Microsoft®
SharePoint

Configure a two-way hybrid Search environment with SharePoint Server 2013 and Office 365

Configure a two-way hybrid Search environment with SharePoint Server 2013 and Office 365

This is preliminary documentation that is subject to change. For additional assistance, please work with your Microsoft consultant.

Kelley Vice

Joseph Davies

Aldon Schwimmer

Tracy Paddock

Microsoft Corporation

December 2012

Applies to: SharePoint Server 2013, Office 365 Enterprise

Summary: This document describes how to configure a hybrid environment that integrates SharePoint Server 2013 and the newest version of Microsoft Office 365 Enterprise, which includes the new SharePoint Online, with single sign-on, identity management, and bi-directional federated search.

For additional hybrid environment documents, see Hybrid for SharePoint Server 2013.

Contents

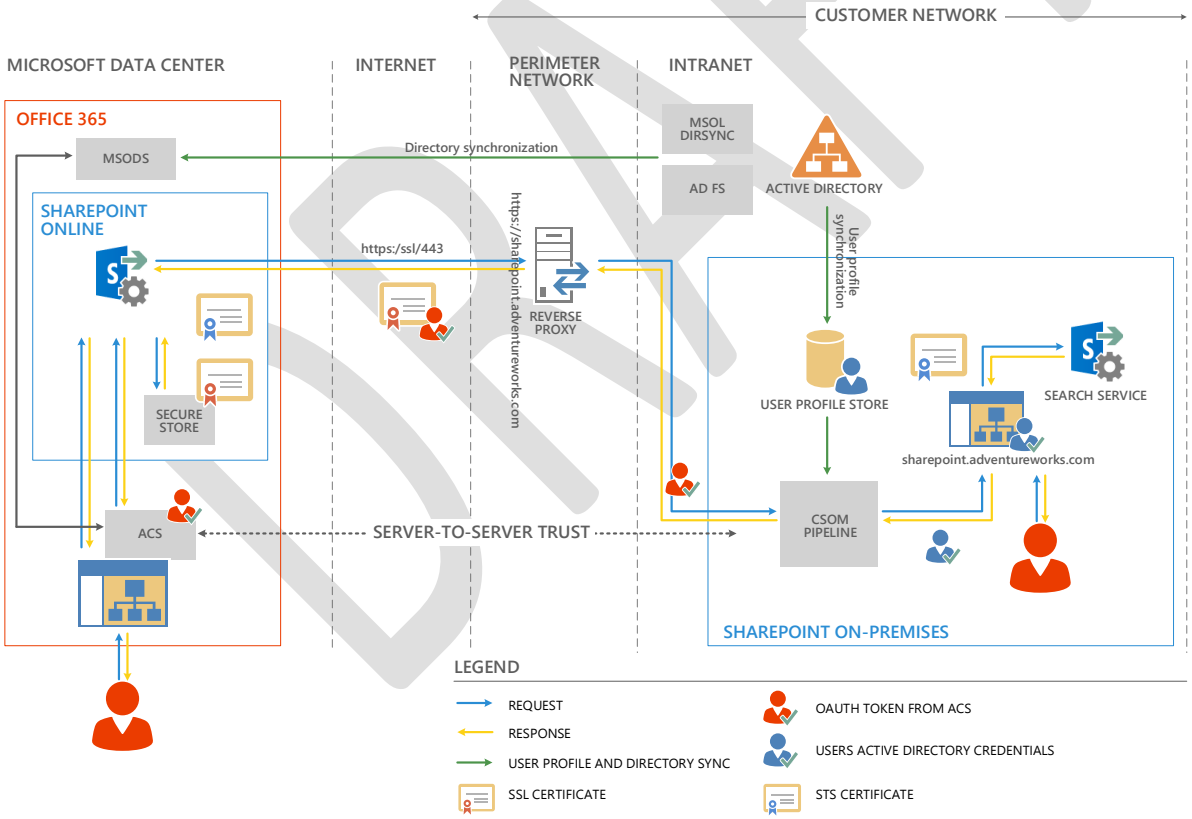
Contents

Introduction

A hybrid SharePoint environment is composed of SharePoint Server, typically deployed on-premises, and the newest version of Microsoft Office 365 Enterprise, which includes the new SharePoint Online. A hybrid environment may be configured to provide one of several levels of integration, depending on the purpose of the integration. This white paper describes how to configure a two-way integration in which an on-premises SharePoint Server 2013 farm and SharePoint Online access search results information from each other.

After you complete the procedures in this white paper, you will have a two-way hybrid SharePoint environment that provides the following functionality:

- **Single sign-on (SSO):** Users who are connected to either the corporate network or Office 365 only have to authenticate once in a given session to access resources in both the on-premises SharePoint farm and SharePoint Online.
- **Directory synchronization:** User accounts in the on-premises Active Directory Domain Services (AD DS) domain automatically synchronize to Office 365.
- **Two-way server-to-server trust:** A certificate-based two-way trust relationship is established between the on-premises SharePoint farm and SharePoint Online.
- **Two-way federated search:** Users in Office 365 and in your on-premises domain environment will be able to get SharePoint search results that encompass content from both locations.



The process of configuring a two-way hybrid SharePoint environment can be divided into the following three major steps:

1. **Prepare your environment.** This step ensures that the required technologies are installed and properly configured. This step includes the following tasks:
    a. Set up an Office 365 Enterprise, which includes the new SharePoint Online, subscription plan

   b. Acquire and install the required certificates
   c. Configure a reverse proxy device
   d. Install and configure AD FS 2.0
2. **Configure SSO, directory synchronization and identity management.** This step creates the basic connections that are necessary for users to connect seamlessly to both your on-premises and Office 365 environments.
3. **Configure search.** This step configures search to return results from both your on-premises SharePoint Server 2013 farm and from Office 365 when you are searching from either environment.

Note: Because SharePoint Server 2013 runs as websites in Internet Information Services (IIS), administrators and users depend on the accessibility features that browsers provide. SharePoint Server 2013 supports the accessibility features of supported browsers. For more information, see the following resources:

- Plan browser support
- Accessibility for SharePoint 2013
- Accessibility features in SharePoint 2013 Products
- Keyboard shortcuts
- Touch

Note: There are Windows PowerShell procedures in this document that must either be executed in the SharePoint 2013 Management Shell or in the Microsoft Online Services Module for Windows PowerShell. For clarity, procedures that contain Windows PowerShell commands use the following conventions:

SharePoint 2013 Management Shell procedures are identified with this icon.

Microsoft Online Services Module for Windows PowerShell procedures are identified with this icon.

Before you begin

Before you begin the procedures in this document, you will need the following:

1. An operational on-premises DS domain in a forest that has a Windows Server 2008, Windows Server 2008 R2 or Windows Server 2012 forest functional level
2. An on-premises server for AD FS 2.0
3. An on-premises server for the Microsoft Online Services Directory Synchronization tool
4. An operational on-premises SharePoint Server 2013 farm that has each of the following:
   a. An Enterprise Search site collection configured with a public external URL (for example http://sharepoint.adventureworks.com) by using alternate access mapping
   b. An SSL certificate issued by a public root authority
   c. An App Management Service Proxy installed and published in the SharePoint farm
   d. A Subscription Settings service application enabled and configured
   e. A Search service application, configured as appropriate. For more information, see Create and configure a Search service application in SharePoint Server 2013 (http://technet.microsoft.com/library/gg502597(v=office.15)).
5. An Office 365 Enterprise, which includes the new SharePoint Online subscription with **15.0.0.4420** as the minimum build number, and provisioned with SharePoint Online by using one of the following subscription plans:
   a. E1
   b. E3

For more information about the supported plans, see the Plans & pricing page on the Office 365 site.

Note: To find the build of your Office 365 tenant, navigate to your site collection at **https://<your Office 365 domain>/_vti_pvt/service.cnf** and find the entry **vti_extenderversion:SR**. The value following this entry must be at least **15.0.0.4420**.

6. A reverse proxy device with an Internet connection that permits unsolicited inbound traffic
7. An Internet domain (such as http://yourcompany.com) and access to DNS records for the domain

Phase 1: Configure your on-premises environment

You have to complete several tasks to configure your on-premises environment:

- Create and install certificates
- Configure DNS in AD DS and your domain registrar
- Configure alternate access mappings for your SharePoint site collection
- Enable and configure the App Management service and the Site and Subscription service in your SharePoint Server 2013 farm
- Configure your on-premises AD DS domain
- Install and configure AD FS 2.0
- Deploy and configure a reverse proxy device

Create and install certificates

Certificates establish trust relationships for several different services and connections in a SharePoint hybrid environment. These certificates include the following:

- **SSL certificate:** This certificate establishes trust for the communication channel between the reverse proxy device and Office 365. It also verifies the trust between the Office 365 target application and the on-premises Search service.
- **STS certificate:** This certificate, which replaces the default SharePoint STS certificate, establishes trust between the on-premises SharePoint site collection and SharePoint Online.

Note that certificates will expire, typically at 1-year intervals, so it is important to plan in advance for certificate renewals to avoid service interruptions.

Create and install the SSL certificate

1. Acquire an SSL wildcard or SAN (Subject Alternative Names) certificate for your domain (for example, *.sharepoint.adventureworks.com) from a well-known certificate authority such as VeriSign. This certificate must support multiple names.
2. Assign the certificate to the published endpoint of your SharePoint site collection on the reverse proxy.
3. In the IIS Manager on each SharePoint web server running the Search service, install the SSL certificate that you created earlier and bind it to the SharePoint site.

Create and install the STS certificate

To learn how to replace the default STS certificate, see Step 1 in the **Part B: Configure server-to-server authentication between the on-premises and SharePoint Online servers** section of this document.

For more information on replacing the STS certificate in a SharePoint Server farm, see Configure the security token service (http://technet.microsoft.com/library/ee806864.aspx).

Configure DNS

1. In your on-premises DNS, create an A record for the external connection (for example, external.sharepoint.adventureworks.com).
2. In your Internet domain registrar's DNS, create an identical A record for the external connection.

Configure alternate access mapping

In SharePoint Central Administration, create an alternate access mapping for your SharePoint site collection by using the DNS A record that you created (for example, https://external.sharepoint.adventureworks.com).

1. Create a new IIS website with all default settings, with attention to the following:
    - Name the site something meaningful, such as SharePoint
    - Assign port 80
    - Leave the Host Header blank
    - Choose NTLM authentication
    - Do not enable SSL
    - Do not supply a public URL
    - Apply the Default Zone
2. Extend and map a new web application to the original.
    - Name the web application something meaningful, such as SharePoint Hybrid
    - Assign port 80
    - Supply the Internal URL (the incoming URL from the reverse proxy) in the Host Header
    - Do not change the SSL setting
    - Supply the external URL (such as https://external.sharepoint.adventureworks.com) for Public URL
    - Select the Internet Zone
3. Add the internal URL for the site to the alternate access mapping.
    a. In Central Administration, in the **Application Management** section, click **Configure Alternate Access Mappings**.
    b. Click **Add Internal URLs**.
    c. In the Add Internal URL field, add the URL of the SharePoint site (such as http://sharepoint.adventureworks.com).
    d. Apply the Internet zone
4. In a command prompt, run `iisreset /noforce`.

Configure SharePoint services

To configure the App Management and Subscription Settings services, see the "Configure the Subscription Settings and App Management service applications" section of Configure an environment for apps for SharePoint (SharePoint 2013) (http://technet.microsoft.com/library/fp161236(v=office.15).aspx).

Configure your AD DS domain

To synchronize domain accounts with Office 365, you must set the User Principal Name (UPN) suffix for user accounts to match the public domain namespace if your on-premises domain name does not match your public domain namespace.

> **Important:** You must only complete this step if your on-premises domain name does not match your public domain namespace.

1. On an AD DS domain controller, open the **Active Directory Domains and Trusts** management application.
2. Right-click on the top node in the navigation window, and then click **Properties**.
3. Add the UPN suffix for your domain. This must be the fully qualified domain name for the domain.
4. Set the new UPN suffix for each user account in the domain for which you want to enable SSO. User accounts with UPN suffixes that do not match the public domain namespace will be replicated to the SharePoint Online directory during directory synchronization, but will be prompted to provide online credentials when the user logs in to the SharePoint Online tenancy.

   This must be the fully qualified domain name for the domain. For more information, see HOW TO: Add UPN Suffixes to a Forest (http://support.microsoft.com/kb/243629).

Install and configure AD FS 2.0

Installation and configuration of ADFS 2.0 for use with Office 365 is covered in Part A: Configure SSO for Office 365 later in this document. For more information about how to install and configure AD FS 2.0, see Plan for and deploy AD FS 2.0 for use with single sign-on.

Configure a reverse proxy device

Because a two-way hybrid SharePoint environment requires SharePoint Online to be able to connect to the on-premises SharePoint farm, you must configure a reverse proxy device that can accept unsolicited inbound traffic from the Internet.

The reverse proxy device must meet the following requirements:

- Be configured with two network cards, one connected to the Internet with a public IP address, and the other connected to the internal company network
- Be able to accept unsolicited inbound traffic on port 443 (HTTPS) and route this traffic to the on-premises SharePoint farm
- Be able to bind an SSL certificate to the published endpoint
- Be able to forward traffic to the on-premises SharePoint farm without rewriting packet headers (without port forwarding)

Currently supported reverse proxy devices for a hybrid SharePoint environment include:

- Microsoft Forefront Threat Management Gateway (TMG)
- F5 Big IP
- Cisco business-class routers

Additional reverse proxy devices will be supported as they are tested for compatibility.

Phase 2: Configure the identity management infrastructure

This section describes how to configure the following elements of identity management for a hybrid environment:

- Single sign-on (SSO) for the on-premises farm and the Office 365 subscription
- Server-to-server authentication between the on-premises farm and SharePoint Online

When an organization subscribes to Microsoft Office 365 Enterprise, which includes the new SharePoint Online, the organization receives the following features:

- An online directory tenancy in Microsoft Online Directory Service.

  This provides user account storage in Office 365.

- A Windows Azure Access Control Service (ACS) tenancy.

  This provides authentication services for Office 365 user accounts and federated accounts from a connected on-premises AD DS domain.

- A SharePoint Online subscription.

  This provides SharePoint sites and related services, depending on the Office 365 subscription.

These tenancies enable users who belong to appropriate groups to configure the SharePoint Online subscription.

Part A: Configure SSO for Office 365

SSO enables users to use their AD DS domain credentials to access servers on the on-premises farm and on Office 365. Without SSO, network administrators would have to maintain a separate set of online accounts and credentials. Users would be prompted to provide online credentials every time they accessed a SharePoint resource on Office 365.

SSO requires you to configure the following:

- AD FS 2.0 to provide federated authentication between on-premises and online environments.
- Directory synchronization to ensure that both environments use the same set of on-premises AD DS accounts.

SSO configuration for Microsoft Office 365 consists of the following steps:

1. Deploy Directory Synchronization
2. Deploy single sign-on

Before you proceed to server-to-server authentication configuration, verify the following:

- Users can access the on-premises SharePoint farm without being prompted for credentials.
- Users can access SharePoint Online without being prompted for credentials.
- The People Picker user interface for the on-premises SharePoint farm shows the users and groups in AD DS.
- The People Picker user interface for SharePoint Online shows the users and groups in AD DS.

Part B: Configure server-to-server authentication between the on-premises and SharePoint Online servers

To configure server-to-server authentication for hybrid environments, you have to establish trust with ACS, the trust broker for both the on-premises and online SharePoint servers. After you establish this relationship, each server trusts the security tokens that ACS issues for access to resources on behalf of an identified user.

Step 1. Replace the default STS certificate of your on-premises farm with a certificate from a well-known certification authority or a self-signed certificate

ACS cannot use the default certificate that the Security Token Service (STS) of the on-premises SharePoint farm created to validate incoming tokens that the STS issues. This occurs because the STS issued the tokens based on its own self-signed certificate. Therefore, you must replace the default STS certificate with either a certificate that a public certification authority (CA) that ACS trusts (recommended) issued or a self-signed certificate. We recommend the former because self-signed certificates might have integration issues with other applications and services. If you have already replaced the default STS certificate, then skip to Step 2.

> **Note:** The following procedure creates a new certificate in two types, a Personal Information Exchange file (.pfx) and a Security Certificate file (.cer). Each of these different certificate types is required in later steps.

Perform this procedure during a maintenance window because the procedure replaces the STS certificate of the on-premises farm, and you have to restart IIS and the SharePoint timer service.

> **Note:** You must log on to a farm web front-end server as a member of the Administrators group on the local computer to complete these steps.

To use the IIS snap-in to generate a self-signed certificate, complete the following steps:

1. From the Windows Server desktop on an on-premises SharePoint server, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the console tree, click the server name.
3. In the details pane, double-click **Server Certificates** in the IIS group.
4. In the **Actions** pane, click **Create Self-Signed Certificate**.

5. On the **Specify Friendly Name** page, type a name for the certificate, and then click **OK**.
6. In the details pane, right-click the new certificate, and then click **Export**.
7. In **Export Certificate**, specify a path and name to store the .pfx file for the certificate in **Export to**, and a password for the certificate file in **Password** and **Confirm password**. This creates a .pfx file containing the private key that will be needed in the following procedure.
8. In the details pane, right-click the new certificate, and then click **View**.
9. Click the **Details** tab, and then click **Copy to File**.
10. On the Welcome to the Certificate Export Wizard page, click **Next**.
11. On the Export Private Key page, click **Next**.
12. On the Export File Format page, click **Base-64 encoded X.509 (.CER)**, and then click **Next**.
13. On the File to Export page, type a path and file name for the .cer file, and then click **Next**.
14. On the Completing the Certificate Export Wizard page, click **Finish**, and then click **OK** twice. The resulting .cer file will be needed in Step 3.

Note: You must log on to a farm web front-end server with an account that is a member of the following groups to complete the steps below:

- Local computer administrators
- SharePoint farm administrators

To replace the default STS certificate with your new self-signed certificate or a certificate obtained from a CA that ACS trusts, on a SharePoint web server in your farm, run the following commands from the SharePoint 2013 Management Shell prompt:

```
$certPrkPath="<path to replacement certificate (.pfx file)>"
$stsCertificate=New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2 $certPrKPath,
"<replacement certificate password>", 20
Set-SPSecurityTokenServiceConfig -ImportSigningCertificate $stsCertificate
iisreset
net stop SPTimerV4
net start SPTimerV4
```

Note: None of these commands will display any output if they are successful.

To validate this step, type the following command at the SharePoint 2013 Management Shell prompt:

```
$stscertificate |fl
```

In the output, confirm that the certificate has the new friendly name.

For more information on replacing the STS certificate in a SharePoint Server farm, see Configure the security token service (http://technet.microsoft.com/library/ee806864.aspx).

Step 2. Install the Office 365 Sign-on Assistant and connect to the online tenancy

In this step, you will install the Microsoft Online Services Sign-In Assistant and the Microsoft Online Services Module for Windows PowerShell on a single SharePoint web server in your on-premises farm, and then authenticate with your Office 365 tenant.

For more information about these tools, see Use Windows PowerShell to manage Office 365 (http://onlinehelp.microsoft.com/en-us/office365-enterprises/hh124998.aspx).

1. Set up remoting in Windows PowerShell.
   On a SharePoint web server in your on-premises farm, run the following commands from the Windows PowerShell prompt as local computer administrator:


   ```
   enable-psremoting
   new-pssession
   ```

   For more information, see about_Remote_Requirements.
2. Install the Microsoft Online Services Sign-In Assistant for IT Professionals:

   - Microsoft Online Services Sign-In Assistant (IDCRL7) (32 bit version) (http://go.microsoft.com/fwlink/p/?linkid=236299)
   - Microsoft Online Services Sign-In Assistant (IDCRL7) (64 bit version) (http://go.microsoft.com/fwlink/p/?linkid=236300)
3. Install the Microsoft Online Services Module for Windows PowerShell:

   - Microsoft Online Services Module for Windows PowerShell (32 bit version) (http://go.microsoft.com/fwlink/p/?linkid=236298)
   - Microsoft Online Services Module for Windows PowerShell (64 bit version) (http://go.microsoft.com/fwlink/p/?linkid=236297)
4. Open the Microsoft Online Services Module for Windows PowerShell window (as local computer administrator), and then run the following commands:


   ```
   Import-Module MSOnlineExtended –force -verbose
   Connect-MsolService
   ```

5. Type your SharePoint Online administrator credentials.

Leave the Microsoft Online Services Module for Windows PowerShell window (run as local computer administrator) open for the following steps.

Step 3. Upload the signing certificate of the on-premises server to the SharePoint principal object of the Office 365 tenancy

The following commands add the public key of the signing certificate of the STS of the on-premises SharePoint server to the SharePoint principal object of the Office 365 tenancy.

Note: The user account that performs this step must be a SharePoint Online administrator.

Run the following commands from the Microsoft Online Services Module for Windows PowerShell window:


```
$spoappid="00000003-0000-0ff1-ce00-000000000000"
$certpath="<path to .pfx>"
$certpass="<certificate password>"
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
-ArgumentList $certpath, $certpass
$cer=New-Object system.security.cryptography.X509certificates.X509certificate2
$cer.Import("<path to replacement certificate (.cer file) from step 1>")
$binCert = $cer.GetRawCertData()$credValue =
[System.Convert]::ToBase64String($binCert);
New-MsolServicePrincipalCredential -AppPrincipalId $spoappid -Type asymmetric -
Usage Verify -Value $credValue -StartDate $cer.GetEffectiveDateString() -EndDate
$cer.GetExpirationDateString()
```

Step 4. Add the host name of the on-premises SharePoint server to the SharePoint principal object of the Office 365 tenancy

These commands add the host name of the on-premises SharePoint server to the SharePoint principal object of the Office 365 tenancy.

Note: The user account that performs this step must be a SharePoint Online administrator.

- Run the following commands from the Microsoft Online Services Module for Windows PowerShell window:


  ```
  $SharePoint = Get-MsolServicePrincipal -AppPrincipalId $spoappid
  $spns = $SharePoint.ServicePrincipalNames
  $spns.Add("$spoappid/<FQDN of the external SharePoint site URL>")
  Set-MsolServicePrincipal -AppPrincipalId $spoappid -ServicePrincipalNames
  $spns
  ```

These commands add the external URL of the on-premises SharePoint server (<FQDN of the SharePoint site URL>) to the SharePoint principal object (identified by 00000003-0000-0ff1-ce00-000000000000) of the Microsoft online directory tenancy.

For example, if the public URL of your on-premises SharePoint server is sharepoint.adventureworks.com, then the $spns.Add command becomes:

```
$spns.Add("$spoappid/sharepoint.adventureworks.com")
```

Step 5. Get the application principal ID and context ID of the organization's tenancy

Note: The user account that performs this step must be a SharePoint Online administrator.

1. Run the following Windows PowerShell command from the Microsoft Online Services Module Windows PowerShell window:


```
(Get-MsolCompanyInformation).ObjectID
```

This command displays the GUID for the context ID of the Microsoft online directory tenancy. This value is referred to as the <ContextID property of the Microsoft online directory tenancy> value in Step 6 and Step

2. Run the following Windows PowerShell command from the Microsoft Online Services Module Windows PowerShell window:


```
Get-MsolServicePrincipal -ServicePrincipalName $spoappid
```

This command displays the GUID for the AppPrincipalID property of the SharePoint Online STS principal. This value is referred to as the <AppPrincipalID property of the SharePoint Online STS principal object> value in Step 6.

Step 6. Register the SharePoint Online server-to-server principal object with the on-premises SharePoint STS

Note: The user account that performs this step must be a member of the Farm Administrators group in your on-premises SharePoint farm. This account does not have to be a SharePoint Online administrator.

- Run the following Windows PowerShell commands from the SharePoint 2013 Management Shell:


```
$site=Get-Spsite <root URL of your site>
$appPrincipal = Register-SPAppPrincipal -site $site.rootweb -nameIdentifier
"<nameID>" -displayName "SharePoint Online"
```

The <nameID> of the organization's SharePoint Online tenancy has the following form:

```
<AppPrincipalID property of the SharePoint Online S2S principal
object>@<ContextID property of the Microsoft online directory tenancy>
```

- <AppPrincipalID property of the SharePoint Online S2S principal object> is the GUID from the Get- Get-MsolServicePrincipal Windows PowerShell command in Step 5. You can copy and paste this GUID from the open Microsoft Online Services Module Windows PowerShell window.
- <ContextID property of the Microsoft Online directory tenancy> is the GUID from the Get-MsolCompanyInformation Windows PowerShell command in Step 5. You can copy and paste this GUID from the open Microsoft Online Services Module Windows PowerShell window.

This command registers the SharePoint Online app principal to the Application Management shared service of the on-premises server, if one does not already exist.

Step 7. Set the SharePoint authentication realm to the context ID of the organization's Office 365 tenancy

Note: The user account that performs this step must be a member of the Farm Administrators group in your on-premises SharePoint farm. This account does not have to be a SharePoint Online administrator.

- Run the following Windows PowerShell command from the SharePoint 2013 Management Shell:

```
Set-SPAuthenticationRealm -realm <ContextID property of the Microsoft
Online directory tenancy>
```

Where:

<ContextID property of the Microsoft Online directory tenancy> is the GUID from the MsolCompanyInformation Windows PowerShell command in Step 5. You can copy and paste this GUID from the open Microsoft Online Services Module Windows PowerShell window.

This sets the realm on the on-premises server to the realm of the SharePoint Online tenancy.

Important You must now update your farm setup scripts in which you have configured the farm authentication realm value for this new value. For more information about the requirements for realm values in farm setup scripts, see Plan for server-to-server authentication. Because you have now configured this SharePoint farm to participate in the hybrid configuration, the SharePoint farm authentication realm value must always match the tenant context identifier. If you change this value, the farm will no longer participate in hybrid functionality.

Step 8. Configure an on-premises ACS proxy and set up a trust with the ACS tenancy

Note: The user account that performs this step must be a member of the Farm Administrators group in your on-premises SharePoint farm. This account does not have to be a SharePoint Online administrator.

- Run the following Windows PowerShell commands from the SharePoint 2013 Management Shell:

```
New-SPAzureAccessControlServiceApplicationProxy -Name "ACS" -
MetadataServiceEndpointUri "<Metadata endpoint URL of ACS>" -
DefaultProxyGroup

New-SPTrustedSecurityTokenIssuer -MetadataEndpoint "<Metadata endpoint URL
of ACS>" -IsTrustBroker -Name "ACS"
```

Where the `<Metadata endpoint URL of ACS>` for SharePoint Online 2013 is "https://accounts.accesscontrol.windows.net/<contextID property of the Microsoft online directory tenancy>/metadata/json/1"

For example, if the context ID of an Office 365 tenant is 3bdbdd27-2373-4baf-9469-4b10e76564f7, the URL is "https://accounts.accesscontrol.windows.net/3bdbdd27-2373-4baf-9469-4b10e76564f7/metadata/json/1".

The New-SPAzureAccessControlServiceApplicationProxy cmdlet configures an on-premises ACS proxy. The New-SPTrustedSecurityTokenIssuer cmdlet sets up a trust with the ACS tenancy.

Phase 3: Configure search

In a hybrid SharePoint environment, there might be some content in the SharePoint Server 2013 (on-premises) farm and other content in SharePoint Online.

In this section:

- Create a target application to store the SSL certificate

  Create a target application in SharePoint Online for an SSL certificate.
- View search results in SharePoint Server 2013

  Configure the hybrid environment so that people who are working in the SharePoint Server 2013 farm can view search results from content that is in both environments.
- Get and display hybrid search results by using SharePoint Online

  Configure the hybrid environment so that people who are working in SharePoint Online can view search results from content that is in both environments.

Create a target application to store the SSL certificate

This section describes how to create a target application in SharePoint Online for an SSL certificate.

When you configure SharePoint Online for a hybrid environment that provides search or Business Connectivity Services functionality, we recommend that you create an SSL certificate that the O365 search or Business Connectivity Services will use to authenticate with the reverse proxy server. This is required to enable search results from the on-premises SharePoint farm to be returned to users on SharePoint Online. If you use this approach, you must create and name a target application in the Secure Store service application in SharePoint Online to store the SSL certificate.

In the following procedure, you must provide the name of the SSL certificate. This is the name of an exported SSL certificate that is on the computer that hosts the reverse proxy. For more information about this certificate, see "Configure a reverse proxy device" earlier in this white paper.

In the following procedure, you will need a certificate that contains a private key.

Use the following procedure in SharePoint Online to create a target application for the SSL certificate.

To create a target application to store the reverse proxy certificate

1. Verify that the user account that is performing this procedure is a global administrator or a SharePoint Online administrator for the Office 365 service that you want to configure.
2. In the SharePoint Online Administration Center, in the left pane, click **secure store**.
3. In the **Edit** tab, click **New** to create a Secure Store target application in the Secure Store service application.

   This creates the Secure Store target application into which you will place the reverse proxy certificate.
4. In the **Target Application Settings** section, do the following:

   a) In the **Target Application ID** text box, type the name (which will be the ID) that you want to use for the target application—for example, **TargetAppIDforSearchOrBCS**. Do not use spaces in this name.

Note: You create the ID in this step—you do not get the ID from somewhere else. This ID is a unique target application name that cannot be changed.

b) In the **Display Name** text box, type the name that you want to use as the display name for the new target application, for example, **Target App ID for Search Or BCS**.

c) In the **Contact E-mail** text box, type the name of the primary contact for this target application.

d) In the **Credential Fields** section, name two fields by doing the following:

i. Under **Field Name**, in the first row, delete any existing text that is in the text box, and then type **Certificate** in the text box.

ii. Under **Field Type**, in the first row, in the drop-down list, select **Certificate**.

iii. Under **Field Name**, in the second row, delete any existing text that is in the text box, and then type **Certificate Password** in the text box.

iv. Under **Field Type**, in the second row, in the drop-down list, select **Certificate Password**.

e) In the **Target Application Administrators** section, in the text box, type the names of users who will have access to manage the settings of this target application. Make sure to add any users who will be testing the hybrid configuration.

f) In the **Members** section, in the text box, type the names of users and Microsoft Online Directory Service (MSODS) groups mapped to the credentials that are defined for this target application.
The Office 365 global administrator can create MSODS groups. These are domain groups, not SharePoint groups.

g) Click **OK**.

h) On the **Edit** tab, under **Target Application ID**, do the following:

i. Select the check box next to the ID of the target application that you created—for example, **TargetAppIDforSearchOrBCS**.

ii. On the **Edit** tab, in the **Credentials** group, click **Set**.

i) In the **set credentials for secure store target application** dialog box, do the following:

i. Next to the **Certificate Name** field, click **Browse**.

ii. Browse to the location of the certificate that was exported on the computer that hosts the reverse proxy, click the exported certificate, and then click **OK**.

iii. In the **Certificate Password** field, type the name of the password of the exported certificate.

iv. In the **Confirm Certificate Password** field, type the name of the password of the exported certificate.

v. Click **OK**.

For more information, see Configure the Secure Store Service in SharePoint 2013.

View hybrid search results in SharePoint Server 2013

This section describes how to configure search functionality in a hybrid SharePoint environment so that end users view search results in the SharePoint Server 2013 farm from content that is in both environments.
To configure search functionality in a hybrid SharePoint environment in this way, you perform the following two procedures in the SharePoint Server 2013 farm:

Step 1: Create a result source.

Step 2: Create a query rule that uses the result source.

Before you proceed, verify that the user account that you use to perform these steps is an administrator for the Enterprise Search site or site collection that you want to configure.

Step 1: Create a result source

In this procedure, you create a result source in the SharePoint Server 2013 farm. This result source is a definition that specifies the SharePoint Online location to get search results from, and the protocol for getting those results.

To create the result source

1. Go to the Site Settings page for the Enterprise Search site by doing the following:

    a) In Site Settings, in the **Site Collection Administration** section, click **Search Result Sources**.

    b) On the **Manage Result Sources** page, click **New Result Source**.

    Note: Result sources can be created at the Search service application level, the site collection level, or the site level. In this procedure, you create the result source at the site level.

2. On the **Search Result Sources** page, do the following:

    a) In the **Name** text box, type a name for the new result source—for example, "SharePoint Online result source".

    b) Optionally, in the **Description** text box, type a description of the new result source.

    c) For the **Protocol**, select **Remote SharePoint**.

    d) For the **Remote Service URL**, type the address of the root site collection that you want to search in SharePoint Online, such as **http://sharepoint.adventureworks.com**.

    e) For the **Type**, select **SharePoint Search Results**. This specifies that the search system will search the entire SharePoint Online content index when a user submits a query.

    f) For **Query Transform**, optionally type a new query transform in the text box (such as author:Geoff or path:http://myteamsite.adventureworks.com), or click **Launch Query Builder** to build a query template. The default template is **{searchTerms}**, which is the query that the user typed, as changed by the most recent transform.

    g) For **Credentials Information**, select **Default Authentication**.

    h) Click **OK** to save the new result source.

Step 2: Create a query rule that uses the result source

In this procedure, you create a query rule that uses the result source you created in Step 1. When this query rule runs, it causes search results from the SharePoint Server 2013 farm and SharePoint Online to be displayed on a results page in the SharePoint Server 2013 farm. For more information about query rules, see Overview of query processing in SharePoint 2013 (http://technet.microsoft.com/library/jj219620(v=office.15).

To create the query rule

1. On the **Manage Result Sources** page, click **Search Query Rules**.
2. On the **Manage Query Rules** page, do the following:
    a) In the **Select a Result Source** drop-down list, select the result source that you created in the previous procedure -- for example, "Local SharePoint Results (System)". This will show all the query rules associated with that result source.
    b) Click **New Query Rule**.
3. On the **Add Query Rule** page, do the following:
    a) In the **General Information** section, in the **Rule Name** box, type a name for the new query rule.
    b) In the **Context** section, do the following:
        i. Under **Query is on these sources**, select **All Sources** or **One of these sources**.
        Note: If you select **One of these sources**, the rule will fire only on the result sources that are listed. Therefore, make sure that the name of the result source that you created in the previous procedure—for example, "SharePoint Online result source"—appears in the list.
        ii. Under **Query is performed from these categories**, optionally specify the topic categories (based on terms for topic categories in the term store in a Managed Metadata service application) to perform the query from.
        iii. Under **Query is performed by these user segments**, optionally define user segments (based on terms that describe users in the term store of a Managed Metadata service application) to which you want the query rule to apply.
    c) In the **Query Conditions** section, specify conditions to control when the rule will fire, or click **Remove Condition**.
    Note: If you want the rule to fire for every query whenever the rule is active, click **Remove Condition.** (See the information about the **Is Active** setting later in this procedure.)
    d) In the **Actions** section, under **Result Blocks**, click **Add Result Block**.
    e) In the **Add Result Block** dialog box, do the following:
        i. In the **Block Title** section, in the **Title** text box, accept the default title (which is **Results for "{subjectTerms}"**), or type a different title.
        ii. In the **Query** section, do the following:
            a. In the **Configure Query** text box, use the default query, which is **{subjectTerms}**, or specify a query configuration to transform the query.

            You can click **Launch Query Builder** to help you configure a query transform.

b. In the **Search this Source** drop-down list, select the name of the result source that you created in the previous procedure—for example, "SharePoint Online result source".

c. In the **Items** drop-down list, select the number of search results from SharePoint Online that you want to show in a group on the search results page. For example, select **3** to display three results in a group from SharePoint Online.

iii. In the **Settings** section, do the following:

a. If you want to display a **Show More** link at the bottom of the result block, select **More link goes to the following URL**, and type the URL for the link to a page that displays more results. When end-users click **Show More**, they will see more results for the result block.

b. For the placement of the block of results from SharePoint Online relative to the results from SharePoint Server 2013, do one of the following:

Note: In this case, core results are the results from SharePoint Server 2013.

- Select **This block is always shown above core results** to display the result block so that it is readily visible on the first page. By default, the result block will be shown at the top of the page. This option is useful when most of the relevant content is located in a remote system. If you select this option for more than one result block, you can configure the order in which the result blocks are displayed by ranking the associated query rules.
- Select **This block is ranked within core results (may not show)** to display the result block on the first page of search results unless the block does not rank high enough compared to core results or search results in other result blocks. This is the default option and is typically the more appropriate choice. As with individual results, the rank of the result block might be different when users perform the same query later. For example, if users click search results in the result block, the result block will be ranked higher in the search results over time. Otherwise, the result block will be ranked lower over time.

c. In the **Group Display Template** drop-down list, select a group display template.

d. In the **Item Display Template** drop-down list, select an item display template.

iv. Skip the **Routing** section.

v. Click **OK** to add the result block.

f) On the **Add Query Rule** page, in the **Publishing** section, do the following:

i. Select **Is Active**. When a query rule is active, it fires whenever the query conditions are satisfied.

ii. Optionally, specify a **Start Date**, an **End Date**, a **Review Date**, and a **Contact**.

If you do not specify a start date, the rule will be active until an end date that you specify. If you specify a start date without an end date, the rule will always be active after the start date. If you specify an end date without a start date, the rule will always be active until the end date. If you do not specify a start date or an end date, the rule will always be active.

g) Click **Save**.

After a few moments, when users submit queries from the Search Center, they will see results from there and from SharePoint Online on a search results page in the SharePoint Server 2013 farm. Also, the refinement panel on the search

results page automatically merges item counts and values from both environments and thus provides filtering for the results from both.

Validate your SharePoint Server search configuration

You can validate your search configuration and see troubleshooting information with the following procedure:

1. In Site Settings, under Site Collection Administration, click **Search Result Sources**.
2. In the **Manage Result Sources** page, click the result source you created in the previous procedure—for example, "SharePoint Online result source".
3. In the **Edit Result Source** page, click the **Launch Query Builder** button.
4. In the **Build Your Query** page, select the **Test** tab.
5. Click **Show more**.
6. Type a search term of your choice in **{subject terms}** and click the **Test Query** button.

Relevant search results will be displayed in the **Search Result Preview** window if your configuration is valid. If there are problems with your configuration, troubleshooting information will be displayed.

View hybrid search results on SharePoint Online

This section describes how to configure search functionality in a hybrid SharePoint environment so that end users can view search results in SharePoint Online from content that is in both environments.

To configure search functionality in a hybrid SharePoint environment in this way, you perform the following two procedures in SharePoint Online:

Step 1: Create a result source.

Step 2: Create a query rule that uses the result source.

Before you proceed, verify that the user account that you use to perform the procedures is a global administrator or a SharePoint Online administrator for the Office 365 subscription that you want to configure.

Step 1: Create a result source

In this procedure, you create a result source in SharePoint Online. This result source is a definition that specifies each of the following:

- The URL that is exposed through the reverse proxy, which forwards the search query to the SharePoint Server 2013 farm.
- The protocol for getting search results from the SharePoint Server 2013 farm.
- The ID of the target application that stores the reverse proxy certificate.

To create the result source

1. In the SharePoint Administration Center, in the Quick Launch, click **search**.
2. On the **search administration** page, click **Manage Result Sources**.
3. Click **New Result Source**.

   Note: Result sources can be created at the SharePoint Administration Center level, the site collection level, or the site level. In this procedure, you create the result source at the SharePoint Administration Center level in SharePoint

Online. This makes the result source available to any query rule that is created at the same level, and also to any query rule that is created for a site collection or site.

4. On the **Edit Result Source** page, do the following:

   a) In the **Name** box, type a name for the new result source—for example, "SharePoint Server 2013 result source".

   b) Optionally, in the **Description** text box, type a description of the new result source.

   c) For the **Source Information Protocol**, select **Remote SharePoint**.

   d) For the **Remote Service URL**, type the address of the root site collection that you want to search in the SharePoint Server 2013 farm, such as **https://hybrid.contoso.com**.

   e) For the **Type**, select **SharePoint Search Results**. This specifies that the search system will search the entire SharePoint Server 2013 search index when a user submits a query.

   f) For **Query Transform**, optionally type a new query transform in the text box (such as author:Geoff or path:http://myteamsite.contoso.com), or click **Launch Query Builder** to build a query template. The default template is **{searchTerms}**, which is the query that the user typed, as changed by the most recent transform.

   g) If you are connecting to your organization's intranet through a reverse proxy, for **Credentials Information**, do each of the following:

      i. Select **SSO Id**.

      ii. In the **Reverse proxy certificate (Secure Store Id)** text box, enter the name of the target application—for example, **TargetAppIDforSearchOrBCS—**that stores the Windows certificate that will be used to authenticate to the reverse proxy. For information about the name of the appropriate target application, see "Create a target application to store the SSL certificate" earlier in this white paper.

   h) Click **OK** to save the new result source.

Step 2: Create a query rule that uses the result source

In this procedure, you create a query rule that uses the result source that you created in the previous procedure. When this rule runs, it causes search results from SharePoint Online and the SharePoint Server 2013 farm to be displayed on a results page in SharePoint Online. For more information about query rules, see Overview of query processing in SharePoint Server 2013 (http://technet.microsoft.com/library/jj219620(v=office.15).

To create the query rule

1. In the SharePoint Administration Center, in the Quick Launch, click **search**.
2. On the **search administration** page, click **Manage Query Rules**.
3. On the **Manage Query Rules** page, do the following:

   a) In the **Select a Result Source** drop-down list, select the result source that you created in the previous procedure—for example, "SharePoint Server 2013 result source".

   b) Click **New Query Rule**.

Note: In this procedure, you create a query rule in SharePoint Online at the SharePoint Administration Center level. Because you are creating the rule at this level, the rule applies to any queries that users submit in this instance of SharePoint Online.

4. On the **Add Query Rule** page, do the following:

   a) In the **General Information** section, in the **Rule Name** box, type a name for the new query rule.

   b) In the **Context** section, do the following:

      i. Under **Query is on these sources**, select **All Sources** or **One of these sources**.
      Note: If you select **One of these sources**, the rule will fire only on the result sources that are listed. Therefore, you should make sure that the name of the result source that you created in the previous procedure—for example, "SharePoint Server 2013 result source"—appears in the list.

      ii. Under **Query is performed from these categories**, optionally specify the topic categories (based on terms for topic categories in the term store in a Managed Metadata service application) to perform the query from.

      iii. Under **Query is performed by these user segments**, optionally define user segments (based on terms that describe users in the term store of a Managed Metadata service application) to which you want the query rule to apply.

   c) In the **Query Conditions** section, specify conditions to control when the rule will fire, or click **Remove Condition.**
   Note: If you want the rule to fire for every query whenever the rule is active, click **Remove Condition.** (See the information about the **Is Active** setting later in this procedure.)

   d) In the **Actions** section, under **Result Blocks**, click **Add Result Block**.

   e) In the **add result block** dialog box, do the following:

      i. In the **Block Title** section, in the **Title** text box, accept the default title (which is **Results for "{subjectTerms}"**), or type a different title.

      ii. In the **Query** section, do the following:

         a. In the **Configure Query** box, use the default query (which is **{subjectTerms}**), or specify a query configuration to transform the query. You can click **Launch Query Builder** if you want Query Builder to help you configure a query transform.

         b. In the **Search this Source** drop-down list, select the name of the result source that you created in the previous procedure—for example, "SharePoint Server 2013 result source".

         c. In the **Items** drop-down list, select the number of search results from SharePoint Server 2013 that you want to show in a group on the search results page. For example, select **3** to display three results in a group from SharePoint Server 2013.

      iii. In the **Settings** section, do the following:

         a. If you want to display a **Show More** link at the bottom of the result block, select **More link goes to the following URL**, and type the URL for the link to a page that displays more results. When end-users click **Show More**, they will see more results for the result block.

b. For the placement of the block of results from SharePoint Server 2013 relative to the results from SharePoint Online, do one of the following:

- Select **This block is always shown above core results** to display the result block so that it is readily visible on the first page. In this case, core results are the results from SharePoint Online. By default, the result block will be shown at the top of the page. This option is useful when most of the relevant content is located in a remote system. If you select this option for more than one result block, you can configure the order in which the result blocks are displayed by ranking the associated query rules.
- Select **This block is ranked within core results (may not show)** to display the result block on the first page of search results unless the block does not rank high enough compared to core results or search results in other result blocks.
  This is the default option and is typically the more appropriate choice. As with individual results, the rank of the result block might be different when users perform the same query later. For example, if users click search results in the result block, the result block will be ranked higher in the search results over time. Otherwise, the result block will be ranked lower over time.

c. In the **Group Display Template** drop-down list, select a group display template.

d. In the **Item Display Template** drop-down list, select an item display template.

iv. Skip the **Routing** section.

v. Click **OK** to add the result block.

f) On the Add Query Rule page, in the **Publishing** section, do the following:

i. Select **Is Active**. When a query rule is active, it runs whenever the query conditions are satisfied.

ii. Optionally, specify a **Start Date**, an **End Date**, a **Review Date**, and a **Contact**.

The start date and end date specify when the query rule will be active. If you do not specify a start date, the rule will be active until an end date that you specify. If you specify a start date without an end date, the rule will always be active after the start date. If you specify an end date without a start date, the rule will always be active until the end date. If you do not specify a start date or an end date, the rule will always be active.

g) Click **Save**.

After a few moments, when users submit a query in SharePoint Online, they will see results from both SharePoint Online and SharePoint Server 2013 on a search results page in SharePoint Online. Also, the refinement panel on the search results page automatically merges item counts and values from both environments and thus provides filtering for the results from both.

Validate your SharePoint Online search configuration

You can validate your search configuration and see troubleshooting information with the following procedure:

1. On the SharePoint admin center page, click **Search**.
2. Under Search Administration, click **Manage Result Sources**.

3. In the Manage Result Sources page, click the result source you created in the previous procedure—for example, "SharePoint Server 2013 result source".
4. In the Edit Result Source page, under Query Transform, click the **Launch Query Builder** button.
5. In the **Build Your Query** page, type a search term of your choice in the **Query text** box and click the **Test Query** button.

Relevant search results will be displayed in the **Search Result Preview** window if your configuration is valid. If there are problems with your configuration, troubleshooting information will be displayed.