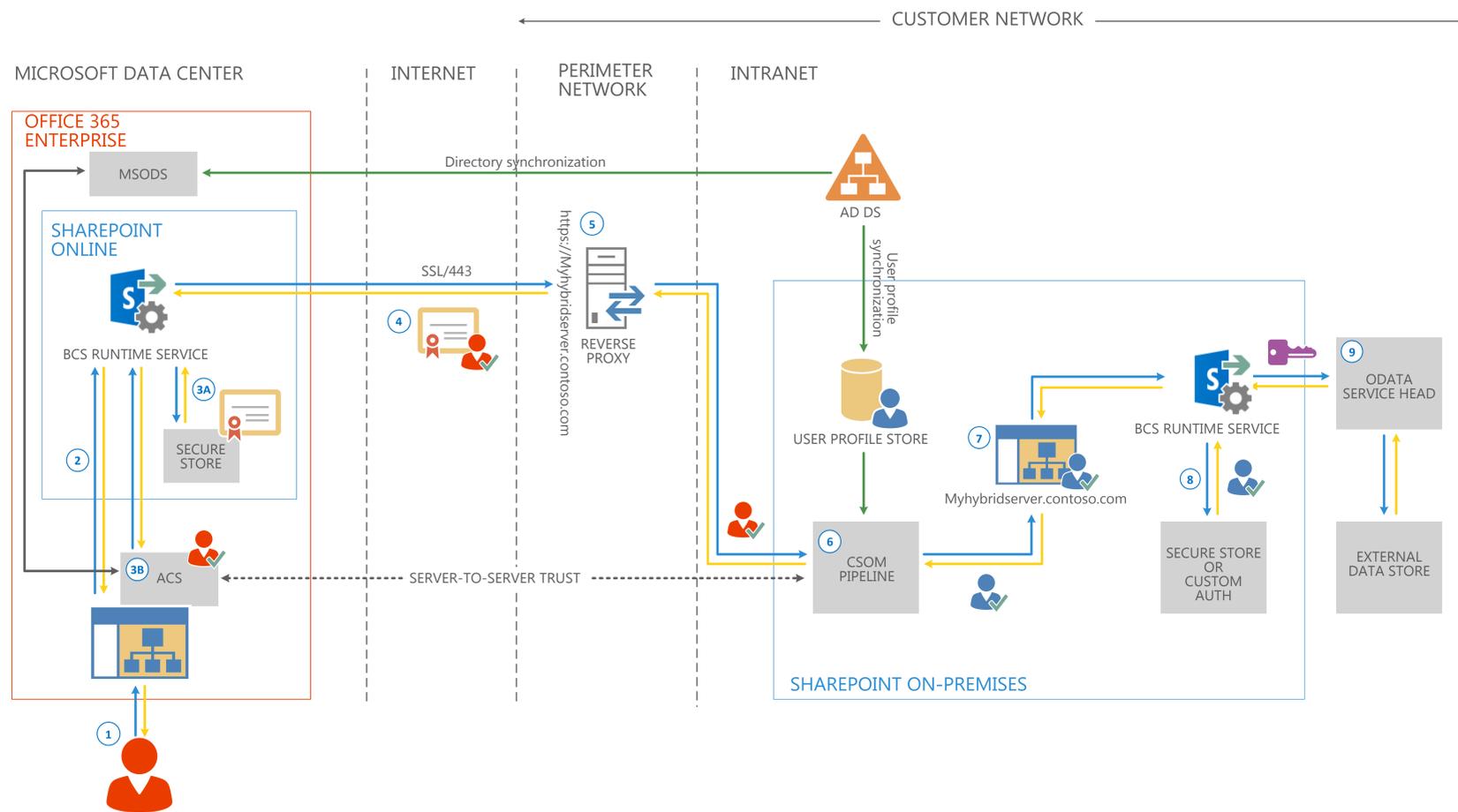


Business Connectivity Services Hybrid Flow in SharePoint 2013



BCS Hybrid Flow



BCS FLOW LIST

- 1 An information worker logs on to the user's SharePoint Online tenancy and opens an app for SharePoint or external list that needs data from an on-premises OData data source.
- 2 The external list creates a request for the data and sends it to Business Connectivity Services. BCS looks at the connection settings object and the external content type to see how to connect to the data source and what credentials to use.
- 3A BCS retrieves the client SSL certificate from the Secure Store in SharePoint Online. This is used for SharePoint Online authentication to the reverse proxy.
- 3B BCS retrieves an OAuth token from the Access Control Service. This is the user's credentials used for user authentication to the SharePoint 2013 on-premises farm. The Access Control Service is part of every SharePoint Online subscription. It is a Security Token Service that manages security tokens for users of SharePoint Online.
- 4 BCS sends an HTTPS request to the published endpoint for the data source. The request includes the client certificate from the Secure Store and the user's OAuth security token as well as a request for the data.
- 5 The reverse proxy authenticates the request by using the client certificate and forwards it to the 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 user's OAuth security token from the Access Control Service and the user's domain credentials from AD DS. If one exists, the user's domain credentials are returned to the request.
- 7 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.
- 8 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.
- 9 The 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.

LEGEND

- REQUEST
- RESPONSE
- USER PROFILE SYNC AND DIRECTORY SYNCH
- 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.
- OAUTH 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 user's 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.

Overview of Hybrid BCS

Business Drivers

What is a SharePoint Business Connectivity Services (BCS) Hybrid solution?
If your company has an on-premises SharePoint 2013 farm and a SharePoint Online 2013 tenancy, you can use BCS to create a secure connection between the two to make line-of-business (LOB) data available 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 safely 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 the 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 it through a Client-Side Object Model (CSOM) endpoint out to the BCS services in SharePoint Online.

Hybrid BCS Flow Components

Office 365 and SharePoint Online Components

Azure Access Control Service This is 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 Microsoft Online Directory Services (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.

BCS Runtime Service Online The BCS runtime service is a SharePoint service application that manages all BCS functionality, such as administration, security, and communications.

Office 365 Every Microsoft Office 365 subscription hosts a SharePoint Online tenancy. The Office 365 subscription also provides the Access Control Service (ACS) and Microsoft Online Directory Services (MSODS).

Office 365 Microsoft Online Directory Services (MSODS) Provides directory services in Office 365 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 Hosts the sites that surface the on-premises LOB data, the BCS runtime service and metadata store, and the Secure Store Service.

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.

On-Premises Components

AD DS A Windows Server service that stores and manages users accounts, security groups, distribution groups, and computer accounts.

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.

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.

External Data The line-of-business (LOB) data that the SharePoint BCS Hybrid solution works with.

OData Service Head The SharePoint BCS Hybrid solution only supports the OData protocol. If the 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.

Reverse Proxy This server is responsible for accepting and authenticating inbound traffic from the Internet and publishing out the CSOM service endpoint for the inbound request to connect to. It is in the perimeter network.

On-Premises Components

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.

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.

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.

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.

Directory and User Profile

Directory Synchronization The BCS Hybrid solution depends on the on-premises Active Directory being synchronized with MSODS. This allows the users to log on to SharePoint Online by using the same user principal name (UPN) as they use for on-premises authentication.

User Profile Synchronization The SharePoint user profile service pulls user information from Active Directory into SharePoint, making it available for SharePoint User Profiles. The BCS Hybrid solution depends on Active Directory information being available in the user profile store for the CSOM pipeline to perform the user OAuth credential to user domain credential mapping.

