Microsoft®
SharePoint

SharePoint 2013 Business Connectivity Services Hybrid Overview

Christopher J Fox
Microsoft Corporation

November 2012

Applies to: SharePoint 2013, SharePoint Online

Summary: A hybrid SharePoint environment consists of a SharePoint 2013 farm that is deployed on-premises, and a Microsoft Office 365 SharePoint Online tenancy. The integration of SharePoint 2013 on-premises and SharePoint Online allows you to use Business Connectivity Services to securely publish internal Line of Business (LOB) data to SharePoint Online.

Contents

Business Drivers

A Business Connectivity Services (BCS) Hybrid solution enables you to securely publish internal LOB data to your users in SharePoint Online. It solves a very specific business problem in a certain way. This section helps you understand this solution and when you should use it.

What is a SharePoint Business Connectivity Services Hybrid Solution?

If your company has an on-premises SharePoint 2013 farm and a SharePoint Online 2013 tenancy, you can create a secure connection between the two to make line-of-business (LOB) data available, by using BCS, to applications for SharePoint and external lists in SharePoint Online. This is called a SharePoint BCS Hybrid solution. SharePoint Online 2013 supports only one-way connections from online to on-premises and to only one on-premises farm. The LOB data must be published as an OData source.

Why use a SharePoint BCS Hybrid Solution?

A SharePoint 2013 BCS Hybrid solution provides a bridge for companies that want to take advantage of cloud-based SharePoint Online to access on-premises LOB data while keeping that proprietary data safe maintained on their corporate intranet. The SharePoint BCS Hybrid solution does not require opening holes in the firewall to allow traffic through and it does not require you to move your LOB data out into the perimeter network. The SharePoint BCS Hybrid solution uses the on-premises BCS services to connect to the LOB data and then, through a reverse proxy, securely publish the endpoint out to the BCS services in SharePoint Online 2013.

.

BCS Hybrid Architecture

The BCS Hybrid solution has components in the Cloud in Office 365 and On-Premises.

Office 365 and SharePoint Online

- O365 – Every Microsoft Office 365 subscription hosts a SharePoint Online tenancy. The O365 subscription also provides the Access Control Service (ACS) and Microsoft Online Directory Services (MSODS).
- SharePoint Online – Hosts the sites that surface the on-premises LOB data, the BCS runtime service and metadata store, and the Secure Store Service.
- BCS Runtime Service Online - The BCS runtime service is a SharePoint service application that manages all BCS functionality, such as administration, security, and communications.
- O365 Microsoft Online Directory Services (MSODS) – Provides directory services in O365 that you can synchronize with your on-premises Active Directory Domain Services (AD DS). The synchronization is done through user profile synchronization and allows users to use the same account for both on-premises and cloud authentication.
- SharePoint Online Secure Store Service – This is the credential mapping SharePoint service application. In the SharePoint BCS Hybrid solution, SharePoint Online stores an SSL Server certificate that authenticates the SharePoint Online request to the reverse proxy.
- Azure Access Control Service – This the Azure security token service that performs authentication and issues security tokens when a user logs in to a SharePoint Online site. It looks up credentials in the MSODS, which has been synchronized with the on-premises Active Directory accounts. This allows the user to use the same set of credentials for both the on-premises and online environments.

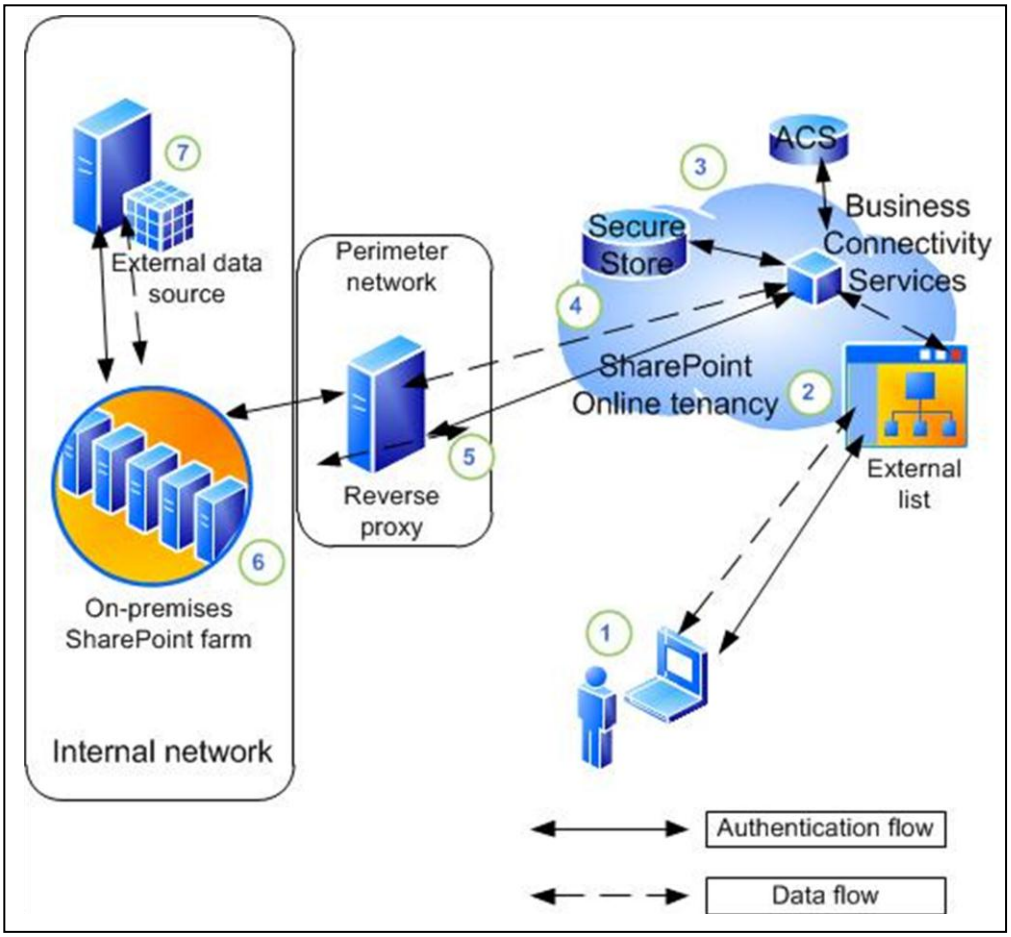
On-Premises

- Reverse Proxy – This server is responsible for accepting and authenticating inbound traffic from the Internet and publishing out the endpoint for the inbound request to connect to. It is in the perimeter network.
- SharePoint On-Premises – A SharePoint 2013 server farm, this hosts the BCS service, the site that accepts the inbound hybrid requests and the Secure Store Service.
- AD DS – A Windows Server service that stores and manages user accounts, security groups, distribution groups, and computer accounts.
- User Profile Store – A SharePoint database used to store user profile information. User profiles contain detailed information about people in an organization. A user profile organizes and displays all of the properties related to each user, together with social tags, documents, and other items related to that user. In the BCS Hybrid scenario, it is used to map the users ACS OAuth credentials to the users' domain credentials.

- CSOM Pipeline – The Client-Side Object Model receives the incoming request from the reverse proxy and maps the OAuth user token from ACS to the users' domain credentials.
- Site/Site Collection – A site collection created expressly for the purpose of facilitating all hybrid request communication. The web application that this site collection is in has an alternate access mapping configured.
- BCS Runtime Service SharePoint On-Premises – The BCS Runtime service is a SharePoint service application that manages all BCS functionality, such as administration, security, and communications.
- Secure Store Service SharePoint On-Premises – This is the credential mapping SharePoint service application. In the SharePoint BCS Hybrid solution, SharePoint On-Premises stores the mapping of the users' domain credentials to the credentials that are used to access the external data source.
- OData Service Head – The SharePoint BCS Hybrid Solution only supports the OData protocol. If your external data is not natively accessible via an OData source, you must use Visual Studio to build and deploy an OData service head for it.
- External Data – The line-of-business (LOB) data that the SharePoint BCS Hybrid solution works with.

BCS Hybrid Data Flow

In SharePoint Online, you make external data available through external lists or apps for SharePoint. This example uses an external list.



1. An information worker logs on to their SharePoint Online tenancy and opens an external list which requires data from an on-premises OData source.
2. The external list creates a request for the data and sends it to Business Connectivity Services. BCS looks at the request and refers to the external content type and the connection settings object to see how to connect to the data source and which credentials to use.
3. Business Connectivity Services retrieves a client certificate from the Secure Store service in SharePoint Online. The client certificate is an SSL certificate and it is used for authentication to the reverse proxy. BCS also retrieves an OAuth token form the Access Control Service. These are the uses credentials which are used for user authentication to the SharePoint 2013 on-premises farm.

4. The Business Connectivity Service sends a HTTPS request to the endpoint for the data source that is published by the reverse proxy.
5. The reverse proxy authenticates the request by using the client certificate and forwards it to the Client Side Object Model (CSOM) pipeline of the on-premises SharePoint 2013 farm.
6. The CSOM pipeline consults the User Profile Service to look for a mapping between the users OAuth security token from ACS and the user's domain credentials from AD DS. If one exists, the user's domain credentials are returned to the request. The user's domain credentials are used to authenticate to the SharePoint on-premises Site that receives Hybrid requests and the request is passed to the SharePoint On-Premises BCS service.
7. The SharePoint On-Premises BCS retrieves the credentials that are used to authenticate to the external data source from the SharePoint On-Premises Secure Store Service. Then SharePoint on-premises BCS service passes the request for data along with the external data credentials to the OData service head which then performs the desired operations on the external data and returns the results to the SharePoint Online user.

Types of Certificates and Credentials

The BCS hybrid solution is a combination of the SharePoint Hybrid configuration and a BCS configuration. Each configuration requires different sets of certificates and user credentials and you need both sets in order for the BCS Hybrid solution to work.

Server and SharePoint Certificates

SSL certificate - This certificate is used to establish trust for the communication channel between the reverse proxy device and O365. This can be a wild card certificate; it should be from a well-known certificate authority.

Server to Server – Server-to-Server authentication configuration for SharePoint Hybrid environments consists of establishing a trust between SharePoint on-premises and Access Control Service (ACS). ACS is then the trust broker for both SharePoint on-premises and SharePoint Online server. When Server-to-Server trust is fully configured, each server farm trusts the security tokens that are issued by ACS and are used for authenticating access to resources on behalf of the identified user.

User Credentials

OAuth security token from ACS – When a user logs on to SharePoint Online, the user is authenticated by ACS. ACS issues an OAuth security token, which represents the user to all SharePoint Online processes and objects that the user tries to access. This security token is embedded in the request for external data and passed, along with the SSL certificate, to the

reverse proxy. From there, it is passed to the Client-Side Object Model (CSOM) pipeline in SharePoint on-premises and is mapped to the users domain credentials

Users Active Directory credentials – This is another security token that represents the user in the user's Active Directory domain. It represents the user to all domain resources that the user tries to access. In the SharePoint BCS Hybrid configuration, it is used to authenticate the user to SharePoint on-premises.

External Data Credentials - The OData service is secured by using either basic authentication or Windows authentication, or by using a custom authentication provider.