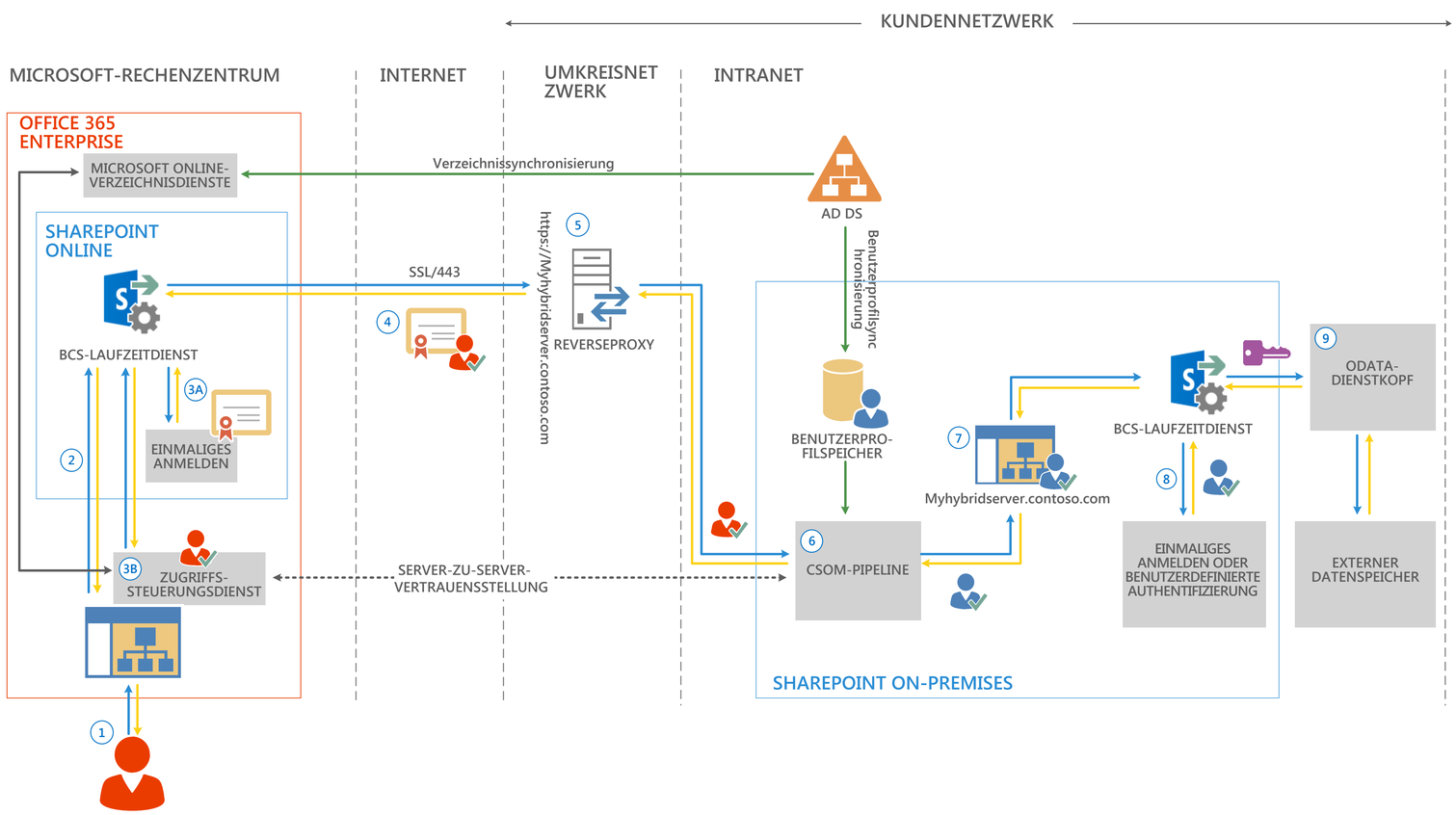
Hybridfluss bei Business Connectivity Services

in SharePoint 2013

BCS-Hybridfluss



BCS-FLUSSLISTE

1. Information Worker melden sich bei der SharePoint Online-Benutzerinstanz an und öffnen eine App für SharePoint oder eine externe Liste, die Daten von einer lokalen OData-Datenquelle benötigt.
2. Die externe Liste erstellt eine Anforderung für die Daten und sendet diese zu Business Connectivity Services. BCS überprüft das Objekt für die Verbindungseinstellung und den externen Inhaltstyp, um zu ermitteln, wie eine Verbindung zur Datenquelle hergestellt werden kann und welche Anmeldedaten zu verwenden sind.
3A. BCS ruft das Client-SSL-Zertifikat von Secure Store in SharePoint Online ab. Dies wird für die SharePoint Online-Authentifizierung beim Reverseproxy verwendet.
3B. BCS ruft ein OAuth-Token vom Zugriffssteuerungsdienst ab. Dies sind die Benutzeranmeldedaten, die für die Benutzerauthentifizierung bei der lokalen SharePoint 2013-Farm verwendet werden. Der Zugriffssteuerungsdienst ist Teil jedes SharePoint Online-Abonnements. Es handelt sich um einen Sicherheitstokendienst, der Sicherheitstoken für SharePoint Online-Benutzer verwaltet.
4. BCS sendet eine HTTPS-Anforderung an den veröffentlichten Endpunkt für die Datenquelle. Die Anfrage umfasst das Clientzertifikat von Secure Store, das OAuth-Sicherheitstoken des Benutzers sowie eine Anfrage für die Daten.
5. Der Reverseproxy authentifiziert die Anfrage mit dem Clientzertifikat, das an die CSOM-Pipeline der lokalen SharePoint 2013-Farm weitergeleitet wird.
6. Die CSOM-Pipeline prüft beim Benutzerprofildienst, ob eine Verknüpfung zwischen dem OAuth-Sicherheitstoken des Benutzers vom Zugriffssteuerungsdienst und den Domänenanmeldeinformationen des Benutzers von AD DS besteht. Ist eine vorhanden, werden die Domänenanmeldeinformationen der Anfrage zurückgegeben.
7. Die Domänenanmeldeinformationen des Benutzers werden verwendet, um eine Authentifizierung für die SharePoint On-Premises-Website auszuführen, die Hybridanfragen erhält. Die Anfrage wird dann dem BCS-Dienst für SharePoint On-Premises weitergeleitet.
8. Die SharePoint On-Premises BCS-Dienste rufen die Anmeldeinformationen ab, die für die Authentifizierung bei der externen Datenquelle vom SharePoint On-Premises-Secure Store Service verwendet werden.
9. Der SharePoint On-Premises BCS-Dienst leitet die Datenanfrage mit den Anmeldeinformationen für externe Daten an den OData-Dienstkopf weiter, der dann die gewünschten Operationen bei den externen Daten ausführt und die Ergebnisse dem SharePoint Online-Benutzer zurückgibt.

LEGENDE

- ANFORDERUNG
- REAKTION
- BENUTZERPROFIL- UND VERZEICHNISSYNCHRONISIERUNG

SSL-ZERTIFIKAT – Dieses Zertifikat wird verwendet, um eine Vertrauensstellung für den Kommunikationskanal zwischen dem Reverseproxy und Office 365 aufzubauen. Dabei kann es sich um ein Platzhalterzertifikat handeln. Es sollte von einer bekannten Zertifizierungsstelle stammen.

Die Konfiguration der **Server-zu-Server**-Authentifizierung für SharePoint-Hybridumgebungen besteht darin, eine Vertrauensstellung zwischen SharePoint On-Premises und dem Zugriffssteuerungsdienst aufzubauen. Der Zugriffssteuerungsdienst ist damit für das Herstellen einer Vertrauensstellung sowohl bei SharePoint On-Premises- als auch bei SharePoint Online-Servern verantwortlich. Wenn die Server-zu-Server-Vertrauensstellung vollständig konfiguriert ist, vertraut jede Serverfarm den Sicherheitstoken, die vom Zugriffssteuerungsdienst ausgegeben und für die Authentifizierung des Ressourcenzugriffs im Namen des identifizierten Benutzers verwendet werden.

OAUTH-TOKEN VOM ZUGRIFFSSTEUERUNGSDIENST – Wenn sich Benutzer bei SharePoint Online anmelden, werden sie vom Zugriffssteuerungsdienst authentifiziert. Der Zugriffssteuerungsdienst erstellt ein OAuth-Sicherheitstoken, das den Benutzer für alle SharePoint Online-Prozesse und -Objekte repräsentiert, auf die der Benutzer zugreifen möchte. Dieses Sicherheitstoken ist in der Anfrage für externe Daten eingebettet und wird mit dem SSL-Zertifikat an den Reverseproxy weitergeleitet. Von dort aus wird es der Pipeline des clientseitigen Objektmodells (CSOM) in SharePoint On-Premises weitergeleitet und den Domänenanmeldeinformationen des Benutzers zugeordnet.

ACTIVE DIRECTORY-ANMELDEINFORMATIONEN VON BENUTZERN – Dies ist ein weiteres Sicherheitstoken, mit dem der Benutzer in seiner Active Directory-Domäne dargestellt wird. Es repräsentiert den Benutzer für alle Domänenressourcen, auf die der Benutzer zugreifen möchte. In der SharePoint BCS-Hybridkonfiguration wird es zur Authentifizierung des Benutzers bei SharePoint On-Premises verwendet.

EXTERNE DATENANMELDEINFORMATIONEN – Der OData-Dienst wird entweder mit der Standardauthentifizierung, der Windows-Authentifizierung oder mit einem benutzerdefinierten Authentifizierungsanbieter gesichert.

Übersicht über die BCS-Hybridlösung

Betriebswirtschaftliche Faktoren

Was ist eine SharePoint Business Connectivity Services-Hybridlösung (BCS)?

Wenn Ihr Unternehmen über eine lokale SharePoint 2013-Farm und eine SharePoint Online 2013-Instanz verfügt, können Sie BCS verwenden, um eine sichere Verbindung zwischen beiden herzustellen und so Branchendaten für SharePoint-Anwendungen und externe Listen in SharePoint Online zur Verfügung zu stellen. Dies wird als SharePoint BCS-Hybrid-Lösung bezeichnet. SharePoint Online 2013 unterstützt nur unidirektionale Verbindungen von der Onlineinstanz zur lokalen Lösung und nur zu einer lokalen Farm. Die Branchendaten müssen als OData-Quelle veröffentlicht werden.

Was spricht für eine SharePoint BCS-Hybridlösung?

Eine SharePoint 2013 BCS-Hybridlösung bildet eine Art Brücke für Unternehmen, die das Cloud-basierte SharePoint Online für den Zugriff auf lokale Branchendaten nutzen und gleichzeitig diese unternehmenseigenen Daten sicher im Unternehmensnetzwerk verwalten möchten. Für die SharePoint BCS-Hybridlösung sind keine Öffnungen in der Firewall für Datenverkehr notwendig, und Sie müssen auch nicht die Branchendaten in das Umkreisnetzwerk verschieben. Die SharePoint BCS-Hybridlösung verwendet die lokalen BCS-Dienste, um eine Verbindung zu den Branchendaten herzustellen, und veröffentlicht diese dann über einen Reverseproxy und einen Endpunkt für ein clientseitiges Objektmodell (Client-Side Object Model, CSOM) sicher in den BCS-Diensten in SharePoint Online.

Hybrid BCS-Flusskomponenten

Office 365- und SharePoint Online-Komponenten

Azure-Zugriffssteuerungsdienst Dabei handelt es sich um den Azure-Sicherheitstokendienst, der die Authentifizierung ausführt und Sicherheitstoken ausgibt, wenn Benutzer sich bei einer SharePoint Online-Website anmelden. Dieser sucht die Anmeldeinformationen in den Microsoft Online-Verzeichnisdiensten (MSODS, Microsoft Online Directory Services), die mit den lokalen Active Directory-Konten synchronisiert wurden. Dadurch können Benutzer für die lokalen und Onlineumgebungen dieselben Anmeldeinformationen verwenden.

BCS-Onlinelaufzeitdienst Der BCS-Laufzeitdienst ist eine SharePoint-Dienstanwendung, mit der alle BCS-Funktionen wie Administration, Sicherheit und Kommunikation verwaltet werden.

Office 365 Für jedes Microsoft Office 365-Abonnement wird eine SharePoint Online-Instanz gehostet. Das Office 365-Abonnement umfasst auch den Zugriffssteuerungsdienst und die Microsoft Online-Verzeichnisdienste (MSODS).

Microsoft Online-Verzeichnisdienste (MSODS) für Office 365 Bietet Verzeichnisdienste in Office 365, die Sie mit Ihren lokalen Active Directory-Domänendiensten (AD DS, Active Directory Domain Services) synchronisieren können. Die Synchronisierung erfolgt über die Benutzerprofilsynchronisierung. Benutzer können außerdem für die lokale und die Cloud-Authentifizierung dasselbe Konto verwenden.

SharePoint Online hostet die Websites, auf denen die lokalen Branchendaten, der BCS-Laufzeitdienst, der Metadatenspeicher sowie Secure Store Service dargestellt werden.

SharePoint Online-Secure Store Service Dies ist die SharePoint-Dienstanwendung für die Zuordnung von Anmeldeinformationen. In der SharePoint BCS-Hybridlösung speichert SharePoint Online ein SSL-Serverzertifikat, mit dem die SharePoint Online-Anfrage beim Reverseproxy authentifiziert wird.

Lokale Komponenten

AD DS Ein Windows Server-Dienst, der Benutzerkonten, Sicherheits- und Verteilungsgruppen sowie Computerkonten speichert und verwaltet.

BCS-Laufzeitdienst für SharePoint On-Premises Der BCS-Laufzeitdienst ist eine SharePoint-Dienstanwendung, mit der alle BCS-Funktionen wie Administration, Sicherheit und Kommunikation verwaltet werden.

CSOM-Pipeline Das clientseitige Objektmodell empfängt die eingehende Anfrage vom Reverseproxy und ordnet das OAuth-Benutzertoken vom Zugriffssteuerungsdienst den Domänenanmeldeinformationen der Benutzer zu.

Externe Daten Die Branchendaten, die die SharePoint BCS-Hybridlösung verwendet.

OData-Dienstkopf Die SharePoint BCS-Hybridlösung unterstützt nur das OData-Protokoll. Wenn auf die externen Daten nicht direkt über eine OData-Quelle zugegriffen werden kann, verwenden Sie Visual Studio, um für die Daten einen OData-Dienstkopf zu erstellen und zu implementieren.

Reverseproxy Dieser Server ist verantwortlich für das Akzeptieren und Authentifizieren von eingehendem Datenverkehr aus dem Internet sowie für das Veröffentlichen des CSOM-Dienstendpunkts für die eingehende Anfrage, zu der eine Verbindung hergestellt werden soll. Er befindet sich im Umkreisnetzwerk.

Lokale Komponenten

Secure Store Service-SharePoint On-Premises Dies ist die SharePoint-Dienstanwendung für die Zuordnung von Anmeldeinformationen. In der SharePoint BCS-Hybridlösung speichert SharePoint On-Premises die Zuordnung der Domänenanmeldeinformationen des Benutzers bei den Anmeldeinformationen, die für den Zugriff der externen Datenquelle verwendet werden.

SharePoint On-Premises Eine SharePoint 2013-Serverfarm. Hier wird der BCS-Dienst gehostet; die Website, die eingehende Hybridanfragen und Secure Store Service akzeptiert.

Website/Websitesammlung Eine Websitesammlung, die ausdrücklich zur Unterstützung der gesamten Kommunikation mit Hybridanfragen erstellt wurde. Für die Webanwendung, in die diese Websitesammlung eingebunden ist, ist eine alternative Zugriffszuordnung konfiguriert.

Benutzerprofilspeicher Eine Profildatenbank, in der Benutzerprofilinformationen gespeichert werden. Benutzerprofile enthalten detaillierte Informationen zu Personen in einer Organisation. In einem Benutzerprofil werden alle Eigenschaften des jeweiligen Benutzers sowie thematische Kategorien, Dokumente und andere Elemente im Zusammenhang mit diesem Benutzer organisiert. Im BCS-Hybridszenario dient er zum Zuordnen der OAuth-Anmeldeinformationen des Benutzers vom Zugriffssteuerungsdienst zu den Domänenanmeldeinformationen des Benutzers.

Synchronisierung von Verzeichnissen und

Verzeichnissynchronisierung Die BCS-Hybridlösung hängt von dem lokalen Active Directory ab, das mit MSODS synchronisiert wird. Dadurch können sich Benutzer bei SharePoint Online mit demselben Benutzerprinzipalnamen (UPN, User Principal Name) anmelden, den sie bei der lokalen Authentifizierung verwenden.

Benutzerprofilsynchronisierung Der SharePoint-Benutzerprofildienst ruft Benutzerinformationen von Active Directory für SharePoint ab und stellt sie so für SharePoint-Benutzerprofile zur Verfügung. Die BCS-Hybridlösung hängt von Active Directory-Informationen ab, die im Benutzerprofilspeicher für die CSOM-Pipeline zur Verfügung stehen, um die Zuordnung von OAuth-Benutzeranmeldeinformationen mit Benutzerdomänen-Anmeldeinformationen auszuführen.