Dhaka
61	(UTC+06:30) Yangon (Rangoon)
22	(UTC+07:00) Bangkok, Hanoi, Jakarta
64	(UTC+07:00) Krasnoyarsk
45	(UTC+08:00) Beijing, Chongqing, Hong Kong S.A.R., Urumqi
63	(UTC+08:00) Irkutsk
21	(UTC+08:00) Kuala Lumpur, Singapore
73	(UTC+08:00) Perth
75	(UTC+08:00) Taipei
94	(UTC+08:00) Ulaanbaatar
20	(UTC+09:00) Osaka, Sapporo, Tokyo
72	(UTC+09:00) Seoul
70	(UTC+09:00) Yakutsk
19	(UTC+09:30) Adelaide
44	(UTC+09:30) Darwin
18	(UTC+10:00) Brisbane
76	(UTC+10:00) Canberra, Melbourne, Sydney
43	(UTC+10:00) Guam, Port Moresby
42	(UTC+10:00) Hobart
68	(UTC+10:00) Vladivostok
41	(UTC+11:00) Magadan, Solomon Is., New Caledonia
17	(UTC+12:00) Auckland, Wellington
97	(UTC+12:00) Coordinated Universal Time+12
40	(UTC+12:00) Fiji
92	(UTC+12:00) Petropavlovsk-Kamchatsky - Old
67	(UTC+13:00) Nuku'alofa

Calendar

You can specify the type of calendar that you want to use as your primary calendar for your SharePoint sites. You can change the calendar for a Web site by using the Regional Settings page. The following list shows the calendars available in SharePoint Server 2010:

- Gregorian
- Japanese Emperor Era
- Korean Tangun Era
- Hijiri
- Buddhist
- Hebrew Jewish
- Gregorian Middle East French Calendar

- Gregorian Arabic Calendar
- Gregorian Transliterated English Calendar
- Gregorian Transliterated French Calendar
- Saka Era

If you want to know the date in another calendar type, you can display an additional calendar next to your primary calendar.

Currency

You can set the currency for your SharePoint sites to any one of the currencies shown in the following table. The default value of the currency is determined by the locale that you specified in your regional settings, but users can change the value if they want. The currency is set on the Create Column page when you work with lists.

Note:
The currencies listed below are valid only when they are used with a locale that formats numbers by using a comma for digit grouping and a period as the decimal separator.

ID	Currency
1052	123,456.00 Lek (Albania)
5121	123,456.00 د.ج. (Algeria)
11274	$ 123,456.00 (Argentina)
1067	123,456.00 դր. (Armenia)
3081	$123,456.00 (Australia)
3079	€ 123,456.00 (Austria)
1068	123,456.00 man. (Azerbaijan)
2092	123,456.00 ман. (Azerbaijan)
15361	123,456.00 د.ب. (Bahrain)
1059	123,456.00 р. (Belarus)
2067	€ 123,456.00 (Belgium)
10249	BZ$123,456.00 (Belize)
16394	$b 123,456.00 (Bolivia)
1046	R$ 123,456.00 (Brazil)
2110	$123,456.00 (Bruni Darussalam)
1026	123,456.00 лв (Bulgaria)
3084	123,456.00 $ (Canada)
4105	$123,456.00 (Canada)
13322	$ 123,456.00 (Chile)
9226	$ 123,456.00 (Columbia)
5130	₡123,456.00 (Costa Rica)
1050	123,456.00 kn (Croatia)
1029	123,456.00 Kč (Czech Republic)
1030	kr 123,456.00 (Denmark)
7178	RD$123,456.00 (Dominican Republic)
12298	$ 123,456.00 (Ecuador)

ID	Currency
3073	123,456.00 م.ج. (Egypt)
17418	$123,456.00 (El Salvador)
1061	123,456.00 kr (Estonia)
1080	kr 123,456.00 (Faroe Islands)
1035	123,456.00 € (Finland)
1036	123,456.00 € (France)
1079	123,456.00 Lari (Georgia)
1031	123,456.00 € (Germany)
1032	123,456.00 € (Greece)
4106	Q123,456.00 (Guatemala)
18442	L. 123,456.00 (Honduras)
3076	HK$123,456.00 (Hong Kong S.A.R.)
1038	123,456.00 Ft (Hungary)
1039	123,456.00 kr. (Iceland)
1081	123,456.00 (India)
1094	123,456.00 (India)
1095	123,456.00 (India)
1097	123,456.00 (India)
1098	123,456.00 (India)
1099	123,456.00 (India)
1057	Rp123,456.00 (Indonesia)
1065	123,456.00 ريال (Iran)
2049	123,456.00 د.ع. (Iraq)
6153	€ 123,456.00 (Ireland)
1040	€ 123,456.00 (Italy)
1037	₪ 123,456.00 (Israel)
8201	J$123,456.00 (Jamaica)
1041	¥ 165;123,456.00 (Japan)
11265	123,456.00 د.ا. (Jordan)
1087	T123,456.00 (Kazakhistan)
1089	S123,456.00 (Kenya)
1042	₩123,456.00 (Korea)
13313	123,456.00 د.ك. (Kuwait)
1088	123,456.00 сом (Kyrgyzstan)
1062	Ls 123,456.00 (Latvia)
12289	123,456.00 ل.ل. (Lebanon)
4097	123,456.00 د.ل. (Libya)
5127	CHF 123,456.00 (Liechtenstein)
1063	123,456.00 Lt (Lithuania)
5132	123,456.00 € (Luxembourg)
5124	MOP123,456.00 (Macau S.A.R.)
1071	123,456.00 ден. (Macedonia (FYROM))

ID	Currency
1086	R123,456.00 (Malaysia)
1125	123,456.00 (Maldives)
2058	$123,456.00 (Mexico)
6156	123,456.00 € (Monaco)
1104	123,456.00₮ (Mongolia)
6145	123,456.00 د.م. (Morocco)
1043	€ 123,456.00 (Netherlands)
5129	$123,456.00 (New Zealand)
19466	C$ 123,456.00 (Nicaragua)
1044	kr 123,456.00 (Norway)
8193	123,456.00 ر.ع. (Oman)
1056	Rs123,456.00 (Pakistan)
6154	B/. 123,456.00 (Panama)
15370	Gs 123,456.00 (Paraguay)
2052	￥123,456.00 (People's Republic of China)
10250	S/. 123,456.00 (Peru)
13321	Php123,456.00 (Philippines)
1045	123,456.00 zł (Poland)
2070	123,456.00 € (Portugal)
20490	$ 123,456.00 (Puerto Rico)
16385	123,456.00 ر.ق. (Qatar)
1048	123,456.00 lei (Romania)
1049	123,456.00р. (Russia)
1025	123,456.00 ر.س. (Saudi Arabia)
2074	123,456.00 Din. (Serbia)
3098	123,456.00 Дин. (Serbia)
4100	$123,456.00 (Singapore)
1051	123,456.00 Sk (Slovakia)
1060	123,456.00 SIT (Slovenia)
7177	R 123,456.00 (South Africa)
3082	123,456.00 € (Spain)
1053	123,456.00 kr (Sweden)
2055	SFr. 123,456.00 (Switzerland)
10241	123,456.00 ل.س. (Syria)
1028	NT$123,456.00 (Taiwan)
1054	฿123,456.00 (Thailand)
11273	TT$123,456.00 (Trinidad and Tobago)
7169	123,456.00 د.ت. (Tunisia)
1055	123,456.00 YTL (Turkey)
1058	123,456.00 грн. (Ukraine)
14337	123,456.00 د.إ. (United Arab Emirates)
2057	£163;123,456.00 (United Kingdom)

ID	Currency
1033	$123,456.00 (United States)
14346	$U 123,456.00 (Uruguay)
1091	123,456.00 su'm (Uzbekistan)
2115	123,456.00 сўм (Uzbekistan)
8202	Bs 123,456.00 (Venezuela)
1066	123,456.00 ₫ (Vietnam)
9217	123,456.00 ر.ي. (Yemen)
12297	Z$123,456.00 (Zimbabwe)

Concepts

Language packs (SharePoint Server 2010)

Other Resources

Deploy language packs (SharePoint Server 2010)
(*http://technet.microsoft.com/library/26c07867-0150-463d-b21a-a6d42aecf05a(Office.14).aspx*)

Managed metadata input file format (SharePoint Server 2010)

Updated: January 7, 2011

Managed metadata in SharePoint Server 2010 is imported from a comma-separated values (csv) file. Each file must contain one term set, and the terms within the term set may be nested as many as seven levels deep.

Even if your organization does not have data to import, you could consider creating your taxonomy outside the Term Store Management tool, and then importing the taxonomy. The Term Store Management Tool provides a convenient, simple way to create term sets and manage terms, but using it to create many term sets might take longer than importing the term sets. The Term Store Management Tool is convenient to use for the day-to-day management of term sets after the term sets have been created.

In this article:

- Format of the managed metadata import file
- View a sample managed metadata import file
- Import managed metadata

Before reading this article, you should understand the concepts described in the What Is Managed Metadata? (*http://technet.microsoft.com/library/e580fcae-b768-4b81-afda-c037fbd7bd6d(Office.14).aspx*) topic.

Format of the managed metadata import file

The managed metadata import file is a comma-separated values (.csv) file that contains a header row and additional rows that define the term set and the terms in the term set.

The first line of the file must contain 12 items separated by commas. Consider these items to be column headings (such as in a table) for the values that you will provide in the next lines. It is good practice to enclose each value in quotation marks (“”
).

The following line is the first line from the sample managed metadata import file. For more information about how to view the sample managed metadata import file, see View a sample managed metadata import file.

```
"Term Set Name","Term Set Description","LCID","Available for Tagging","Term
Description","Level 1 Term","Level 2 Term","Level 3 Term","Level 4 Term","Level 5
Term","Level 6 Term","Level 7 Term"
```

The second line of the managed metadata import file represents the term set, and should contain the following information, in the order specified:

1. The name of the term set

Note:
It is recommended that the name of the term set, the name of a term, and all descriptions be enclosed in quotation marks (“”
). Quotation marks are optional, unless the value itself contains a comma. It is safer always to use the quotation marks.

2. A comma (`,`
)
3. Optionally, a description of the term set
4. Two commas (`,,`
)
5. The word `TRUE`
   or the word `FALSE`
   that indicates whether users should be able to add the terms in this term set to Microsoft SharePoint Server items. If you do not provide a value, the term set is available for tagging.
6. Eight commas (`,,,,,,,,`
)

The third line of the managed metadata import file and each successive line represents a term. Separate the values in the third line and in each successive line with commas. You may omit an optional value, but do not omit the accompanying comma, because commas are required as separators regardless of whether values are present.
The values in a line represent the following information, and must be provided in the order in which they are listed:

1. Term set name: Leave this value blank.
2. Term set description: Leave this value blank.
3. Locale identifier: The decimal value that identifies the locale that corresponds to the language of the term. If you do not provide a value, the default locale of the term store to which you import this managed metadata is used.
4. Available for tagging: This value determines whether users should be able to add this term to a SharePoint Server item. Use the word TRUE to let users use the term; use the word FALSE to forbid users to use the term. If you do not provide a value, users can use the term.
5. Term description: A description of the term. This value is optional.
6. Level 1 term -- level 7 term: If the term set is organized as a hierarchy, a level 1 term is a term at the top of the hierarchy, a level 2 term is lower than a level 1 term, and so on. You must provide a value for all levels down to the level of the term that you are representing. This is best illustrated by the example that follows this list.

In this example, you want to import a term set that represents all the office locations of your organization. The term set will be organized hierarchically. The following list is a fragment of the term set:

- Sites (term set)
  - North America
  - Washington
  - Seattle
  - Redmond
  - Tacoma
  - Massachusetts
  - Boston
  - Cambridge

“North America” is a level 1 term. “Washington” and “Massachusetts” are level 2 terms. “Redmond”, “Seattle”, “Tacoma”, “Boston”, and “Cambridge” are level 3 terms. To import this term set, you would use a file that contained the following lines:

```
"Term Set Name","Term Set Description","LCID","Available for Tagging","Term
Description","Level 1 Term","Level 2 Term","Level 3 Term","Level 4 Term","Level 5
Term","Level 6 Term","Level 7 Term"
"Sites","Locations where the organization has offices",,TRUE,,,,,,,,
,,1033,TRUE,,"North America",,,,,,
,,1033,TRUE,,"North America","Washington",,,,,
,,1033,TRUE,,"North America","Washington","Redmond",,,,
,,1033,TRUE,,"North America","Washington","Seattle",,,,
,,1033,TRUE,,"North America","Washington","Tacoma",,,,
,,1033,TRUE,,"North America","Massachusetts",,,,,
,,1033,TRUE,,"North America","Massachusetts","Boston",,,,
,,1033,TRUE,,"North America","Massachusetts","Cambridge",,,,
```

Note:
It is possible to combine the line that defines the term set (line 2) and the first line that defines a term (line 3). This is done in the sample import file.

You cannot represent synonyms or translations of terms by using a managed metadata import file. To create synonyms or translations you must either use the Term Store Management Tool or write a custom program to import and add the synonyms or translations.
See Wictor Wilén's blog (*http://go.microsoft.com/fwlink/?LinkId=190541&clcid=0x409*) for information about a tool to import term sets that was developed by a member of the SharePoint community.

View a sample managed metadata import file

You can view a sample import file by clicking **View a sample import file** from the properties pane of a managed metadata service in the Term Store Management Tool. The simplest way to create an import file for your term set is to use the sample import file as a template. Save the sample import file; delete everything except the first row. Then add more rows to represent your term set and terms.

Import managed metadata

For instructions about how to import metadata, see Office.com (*http://go.microsoft.com/fwlink/?LinkId=207785&clcid=0x409*).

Other Resources

What Is Managed Metadata? (*http://technet.microsoft.com/library/e580fcae-b768-4b81-afda-c037fbd7bd6d(Office.14).aspx*)
Plan to import managed metadata (*http://technet.microsoft.com/library/174916ae-414c-4e90-8992-eb55936e1719(Office.14).aspx*)

User experience on read-only sites (SharePoint Server 2010)

Published: May 12, 2010

This article describes how the user interface is modified on a Microsoft SharePoint Server 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
FAST Search page	The ribbon is not displayed
Search page	The ribbon is not displayed
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 Check Out Check In Discard Check Out Edit Properties Version History Delete Document

Object	Interface elements disabled on a read-only site
	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 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

Object	Interface elements disabled on a read-only site
	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
- Portal Configuration

Common tasks that are 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	SharePoint returns the “Error: Access Denied” message.

Component or area	Type of operation or action	Behavior or error message
	click **OK**.	
Site Features	Click **Activate** or **Deactivate**.	SharePoint returns the “Error: Access Denied” message.
Delete this site		SharePoint returns the “Error: Access Denied” 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.
Search Settings	Change any settings, and then click **OK**.	SharePoint returns the “Error: Access Denied” message.
Search Scopes	Click **New Scope**, change any settings, and then click **OK**. Click **Display Group**, **New Display Group**, change any settings, and then click **OK**.	SharePoint returns the “Could not save due to the following error: Attempted to perform an unauthorized operation” 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.”

Scripted deployment reference (SharePoint Server 2010)

Published: May 12, 2010

This article describes the commands and syntax that is used in scripted deployment of a Microsoft SharePoint Server 2010 farm. It also contains a table of common templates used in Installing SharePoint Server 2010 by using Windows PowerShell (*http://technet.microsoft.com/library/7443092a-87a6-4063-a7d0-8d10d9d23682%20.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 Server 2010, see Installing SharePoint Server 2010 by using Windows PowerShell (*http://technet.microsoft.com/library/7443092a-87a6-4063-a7d0-8d10d9d23682%20.aspx*).
In this article:

- Install-SharePoint (*http://technet.microsoft.com/library/46e48389-01a5-42f3-8548-498af130ee03(Office.14).aspx#section2*)
- New-SharePointFarm (*http://technet.microsoft.com/library/46e48389-01a5-42f3-8548-498af130ee03(Office.14).aspx#section3*)
- Join-SharePointFarm (*http://technet.microsoft.com/library/46e48389-01a5-42f3-8548-498af130ee03(Office.14).aspx#section4*)
- Common site collection templates

Install-SharePoint

The Install-SharePoint command installs SharePoint Server 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, a product key (PIDKey), 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, there are two required parameters, **SetupExePath** and **PIDKey**. All other parameters are optional. If no value is specified for the optional **LogPath** parameter, the default value is *%Temp%*.
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 Server 2010 by using Windows PowerShell (*http://technet.microsoft.com/library/7443092a-87a6-4063-a7d0-8d10d9d23682%20.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

Account permissions and security settings (SharePoint Server 2010)

Published: May 12, 2010

In this article:

- About account permissions and security settings
- Administrative accounts
- Service application accounts
- Database roles
- Group permissions

This article describes Microsoft SharePoint Server 2010 administrative and services account permissions. It covers the following areas: Microsoft SQL Server, the file system, file shares, and registry entries.

About account permissions and security settings

Many of the SharePoint Server 2010 baseline account permissions and security settings are configured by the SharePoint Configuration Wizard (Psconfig) and the Farm Creation Wizard, both of which are run during a Complete installation.

Administrative accounts

Most of the SharePoint Server 2010 administrative account permissions are configured automatically during the setup process by one of the following SharePoint Server 2010 components:

- The SharePoint Configuration Wizard (Psconfig).
- The Farm Creation Wizard.
- The SharePoint Central Administration Web site.
- Windows PowerShell.

Setup user administrator account

This account is used to set up each server in your farm by running The SharePoint Configuration Wizard, the initial Farm Creation Wizard, and Windows PowerShell. For the examples in this article, the setup user administrator account is used for farm administration, and it can be managed using Central Administration. Some configuration options require local administration permissions: for example, configuration of the SharePoint Server 2010 Search query server. The setup user administrator account requires the following permissions:

- It must have domain user account permissions.
- It must be a member of the local administrators group on each server in the SharePoint Server 2010 farm, excluding SQL Server and the Simple Mail Transfer Protocol (SMTP) server.
- This account must have access to the SharePoint Server 2010 databases.
- If you use any Windows PowerShell operations that affect a database, the setup user administrator account must be a member of the db_owner role.

- This account must be assigned to the securityadmin and dbcreator SQL Server security roles during setup and configuration.

Note:
The securityadmin and dbcreator SQL Server security roles might be required for this account during a complete version to version upgrade because new databases might have to be created and secured for services.

After you run the configuration wizards, machine-level permissions for the setup user administrator account include:
- Membership in the WSS_ADMIN_WPG Windows security group.
- Membership in the IIS_WPG role.

After you run the configuration wizards, database permissions include:
- db_owner on the SharePoint Server 2010 server farm configuration database.
- db_owner on the SharePoint Server 2010 Central Administration content database.

Warning:
If the setup user administrator account is removed as a login from the computer running SQL Server, the configuration wizards will not run correctly. If you run the configuration wizards using an account that does not have the appropriate special SQL role membership, or access as db_owner on the databases, the configuration wizards will not run correctly.

Farm service account
The server farm account is also referred to as the database access account and is used as the application pool identity for Central Administration, and as the process account for the Microsoft SharePoint Foundation 2010 Timer service. The server farm account requires the following permissions:
- It must have domain user account permissions.

Additional permissions are automatically granted to the server farm account on Web servers and application servers that are joined to a server farm.
After you run the SharePoint Configuration Wizard, machine-level permissions include:
- Membership in the WSS_ADMIN_WPG Windows security group for the SharePoint Foundation 2010 Timer service.
- Membership in WSS_RESTRICTED_WPG for the Central Administration and Timer service application pools.
- Membership in WSS_WPG for the Central Administration application pool.

After you run the configuration wizards, SQL Server and database permissions include:
- Dbcreator fixed server role.
- Securityadmin fixed server role.
- db_owner for all SharePoint Server 2010 databases.
- Membership in the WSS_CONTENT_APPLICATION_POOLS role for the SharePoint Server 2010 server farm configuration database.
- Membership in the WSS_CONTENT_APPLICATION_POOLS role for the SharePoint Server 2010 SharePoint_Admin content database.

Microsoft SharePoint Foundation 2010 search service account
The SharePoint Foundation 2010 search service account is used as the service account for the SharePoint Foundation 2010 Search service. The SharePoint Foundation 2010 search service account requires the following permission configuration settings:
- This account must have domain user account permissions.

The following machine-level permission is configured automatically: The search service account is a member of WSS_WPG.
The following SQL Server and database permissions are conferred by membership in the WSS_CONTENT_APPLICATION_POOLS role in the server farm configuration database:

- Read access to the server farm configuration database.
- Read access to the SharePoint_Admin content database.
- This account is assigned the db_owner role for the SharePoint Foundation 2010 search database.

Microsoft SharePoint Foundation 2010 search content access account
The SharePoint Foundation 2010 search content access account is used by the SharePoint Foundation 2010 Search service to crawl content across sites. The SharePoint Foundation 2010 search content access account requires the following permission configuration settings:

- This account must have domain user account permissions.
- This account must not be a member of the farm administrators group.

The following SQL Server and database permissions are configured automatically:

- Read access to the server farm configuration database.
- Read access to the SharePoint_Admin content database.
- This account is assigned to the db_owner role for the SharePoint Foundation 2010 search database.

A full Read policy for the SharePoint Foundation 2010 search content access account is created on all Web applications.

Service application accounts

This section describes the service application accounts that are setup by default during installation.
Application pool account
The application pool account is used for application pool identity. The application pool account requires the following permission configuration settings:
The following machine-level permission is configured automatically: The application pool account is a member of WSS_WPG.
The following SQL Server and database permissions for this account are configured automatically:

- The application pool accounts for Web applications are assigned to the db_owner role for the content databases.
- This account is assigned to the WSS_CONTENT_APPLICATION_POOLS role associated with the farm configuration database.
- This account is assigned to the WSS_CONTENT_APPLICATION_POOLS role associated with the SharePoint_Admin content database.

SharePoint Server search service account
The SharePoint Server 2010 Search service account is used as the service account for the SharePoint Server 2010 Search service. The SharePoint Server Search Service is an NT Service, which is used by all Search Service Applications. For any given server, there is only one instance of this service. The SharePoint Server 2010 search service account requires the following permission configuration setting: The SharePoint Server 2010 search service account is granted access to the propagation location share (or shares) on all search query servers in a farm.
The following machine-level permission is configured automatically: The SharePoint Server 2010 search service account is a member of WSS_WPG.

The following SQL Server and database permissions are configured automatically:

- This account is assigned to the WSS_CONTENT_APPLICATION_POOLS role associated with the farm configuration database.
- This account is assigned to the WSS_CONTENT_APPLICATION_POOLS role associated with the SharePoint_Admin content database.

Default content access account

The default content access account is used within a specific service application to crawl content, unless a different authentication method is specified by a crawl rule for a URL or URL pattern. This account requires the following permission configuration settings:

- The default content access account must be a domain user account and it must have read access to external or secure content sources that you want to crawl by using this account.
- For SharePoint Server sites that are not part of the server farm, this account must be explicitly granted full read permissions to the Web applications that host the sites.
- This account must not be a member of the farm administrators group.

Content access accounts

Content access accounts are accounts that are configured to access content by using the Search administration crawl rules feature. This type of account is optional and can be configured when you create a new crawl rule. For example, external content (such as a file share) might require this separate content access account. This account requires the following permission configuration settings:

- The content access account must have read access to external or secure content sources that this account is configured to access.
- For SharePoint Server sites that are not part of the server farm, this account must be explicitly granted full read permissions to the Web applications that host the sites.

Excel Services unattended service account

The Excel Services unattended service account is used by Excel Services to connect to external data sources that require a user name and password that are based on operating systems other than Windows for authentication. If this account is not configured, Excel Services will not attempt to connect to these types of data sources. Although account credentials are used to connect to data sources of operating systems other than Windows, if the account is not a member of the domain, Excel Services cannot access it. This account must be a domain user account.

My Sites application pool account

The My Sites application pool account must be a domain user account. This account must not be a member of the farm administrators group.

The following machine-level permission is configured automatically: This account is a member of WSS_WPG.

The following SQL Server and database permissions are configured automatically:

- This account is assigned to the WSS_CONTENT_APPLICATION_POOLS role associated with the farm configuration database.
- This account is assigned to the WSS_CONTENT_APPLICATION_POOLS role associated with the SharePoint_Admin content database.

Other application pool accounts

The other application pool account must be a domain user account. This account must not be a member of the administrators group on any computer in the server farm.

The following machine-level permission is configured automatically: This account is a member of WSS_WPG.

The following SQL Server and database permissions are configured automatically:

- This account is assigned to the db_owner role for the content databases.

- This account is assigned to the db_owner role for search databases associated with the Web application.
- This account must have read and write access to the associated service application database.
- This account is assigned to the WSS_CONTENT_APPLICATION_POOLS role associated with the farm configuration database.
- This account is assigned to the WSS_CONTENT_APPLICATION_POOLS role associated with the SharePoint_Admin content database.

Database roles

This section describes the database roles that are either setup by default during installation, or that can be optionally configured.

WSS_CONTENT_APPLICATION_POOLS database role

The WSS_CONTENT_APPLICATION_POOLS database role applies to the application pool account for each Web application that is registered in SharePoint. This enables the Web applications to query and update the site map, and have read-only access to other items in the configuration database. Setup assigns the WSS_CONTENT_APPLICATION_POOLS role to the following databases:

- The SharePoint_Config database (the configuration database).
- The SharePoint_AdminContent database.

Members of the WSS_CONTENT_APPLICATION_POOLS role are granted the execute permission for a subset of the stored procedures for the database. In addition, members of this role are granted the select permission to the Versions table (dbo.Versions) in the SharePoint_AdminContent database. For other databases, the accounts planning tool indicates that access to read these databases is automatically configured. In some cases, limited access to write to a database is also automatically configured. To provide this access, permissions for stored procedures are configured. For the SharePoint_Config database, for example, access to the following stored procedures is automatically configured:

- proc_dropEmailEnabledList
- proc_dropEmailEnabledListsByWeb
- proc_dropSiteMap
- proc_markForDeletionEmailEnabledList
- proc_markForDeletionEmailEnabledListsBySite
- proc_markForDeletionEmailEnabledListsByWeb
- proc_putDistributionListToDelete
- proc_putEmailEnabledList
- proc_putSiteMap

WSS_SHELL_ACCESS database role

The secure WSS_SHELL_ACCESS database role on the configuration database replaces the need to add an administration account as a db_owner on the configuration database. By default, the setup account is assigned to the WSS_SHELL_ACCESS database role. Membership in this role is granted and removed by using a Windows PowerShell command. Setup assigns the WSS_SHELL_ACCESS role to the following databases:

- The SharePoint_Config database (the configuration database).
- One or more of the SharePoint Content databases. This is configurable by using the Windows PowerShell command that manages membership, and the object assigned to this role.

Members of the WSS_SHELL_ACCESS role are granted the execute permission for all of the stored procedures for the database. In addition, members of this role are granted the read and write permissions on all of the database tables.

Group permissions

This section describes permissions of groups that are created by the SharePoint Server 2010 setup and configuration tools.

WSS_ADMIN_WPG

WSS_ADMIN_WPG has read and write access to local resources. The application pool accounts for the Central Administration and Timer services are in WSS_ADMIN_WPG. The following table shows the WSS_ADMIN_WPG registry entry permissions.

Key name	Permissions	Inherit	Description
HKEY_CLASSES_ROOT\APPID\{58F1D482-A132-4297-9B8A-F8E4E600CDF6}	Full control	N/A	This is the SharePoint Server 2010 Search service COM Application.
HKEY_CLASSES_ROOT\APPID\{6002D29F-1366-4523-88C1-56D59BFEF8CB}	Full control	N/A	This is the SharePoint Foundation 2010 Search service COM Application.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS	Full control	N/A	N/A
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\14.0\Registration\{90120000-110D-0000-0000-0000000FF1CE}	Read, write	N/A	N/A
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office Server	Read	No	This key is the root of the SharePoint Server 2010 registry settings tree. If this key is altered, SharePoint Server 2010 functionality will fail.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office Server\14.0	Full control	No	This key is the root of the SharePoint Server 2010 registry settings.
HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\LoadBalancerSettings	Read, write	No	This key contains settings for the document conversion service. Altering this key will break document conversion functionality.
HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\LauncherSettings	Read, write	No	This key contains settings for the document conversion service. Altering this key will break document conversion functionality.
HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\Search	Full control	N/A	N/A
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\Search	Full control	N/A	N/A

Key name	Permissions	Inherit	Description
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\Secure	Full control	No	This key contains the connection string and the ID of the configuration database to which the machine is joined. If this key is altered, the SharePoint Server installation on the machine will not function.
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\WSS	Full control	Yes	This key contains settings used during setup. If this key is altered, diagnostic logging may fail and setup or post-setup configuration may fail.

The following table shows the WSS_ADMIN_WPG file system permissions.

File system path	Permissions	Inherit	Description
%AllUsersProfile%\Application Data\Microsoft\Sharepoint	Full control	No	This directory contains the file-system-backed cache of the farm configuration. Processes might fail to start and the administrative actions might fail if this directory is altered or deleted.
C:\Inetpub\wwwroot\wss	Full control	No	This directory (or the corresponding directory under the Inetpub root on the server) is used as the default location for IIS Web sites. SharePoint sites will be unavailable and administrative actions might fail if this directory is altered or deleted, unless custom IIS Web site paths are provided for all IIS Web sites extended with SharePoint Server.
%ProgramFiles%\Microsoft Office Servers\14.0	Full control	No	This directory is the installation location for SharePoint Server 2010 binaries and data. The directory can be changed during installation. All SharePoint Server 2010 functionality will fail if this directory is removed, altered, or removed after installation. Membership in the WSS_ADMIN_WPG Windows security group is required for some SharePoint Server 2010 services to be able to store data on disk.

File system path	Permissions	Inherit	Description
%ProgramFiles%\Microsoft Office Servers\14.0\WebServices	Read, write	No	This directory is the root directory where back-end Web services are hosted, for example, Excel and Search. The SharePoint Server 2010 features that depend on these services will fail if this directory is removed or altered.
%ProgramFiles%\Microsoft Office Servers\14.0\Data	Full control	No	This directory is the root location where local data is stored, including search indexes. Search functionality will fail if this directory is removed or altered. WSS_ADMIN_WPG Windows security group permissions are required to enable search to save and secure data in this folder.
%ProgramFiles%\Microsoft Office Servers\14.0\Logs	Full control	Yes	This directory is the location where the run-time diagnostic logging is generated. Logging functionality will not function properly if this directory is removed or altered.
%ProgramFiles%\Microsoft Office Servers\14.0\Data\Office Server	Full control	Yes	Same as the parent folder.
%windir%\System32\drivers\etc\HOSTS	Read, write	N/A	N/A
%windir%\Tasks	Full control	N/A	N/A
%COMMONPROGRAMFILES%Microsoft Shared\Web Server Extensions\14	Modify	Yes	This directory is the installation directory for core SharePoint Server files. If the access control list (ACL) is modified, feature activation, solution deployment, and other features will not function correctly.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\ADMISAPI	Full control	Yes	This directory contains the soap services for Central Administration. If this directory is altered, remote site creation and other methods exposed in the service will not function correctly.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\CONFIG	Full control	Yes	This directory contains files used to extend IIS Web sites with SharePoint Server. If this directory or its contents are altered, Web application provisioning will not function correctly.
%COMMONPROGRAMFILES%\Micro	Full control	No	This directory contains setup and

File system path	Permissions	Inherit	Description
soft Shared\Web Server Extensions\14\LOGS			run-time tracing logs. If the directory is altered, diagnostic logging will not function correctly.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\Data	Full control	Yes	N/A
%windir%\temp	Full control	Yes	This directory is used by platform components on which SharePoint Server depends. If the ACL is modified, Web Part rendering and other deserialization operations might fail.
%windir%\System32\logfiles\SharePoint	Full control	No	This directory is used by SharePoint Server usage logging. If this directory is modified, usage logging will not function correctly.
%systemdrive\program files\Microsoft Office Servers\14 folder on Index servers	Full control	N/A	This permission is granted for a %systemdrive\program files\Microsoft Office Servers\14 folder on Index servers.

WSS_WPG

WSS_WPG has read access to local resources. All application pool and services accounts are in WSS_WPG. The following table shows WSS_WPG registry entry permissions.

Key name	Permissions	Inherit	Description
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office Server\14.0	Read	No	This key is the root of the SharePoint Server 2010 registry settings.
HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\Diagnostics	Read, write	No	This key contains settings for the SharePoint Server 2010 diagnostic logging. Altering this key will break the logging functionality.
HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\LoadBalancerSettings	Read, write	No	This key contains settings for the document conversion service. Altering this key will break document conversion functionality.
HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\LauncherSettings	Read, write	No	This key contains settings for the document conversion service. Altering this key will break document conversion functionality.
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\Secure	Read	No	This key contains the connection string and the ID of the configuration database to which the machine is joined. If this key is altered, the SharePoint Server installation on the machine will not function.

Key name	Permissions	Inherit	Description
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\WSS	Read	Yes	This key contains settings used during setup. If this key is altered, diagnostic logging may fail and setup or post-setup configuration may fail.

The following table shows the WSS_WPG file system permissions.

File system path	Permissions	Inherit	Description
%AllUsersProfile%\Application Data\Microsoft\Sharepoint	Read	No	This directory contains the file-system-backed cache of the farm configuration. Processes might fail to start and the administrative actions might fail if this directory is altered or deleted.
C:\Inetpub\wwwroot\wss	Read, execute	No	This directory (or the corresponding directory under the Inetpub root on the server) is used as the default location for IIS Web sites. SharePoint sites will be unavailable and administrative actions might fail if this directory is altered or deleted, unless custom IIS Web site paths are provided for all IIS Web sites extended with SharePoint Server.
%ProgramFiles%\Microsoft Office Servers\14.0	Read, execute	No	This directory is the installation location for the SharePoint Server 2010 binaries and data. It can be changed during installation. All SharePoint Server 2010 functionality will fail if this directory is removed, altered, or moved after installation. WSS_WPG read and execute permissions are required to enable IIS sites to load SharePoint Server 2010 binaries.
%ProgramFiles%\Microsoft Office Servers\14.0\WebServices	Read	No	This directory is the root directory where back-end Web services are hosted, for example, Excel and Search. The SharePoint Server 2010 features that depend on these services will fail if this directory is removed or altered.
%ProgramFiles%\Microsoft Office Servers\14.0\Logs	Read, write	Yes	This directory is the location where the run-time diagnostic logging is generated. Logging functionality will not function properly if this directory is removed or altered.

File system path	Permissions	Inherit	Description
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\ADMISAPI	Read	Yes	This directory contains the soap services for Central Administration. If this directory is altered, remote site creation and other methods exposed in the service will not function correctly.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\CONFIG	Read	Yes	This directory contains files used to extend IIS Web sites with SharePoint Server. If this directory or its contents are altered, Web application provisioning will not function correctly.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\LOGS	Modify	No	This directory contains setup and run-time tracing logs. If the directory is altered, diagnostic logging will not function correctly.
%windir%\temp	Read	Yes	This directory is used by platform components on which SharePoint Server depends. If the ACL is modified, Web Part rendering, and other deserialization operations may fail.
%windir%\System32\logfiles\SharePoint	Read	No	This directory is used by SharePoint Server usage logging. If this directory is modified, usage logging will not function correctly.
%systemdrive\program files\Microsoft Office Servers\14	Read, execute	N/A	The permission is granted for %systemdrive\program files\Microsoft Office Servers\14 folder on Index servers.

Local service

The following table shows the local service registry entry permission:

Key name	Permissions	Inherit	Description
HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\LoadBalancerSettings	Read	No	This key contains settings for the document conversion service. Altering this key will break document conversion functionality.

The following table shows the local service file system permission:

File system path	Permissions	Inherit	Description
%ProgramFiles%\Microsoft Office Servers\14.0\Bin	Read, execute	No	This directory is the installed location of the SharePoint Server 2010 binaries. All the SharePoint Server 2010 functionality will fail if this directory is removed or altered.

Local system
The following table shows the local system registry entry permissions:

Key name	Permissions	Inherit	Description
HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\LauncherSettings	Read	No	This key contains settings for the document conversion service. Altering this key will break document conversion functionality.
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\Secure	Full control	No	This key contains the connection string and the ID of the configuration database to which the machine is joined. If this key is altered, the SharePoint Server installation on the machine will not function.
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\Secure\FarmAdmin	Full control	No	This key contains the encryption key used to store secrets in the configuration database. If this key is altered, service provisioning and other features will fail.
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\WSS	Full control	Yes	This key contains settings used during setup. If this key is altered, diagnostic logging may fail and setup or post-setup configuration may fail.

The following table shows the local file system permissions:

File system path	Permissions	Inherit	Description
%AllUsersProfile%\Application Data\Microsoft\Sharepoint	Full control	No	This directory contains the file-system-backed cache of the farm configuration. Processes might fail to start and administrative actions might fail if this directory is altered or deleted.
C:\Inetpub\wwwroot\wss	Full control	No	This directory (or the corresponding directory under the Inetpub root on the server) is used as the default location for IIS Web sites. SharePoint sites will be unavailable and administrative actions might fail if this directory is altered or deleted, unless custom IIS Web site paths are provided for all IIS Web sites extended with SharePoint Server.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\ADMISAPI	Full control	Yes	This directory contains the soap services for Central Administration. If this directory is altered, remote site creation and other methods exposed

File system path	Permissions	Inherit	Description
			in the service will not function correctly.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\CONFIG	Full control	Yes	If this directory or its contents are altered, Web Application provisioning will not function correctly.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\LOGS	Full control	No	This directory contains setup and run-time tracing logs. If the directory is altered, diagnostic logging will not function correctly.
%windir%\temp	Full control	Yes	This directory is used by platform components on which SharePoint Server depends. If the ACL is modified, Web Part rendering, and other deserialization operations might fail.
%windir%\System32\logfiles\SharePoint	Full control	No	This directory is used by SharePoint Server for usage logging. If this directory is modified, usage logging will not function correctly.

Network service
The following table shows the network service registry entry permission:

Key name	Permissions	Inherit	Description
HKEY_LOCAL_MACHINE\Software\Microsoft\Office Server\14.0\Search\Setup	Read	N/A	N/A

Administrators
The following table shows the administrators registry entry permissions:

Key name	Permissions	Inherit	Description
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\Secure	Full control	No	This key contains the connection string and the ID of the configuration database to which the machine is joined. If this key is altered, the SharePoint Server installation on the machine will not function.
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\Secure\FarmAdmin	Full control	No	This key contains the encryption key used to store secrets in the configuration database. If this key is altered, service provisioning and other features will fail.
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\WSS	Full control	Yes	This key contains settings used during setup. If this key is altered, diagnostic logging may fail and setup or post-setup configuration

Key name	Permissions	Inherit	Description
			may fail.

The following table shows the administrators file system permissions:

File system path	Permissions	Inherit	Description
%AllUsersProfile%\Application Data\Microsoft\Sharepoint	Full control	No	This directory contains the file-system-backed cache of the farm configuration. Processes might fail to start and administrative actions might fail if this directory is altered or deleted.
C:\Inetpub\wwwroot\wss	Full control	No	This directory (or the corresponding directory under the Inetpub root on the server) is used as the default location for IIS Web sites. SharePoint sites will be unavailable and administrative actions might fail if this directory is altered or deleted, unless custom IIS Web site paths are provided for all IIS Web sites extended with SharePoint Server.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\ADMISAPI	Full control	Yes	This directory contains the soap services for Central Administration. If this directory is altered, remote site creation and other methods exposed in the service will not function correctly.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\CONFIG	Full control	Yes	If this directory or its contents are altered, Web application provisioning will not function correctly.
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\LOGS	Full control	No	This directory contains setup and run-time tracing logs. If the directory is altered, diagnostic logging will not function correctly.
%windir%\temp	Full control	Yes	This directory is used by platform components on which SharePoint Server depends. If the ACL is modified, Web Part rendering, and other deserialization operations might fail.
%windir%\System32\logfiles\SharePoint	Full control	No	This directory is used for SharePoint Server usage logging. If this directory is modified, usage logging will not function correctly.

WSS_RESTRICTED_WPG

WSS_RESTRICTED_WPG can read the encrypted farm administration credential registry entry. WSS_RESTRICTED_WPG is only used for encryption and decryption of passwords stored in

the configuration database. The following table shows the WSS_RESTRICTED_WPG registry entry permission:

Key name	Permissions	Inherit	Description
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Web Server Extensions\14.0\Secure\FarmAdmin	Full control	No	This key contains the encryption key used to store secrets in the configuration database. If this key is altered, service provisioning and other features will fail.

Users group

The following table shows the users group file system permissions:

File system path	Permissions	Inherit	Description
%ProgramFiles%\Microsoft Office Servers\14.0	Read, execute	No	This directory is the installation location for SharePoint Server 2010 binaries and data. It can be changed during installation. All SharePoint Server 2010 functionality will fail if this directory is removed, altered, or moved after installation.
%ProgramFiles%\Microsoft Office Servers\14.0\WebServices\Root	Read, execute	No	This directory is the root directory where back-end root Web services are hosted. The only service initially installed on this directory is a search global administration service. Some of the search administration functionality using the server-specific Central Administration Search Settings page will not work if this directory is removed or altered.
%ProgramFiles%\Microsoft Office Servers\14.0\Logs	Read, write	Yes	This directory is the location where the run-time diagnostic logging is generated. Logging will not function properly if this directory is removed or altered.
%ProgramFiles%\Microsoft Office Servers\14.0\Bin	Read, execute	No	This directory is the installed location of SharePoint Server 2010 binaries. All of the SharePoint Server 2010 functionality will fail if this directory is removed or altered.

All Office SharePoint Server service accounts

The following table shows the all Office SharePoint Server service accounts file system permission:

File system path	Permissions	Inherit	Description
%COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\LOGS	Modify	No	This directory contains setup and run-time tracing logs. If this directory is altered, diagnostic logging will not function correctly. All SharePoint

File system path	Permissions	Inherit	Description
			Server service accounts must have write permission to this directory.

PerformancePoint Services glossary

This glossary contains terminology for all the servers, applications, and tools that are part of PerformancePoint Services in Microsoft SharePoint Server 2010.

Terms

Term	Definition
ActiveX Data Objects MultiDimensional.NET	A .NET managed data provider that provides access to multidimensional data sources, such as Microsoft SQL Server Analysis Services.
actual value	The value for a key performance indicator (KPI). This value is measured against a pre-determined target value for the KPI.
ADOMD.NET	See Other Term: ActiveX Data Objects MultiDimensional.NET
aggregate	A single value that is composed of multiple values. For KPIs, aggregation determines the mathematical formula that is used to combine members (SUM, AVERAGE, and so on).
analytic chart	A report type that displays cube data in a visual, interactive chart format.
analytic grid	A report type that displays cube data in a visual, interactive tabular format.
average weighted	A type of rollup. It indicates an average that considers the weighted value of all child KPIs. This rollup reflects overall performance.
balanced scorecard	A business oriented scorecard that conveys key metrics related to the service and business of providing service. A balanced scorecard contains a balance of operational, financial, and quality driven metrics.
balanced scorecard methodology	A scorecard system that adheres to the framework and components established by the Balanced Scorecard Collaborative.
banding	The use of bands to represent ranges of performance based on thresholds.
banding settings	A setting that defines thresholds, or boundaries between changes in indicator status.
bulk edit	A procedure by which a user can

Term	Definition
	simultaneously change specified properties for a group of selected items.
cache interval	The length of time that a stored copy of the views that are shown in a dashboard can exist on the server.
calculated metric	A metric that is based on the result of an expression, rather than originating from a data source.
Calculated Metrics	A feature that enables users to create simple calculations by using one or more KPI values. This reduces the amount of MDX that is required to create complex scorecards.
centered indicator	The indicator set that can be used when the "closer to target" scoring pattern is selected when you edit the band settings.
collapse	An analysis tool, similar to drill up, that displays less detail about an item while maintaining the current display of other items.
cube	A set of data that is organized and summarized into a multidimensional structure that is defined by a set of dimensions and measures.
custom table	A type of filter that enables users to choose from a list and then drive dashboard content from multiple data sources.
customized scorecard	A scorecard that is created without using a template.
dashboard	A related group of interactive scorecard and report views that are organized together in a SharePoint or Web-hosted site. Dashboard elements may share common filters that control the data displayed within the elements.
Dashboard Designer	See Other Term: PerformancePoint Dashboard Designer
data source	A source of business data used by PerformancePoint applications. PerformancePoint data sources may include cubes or data source views (DSV) based on online analytical processing (OLAP) cubes, relational databases, CSV files, Microsoft Excel spreadsheets, or any other Open Database Connectivity (ODBC) or multidimensional (ADOMD.NET) data source.
data source formatting	A type of conditional formatting that is configured within Microsoft SQL Server Analysis Services. It causes individual cells to be highlighted when certain conditions, based on business rules, are met. For example, if

Term	Definition
	Gross Margin is over 28%, the cell is shown with a green background. Known as "OLAP Server Formatting" in Excel.
Decomposition Tree	A data visualization tool that helps users analyze complex information using a hierarchical scheme. The Decomposition Tree can help users find the root cause that is driving a value. For example, if sales in Canada are poor in March, the Decomposition Tree will help determine whether that is being driven by a particular product line, a certain sales territory, or an increase in returns.
deploy	To create a SharePoint page from a PerformancePoint dashboard so that users can access it.
dimension	A structural attribute of a cube that organizes data into levels. For example, a Geography dimension might include the members Country, Region, State or Province, and City.
display item	A folder into which attributes, measures, calculated members, KPIs, and PerformancePoint items can be organized to facilitate browsing by users.
drill down/drill up	A technique for navigating through levels of data ranging from the most summarized (up) to the most detailed (down). For example, when viewing the details of sales data by year, a user can drill down to display sales data by quarter, and further to display data by month.
filter	A control that is added to a dashboard or dashboard content so that users can modify the view. With this control, users can view a subset of data that is displayed in reports and scorecards that are returned by their corresponding data sources.
filter link	An association between a filter control and a parameter. This association is defined on a report or scorecard in a dashboard. Items with links to a filter change when the filter is modified.
Filter Web Part	A feature that enables users to modify dashboard views by changing the subset of data that is displayed in reports or scorecards.
fixed value	A user-entered value or a static value from an Excel spreadsheet that does not change unless manually altered by the user. Contrast this with dynamic values that are queried from a SQL Server database, OLAP cube, or other data

Term	Definition
	source.
formatting dimension	The dimension (usually "Measures") that numeric formatting is applied to. Some cubes use a Scenario dimension that is more desirable for numeric formatting.
hierarchy	1. A logical tree structure that organizes the members of a dimension such that each member has one parent member and zero or more child members. 2. A logical tree structure that organizes the members of a set into parent-child relationships. A ranked structure with a top level and subordinate levels.
hierarchy level	In a hierarchy, members are classified into levels (branches). Leaf level is the bottom level in the hierarchy. In a Time dimension, levels can also have names associated with them. For example, in a [Time] dimension, leaf level can represent Months and level above -- Years.
import	To bring information from one system or program into another. The system or program receiving the data must somehow support the internal format or structure of the data.
indicator	A set of graphics, text, and colors for defining different levels of performance when comparing an actual value and a target value within a KPI.
indicator count	A type of rollup. It gives the total numbers of indicators in the tree below it, rolled up according to status
Internet Protocol Security (IPsec)	A set of industry-standard, cryptography-based protection services and protocols. IPSec protects all protocols in the TCP/IP protocol suite and Internet communications by using Layer Two Tunneling Protocol (L2TP).
IPsec	See Other Term: Internet Protocol Security (IPsec)
key performance indicator (KPI)	A predefined measure that is used to track performance of a strategic goal, objective, plan, initiative, or business process. A KPI is evaluated against a target. An explicit and measurable value taken directly from a data source. Key performance indicators (KPIs) are used to measure performance in a specific area, for example, revenue per customer.
KPI	See Other Term: key performance indicator (KPI)
KPI details report	A report type that shows information about a KPI that is selected in a scorecard.

Term	Definition
level	A degree of granularity in hierarchies. Levels enable you to view data in various degrees of detail. The Time dimension, for example, can have the levels Year, Quarter, Month, and Day.
list	A Web site component that stores and displays information that users can add to by using their browsers. For PerformancePoint Services, the site requires a Web server that is running Microsoft SharePoint Server.
MDX	See Other Term: multidimensional expression (MDX)
MDX formula	The online analytical processing (OLAP) equivalent of an SQL query.
measure	A quantified value that is indicative of the size, quantity, scale, importance, or extent of something important to an organization.
measure group	A collection of related measures in an Analysis Services cube. The measures are generally from the same fact table.
member	A single position or item in a dimension. The Account dimension, for example, could have a dimension member called Travel Expenses. Dimension members can be user-defined or predefined and can have properties associated with them. See dimension member property for details.
metadata	Information about the properties of data, such as the type of data in a column (numeric, text, and so on) or the length of a column. It can also be information about the structure of data or information that specifies the design of objects such as cubes or dimensions.
metric	An actual or target value of a KPI. A metric may be used as a scorecard element.
Microsoft SharePoint Products and Technologies	A set of products and technologies that allow users in an organization to create, manage, and build their own collaborative Web sites and make them available throughout their organizations. These products and technologies include SharePoint Portal Server for portal sites and Windows SharePoint Services for team sites.
Microsoft XML Core Services (MSXML)	Technology that allows users to build high-performance XML-based applications that provide interoperability with other applications that adhere to the XML 1.0 standard.
MSXML	See Other Term: Microsoft XML Core Services

Term	Definition
	(MSXML)
multidimensional expression (MDX)	A language for querying and manipulating data in multidimensional objects (OLAP cubes).
named set	A grouping of dimension members or items from a data source that are named and treated as a single unit and can be referenced or reused multiple times.
objective	A group of key performance indicators (KPIs) that correspond to the functional areas or strategic initiatives of an organization.
objective KPI	A KPI that derives its target value and score from a rollup of its child KPIs. Objective KPIs do not have actual values and do not connect to external data sources. They indicate performance by showing a normalized aggregation of the KPIs one level below them in the scorecard.
ODBC	See Other Term: Open Database Connectivity (ODBC)
OLAP	See Other Term: online analytical processing (OLAP)
OLAP cube	See Other Term: cube
online analytical processing (OLAP)	A technology that uses multidimensional structures to provide rapid access to data for analysis. The source data for OLAP is commonly stored in data warehouses in a relational database.
Open Database Connectivity (ODBC)	An application programming interface (API) that enables database applications to access data from a variety of existing data sources.
parameter	A field defined on a dashboard item that can receive data from a filter control. Data supplied to this field modifies content that is displayed in the dashboard scorecard or report.
PerformancePoint Content List	A list that stores the elements that are used to construct a PerformancePoint dashboard. A PerformancePoint dashboard is a related group of interactive scorecards, filters, and report views that are organized together into a set of Web pages.
PerformancePoint Dashboard Designer	A client application that you use to create and manage dashboards, scorecards, reports, and other PerformancePoint items prior to deploying them within a dashboard to a SharePoint site.
PerformancePoint Data Connections Library	A SharePoint document library that may contain Office Data Connections (ODC), Universal Data Connection (UDC) files, and PerformancePoint

Term	Definition
	data connections. Data connections identify a source of business data that may include cubes or perspectives that are based on online analytical processing (OLAP) cubes, relational databases, CSV files, Microsoft Excel Services spreadsheets, or other data sources.
PerformancePoint PowerShell Cmdlet	A task-oriented command that is used in the Windows PowerShell environment. Or A small, basic command, named in the form "verb-noun'" and implemented as a .NET class that derives from a base cmdlet class. Examples: get-process, new-drive.
PerformancePoint Server	See Other Term: PerformancePoint Services in Microsoft SharePoint Server
PerformancePoint Service	The SharePoint service application that enables dashboarding capabilities by means of scorecards, analytic grids and charts, and other decision-making tools for the enterprise.
PerformancePoint Service application	The PerformancePoint component that runs as a SharePoint shared service. It is one of many service applications that plug into SharePoint. Other examples include Excel Services, Search Service, and Visio Graphics Service.
PerformancePoint Service application proxy	The PerformancePoint Web Front End (WFE) service interface. It abstracts the communication layer between WFE components and the service application.
PerformancePoint Services	See Other Term: PerformancePoint Services in Microsoft SharePoint Server
PerformancePoint Services Central Administration	A collection of SharePoint administration pages that the administrator can use to configure PerformancePoint Services for SharePoint.
PerformancePoint Services in Microsoft SharePoint Server	A collection of services for Microsoft SharePoint Server that enables users to monitor organizational goals, to analyze performance information through up-to-date content and context-rich dashboards and scorecards, and to use that information to make business decisions. These capabilities were formerly part of the PerformancePoint Server product.
PerformancePoint Settings Database	A PerformancePoint-specific database that stores the annotations for each dashboard element, user-based filter selections, and other information about dashboard elements.
PerformancePoint trusted location	A location within Microsoft SharePoint Server from which dashboard content can run. The default is to trust all locations.The PerformancePoint Services administrator must

Term	Definition
	change it to make it more restrictive.
PerformancePoint Web Parts	Functionality in PerformancePoint Services that makes it possible to display dashboard views that are defined in Dashboard Designer to users of a SharePoint site.
PerformancePoint Web Services	A collection of Web services that determines how PerformancePoint Services operates.
pie chart	A round chart that shows the size of items in a single data series, proportional to the sum of the items.
refresh	The activity of synchronizing dashboards and dashboard elements between the local workspace and PerformancePoint Services in Microsoft SharePoint Server.
relational database	A database or database management system that stores information in tables. In conducting searches, a relational database matches information from a field in one table with information in a corresponding field of another table to produce a third table that combines requested data from both tables.
report	A visual display of data in a dashboard that can be coordinated with other report views by using filters. Reports include analytic grids and charts, KPI details, Excel Services spreadsheets, SQL Server Reporting Services reports, strategy maps, ProClarity Analytics Server reports, and Web pages.
report view group	Reports that are grouped together in a single dashboard zone. These reports can be conditionally shown, based on the selected KPI.
Report Web Part	A feature that allows users to view and interact with reports that are created in PerformancePoint Dashboard Designer.
Reporting Services report	A report type that acts as a wrapper for a SQL Server Reporting Services report so that the Reporting Services report can be displayed in a PerformancePoint dashboard.
ribbon	The ribbon is part of the Microsoft Office Fluent user interface (UI). In Dashboard Designer, It consists of contextual tools for creating, editing, and exporting dashboards and their elements.
rollup	The calculated value of a KPI is derived from the aggregated scores of child or descendant KPIs.
scorecard	A report type that depicts organizational performance by displaying a collection of key

Term	Definition
	performance indicators (KPIs) together with performance targets for those KPIs. A scorecard can be organized hierarchically.
scorecard element	Any one of the individual components of a scorecard, such as key performance indicators (KPIs), members, properties, actuals, targets, or MDX expressions.
Scorecard Web Part	A feature that enables users to view and interact with scorecards that are created in PerformancePoint Dashboard Designer.
SharePoint Products and Technologies	See Other Term: Microsoft SharePoint Products and Technologies
Stack Selector Web Part	A feature that enables users to show more than one view in a single location on a dashboard, and provides a control to switch between them.
standard indicator	An indicator set that can be used when either the "increasing is better" or "decreasing is better" scoring patterns are selected when you edit the band settings.
strategy map	A performance management tool for visually presenting an organization's or organizational unit's objectives and goals, their groupings of objectives and goals, and their mappings of objectives and goals to themes, initiatives, KPIs, targets, business processes, and action plans. Each item in the visualization contains a set of metadata, which itself is customizable.
target	As one aspect of a KPI, a target is the desired level of performance with respect to a specific business goal or strategy. Actual values are evaluated against the target to determine KPI score and status.
time dimension	A dimension that breaks time down into levels such as Year, Quarter, Month, and Day. In Analysis Services, a special type of dimension created from a date/time column.
time formula	An expression that is created following the Simple Time Period Syntax. It takes the form of a time unit plus or minus a whole number, such as Year-1 or Month-6. It is the formula that is applied when you are using time intelligence on a dashboard.
time intelligence filter	A dynamic dashboard filter that can be linked to scorecards and reports so that they will update automatically relative to the current time.
unattended service account	The security account that is used when a data

Term	Definition
	source is configured to connect as a single shared identity for all users.
update	To retrieve the most current data from the data source that is associated with a scorecard.
validate	To ensure that all data sources that are used by a KPI or scorecard are available.
variance	The difference between two values, such as the difference between estimated and actual expenses.
Web page report view	A report type that contains a Web page.
Web Part	Microsoft SharePoint Products and Technologies functionality that is the basic building block for a page on a SharePoint site. A modular unit of information that consists of a title bar, a frame, and content.
Web Part description file (.dwp)	An .xml file that defines the default property settings for a Web Part, including references to other files that are required to run and display the part.
weight	The value of a scorecard KPI in relation to the values of other KPIs. For example, you might have an objective with two key performance indicators (KPIs), the first with a weight of one and the second with a weight of three. This means that the second KPI is three times more important than the first. The weights that are assigned to the KPIs are part of the calculation when their values are rolled up to derive the value for their parent objective.
what you see is what you get (WYSIWYG)	pronounced wizzywig. Allowing a user to view a document as it will appear in the final product, and to directly edit the text, graphics, or other elements within that view. A WYSIWYG language is often easier to use than a markup language, which provides no immediate visual feedback regarding the changes being made. Compare markup language. A type of program that allows creation and editing of web pages, text, or graphical user interfaces so that users can see what the end results will look like while the documents are being created.
workspace	The user interface area in Dashboard Designer that contains the dashboard items that are being edited by a user. The contents of the workspace can be saved as a file with a .ddwx extension.
worst indicator	A type of rollup of child KPIs. It moves the indicator of the lowest performing KPI to the

Term	Definition
	objective KPI row.
WYSIWYG	See Other Term: what you see is what you get (WYSIWYG)

Word Automation Services Troubleshooting (SharePoint Server 2010)

Published: July 8, 2010

This article describes how Word Automation Services handles errors that can occur at the conversion item or system level, and provides common troubleshooting steps for resolving these errors.

In this article:

- How Word Automation Services reacts to potential system failures
- How to troubleshoot failed conversions
- How to troubleshoot specific events
- Known failures that do not have Word Automation Services events for SharePoint Server 2010

How Word Automation Services reacts to potential system failures

System administrators are alerted to potential system failures in multiple ways; for example:

- Users communicate perceived failures or events to a system administrator when files are not converted successfully. For example, during a conversion a message directs the user to contact a system administrator.
- Windows Events that list a source of "Word Automation Services" occur on the server where a failure was detected.
- When available, System Center Operations Manager (SCOM) indicates that Word Automation Services is unhealthy.

When a conversion job fails, the solution typically provides the string that is displayed in the ConversionItemInfo.ErrorMessage for each failed conversion and directs the user to perform any needed actions on the file. In some cases ConversionItemInfo.ErrorMessage does not contain enough information for an administrator to diagnose and correct a potential system failure. For more information about the details that the ConversionItemInfo.ErrorMessage provides for a conversion job, see ConversionItemInfo Members (*http://go.microsoft.com/fwlink/?LinkId=196477*).

In the event of a known system failure, Word Automation Services also generates a Windows Event on the server where the failure was detected. Events are intended to be available to administrators to diagnose and troubleshoot individual system failures. Each event can include much information that requires additional investigation by the administrator. End users do not see events.

An event resides on the server that emitted it. Events can be viewed by accessing the server's Event Viewer. Search for events that have "Word Automation Services" as the event source. You can also use a SCOM Console to aggregate the emitted events of the whole farm in a single view. SCOM presents the health status of Word Automation Services and the servers it is running on.

Consistent interruptions in Word Automation Services can also indicate system failure. See How to troubleshoot failed conversions for more troubleshooting help.

How to troubleshoot failed conversions

This section describes the steps to troubleshoot a failed conversion.

1. Confirm that the file that is being converted meets the following criteria:
   - Is not blocked by file type
   - Is not password protected
   - Does not require IRM to be opened
   - Is of a type that is supported by the version of Word Automation Services for SharePoint Server 2010 that you are using
2. If the ConversionJobItem.ErrorCode is 131182, the file is likely corrupted. If the ErrorCode is not 131182, confirm that the file is not corrupted by comparing the ErrorCode against its corresponding Word Automation Services ConversionItemInfo.ErrorMessage string. Then follow the instructions to resolve the conversion item failures. Also, an administrator can try opening the file in the client version of Microsoft Word and saving the file. This process eliminates corruption or repairs the file if it is corrupted. Then submit the file again for conversion.
3. If the file is valid but the conversion still fails, begin polling the Event logs of individual servers for events that have Word Automation Services as the event source. Windows system events can be viewed by using the Event Viewer. Or, you can use SCOM to view an aggregated view of all events from all servers in the farm. An unusually large number of Word Automation Services events can indicate a failure condition that is detected during multiple file conversions. Follow the troubleshooting steps that are specified in the event message for each type of event and perform the needed action to resolve the issue.
   Note:
   Make sure that on the Diagnostic Logging page in Central Administration, the **Least critical event to report to the event log** setting for the **Word Automation Services** category is not set or is set to **Warning** or a less severe level, such as **Informational** or **Verbose**. Otherwise, some important events might not be generated by Word Automation Services.
4. If the event message and prescribed actions do not lead to a resolution of the issue, see How to troubleshoot specific events.
5. If the instructions of the event message and the "How to Troubleshoot Specific Events" section are insufficient to resolve the problem, or if there are no events emitted, review the ULS trace logs for the affected servers to learn more about the issue.
   To prepare these logs for troubleshooting, on the Diagnostic Logging page in Central Administration, set the **Least critical event to report to the trace log** setting for the **Word Automation Services** category.
   Warning:
   Turning on Verbose tracing will affect performance for all application servers. Make sure to set **Least critical event to report to the trace log** back to Medium after you complete troubleshooting activities.
   With Verbose tracing turned on, test Word Automation Services under load to manifest the detected failures. When the failures occur, open the ULS trace logs in a text editor for servers where the failures occurred. Note that trace files are typically very large (for example, multiple gigabytes in a production environment) and might require significant time to download, open, and review. Filter the tracing log by the Word Automation Services area of the trace.
   The quality and readability of trace log entries, also known as *traces*, will vary. Traces are not localized and are not necessarily intended for external use. Trace logs may contain a limited amount of Personally Identifiable Information about file conversion items or jobs.

ULS trace logs can typically be found on each server in the following location: %COMMONPROGRAMFILES%\Microsoft Shared\Web Server Extensions\14\LOGS

6. If the previous steps do not yield a resolution, visit the Technical Support for Microsoft Products (*http://go.microsoft.com/fwlink/?LinkID=15029*) Web site and contact a support representative to help diagnose and resolve the issue.

How to troubleshoot specific events

This section lists the events that are logged for specific failure conditions, describes the causes of the events, and provides resolution steps for each error.

Note:
Events with IDs that start with 80 can be generated with very high frequency when a system failure occurs. These events are generated for every conversion attempt that encounters the relevant failure. By default, Microsoft SharePoint Server 2010 disallows the generation of more than five events with the same ID on the same server every two minutes. This default setting reduces the number of events logged in persistent error situations. In the Windows Event Log, when you view event IDs that start with 80, you might find five events of the same ID followed soon after by a SharePoint Server event ID 2159. The message for event 2159 will indicate which event is suppressed and the number of times it was suppressed.

Note:
The SharePoint Server 2010 management pack for Microsoft System Center Operations Manager 2007 contains a SCOM Monitor to detect each Windows Event and surface health information about Word Automation Services to administrators more easily. For more information about the SCOM Monitor, see Microsoft SharePoint 2010 Products (Beta) Management Pack (*http://go.microsoft.com/fwlink/?LinkId=196473*).

Event 8004 and 8005: The PDF/XPS converter '[file path & name]' failed during file conversion
Word Automation Services includes a default converter for converting files to both XPS and PDF file formats. Word Automation Services also supports third-party converters. Third-party converters could have bugs that cause file conversions to fail in an unpredictable manner. Word Automation Services emits one of these two events when a third-party converter fails:

Event ID	Event message string	Related message ID	Additional details
8004	The PDF converter '[file path & name]' failed during file conversion. Contact the vendor of this component to see whether an updated version is available. If this does not resolve the failure, uninstall the third-party PDF converter to prevent this failure from recurring.	131183	Log Name: Application Source: Word Automation Services Event Level: Error

Event ID	Event message string	Related message ID	Additional details
8005	The XPS converter '[file path & name]' failed during file conversion. Contact the vendor of this component to see whether an updated version is available. If this does not resolve the failure, uninstall the third-party XPS converter to prevent this failure from recurring.	131184	Log Name: Application Source: Word Automation Services Event Level: Error

Word Automation Services also sets the conversion item's failure message as follows:

Message ID	ConversionItemInfo.ErrorMessage string	Related event ID
131183	The third-party PDF converter failed. Please contact a system administrator.	8004
131184	The third-party XPS converter failed. Please contact a system administrator.	8005

Resolution

1. If these kinds of failures occur, follow these steps to update the converters:
    a) Acquire the latest DLL for the custom PDF or XPS converter from the vendor of the converter.
    b) Overwrite the old DLL with the new DLL in %COMMONPROGRAMFILES%\Microsoft Office Servers\14.0\WebServices\WordServer\Core on each application in the farm.
    c) If the DLL is working correctly, new conversions should now succeed.
2. If the third-party converters continue to fail after all available updates have been applied, uninstall the third-party converters and use the default converters.
    - Delete the corresponding DLL for the PDF or XPS converter from this folder: %COMMONPROGRAMFILES%\Microsoft Office Servers\14.0\WebServices\WordServer\Core.
    - New conversions should now succeed.
3. If the file still does not convert, the file is likely corrupted or otherwise invalid. In this case try to open the file in the client version of Word, resave the file, and then resubmit the file for conversion.

Event 8010: A file that was created using a new version of Office client or Word Services has been encountered

Event 8010 is emitted when Word Automation Service encounters a file that was saved by a version of Microsoft Word newer than the currently installed version of the Word Automation Service. This might result in a conversion of decreased quality, depending on the contents of the document. If this event is emitted, upgrade Word Automation Services as soon as possible by following the link in the event message.

Note:
This event does not necessarily indicate that conversions are failing. Therefore there is no single Error Message ID that correlates with this event.

Event ID	Event message string	Related message ID	Additional details
8010	A file that was created by using a new version of Office client or Word Services has been encountered. Please visit http://go.microsoft.com/fwlink/?LinkId=157217 to download the latest Word Automation Services converter. Use the latest converter to make sure that newer Office documents are converted at the highest level of quality possible.	Not applicable	Log Name: Application Source: Word Automation Services Event Level: Error

Resolution
1. Download (http://go.microsoft.com/fwlink/?LinkId=157217) the latest Word Automation Services converter from the Microsoft SharePoint 2010 Software Development Kit (SDK).
2. Follow the instructions to install the new converter.
3. Convert the files. The files will be converted with the best possible quality and this event will not be generated unless files are encountered that require an update to the Word Automation Services converter.

Event 8012: One or more localized components could not be loaded for the specified language
When a conversion item fails, a ConversionItemInfo.ErrorCode and corresponding ConversionItemInfo.ErrorMessage are generated. The error message is intended to be presentable to the user who submitted the conversion job. The error message is localized to the browser language of the user who submitted the conversion job. However, if the server farm application servers do not have the language pack that corresponds to the user's browser language, the error messages cannot be presented for the end user's browser language. This event is emitted when this situation occurs for a failing conversion item. Also be aware that the error message itself will instead be presented in the default language of the farm.

Event ID	Event message string	Related message ID	Additional details
8012	One or more localized components could not be loaded for the specified language. Please check that the required language pack is installed and correctly configured.	Not applicable	Log Name: Application Source: Word Automation Services Event Level: Error

Resolution
- Download and deploy the required SharePoint Server 2010 language packs. Download language packs from the Microsoft Download Center (*http://go.microsoft.com/fwlink/?LinkID=141342*).

Event 1001: SQL Database Access Error. Error Code: %1. Error Message: %2. Error Link: %3

System failures for Word Automation Services are typically detected when the service communicates with the document queue. During each file conversion process, multiple communications occur between the service and the document queue. When a failure occurs, SQL Server generates a SQLException error with a large amount of relevant information. Word Automation Services detects any SQLException error generated by SQL Server when the service is communicating with the document queue, and emits this event:

Event ID	Event message string	Related message ID	Additional details
1001	SQL Database Access Error. Error Code: %1. Error Message: %2. Error Link: %3.	6, 7	Log Name: Application Source: Word Automation Services Event Level: Critical

This event message contains a subset of the SQLException properties to help administrators with troubleshooting failures that are detected when the Word Automation Services communicate with the document queue. These parameters are as follows:

Name	MSDN Description
ErrorCode	Gets the HRESULT of the error. (Inherited from ExternalException.)
HelpLink	Gets or sets a link to the Help file associated with this exception. (Inherited from Exception.)
Message	Overloaded.

The following is an example of the event message that the Word Automation Services generates if the document queue database is removed or renamed:
Sql Database Access Error. Error Code: 0x80131904. Error Message: Invalid object name 'dbo.ConversionItemQueue'. Error Link: None.
Error Code (SqlException.ErrorCode) is a SQL Server code that is not specific to Word Automation Services. You can use the SQL Server code to relate this failure to existing SQL Server troubleshooting information.
Error Message (SqlException.Message) is a SQL Server-specific string that contains human-readable information that describes the error and specifies the affected database. Administrators should investigate the server that maintains the database that is referenced in this string as recommended by SQL Server troubleshooting Help.
Error Link (SqlException.HelpLink) is a SQL Server-specific link to more SQL Server Help information.
Resolution
1. Note the error code, error message, and error link in the event message.
2. Use this information to help troubleshoot the SQL Server errors. For information about how to troubleshoot SQL Server error codes, see SQL Server Solution Center (*http://go.microsoft.com/fwlink/?LinkId=196474*).

Event 1002: Conversion jobs may not execute because the timer job '%1' for service application '%2' does not appear to be active

The timer job for the Word Automation Service processes and distributes queued job items to application servers. If the timer job does not run, queued job items will not start to convert. Event 1002 will be emitted if a new job is submitted at a time when the timer job appears to be inactive. Specifically, this event will be emitted if one or more of the following conditions are true:

1. The timer job is not online. This can occur if the job definition was not provisioned correctly.
2. The timer job is disabled. This can occur if an administrator disabled the timer job on the Edit Timer Job page in Central Administration.
3. The timer job has missed two scheduled runs according to the current settings in Central Administration.
4. The timer job misses scheduled runs because of an external issue, such as the OWSTimer service is turned off. OWSTimer is the SharePoint Timer Service.

Note:
SharePoint Server might require approximately 90 minutes to process the error condition and generate this event.

Event ID	Event message string	Related message ID	Additional details
1002	Conversion jobs may not execute because the timer job '%1' for service application '%2' does not appear to be active.	Not applicable	Log Name: Application Source: Word Automation Services Event Level: Warning

This event message contains the name of the timer job that is not running and the name of the service application that is associated with the timer job. The following is an example message for this event:
"Conversion jobs may not execute because the timer job 'e39db2de-1b89-4f74-91da-5da998df0a9c' for service application 'Word Automation Service Application' does not appear to be active."

Resolution

- Enable the Word Automation Services Timer job:
  1. On the Central Administration Home page, click **Monitoring**.
  2. On the Monitoring page, under **Timer Jobs**, click **Job Definitions**.
     Note if the Word Automation Services Timer Job is a scheduled Timer job.
  3. If the schedule type for Word Automation Services Timer Job is disabled, click **Word Automation Services Timer Job**.
  4. On the Edit Timer Job page, click **Enable**.
     Queued jobs should start to convert when the Timer job runs.

If the Word Automation Services Timer Job is not a scheduled Timer job, Word Automation Services is not installed or is installed incorrectly.

Known failures that do not have Word Automation Services events for SharePoint Server 2010

Word Automation Services does not generate unique Windows Events for these known failure conditions:

- Any failure that results in an SPException (*http://go.microsoft.com/fwlink/?LinkId=196475*) that is generated by SharePoint Server.
- Any failure that results in an UnauthorizedAccessException (*http://go.microsoft.com/fwlink/?LinkId=196476*) that is generated by SQL Server or SharePoint Server.
  Example: A user's permissions for accessing a content database have changed.
- Failures that clearly affect the whole server and not only the Word Automation Services service. Such failures are detected and surfaced in Windows and SharePoint Server.
  Example: Insufficient disk space.

Timer job reference (SharePoint Server 2010)

Published: July 15, 2010

This article describes the default timer jobs for SharePoint Server 2010. A timer job runs in a specific Windows service for SharePoint Server. 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 Server rely on timer jobs to run services according to a schedule.

In this article:

- Manage timer jobs
- Default timer jobs

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 Server 2010) (*http://technet.microsoft.com/library/4ad542f7-84ad-456b-bfc4-6200c949e9f7(Office.14).aspx*).

Default timer jobs

The following table lists the default timer jobs for SharePoint Server 2010.

Timer job title	Description	Schedule type
Audit Log Trimming	Trims audit trail entries from site collections.	Monthly
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
Change Log	Documents changes to sites and pages in a Web application since the last time that the timer job was run.	Daily
Config Refresh	Checks the configuration database for configuration changes.	15 seconds
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
Delete Job History	Deletes old entries from the timer job history.	Weekly
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 the first server found in the farm that runs 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	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	Daily

Timer job title	Description	Schedule type
Foundation Timer, Any Server)	Service application.	
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 Foundation Web Application, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs SharePoint Web applications and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Daily, SSP Job Control Service, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs the SSP Job Control Service and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Daily, Visio Graphics Service, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs Visio Services and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Daily, Web Analytics Data Processing Service, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs a Web Analytics Data Processing Service application and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Daily, Web Analytics Web Service, Any Server)	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs a Web Analytics Service application and the Usage and Health Data Collection Service application.	Daily
Health Analysis Job (Hourly, Security Token Service, 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	Runs SharePoint Health Analyzer jobs on the first server found in the farm that runs Profile Services and	Hourly

Timer job title	Description	Schedule type
Profile Service, Any Server)	the Usage and Health Data Collection Service application.	
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 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.	Weekly
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	Daily

Timer job title	Description	Schedule type
	to force a check on 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
State Service Delete Expired Sessions	Deletes expired data that is stored in the state service databases.	Hourly
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.	1 minute
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.	1 minute
CEIP Data Collection	Gathers farm data for the Customer Experience Improvement Program.	Daily
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 and stores the data in the logging database. **Important:** The timer service account must have	5 minutes

Timer job title	Description	Schedule type
	sufficient permission to collect counters on the database server. The account should be a member of the Performance Monitor Users (PMU) group.	
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: SQL DMV	Collects SQL Dynamic Management Views (DMV) data.	30 minutes
Diagnostic Data Provider: SQL Memory DMV	Collects SQL Dynamic Management Views (DMV) data.	15 seconds
Diagnostic Data Provider: Trace Log	Collects Trace Log entries and stores the usage data in the logging database.	10 minutes
SharePoint Server CEIP Data Collection	Gathers farm data for the Customer Experience Improvement Program.	Daily
Document ID assignment job	Work item that assigns document ID to all items in the site collection.	Daily
Document ID enable/disable job	Work item that propagates content type changes across all sites when the Document ID feature is reconfigured.	Daily
Document Set fields synchronization job	Synchronizes metadata from the document set to the items inside the document library.	15 seconds
Content Type Hub	Tracks content type log maintenance and manages unpublished content types.	15 minutes
Content Type Subscriber	Retrieves content types packages from the hub and applies them to the local content type gallery. For more information about content types, see Plan to share terminology and content types (*http://technet.microsoft.com/library/57325cc3-bce2-4dd3-9b26-12fec99140ad(Office.14).aspx*)	Hourly
Enterprise Metadata site data update	Updates all site collections after a language pack addition or an Enterprise Metadata Service application restore.	Hourly
Taxonomy Update Scheduler	Updates site collections with the latest term changes that were made to the Enterprise Metadata Service.	Hourly
FAST Search for SharePoint Master Job	Provisions the timer jobs for FAST Search Server 2010 for SharePoint if the Search service application type is set to FAST Query Application.	15 minutes

Timer job title	Description	Schedule type
FAST Search Server 2010 for SharePoint Alternate Access Mapping Extractor Job	Retrieves the managed properties from the configured FAST Search Server 2010 for SharePoint farm that have the IsMapped flag set to true, and caches the properties on the SharePoint farm. These properties are used for alternate access mapping.	5 minutes
FAST Search Server 2010 for SharePoint Click Through Extractor Job	Extracts clickthrough data and uploads them to the configured FAST Search Server 2010 for SharePoint farm. The collected clickthrough data is used for relevancy tuning.	Daily
FAST Search Server 2010 for SharePoint Dictionary Compilation Job	Detects dictionary changes that are made by using Central Administration and exports the changes to the FAST Search Server 2010 for SharePoint farm.	5 minutes
InfoPath Forms Services Maintenance	Performs maintenance operations on administrator-approved InfoPath Forms Services form templates across all front-end Web servers.	Daily
Application Server Administration Service Timer Job	Manages shared service instances that may perform highly privileged operations. Requires that the SharePoint Administration service is running. The Search service instance is managed by this job on deployments other than stand-alone server deployments.	1 minute
Application Server Timer Job	Manages shared service instances that do not perform highly privileged operations. The Search service instance is managed by this job on stand-alone server deployments.	1 minute
Licensing Synchronizer Job	Synchronizes trial expiration time licensing information to the configuration database.	Hourly
Application Addresses Refresh Job	Synchronizes connection information for remote service applications.	15 minutes
SharePoint BI Maintenance	Deletes temporary dashboard objects and user-persistent filter values from the database. The longevity of these values can be set on the PerformancePoint Services Settings page.	Hourly
Project Server 'Project Service Application:pwa' Resource Capacity job	Resource capacity job for Project Server Service application.	Daily
Project Server 'Project Service Application:pwa' Workflow Cleanup job	Workflow cleanup job for Project Server Service application.	Daily

Timer job title	Description	Schedule type
Project Server Service Credential Synchronizing Job	Credential synchronizing job for Project Server Service application.	Minutes
Project Server Synchronizing Job for 'Project Service Application'	Project Server synchronizing job for Project Server Service application.	1 minute
Notification Timer Job	Queries and updates the notification list and sends out pending scheduling notifications.	Daily
Scheduled Approval	Looks for content that is scheduled for approval and moves it to the next stage in the process.	1 minute
Scheduled Unpublish	Looks for content that is scheduled to be unpublished and removes it.	1 minute
Variations Create Hierarchies Job Definition	Creates a complete variations hierarchy by spawning all sites and pages from the source site hierarchy for all variation labels.	Daily
Variations Create Page Job Definition	Creates peer pages in variant sites.	Hourly
Variations Propagate Page Job Definition	Creates or updates peer pages of the source page that has been approved or published in all target labels. The resulting peer pages are in an unpublished state.	1 minute
Variations Propagate Site Job Definition	Creates peer sites of the source site that has been created in all target labels.	1 minute
Content Organizer Processing	Processes documents in the drop-off library that match organizing rules.	Daily
Expiration Policy	Enumerates list items and looks for those with an expiration date that has already occurred. For those items, runs disposition processing. Disposition processing most often results in deleting items, but it can perform other actions, such as processing disposition workflows.	Daily
Hold Processing and Reporting	Generates a hold report by enumerating items in a hold and updating them to remove them from hold, as appropriate.	Daily
Information Management Policy	Loops through all the lists in the site collections in a Web application and collects policy and usage data.	Daily
Search and Process	Processes a search result that is scoped to a site collection and puts search results on hold.	Daily
Crawl Log Cleanup for Search Application Search Service Application	Crawls log cleanup for Search Service applications.	Daily
Crawl Log Report for Search Application Search Service Application	Crawls log report for Search Service applications.	5 minutes

Timer job title	Description	Schedule type
Health Statistics Updating	Updates the statistics for the Usage and Health Data Collection service application.	1 minute
Indexing Schedule Manager on SQL Server	Starts scheduled crawls.	1 minute
Prepare query suggestions	Prepares candidate queries for query suggestion.	Daily
Query Logging	Logs the statistics for the number of queries performed.	15 minutes
Search Health Monitoring - Trace Events	Runs to check the events that are being traced for search health monitoring.	
User Profile Service - Activity Feed Cleanup Job	Cleans up pre-computed activities that are used in activity feeds that are older than 14 days. This job does not affect the User Profile Change Log.	Daily
User Profile Service - Activity Feed Job	Pre-computes activities to be shown in user activity feeds.	Hourly
User Profile Service - Audience Compilation Job	Computes memberships of defined audiences.	Weekly
User Profile Service - My Site Suggestions Email Job	Sends e-mail messages that contain colleague and keyword suggestions to people who do not update their profile often, prompting them to update their profiles.	Monthly
User Profile Service - Social Data Maintenance Job	Aggregates social tags and ratings and cleans the social data change log.	Hourly
User Profile Service - User Profile Change Cleanup Job	Cleans up data that is 14 days old from User Profile Change Log. Migrates user rights from one user to another user, and migrates the user rights and cleans up that user from Active Directory Domain Services (AD DS). This is mainly used when the name of a user is changed in AD DS. The older user name is replaced by a new user name and the older one is removed from AD DS.	Daily
User Profile Service - User Profile Change Job	Processes changes to user profiles. Changes the user profile. User rights can be migrated from one user to another user. This timer job is used when a user has to be migrated, but the previous user profile remains in AD DS.	Hourly
User Profile Service - User Profile Incremental Import Job	Manages provisioning and user profile synchronization. Imports only the user profiles that were added after the last import. **Note:** Do not change the settings or frequency of this Timer job. To change the schedule for incremental synchronization, see Schedule	1 minute

Timer job title	Description	Schedule type
	recurring profile synchronization (*http://technet.microsoft.com/library/53038195-cb59-4779-9bdb-ba0b1cad6f07(Office.14).aspx*).	
User Profile Service - User Profile Language Synchronization Job	Looks for new language pack installations and makes sure that strings that related to the user profile service are localized correctly.	1 minute
User Profile Service Proxy - Social Rating Synchronization Job	Synchronizes rating values between the social database and content database.	Hourly
User Profile to SharePoint Full Synchronization	Synchronizes user information from the user profile application to SharePoint users and synchronizes site memberships from SharePoint to the user profile application.	Hourly
User Profile to SharePoint Quick Synchronization	Synchronizes user information from the user profile application to SharePoint users who were recently added to a site.	5 minutes
My Site Cleanup Job	When a user is deleted, starts a workflow on that user's My Site. The default behavior is to send an e-mail message to the manager with a link to the deleted user's site. The e-mail message contains a request to the manager to move any documents or data that the manager wants to preserve, because the site might be deleted in the future.	Hourly
Web Analytics Trigger Workflows Timer Job	Starts Web Analytics Workflows for Web applications.	Daily
Word Automation Services Timer Job	Processes and distributes queued conversion job items to application servers.	15 minutes
Bulk Workflow Task Processing	Processes bulk workflow task completion.	Daily

SharePoint 2010 Administration Toolkit (SharePoint Server 2010)

Published: July 15, 2010

This article provides information for farm administrators about the April 2011 release of the SharePoint Administration Toolkit version 2.0, which includes the following features:

- The Load Testing Kit, which generates a Visual Studio Team System 2008 (VSTS) load test based on Microsoft Office SharePoint Server 2007 IIS logs. The VSTS load test can be used to generate synthetic load against Microsoft SharePoint Server 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.
- New in SharePoint Administration Toolkit 2.0, the SharePoint Diagnostic Studio 2010 (SPDiag 3.0) provides SharePoint administrators with a unified interface that can be used to gather relevant information from a farm, display the results in a meaningful way, identify performance issues, and share or export the collected data and reports for analysis by Microsoft support personnel.

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.

To download the toolkit, see Microsoft SharePoint 2010 Administration Toolkit (*http://go.microsoft.com/fwlink/?LinkId=196866*).

In this section:

- Installing the SharePoint 2010 Administration Toolkit (SharePoint Server 2010)
- Uninstalling the SharePoint 2010 Administration Toolkit (SharePoint Server 2010)
- Load Testing Kit (SharePoint Server 2010)
- User Profile Replication Engine overview (SharePoint Server 2010)

- Security Configuration Wizard manifest for SharePoint Server 2010
- Content Management Interoperability Services (CMIS) connector overview (SharePoint Server 2010)
- SharePoint Diagnostic Studio 2010 (SPDiag 3.0) (SharePoint Server 2010)

Installing the SharePoint 2010 Administration Toolkit (SharePoint Server 2010)

Published: July 15, 2010

This article describes how to install the SharePoint 2010 Administration Toolkit version 2.0.
The SharePoint Administration Toolkit requires Microsoft SharePoint Server 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, SharePoint Diagnostic Studio: 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://go.microsoft.com/fwlink/?LinkId=216724*).
  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 Server 2010)

Uninstalling the SharePoint 2010 Administration Toolkit (SharePoint Server 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 Server 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 Server 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 Server 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 Server 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, on which the Microsoft SharePoint Server 2010 SCW manifest depends:
   - 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.

4. Register the SharePoint Server 2010 SCW manifest:
   - If you are using Windows Server 2008 Service Pack 2, type **scwcmd register /kbname:MSS2010 /kbfile:MSS2010W2K8.xml** and press ENTER.
   - If you are using Windows Server 2008 R2, type **scwcmd register /kbname:MSS2010 /kbfile:MSS2010W2K8R2.xml** and press ENTER.

You can now run the SCW to create a security policy that incorporate the roles for SharePoint Server 2010.

Concepts

SharePoint 2010 Administration Toolkit (SharePoint Server 2010)

Other Resources

Security Configuration Wizard Documentation (*http://go.microsoft.com/fwlink/?LinkId=162647*)

Load Testing Kit (SharePoint Server 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 Server 2010 farm. The goal of the tool is to assist an administrator to certify that an existing Microsoft Office SharePoint Server 2007 topology running on specific hardware can sustain an upgrade to a Microsoft SharePoint Server 2010 farm, with the same load.

The Load Testing Kit is a command-line tool that will use information from a Office SharePoint Server 2007 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 Office SharePoint Server 2007 farm.

To use the tool, you need to be a member of the Farm Administrators SharePoint group on both the Office SharePoint Server 2007 (original production) and SharePoint Server 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 Office SharePoint Server 2007 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 Office SharePoint Server 2007 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 Office SharePoint Server 2007 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 Office SharePoint Server 2007-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

Parameter name	Value	Required?	Description
			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*).

User Profile Replication Engine overview (SharePoint Server 2010)

Updated: July 22, 2010

This article contains information about the User Profile Replication Engine. The User Profile Replication Engine is an optional component of Microsoft SharePoint Server 2010 and is part of the SharePoint Administration Toolkit. The User Profile Replication Engine enables an administrator of a User Profile Service application to replicate user profiles and social data, such as social tags, notes, and ratings, between User Profile Service applications. This replication can be one-way or bidirectional.

In this article:

- Uses and benefits of the User Profile Replication Engine
- Types of replication
- Components and installation
- Configuring the User Profile Replication Engine

Components and installation

The User Profile Replication Engine is made up of two components:

- Windows service
- Windows PowerShell snap-ins

The User Profile Replication Engine can be installed on any computer that has access to the source User Profile service application and destination User Profile service application. However, we recommend that you install the User Profile Replication Engine on a computer that is part of the source farm or on a computer that is connected to the subnet of the source domain. The User Profile Replication Engine uses the SharePoint Server 2010 User Profile and User Profile Change Log to read and write data between user profile stores.

Prerequisites:

- The account that is used to run the User Profile Replication Engine must be a service application administrator for the source and destination User Profile Service applications and have read access to the source and destination farm.
- You must be a member of the Administrators group on the server on which you install the Replication Engine.
- If the source or target is running Microsoft Office SharePoint Server 2007, that source or target server must be updated with the June 2010 Cumulative Update (*http://go.microsoft.com/fwlink/?LinkId=197406*) or a subsequent cumulative update.

For information about how to install the User Profile Replication Engine tool, see Installing the SharePoint 2010 Administration Toolkit (SharePoint Server 2010).

Important:
Source and destination User Profile Service applications should be set up and configured correctly for your environment before you use the User Profile Replication Engine.

Uses and benefits of the User Profile Replication Engine

Geographically dispersed deployments isolate user profile data and social data in domains. As a result, personalization features, such as User Profiles, Audiences, and People Search, might return inaccurate results within a domain. These inaccurate results include, but are not limited to:

- Inaccurate and inconsistent user profile data (including properties, colleagues, links, and privacy data)
- Inaccurate and inconsistent social data (such as social tags, notes, and ratings)
- Inaccurate audience memberships
- An incomplete and inaccurate people search data corpus and experience

The User Profile Replication Engine solves this problem by replicating both user profile information and social data between two or more User Profile service applications. This maintains consistent user profile data and social data throughout the enterprise.
The User Profile Replication Engine accommodates the service application model. It can perform either a full or incremental replication of both user profile information and social data from a source User Profile Service application to one or more destination User Profile Service applications.

Types of replication

The following table describes the differences between full replication, incremental replication, and recovery, all of which can be run by using the User Profile Replication Engine. For performance purposes, you can specify the maximum number of replication threads allowed on a server that is running the User Profile Replication Engine.

Type	When to use
Full Replication	• When you want all user profile information and all social data replicated from an existing User Profile service application, such as with a new User Profile service application deployment. • Where user profile data or social data is lost or corrupted and a copy exists in another User Profile service application profile database or social database. • When incremental replication has stopped responding over time, full replication is used to update destination User Profile service application profile databases and social databases in order to catch up incremental replication.

Incremental Replication	After full replication is complete, start incremental replication within 14 days to make sure that individual changes are being detected and replicated.
Recovery	• To fully replicate a specific user or set of users whose information did not replicate correctly. For profiles that fail to replicate fully, the user name is logged in a .rcv file located in the log folder in the User Profile Replication installation directory. • To replicate user profile information and social data for a user or set of users by specifying account names. • To replicate user profile information and social data for a user or set of users outside a regularly scheduled replication.

Remarks

Incremental replication also uses the trusted My Site host locations list to determine the My Site host location for a user. This identifies the primary profile for a user. The User Profile service that hosts the personal site for a user is also considered to have the primary profile record for that user. Audiences are used to identify and group related users and associate those users who have particular My Site hosts. For additional information about trusted My Site host locations, see Add or delete a trusted My Site host location (*http://technet.microsoft.com/library/bf71f50d-c4f9-41d9-bca0-6b55b61983bb(Office.14).aspx*).

The incremental replication process depends on the trusted My Site host locations list to avoid cyclical replication. For example, if a user updates his or her **AboutMe** property in User Profile store A, the User Profile Replication Engine synchronizes that change to User Profile store B and the change log will capture that as a change. The instance of the User Profile Replication Engine running against User Profile Store B will attempt to replicate that same change back to the User Profile Store it came from (User Profile Store A) as something that changed since the last replication. However, before replicating it, the User Profile Replication Engine will check the trusted My Site hosts locations list to determine whether the user's profile is the primary profile in the User Profile Store B. If it is, then the User Profile Replication Engine will replicate the change.

There is an exception to the previous example. If feed property names are provided using the *FeedProperties* attribute, the User Profile Replication Engine will ignore the trusted My Site hosts locations list when replicating changes for those properties. Typically, you will want to mark a property as a feed when the data is to be replicated regardless of where the primary user profile is located. Typically this is done when you only have Business Data Connectivity service imports running on one User Profile service application for all users and only want to feed those properties to the other User Profile service applications. Another example is when you have the primary People Search experience on a site connected to User Profile service application-A, which is, the source User Profile service application, and want the Add to my colleagues link to work for the primary user profile that is in User Profile service application-B, which is, the destination User Profile service application.

The User Profile Replication Engine does not replicate data that comes from Active Directory Domain Services (AD DS) because it would automatically be updated from AD DS during profile synchronization.

Note:
To configure the User Profile Replication Engine and to perform any of the previous tasks, the account that is used must have Manage User Profile permission on the User Profile service application for the source and all destination farms.

Note:
The User Profile Replication Engine will not replicate distribution lists or security groups, but it will replicate site memberships (for example, My Sites).

Configuring the User Profile Replication Engine

You must use Windows PowerShell 2.0 to configure the User Profile Replication Engine. The following Windows PowerShell cmdlets are available:

- Get-SPProfilePropertyCollection (*http://technet.microsoft.com/library/4471ae54-d3b0-49ef-83aa-9fa251853eb6(Office.14).aspx*)
- Start-SPProfileServiceFullReplication (*http://technet.microsoft.com/library/2805aa14-039a-43fb-9265-9d5b0fa0c2af(Office.14).aspx*)
- Start-SPProfileServiceIncrementalReplication (*http://technet.microsoft.com/library/45adae7c-686c-4944-ad56-20dad20b4f08(Office.14).aspx*)
- Start-SPProfileServiceRecoveryReplication (*http://technet.microsoft.com/library/651e958d-ff81-4beb-b76b-976769deb78f(Office.14).aspx*)
- Stop-SPProfileServiceIncrementalReplication (*http://technet.microsoft.com/library/1ad28561-1af4-4984-b98f-d5746b564ce1(Office.14).aspx*)

Concepts

SharePoint 2010 Administration Toolkit (SharePoint Server 2010)

Other Resources

User Profile Service overview (SharePoint Server 2010)
(*http://technet.microsoft.com/library/8198232e-8d49-46fa-b9f0-17b1d5ee6b62(Office.14).aspx*)
User Profile Service cmdlets (SharePoint Server 2010)
(*http://technet.microsoft.com/library/419b63a1-a0fd-4421-b184-81040ebb0b8e(Office.14).aspx*)

Content Management Interoperability Services (CMIS) connector overview (SharePoint Server 2010)

Updated: January 20, 2011

This article describes the Content Management Interoperability Services (CMIS) connector for Microsoft SharePoint Server 2010, which enables SharePoint users to interact with content that is stored in any repository that has implemented the CMIS standard. The connector also makes SharePoint Server 2010 content available to any application that has implemented the CMIS standard. The CMIS connector is available as part of the SharePoint 2010 Administration Toolkit. For more information, see SharePoint 2010 Administration Toolkit (SharePoint Server 2010).

The CMIS connector for SharePoint Server 2010 includes two features:

- The Content Management Interoperability Services (CMIS) Consumer Web Part
- The Content Management Interoperability Services (CMIS) Producer

In this article:

- About the CMIS standard and specification
- About the CMIS Producer and CMIS Consumer Web Part
- Installing and configuring the CMIS connector
- Bindings and permissions
- Mapping the CMIS data model to SharePoint concepts

About the CMIS standard and specification

CMIS is a Web services standard that allows content-enabled applications to interact seamlessly with any application that has implemented it. By providing access to multiple repositories with the CMIS Producer and consuming and rendering the data the CMIS Consumer Web Part, SharePoint Server 2010 becomes a CMIS-compliant system that interoperates with any platform that has implemented the CMIS standard.

The CMIS interface can be layered on top of an existing Content Management System (CMS) and its programming interfaces. It defines a universal, generic set of capabilities provided by a CMS and a set of services designed to work with those capabilities. The standard is not intended to prescribe how specific features should be implemented within those CMS, and is not intended to exhaustively expose all of the system's capabilities through the CMIS interfaces. For more information, see the Content Management Interoperability Services (CMIS) Version 1.0 specification (*http://go.microsoft.com/fwlink/?LinkId=199562*).

About the CMIS Producer and CMIS Consumer Web Part

The CMIS connector in the Toolkit is made up of two components:

- The Content Management Interoperability Services (CMIS) Consumer Web Part, which can be added to any SharePoint page. This Web Part displays and lets users interact with the contents of any CMIS-compliant repository.
- The Content Management Interoperability Services (CMIS) Producer, which allows applications to interact with SharePoint lists and document libraries programmatically by using the interfaces that are defined in the CMIS standard.

When these components are installed on SharePoint Server 2010, the server supports CMIS with *connectors* that connect to CMIS Web services and display list views of data from selected CMIS-compliant data sources, or *repositories*, to authenticated users.
The CMIS specification describes data model, services, Restful AtomPub binding, extensions, collections, feeds, resources, and Web services binding details. A data source is CMIS-compliant if it adheres to the CMIS specification. The CMIS components in the Toolkit comply with the CMIS specification.

Note:
Configuring the CMIS Producer and CMIS Consumer Web Part requires an understanding of expected address formats, authentication options, and terminology defined in the CMIS spec. For additional information about details not covered in this article, see the CMIS specification.

Installing and configuring the CMIS connector

The CMIS producer obtains the same results from SOAP and REST Web services. The CMIS Web service exposes SharePoint lists as CMIS repositories. When a request is processed, the CMIS Producer loads a CMIS repository object that holds the basic list information. The Producer returns data in the form of a CMIS response structure, and if needed, it also returns data in the body of the response.
The CMIS Consumer Web Part connects to the CMIS producer and gets repository information based on address and authentication information entered in its **Connection Options** section.

Installing the CMIS connector

The CMIS connector is installed with the SharePoint 2010 Administration Toolkit. To learn how to install the toolkit, see Installing the SharePoint 2010 Administration Toolkit (SharePoint Server 2010). When you install the Toolkit, the CMIS Producer and CMIS Consumer Web Part are installed automatically.

Configuring the CMIS connector

After the installation is complete, activate and configure the CMIS Producer and the CMIS Consumer Web Part, as follows.

To activate and deploy the CMIS connector features

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 to add the solution to the farm solution gallery:
   ```
   Add-SPSolution –LiteralPath 'C:\Program Files\Microsoft\SharePoint 2010 Administration
   Tookit\Content Management Interoperability Services (CMIS) Connectors\spcmis.wsp'
   ```
6. To deploy the solution, from the SharePoint Server 2010 Central Administration Web site, click **System Settings** and then click **Manage Farm Solutions**.

7. Click spscmis.wsp, choose the appropriate deployment settings, and then click **Deploy Solutions**.
   Note:
   When deployment is complete, Solution Properties should show that the solution was successfully deployed to all target sites.
   Important:
   When selecting solution details, remember which site you designate as the producer. In order to avoid an error later that states that the solution cannot be activated, open IIS Manager and verify that the Web application that will host the producer has only one header entry in the **Bindings** section.
8. On the **Site Actions** menu of the site that contains the content to be consumed, click **Site Settings**, choose **Manage site collection features**, and click **Activate** to activate the CMIS Producer feature.
9. On the **Site Actions** menu of the site where the CMIS Consumer Web Part will be added, click **Site Settings**, choose **Manage site collection features**, and click **Activate** to activate the CMIS Consumer Web Part feature.

To add the CMIS Consumer Web Part to a page in the consumer site collection

1. Change the page to **Edit Mode**, click **Insert** on the ribbon, and select the **CMIS Consumer Web Part**.
2. Edit the **Appearance**, **Layout**, and **Advanced** properties.
3. Edit the **Connection Options**.
4. Type the appropriate WSDL address in the **Specify WSDL Address** field, as shown in the following table. The CMIS connector only supports the SOAP WSDL.

Note:
If you are using a third-party CMIS connector, you can connect it to the REST Atom Service binding if you know the address of the producer site, the GUID for the list or library, and the CMIS command that you want to use to interact with the REST ATOM service. For more information, see the CMIS specification.

Protocol	URL format	Description
SOAP WSDL	http://*webURL*/_vti_bin/CMISSoapwsdl.aspx	*webURL* represents the URL that locates the **SPList** on the producer site.
REST Atom Service	http://*web*/_vti_bin/cmis/rest/*[repositoryid]*?*command*	*web* represents the producer site. *[repository id]* is the list or library GUID, and *command* is a command that exists in the CMIS specification (for example, **getRepositoryInfo**).

5. Select the **WS-Security Required** check box, and click **Basic** or **Digest**, depending on the type of CMIS authentication that the CMIS repository is set up to use. For more information, see the "Bindings and permissions" section later in the article.
6. Click **Get Repository list** to query the CMIS producer and return a list of available CMIS-compliant repositories.

Note:
If an error appears after you attempt to sign on to the repository (such as an "Unable to obtain master key" error), you must configure the secure store. For information, see Configure the Secure Store Service (SharePoint Server 2010) (*http://technet.microsoft.com/library/29c0bc76-d835-401b-a2fb-abb069e84125(Office.14).aspx*).

7. Select the repository from the **Select Repository** list that contains the data to display in the CMIS Consumer Web Part.
8. Click **OK** to apply settings and save changes.

Bindings and permissions

The CMIS standard defines a domain model, Web services, and Restful AtomPub bindings that can be used by applications to work with one or more content management repositories. The SOAP and AtomPub bindings defined in the CMIS specification are functionally equivalent and consistent—each protocol only defines the syntax for how methods are invoked and how responses are formatted. All of the same CMIS functionality is exposed regardless of which protocol is used.

Note:
The CMIS Producer uses an ASPX page to generate WSDL, not the standard built-in SharePoint 2010 WSDL redirection logic. Many producer endpoints are defined in the Web.config file, which are used to determine the correct endpoint based on the authorization settings of the Web application.

The CMIS standard has two concepts of permissions, as follows:

- Basic permissions include read, write, and all. A user with Read permissions can only view data from a repository. A user with Write permissions can contribute to a repository, and a user with All permissions has full control.
- Digest permissions are those that are defined by and expressed by a repository. These permissions do not have an explicitly defined meaning in the CMIS specification. They can be looked up at runtime using CMIS interfaces.

The CMIS specification maps allowable actions to the access control level (ACL) permissions defined for a repository. A client application can discover how the permissions that are exposed by the repository affect what actions a user can perform by way of CMIS. Other factors can affect whether a user can perform an action. For example, to check out an object from the repository, a user may need both the appropriate permission and the item must not already be checked out.

Mapping the CMIS data model to SharePoint concepts

The CMIS standard specification uses specific terminology that has equivalents inSharePoint Server 2010. The following table defines key CMIS concepts and maps them to their SharePoint equivalents.

Concept in CMIS specification	Definition	SharePoint equivalent

Concept in CMIS specification	Definition	SharePoint equivalent
Repository	The repository is the conceptual root of the CMIS server instance, and also the root server of CMIS content. All of the other concepts in CMIS are scoped locally within a repository instance.	The **SPList** (T:Microsoft.SharePoint.SPList) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.splist.aspx*) and **SPDocumentLibrary** (T:Microsoft.SharePoint.SPDocumentLibrary) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.SPDocumentLibrary.aspx*) objects
Object type	Definition of the object types allowed or in use in the repository.	The **SPContentType** (T:Microsoft.SharePoint.SPContentType) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.SPContentType.aspx*) object
Document object	The object in a CMIS repository whose object type is a descendant of the Folder base object type. The Folder object can contain Folders.	The **SPFolder** (T:Microsoft.SharePoint.SPFolder) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.SPFolder.aspx*) object
Version series	The collection of objects in the version history of a document object.	The **SPListItem** (T:Microsoft.SharePoint.SPListItem) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.SPListItem.aspx*) and **SPListItemVersion** (T:Microsoft.SharePoint.SPListItemVersion) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.SPListItemVersion.aspx*) objects **Note:** **SPListItem** covers both documents in a document library or list items in a list.
Query	A query supplied by	The **SPQuery** (T:Microsoft.SharePoint.SPQuery) (*http://msdn.microsoft.com/en-*

Concept in CMIS specification	Definition	SharePoint equivalent
	the CMIS consumer by way of the CMIS SQL query grammar that is used to get a collection of results for objects in the repository that match the criteria specified in the query.	*us/library/microsoft.sharepoint.SPQuery.aspx*) object
Change log	A collection of change event entries that record changes made to content in a repository, arranged in ascending order based on when the event occurred.	The **SPChangeCollection** (T:Microsoft.SharePoint.SPChangeCollection) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.SPChangeCollection.aspx*) object
Allowable actions	An enumeration of Booleans representing the set of actions that the current user can perform against a particular object at a point in time. Whether an action is allowed is determined by combining the	Not supported

Concept in CMIS specification	Definition	SharePoint equivalent
	current user's permissions and the current state of the object.	
Access Control Entry (ACE)/Access Control Log (ACL)	An Access Control Entry lists a set of permissions that a principal, such as a user or group, has an on an object.	Not supported
Content stream	See Section 3.1.7 of the CMIS specification.	The **SPFile** (T:Microsoft.SharePoint.SPFile) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.SPFile.aspx*) object that is associated with an **SPListItem** (T:Microsoft.SharePoint.SPListItem) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.SPListItem.aspx*) object
Path	The URL property (Web-relative URL) of the SPFolder object.	The **SPFolder** object (T:Microsoft.SharePoint.SPFolder) (*http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.SPLFolder.aspx*)
Relationship	Not applicable.	Not supported
Rendition	Not applicable.	Not supported

Other Resources

HTTP Extensions for Distributed Authoring (WebDAV) (*http://www.ietf.org/rfc/rfc2518.txt*)
Business Data Connectivity Service Authentication (*http://msdn.microsoft.com/en-us/library/ms566523.aspx*)
Business Data Connectivity Service Authorization (*http://msdn.microsoft.com/en-us/library/ms497953.aspx*)

SharePoint Diagnostic Studio 2010 (SPDiag 3.0) (SharePoint Server 2010)

Published: April 28, 2011

Microsoft SharePoint Diagnostic Studio 2010 (SPDiag version 3.0) was created to simplify and standardize troubleshooting of Microsoft SharePoint 2010 Products, and to provide a unified view of collected data. Administrators of SharePoint 2010 Products can use SPDiag 3.0 to gather relevant information from a farm, display the results in a meaningful way, identify performance issues, and share or export the collected data and reports for analysis by Microsoft support personnel.

The SharePoint 2010 Products platform is highly complex and can be used for a wide variety of uses. Deploying, managing, and troubleshooting SharePoint 2010 Products requires extensive knowledge spanning multiple technology areas, including security, networking, Web technologies such as ASPX, and Microsoft SQL Server.

Traditionally, troubleshooting SharePoint 2010 Products involves manually collecting a wide array of data from servers in the affected farm, and then manually analyzing the data to determine the source of the problem. This process can be complex and time-consuming, and data collection itself can place a significant load on the servers.

SPDiag greatly simplifies the troubleshooting process by providing a single interface for data collection and presentation in a series of preconfigured reports that cover a wide range of data points commonly used to diagnose SharePoint performance and capacity-related issues. Although most common troubleshooting scenarios are addressed by SPDiag, some SharePoint issues might require analysis of additional data not collected by SPDiag.

In this article:

- What's new in SPDiag 3.0
- Installing and configuring SPDiag 3.0
- Using SPDiag 3.0

What's new in SPDiag 3.0

The SharePoint Diagnostic Studio 2010 (SPDiag version 3.0) contains several important updates and new features that increase its effectiveness as a troubleshooting tool. SPDiag 3.0 is a new version and might not include some functionality present in previous versions of SPDiag. The following is a list of new features and changes in SPDiag 3.0:

- **Preconfigured reports** SPDiag provides a selection of preconfigured reports that aggregates data from the SharePoint farm present useful views into common SharePoint troubleshooting scenarios. For more information, see Using preconfigured reports later in this article.
- **Snapshots** You can take snapshots of your farm that aggregate report images, farm topology information, Unified Logging Service (ULS) logs, and usage database data. This makes it easy to consolidate key troubleshooting information about a SharePoint farm and share it with other users or preserve it for comparison and trend analysis.
- **Improved integration with SharePoint Server** Enhanced data collection from more sources.

Installing and configuring SPDiag 3.0

SPDiag is included in the Microsoft SharePoint 2010 Administration Toolkit v2. To download the toolkit, see SharePoint 2010 Administration Toolkit (SharePoint Server 2010).

You can install SPDiag on a farm server, or on a remote computer that is not part of the farm. You must be logged in with a user account that has farm administration privileges to create a new project or access an existing project.

To install SPDiag 3.0, select **SharePoint Diagnostic Studio** from the SharePoint 2010 Administration Toolkit v2 component installation menu. Then, use the following procedure to configure the client computer and the SharePoint Server farm for use with SPDiag.

To configure the client computer and the SharePoint Server farm for use with SPDiag

1. On the computer on which you are installing SPDiag, install the .NET Framework 3.5.
2. On the computer on which you are installing SPDiag, install the Microsoft Chart Controls for the Microsoft .NET Framework 3.5.
3. If you are installing SPDiag on a remote client computer, you must enable Windows PowerShell remoting on the *farm server* to which you will connect SPDiag. In Windows PowerShell on the target server, run the following cmdlets, and enter **Yes** when prompted:
   a) Enable-PSRemoting
   b) Enable-WSManCredSSP server
4. If you are installing SPDiag on a remote client computer, enable Windows PowerShell remoting on the *client computer*. In Windows PowerShell on the client computer, run the following cmdlets, and enter **Yes** when prompted:
   a) Enable-PSRemoting
   b) Enable-WSManCredSSP client
5. Make sure that **Usage and Health Data Collection** has been configured on the target farm. The SPDiag diagnostic provider collects data from the usage database. If the usage database has not been provisioned prior to using SPDiag, you will see the error “Usage Database is not provisioned. Please provision it first.”

For information about how to configure usage and health data collection, see Configure usage and health data collection (SharePoint Server 2010) (*http://technet.microsoft.com/library/33ed78c8-25fc-48ea-b0c1-50b540213cff(Office.14).aspx*).

Using SPDiag 3.0

SPDiag 3.0 is a diagnostic tool that is used to collect, filter, and display data from a SharePoint farm for troubleshooting. SPDiag is a read-only tool, and cannot make any changes to a farm. You can use SPDiag to help you discover problems yourself, or as a way to collect the data needed by support personnel to help troubleshoot a farm.

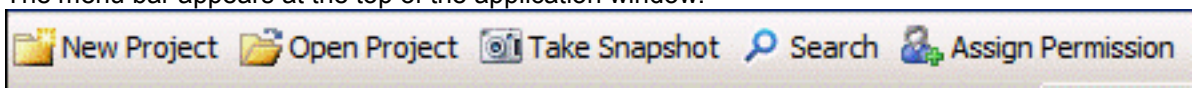
The information in this section will help you understand how to create and import projects, filter and collect data, generate graphs and reports, and export data to a file.

SPDiag collects and aggregates data from ULS logs, Windows Event logs, performance counters, SharePoint logs, and SQL databases and then displays that data in various preconfigured reports that were designed to expose specific capacity and performance characteristics and trends.

The SPDiag application is divided into four main sections: menu bar, Guide pane, Reports pane, and Report Display pane.

Menu bar

The menu bar appears at the top of the application window.



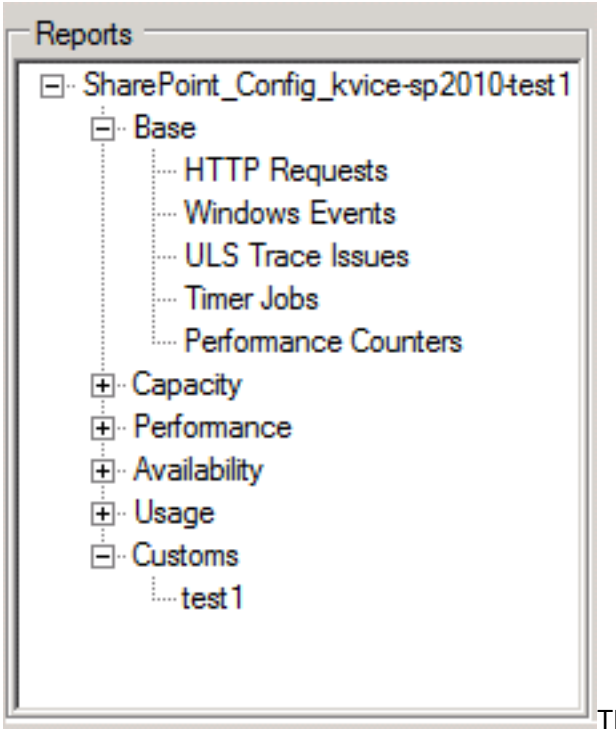
- **New Project** Creates a new SPDiag project.
- **Open Project** Opens an existing SPDiag project from a TTFARM file.
- **Take Snapshot** Creates a snapshot of the farm that consists of PNG images of all open reports, a text document that contains information about the farm topology, and log files from the snapshot process. There are two kinds of snapshot available: Light and Full.
  - **Light Snapshot** Exports the currently open reports and farm topology information
  - **Full Snapshot** All Light Snapshot data, and data from the ULS logs and SharePoint usage database for a specified time range. When Full Snapshot is selected, you can use the Start Time and End Time fields to specify the time range for ULS log and usage database data collection.
- **Search** If you are looking for a specific request and you know the correlation ID or user account from which the request originated, click this button to open the **Search** dialog box. In the **Search** dialog box, you can enter the correlation ID, user account, and estimated date and time of the request, which begins the search from that point.
- **Assign Permission** You can provision SharePoint farm permissions to a specific user account or group to enable access to SPDiag.

Guide pane

The Guide pane appears at the middle left of the application window. It displays information about each report, including a description of the displayed data, instructions about how to manipulate and filter the data, and troubleshooting guidance specific to the report when it is available. Some reports include guidance on how to identify problems and offer suggestions for resolving them.

Reports pane

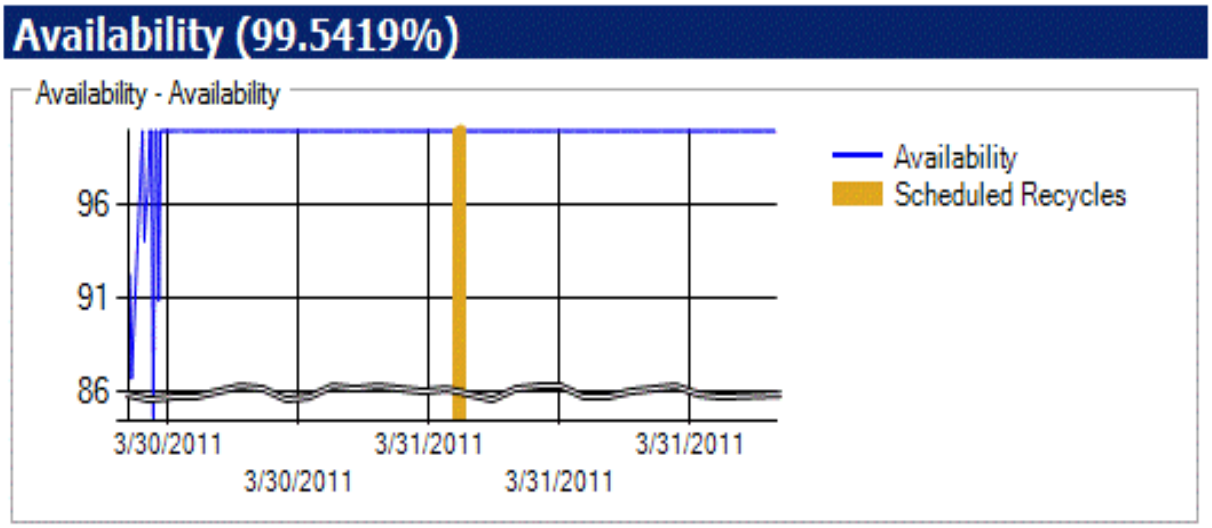
The Reports pane appears at the lower-left corner of the application window.

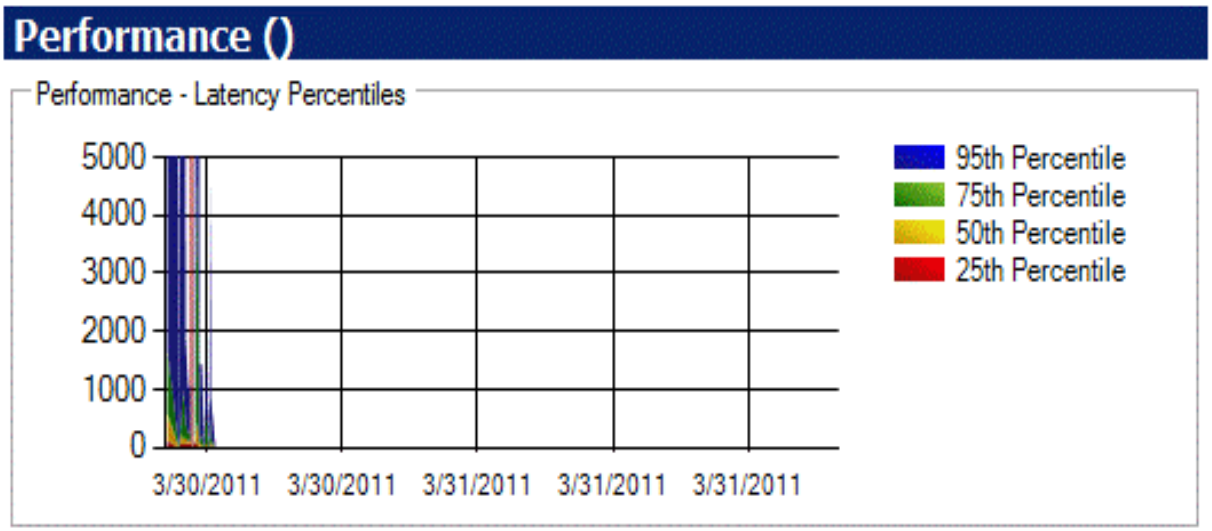


The Reports pane is an expandable menu that contains all of the reports that you can view. Click each node to expand the section and show the contained reports, and double-click on a report to open it in the Report Display pane. When you use the **Save** button on the report toolbar to save a report, it will appear in the Customs node at the bottom of the Reports pane.
For more information and a full list of available reports, see Using preconfigured reports later in this article.

Report Display pane

The Report Display pane consists of the main part of the application window. When a project is created or opened, the overview report is displayed.





Two primary reports are displayed as graphs in the overview report: Availability and Latency Percentiles.

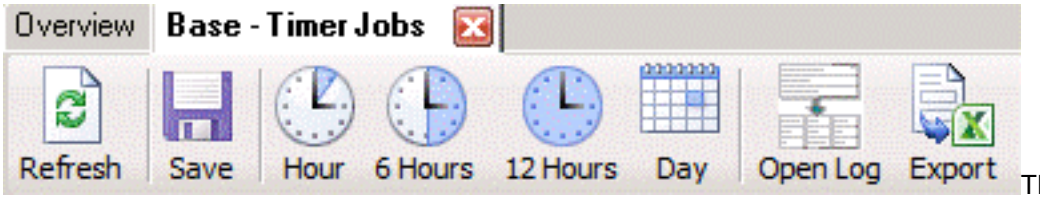
- **Availability report** Charts the availability of the HTTP Web Service.
- **Latency Percentiles report** Indicates how much time it takes to render the fastest and most common requests.

As with all graphs in SPDiag, you can zoom into a specific time range by selecting the area on the graph by using the mouse. Doing this in the overview report opens the selected report in a new tab in the main SPDiag window that contains results from the selected area.

When you open a report by double-clicking it in the Reports pane, SPDiag collects the required data from the farm servers and displays it in a new tab in the main window. This display consists of three components: report toolbar, Filter pane, Data Display pane.

Report toolbar

The report toolbar appears at the top of each open report tab.

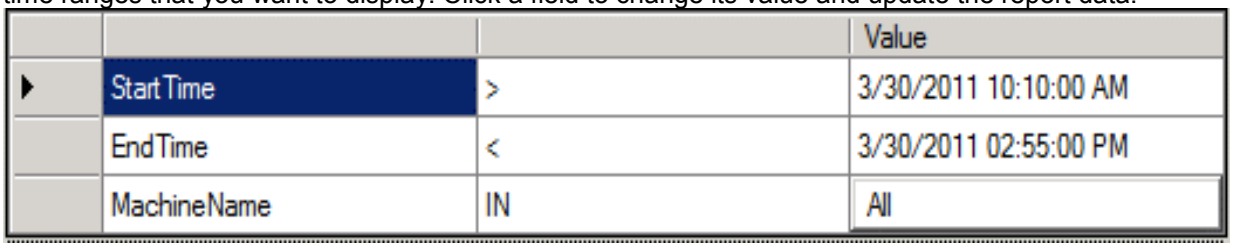


The toolbar provides tools for manipulating report data, including tools to refresh, save, export, and change the displayed time scale of reports.

- **Refresh** Requests fresh data from the farm servers.
- **Save** Saves the current report to an XML file that has an SPR extension. Files are saved to the C:\Users\Administrator\Documents\SharePoint Diagnostic Studio\Custom Reports folder on the SPDiag client computer. These files can be opened in any XML or text editor.
- **Hour** Calibrates the data display to span the last hour. This button and the other three time calibration buttons automatically set the end time for the range to the current time.
- **6 Hours** Calibrates the data display to span the last six hours.
- **12 hours** Calibrates the data display to span the last 12 hours.
- **Day** Calibrates the data display to span the last 24-hour period.
- **Open Log** If data from log files is included in a report, you can select the log from the Filter pane, and then click the **Open Log** button to display the contents of the raw log file.
- **Export** Exports the current report to a PNG image file in the C:\Users\Administrator\Documents\SharePoint Diagnostic Studio\Exported Reports\<date and time> folder on the SPDiag client computer. The name of the final folder is dynamically generated by the date and 24-hour time that the report was exported in the format year.month.day-hour.minute.second. For example, a report exported on March 31, 2011, at 6:11 PM and 22 seconds would be saved to a folder named 2011.3.31-18.11.22.

Filter pane

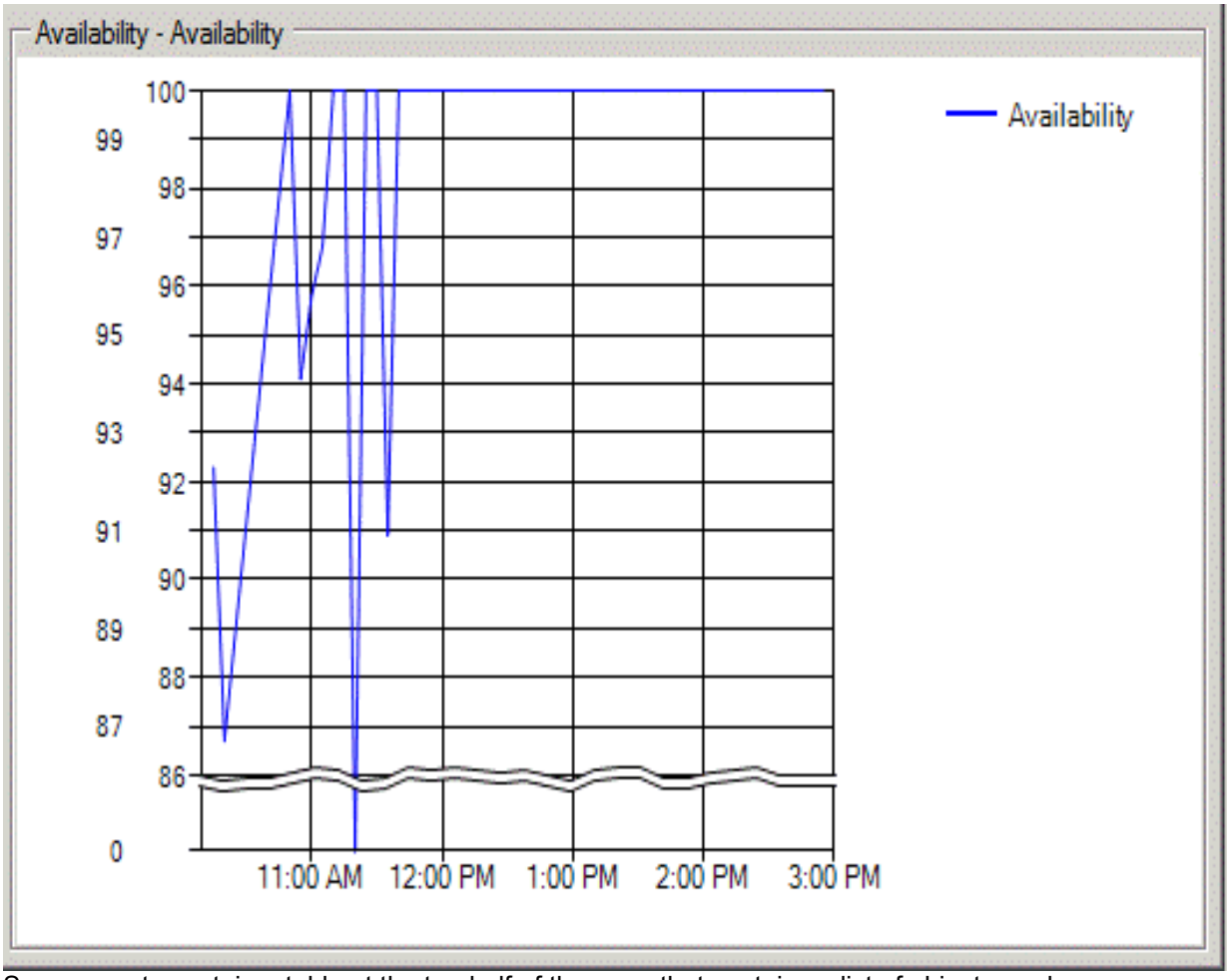
The Filter pane provides report-specific fields that enable you to filter report data and date and time ranges that you want to display. Click a field to change its value and update the report data.



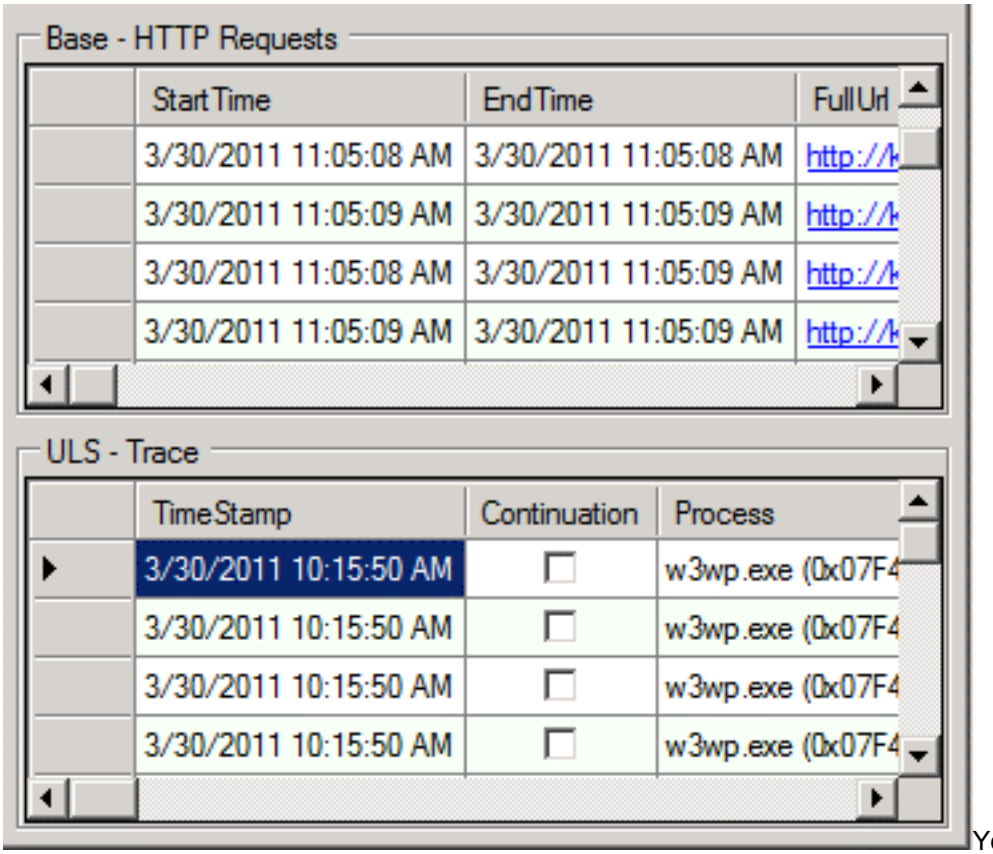
		Value
StartTime	>	3/30/2011 10:10:00 AM
EndTime	<	3/30/2011 02:55:00 PM
MachineName	IN	All

Data Display pane

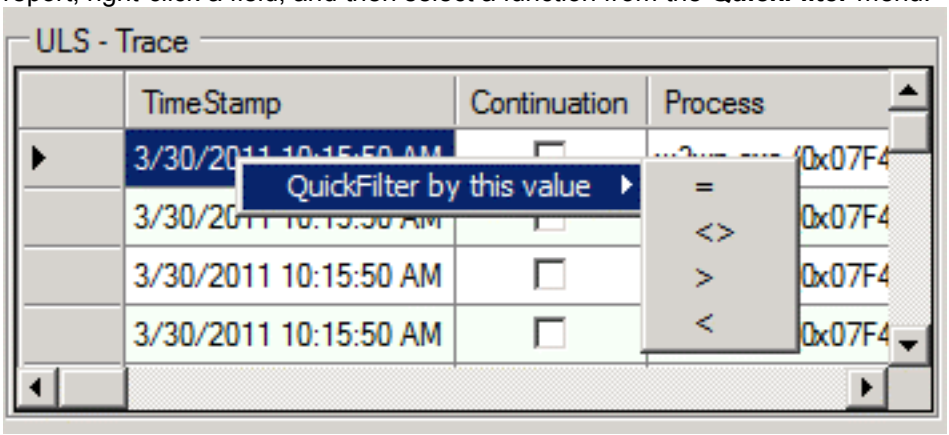
The Data Display pane shows graphs, charts, tables, and log file data for the report that is being displayed.



Some reports contain a table at the top half of the pane that contains a list of objects, and a separate pane at the bottom that shows details about objects that you select from the table. For example, in the Timer Jobs report, a list of timer jobs is displayed in the top half of the Data Display pane. Selecting a timer job from the list displays detailed ULS trace log information about that job in the lower half of the pane.

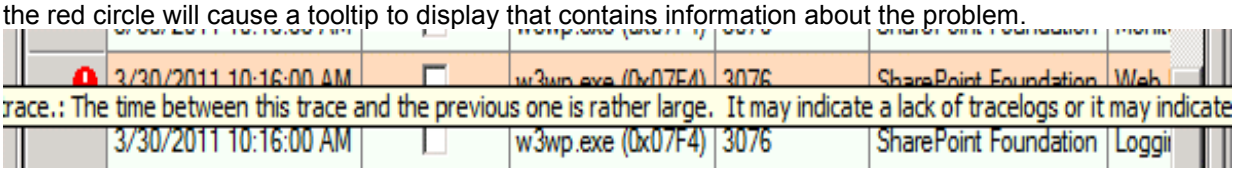


You can also right-click a field to filter the report on that value by using the QuickFilter feature. To update the report, right-click a field, and then select a function from the **QuickFilter** menu.



- **=** Filter by the exact value.
- **<>** Filter by all values within the selected range.
- **>** Filter by all values greater than the selected value.
- **<** Filter by all values smaller than the selected value.

When the data for a specific record in a report indicates that a problem exists, a red circle with an exclamation point will appear at the beginning of the record. Hovering the mouse pointer over the red circle will cause a tooltip to display that contains information about the problem.



When a report contains a graphical display element, such as a chart or graph, you can select areas of the graph by using the mouse to zoom in on a specific time range. To zoom out to the original time range, right-click anywhere on the graph.

Note:
Data collection can take a long time, especially when there is significant network latency between the SPDiag client computer and the farm servers, or during times when the farm is under heavy load. There is no way to cancel the process of collecting data and rendering the report after it has begun, and SPDiag will be unresponsive until this process is completed.

Using preconfigured reports

SPDiag provides various reports that present data from logs, SharePoint databases, and performance counters. Reports collect data from the SharePoint farm and display aggregated information that is focused on specific aspects of farm performance.
You can also begin your investigation by directly opening a report from the Reports pane displayed at the bottom of the guide window. These reports are described in the following paragraphs.

Base
The Base report group contains several reports that display information about key general performance indicators.

HTTP Requests
This report displays all HTTP requests across the farm. When you select a row from the top report, the full trace from the request is fetched and displayed in the bottom pane.
Right-click any cell to add a filter with the column name and value of your selection.
Alternatively, you can filter these results by using the filter list at the top of the report. When using the LIKE operator, '%' is treated as a wildcard character.
Click any column header to sort by that column. For example, to find the slowest requests, click the **Duration** column. Click the header again to reverse the results order.
Once you have customized the filter list, you can save the report so you do not have to generate it again. Saved reports can be found under the Customs node in the Reports pane at the lower-left side of the screen. The next time that you load the report, it will restore the saved sorts and filters, and apply them to the new data.
To save the current set of results to share or to view in a spreadsheet, click the **Export** button.

Windows Events
This report displays critical and SharePoint-related events from the Windows Event logs on all computers in the farm. Use this report to look for critical issues that occurred during the specified time frame.
Right-click any cell to add a filter with the column name and value of your selection.
Alternatively, you can filter these results by using the filter list at the top of the report. When using the LIKE operator, '%' is treated as a wildcard character.

Click any column header to sort by that column.
Once you have customized the filter list, you can save the report so you do not have to generate it again. Saved reports can be found under the Customs node in the Reports pane at the lower-left side of the screen. The next time that you load the report, it will restore the saved sorts and filters, and apply them to the new data.
To save the current set of results to share or to view in a spreadsheet, click the **Export** button.

ULS Trace Issues

This report displays problems detected in the Unified Logging Service (ULS) trace logs. High-level traces that occur at the time of an issue might provide clues as to the cause. When you select a row from the top report, the full trace from the request or timer job is fetched and displayed in the bottom pane.
Right-click any cell to add a filter with the column name and value of your selection. Alternatively, you can filter these results by using the filter list at the top of the report. When using the LIKE clause, '%' is treated as a wildcard character.
Click any column header to sort by that column. For example, to find the slowest requests, click the **Duration** column. Click the header again to sort in the other direction.
Once you have customized the filter list, you can save the report so you do not have to generate it again. Saved reports can be found under the Customs node in the Reports pane at the lower-left side of the screen. The next time that you load the report, it will restore the saved sorts and filters, and apply them to the new data.
To save the current set of results to share or to view in a spreadsheet, click the **Export** button.

Timer Jobs

This report displays all Timer Job executions. When you select a row from the top report, the full trace from the timer job is fetched and displayed in the bottom pane.
Right-click any cell to add a filter with the column name and value of your selection. Alternatively, you can filter these results by using the filter list at the top of the report. When using the LIKE clause, '%' is treated as a wildcard character.
Click any column header to sort by that column. For example, to find the slowest jobs, click the **Duration** column. Click the header again to sort in the other direction.
Once you have customized the filter list, you can save the report so you do not have to generate it again. Saved reports can be found under the Customs node in the Reports pane at the lower-left side of the screen. The next time that you load the report, it will restore the saved sorts and filters, and apply them to the new data.
To save the current set of results to share or to view in a spreadsheet, click the **Export** button.

Performance Counters

This report shows key performance counter data over time for counters that are collected in the Usage database.
Filter by a specific Category, Counter, Instance, or Machine by using the custom filter controls. Select a category of interest, and the additional three filter controls (Counter, Instance, Machine) will be dynamically populated with relevant results. Once filtering selections have been made, click **Refresh** to regenerate the report. Place the pointer over a series in the chart to determine which Category, Counter, Instance, or Machine is related to the value.
You can use the Add-SPDiagnosticsPerformanceCounter Windows PowerShell cmdlet to add other performance counters to servers in the SharePoint farm. Any new counters that you add will automatically be included in the SharePoint Diagnostic Studio dataset.

Capacity

The Capacity report group contains several reports that display information about farm capacity indicators.

SQL Server Query IO Over Time

This report shows expensive stored procedures input/output (I/O) over time.

The top graph shows the five most expensive queries or stored procedures over time based on the SQL Dynamic Management views.
The bottom table contains detailed information about the expensive queries, including total I/O for the time period selected, average I/O per call, execution count, and CPU cost.
Take notice of any spikes or grouping of spikes and the time when they occurred. Such spikes can indicate an expensive stored procedure call or a bad execution plan.
Look for queries that have high values in the **Execution Count** and **Total IO** columns paired with low values in the **Average IO** column. Such queries might be being called to many times.
Click the **Export** button to save the execution plan to a file from which it can be more easily read.

CPU

This report shows the processor usage, expressed in percentage of total processor capacity, consumed by each process on each farm server over time. The data that is used to populate this graph is from the **| Processor | % Processor Time | _Total performance** counter.

Note:
Data from performance counters is available only from the date and time that the SPDiag project was opened for the target farm.

Process Memory (MB)

This report shows the available physical memory, expressed in megabytes (MB) available, on each farm server over time. The data that is used to populate this graph is from the **| Process | Private Bytes | <process name>** performance counter.

Performance

The Performance report group contains several reports that display information about specific farm performance indicators related to latency and SQL Server.

SQL Read Intensive Traces

This report shows SQL Server queries that read more than 50,000 pages (1 page = 8 kilobytes). Queries that read a large volume of data can cause SQL Server to respond slowly by forcing useful data out of memory and causing other queries to perform expensive physical reads. This can affect end-user latency for user operations that query data residing on the same SQL Server.
If a correlation ID is present in the query text, you can use it to find the request or timer job that generated the query. Copy the correlation ID into the filter field of the **HTTP Requests** or Timer Jobs reports.

Latency Tier Breakdown

This report shows a moving average of server-side HTTP request page latency over time. The time that is spent rendering the request is broken down into the three tiers that a typical HTTP request passes through during processing.

- **SQL Server** If SQL Server queries take longer than 250ms, use the SQL Overview report to identify SQL Server bottlenecks.
- **Application Servers** If service calls take longer than 250ms, you can use the **Service Call Duration** column in the HTTP Requests report to find the requests most affected by service calls.
- **Web Server** If there does not appear to be a bottleneck in either the SQL Server or application server tier, and requests take longer than 250ms on the Web server, use the **Duration** column in the HTTP Requests report to see the slowest requests overall. You can examine the Latency All Requests report to see whether the issue is isolated to a single computer. Finally, you can examine the CPU report to determine whether one or more Web servers or application servers are exhibiting excessive processor usage.

Changed Objects
This report displays all object types that have changed over a specific period of time based on information in the change log. The change log is a history of changes that have occurred in a content database. It provides search crawlers and other features a means of querying for only those changes that have occurred since a previous crawl.
Data points are collected once every *k* minutes (where, by default, k is 5). This report displays the data aggregated across all content databases as a stacked bar graph. Each stack represents a different object type (see the corresponding legend).
You can filter these results by the database or the object type. For example, you can customize the report to show only changed objects made on a database named contentdb1, assuming that it is in the filter dropdown. Similarly, you can customize the report to show only data for the changes that have the object type List to see all list-level changes.
This data can contribute to an overall understanding of what kinds of changes are occurring around a specific timeframe. From this data, you can further examine the HTTP Requests report to determine what requests are causing these changes, or you can look at the Changed Objects Per Database report to view the same data by using a different pivot. Additionally, you can look at the Change Types report and the Change Types Per Database report to look further into the kinds of changes being made to the objects.
If you want to save the current set of results to share, click the **Export** button.
Changed Objects Per Database
This report displays all object types that have changed in specific content databases over a specific period of time based on information in the change log. The change log is a history of changes that have occurred in a content database. It provides search crawlers and other features a means of querying for only those changes that have occurred since a previous crawl.
Data points are collected once every *k* minutes (where, by default, k is 5). This report displays the data aggregated across all content databases as a stacked bar graph. Each stack represents a different object type (see the corresponding legend).
You can filter these results by the database or the object type. For instance, you can customize the report to show only changed objects made on a database named contentdb1, assuming that it is in the filter dropdown. Similarly, you can customize the report to show only data for the changes with object type 'List' to see all list-level changes.
This data can contribute to an overall understanding of what kinds of changes are occurring around a specific timeframe. From this data, you can further look at the HTTP Requests report to determine what requests are causing these changes, or you can look at the Changed Objects report to view the same data by using a different pivot. Additionally, you can look at the Change Types report and the Change Types Per Database report to look further into the kinds of changes being made to the objects.
If you want to save the current set of results to share, click the **Export** button.
Change Types
This report displays all object types that have been changed over a specific period of time based on information in the change log. The change log is a history of changes that have occurred in a content database. It provides search crawlers and other features a means of querying for only those changes that have occurred since a previous crawl.
Data points are collected once every *k* minutes (where, by default, k is 5). This report displays the data aggregated across all content databases as a stacked bar graph. Each stack represents a different object type (see the corresponding legend).
You can filter these results by the database or the object type. For example, you can customize the report to show only changed objects made on a database named contentdb1, assuming that it is in the filter dropdown. Similarly, you can customize the report to show only data for the changes that have change type Rename to see all rename-related changes.

This data can contribute to an overall understanding of what kinds of changes are occurring in a specific timeframe. From this data, you can further examine the HTTP Requests report to determine what requests are causing these changes, or you can look at the Change Types Per Database report to view the same data by using a different pivot. Additionally, you can look at the Changed Objects report and the Changed Objects Per Database report to look further into the kinds of objects that are being changed.
If you want to save the current set of results to share, click the **Export** button.

Change Types Per Database

This report displays all object types that have been changed over a specific period of time based on information in the ChangeLog. Data points are collected once every *k* minutes (where, by default, k is 5). This report displays the data aggregated across all databases as a stacked bar graph. Each stack represents a different object type (see the corresponding legend).
You can filter these results by the database or the change type. For example, you can customize the report to show only change types made on database contentdb1, assuming that it is in the filter drop-down list box. Similarly, you can customize the report to show only data for the changes that have the change type Rename to see all rename-related changes.
This data is valuable to obtain an overall understanding of what kinds of changes are occurring around a specific timeframe, and the quantity of changes across each database. From this data, you can further look at the HTTP Requests report to determine what requests are causing these changes, or you can look at the Change Types report to view the same data by using a different pivot. Additionally, you can look at the Changed Objects report and the Changed Objects Per Database report to look further into the kinds of objects that are being changed.
If you want to save the current set of results to share, click the **Export** button.

Latency All Requests

This report plots the duration of all requests (up to a limit of 50,000).
Use this report to spot abnormal patterns in usage. For example, a poorly performing site might consistently take 5 seconds to load, which would present as a horizontal band at the 5-second mark. For a more detailed view, you can zoom in to a smaller area, go to the HTTP Requests report and look for requests that take around 5 seconds.
Latency spikes will appear as columns. If the spikes have a regular period, you can look at the Timer Jobs report to see whether a particular job runs during the same time.

Latency Percentiles

This report shows several key percentile thresholds over time to give you an idea of how many requests are affected by a particular latency spike.
For example, if the fastest 25 percent of all requests take 1 second or more, it is likely that an outage in some shared resource (such as the network or SQL Server computer) is affecting all requests. Use the Latency Tier Breakdown report to look for issues in shared resources.
On the other hand, if 75 percent of all requests complete quickly, but the 95th percentile is very high, you might have to look for a root cause that affects a smaller number of requests, such as blocking in a single database, or custom code that is only used by a subset of sites.
To see logs for the slowest requests, you can view the HTTP Requests report and sort the list by clicking the header of the **Duration** column.
You can also use the usage reports, such as the Requests Per User report and the Application Workload report, to look for users or applications that place an unexpected load on the network.

SQL Deadlocks

This report lists SQL Server deadlocks over time. SQL Server uses deadlock detection to prevent the server from hanging when two incompatible queries are executed. To resolve a deadlock, one or more of the queries are canceled. SharePoint Server can recover from some deadlocks and retry the affected queries. However, deadlocks can sometimes cause certain requests to fail.

SQL Blocking
This report lists SQL queries that have blocked other SQL queries.
Blocking can stop all activity on the farm. When blocked requests cannot be processed by the affected database, all available Web server memory will eventually be consumed, which will cause the affected servers to stop responding or crash.
This report displays the request or timer job responsible for generating the blocking query, if it is possible, and any associated logs. These can be useful if the block is caused by a specific end-user transaction. In such cases, restructuring a list or redesigning an application that uses custom queries might be indicated.
Some blocking cannot be avoided. For example, nightly database maintenance tasks necessarily lock large parts of a database.
Availability
The Availability report group contains several reports that display information about farm availability trends and issues.
Availability
This report charts the availability of the HTTP Web Service. Drops in availability indicate periods when users might have been unable to access their SharePoint sites.
This report calculates availability dividing the number of successful Web requests by the total number of requests sent to the server. An attempt is made to remove requests coming from automated agents, such as a search crawler, from this calculation. However, some unknown automated agents might not be excluded.
Zoom in to a period of low availability by selecting it with your mouse. Subsequent reports used in this investigation will load faster if you select a smaller time range.
Once you have narrowed the time range, you can use the Failed User Requests report to examine details about requests that failed during the selected time period.
Crashes reduce availability by exiting the process without allowing requests to be completed. Because the process does not have an opportunity to write logs during a crash, requests that were running at the time of the crash will not appear in these reports, and their effect on availability will not be displayed in the graph. Regardless, crashes should always be investigated.
Scheduled Worker Process Recycles rarely reduce availability. The server will attempt to gracefully allow requests from one process to complete while at the same time starting another process to handle new requests. Frequent, unscheduled recycles during periods of higher than average traffic can cause some requests to fail if the server cannot respond to the increased demands of running multiple processes in parallel.
SQL Overview report
This report displays information that can help you understand the overall health of the SQL Server computers in your farm. The report focuses on the following three areas:
SQL Server Locking/Blocking
SQL Server query blocking can increase some SQL Server query duration values, and might contribute to availability issues and increased latency.

- **Average Lock Wait Time** Locks are held on SQL Server resources, such as rows read or modified during a transaction, to prevent concurrent use of resources by different transactions. For example, an update will hold an XLOCK and it will block a shared read lock. A high lock wait time means there is a blocking issue in the SQL Server tier, and you should pay attention to slow updating threads, as they will block reads.
- **Average Latch Wait Time** A latch is primarily used to synchronize database pages. Each latch is associated with a single allocation unit. A latch wait occurs when a latch request cannot be granted immediately because the latch is held by another thread in a conflicting mode. Unlike locks, a latch is released immediately after the operation, even in write

operations. High latch wait time might mean that it is taking too long to load a specific page into memory.

When Lock Wait Time is high, examine the SQL Blocking report to identify the queries holding onto the locks.

You can examine the SQL Deadlocks report to identify queries that might have generated failed requests.

SQL Server Disk IO

A common SQL Server performance issue is an I/O bottleneck. When SQL Server does not have sufficient I/O bandwith to process incoming queries, performance across all requests will decrease, and performance across all farm Web servers will be decreased.

- **Average Disk Queue Length** This metric is for overall Disk I/O. Higher values translate to increased overall I/O pressure, and if you have more than 10, it is possible there is an I/O bottleneck.
- **Average Logical Reads / s** This metric is for the Read Disk I/O. Higher values translate to increased Read I/O pressure.
- **Average Logical Writes / s** This metric is for the Write Disk I/O. Higher values translate to increased Write I/O pressure.

When there is an I/O bottleneck, examine the SQL Read-Intensive Traces report to see what specific queries are consuming the most resources.

SQL Server CPU

When SQL Server computer processor usage is excessively high, SQL queries are queued, and Web server performance is decreased. Processor and I/O performance is related. Therefore, when SQL Server processor usage is high, I/O is usually high also. An average processor usage of 80 percent is considered a bottleneck.

When there is a CPU bottleneck, examine the SQL Read-Intensive Traces report, and then click the **CPU** column to sort by the most expensive queries.

Worker Process Recycles

Recycles do not usually affect availability. Internet Information Services (IIS) 7.0 will create a new process, which allows existing requests to complete, and then shuts down the recycled process cleanly. However, the first browse to a new process can be delayed while the process is initialized.

By default, SharePoint Server schedules worker process recycle jobs to take place overnight. Frequent recycles during working hours can increase the latency of end-user requests. Check to see whether Web.config settings might have been changed, or if the recycle settings have been modified in IIS.

Failed User Requests

These user requests failed, or they were so slow that users might have assumed they failed. Select a failed request to fetch its trace logs. Look for traces that mention a failure in some component of the system. If the cause is not apparent, look at the Windows Events report for signs of a system failure on the server or in IIS.

If a request failed because it was too slow, look for a gap in the log, which might be highlighted. If the lines before the gap indicate that the delay occurred in SQL Server, this request was most likely a lock victim. Look at the SQL Blocking report to find the blocking query that is the root cause of the issue.

Some requests, such as downloads of large files, can be expected to be slow.

Crashes

This report displays all of the IIS worker process crashes that occurred in the specified time range. After a row is selected in the top report, the last few seconds of traces from the crashing process are displayed in the bottom panel. These traces might indicate why the crash occurred.

Crashes can significantly affect availability. The availability report might underestimate the effect of crashes because requests that are being executed at the time of a crash are not recorded. Even when a crash does not noticeably affect availability, it could lead to data loss or other problems and should be investigated.

Usage

The Usage report group contains several reports that display information about farm usage trends and issues.

Requests Per URL

This report displays the most frequently requested URLs. You can use this report to identify pages that are often accessed and therefore might be high-priority candidates for optimization.

Requests Per User

This report displays the percentage of requests made by the most common user accounts. Some system accounts, such as the search crawler service account, might be expected to generate many requests. At certain times, individual users might also perform operations that create an unexpected peak in resource usage.

Application Workload

This report displays the time that is spent serving requests from various client applications in a given time range. The report provides an estimate of which resources are being consumed by client requests.

- High total durations indicate a need for additional memory on the Web servers.
- High SQL Server process durations imply high SQL I/O or processor usage, or that requests from client applications might be blocked by other queries.
- High Web server durations might indicate high processor usage on the farm Web servers.

Requests Per Site

This report displays the percentage of requests made to each site in the farm.

Concepts

SharePoint 2010 Administration Toolkit (SharePoint Server 2010)

Conformance statement A-level (SharePoint Server 2010)

Published: July 22, 2010
Conformance statement for Microsoft SharePoint Server 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 Server 2010 and Administration and Configuration features of SharePoint Server 2010. For other product features, see Conformance statement AA-level (SharePoint Server 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 in a form that users can use, preferably machine-readable metadata.	Conforms to 1.4.9 Images of Text (No Exception) - AAA. Conforms to 2.1.3 Keyboard (No Exception) - 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 Server 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 Server 2010)

Published: July 22, 2010
Conformance statement for Microsoft SharePoint Server 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 Server 2010 and Web application features of SharePoint Server 2010 except where limited by Conformance statement A-level (SharePoint Server 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 in a form that users can use, preferably machine-readable metadata.	Conforms to 1.4.9 Images of Text (No Exception) - AAA. Conforms to 2.1.3 Keyboard (No Exception) - 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 Server 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 Server 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 Server 2010) (*http://technet.microsoft.com/library/a6d383c0-3817-4acd-afa9-ad7a9b7e6b5a(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* parameter to specify **overwrite**. **Note:** Outgoing e-mail settings are restored only when content and

Setting or feature	Description
	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 Server 2010) (*http://technet.microsoft.com/library/d849b7df-b26d-45f6-a74f-6641f18788cf(Office.14).aspx*)
Change passwords used for administration accounts (SharePoint Server 2010) (*http://technet.microsoft.com/library/4f52688f-7c27-41b7-8e28-c532d0e93e4d(Office.14).aspx*)
Configure outgoing e-mail (SharePoint Server 2010) (*http://technet.microsoft.com/library/f3ccc8bd-922e-49f6-9929-b5b8a6982d76(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 Server 2010) (-*http://technet.microsoft.com/library/c2eda191-1814-423b-882f-1fdafe9df6c9(Office.14).aspx*)
Define managed paths (SharePoint Server 2010) (*http://technet.microsoft.com/library/0f95a1e6-7044-487e-8681-b1d717caabb3(Office.14).aspx*)

Configure load balancing for sandboxed solutions (SharePoint Server 2010)
(*http://technet.microsoft.com/library/2c0e2a06-b62e-4462-819d-d2de56ba34d8(Office.14).aspx*)
Block or unblock a sandboxed solution (SharePoint Server 2010)
(*http://technet.microsoft.com/library/19eeadde-2e7c-419d-9d60-b3a0ea706364(Office.14).aspx*)
Configure diagnostic logging (SharePoint Server 2010)
(*http://technet.microsoft.com/library/faab1eb4-5848-4970-b13f-ba6df14272fe(Office.14).aspx*)

Peoplepicker-peopleeditoronlyresolvewithinsitecollection: Stsadm property (SharePoint Server 2010)

Published: February 3, 2011

Checks the user against the existing site collection users.

Note:
This operation was added in Microsoft SharePoint Server 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.
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

Other Resources

Peoplepicker-onlysearchwithinsitecollection: Stsadm property (Office SharePoint Server) (*http://technet.microsoft.com/en-us/library/cc261988(office.12).aspx*)

Default user profile properties (SharePoint Server 2010)

Published: April 28, 2011

This article lists the user profile properties that SharePoint Server 2010 provides by default. The following table lists the default user profile properties.

Use profile property	Display name	User profile service data type
AboutMe	About me	HTML
AccountName	Account name	Person
ADGuid	Active Directory Id	binary
Assistant	Assistant	Person
CellPhone	Mobile phone	string (single-value)
Department	Department	string (single-value)
Fax	Fax	string (single-value)
FirstName	First name	string (single-value)
HomePhone	Home phone	string (single-value
LastName	Last name	string (single-value)
Manager	Manager	Person
Office	Office	string (single-value)
PersonalSpace	Personal site	URL
PictureURL	Picture	URL
PreferredName	Name	string (single-value)
PublicSiteRedirect	Public site redirect	URL
QuickLinks	Quick links	string (single-value)
SID	SID	binary
SPS-Birthday	Birthday	date no year
SPS-ClaimID	Claim User Identifier	string (single-value)
SPS-ClaimProviderID	Claim Provider Identifier	string (single-value)
SPS-ClaimProviderType	Claim Provider Type	string (single-value)
SPS-DataSource	Data source	string (single-value)
SPS-DisplayOrder	Display Order	integer
SPS-DistinguishedName	Distinguished Name	string (single-value)
SPS-DontSuggestList	Don't Suggest List	Person
SPS-Dotted-line	Dotted-line Manager	Person
SPS-EmailOptin	Email Notifications	integer
SPS-HireDate	Hire date	date
SPS-Interests	Interests	string (multi-value)
SPS-JobTitle	Job Title	string (single-value)
SPS-LastColleagueAdded	Last Colleague Added	date
SPS-LastKeywordAdded	Last Keyword Added	date

Use profile property	Display name	User profile service data type
SPS-Location	Office Location	string (single-value)
SPS-MemberOf	MemberOf	string (multi-value)
SPS-MySiteUpgrade	My Site Upgrade	boolean
SPS-ObjectExists	Object Exists	string (single-value)
SPS-OWAUrl	Outlook Web Access URL	URL
SPS-PastProjects	Past projects	string (multi-value)
SPS-Peers	Peers	string (single-value)
SPS-PhoneticDisplayName	Phonetic Display Name	string (single-value)
SPS-PhoneticFirstName	Phonetic First Name	string (single-value)
SPS-PhoneticLastName	Phonetic Last Name	string (single-value)
SPS-ProxyAddresses	Proxy addresses	string (multi-value)
SPS-ResourceSID	Resource Forest SID	binary
SPS-Responsibility	Ask Me About	string (multi-value)
SPS-SavedAccountName	Saved Account Name	string (single-value)
SPS-SavedSID	Saved SID	binary
SPS-School	Schools	string (multi-value)
SPS-SipAddress	SIP Address	string (single-value)
SPS-Skills	Skills	string (multi-value)
SPS-SourceObjectDN	Source Object Distinguished Name	string (multi-value)
SPS-StatusNotes	Status Message	string (single-value)
SPS-TimeZone	Time Zone	time zone
Title	Title	string (single-value)
UserName	User name	string (single-value)
UserProfile_GUID	Id	unique identifier
WebSite	Web site	URL
WorkEmail	Work e-mail	E-mail
WorkPhone	Work phone	string (single-value)

Concepts

Default user profile property mappings (SharePoint Server 2010)

Other Resources

Plan for profile synchronization (SharePoint Server 2010)

(*http://technet.microsoft.com/library/8451dde9-bbd1-4285-bc24-71bd795fb912(Office.14).aspx*)

Default user profile property mappings (SharePoint Server 2010)

Published: April 28, 2011

Some user profile properties are mapped automatically to their corresponding directory service attributes after you run a profile synchronization. This topic describes the user profile properties that are mapped by default.

In this topic:

- Default user profile property mappings for Active Directory Domain Services
- Default user profile property mappings for Novell eDirectory, Sun Java System Directory Server, or IBM Tivoli Directory Server

Default user profile property mappings for Active Directory Domain Services

The following table describes the user profile properties that are automatically mapped when you import user profiles from Active Directory Domain Services (AD DS).

User profile property	AD DS attribute
SPS-DistinguishedName	dn
SID	objectSid
Manager	manager
PreferredName	displayName
FirstName	givenName
LastName	sn
SPS-PhoneticDisplayName	msDS-PhoneticDisplayName
SPS-PhoneticFirstName	msDS-PhoneticFirstName
SPS-PhoneticLastName	msDS-PhoneticLastName
WorkPhone	telephoneNumber
WorkEmail	mail
Office	physicalDeliveryOfficeName
SPS-JobTitle	title
Department	department
UserName	sAMAccountName
PublicSiteRedirect	wWWHomePage
SPS-ProxyAddresses	proxyAddresses
SPS-SourceObjectDN	msDS-SourceObjectDN
SPS-ClaimID	<specific to connection>
SPS-ClaimProviderID	<specific to connection>
SPS-ClaimProviderType	<specific to connection>

Default user profile property mappings for Novell eDirectory, Sun Java System Directory Server, or IBM Tivoli Directory Server

The following table describes the user profile properties that are mapped automatically when you import user profiles from Novell eDirectory, Sun Java System Directory Server, or IBM Tivoli Directory Server.

User profile property	Directory service attribute
SPS-DistinguishedName	dn
FirstName	givenName
LastName	sn
WorkPhone	telephoneNumber
WorkEmail	mail
Office	physicalDeliveryOfficeName
SPS-JobTitle	title
UserName	<specific to connection>
SPS-ClaimID	<specific to connection>
SPS-ClaimProviderID	<specific to connection>
SPS-ClaimProviderType	<specific to connection>

Concepts

Default user profile properties (SharePoint Server 2010)

Other Resources

Plan for profile synchronization (SharePoint Server 2010)
(*http://technet.microsoft.com/library/8451dde9-bbd1-4285-bc24-71bd795fb912(Office.14).aspx*)
Configure Profile Synchronization (SharePoint Server 2010)
(*http://technet.microsoft.com/library/144e5f6e-0c9c-4f01-9b1f-26190d527e85(Office.14).aspx*)