SHAREPOINT HYBRID AND IMPLICATIONS OF 2016

Dan Charlton
Senior Consultant
MCSE, MCSA, MCP
• SharePoint Consulting & Development Organization
  • Design
  • Development
  • Administration
  • Management Consulting

• Clients
  • International government agencies
  • Major universities
  • Fortune 100 organizations

• Family owned and operated
• Project Types
  • Design & Consulting
  • Intranets & Extranets
  • Collaboration
  • Enterprise Content Management
  • Application / Workflow Development
  • Reporting & Dashboards
  • Governance & Security Frameworks
  • Branding & UI / UX
  • Business Process Management
  • Migrations
  • Systems Integration
Graduated from Michigan State University in December 2007

Worked in IT 5+ years

Worked at Total Solutions 3+ years

Microsoft Certified Professional

Microsoft Certified Solutions Associate: Office 365

Microsoft Certified Solutions Expert: SharePoint

Certified Scrum Master

Certified Scrum Product Owner
“With SharePoint Server 2013 hybrid, productivity services in SharePoint Online can be integrated with on-premises SharePoint Server 2013 to provide unified functionality and access to data. For enterprises that want to gradually move their existing on-premises SharePoint Server 2013 services to the cloud, SharePoint Server 2013 hybrid provides a staged migration path by extending high-impact SharePoint Server 2013 workloads to SharePoint Online.”

--TechNet
WHAT DOES THAT ACTUALLY MEAN?

SharePoint Hybrid environments consist of some main elements:

- Common Identity Management
- Integrated Services (Search, Business Connectivity, Duet Enterprise)
- New for 2016: Extending cloud-only services (like Delve) to on-premise content

What is this NOT?

- A unified navigation solution
- A means of data replication
- A means of high availability or failover capacity
WHY WOULD MY COMPANY WANT HYBRID?

- We want to do away with on-premises resources over time.
- We have regulatory constraints that require us to keep certain data in-house.
- We want our users to have better access to enterprise content.
- We have a ton of data that would make full-cloud too expensive.
- We want to reduce unsanctioned tech usage.
- We can’t get enough of techie buzz terms like ‘hybrid’ and ‘cloud’.

Copyright 2016 Total Solutions Inc. All Rights Reserved.
An outbound authentication topology lets the on-premises SharePoint Server 2013 farm make authenticated connections to SharePoint Online.

Connections to SharePoint Online that originate from SharePoint Server 2013 are referred to as **outbound connections**.
An inbound authentication topology lets SharePoint Online make authenticated connections to the on-premises SharePoint Server 2013 farm.

Connections to SharePoint Server 2013 that originate from SharePoint Online are referred to as **inbound connections**.
WHAT TYPES OF HYBRID ARE AVAILABLE?

A two-way authentication topology lets SharePoint Online make authenticated connections to the on-premises SharePoint Server 2013 farm and lets the on-premises SharePoint Server 2013 farm make authenticated connections to SharePoint Online.
HOW DO TOPOLOGIES WORK IN PRACTICE?

- **Outbound:**
  - Using SharePoint Online for external user portals
  - Isolating secure content for access on-premise (or over VPN) only
  - Isolating only specific content as available for cloud users

- **Inbound:**
  - SharePoint Server used only for searching on-premise content (i.e. file shares)
  - Maintaining existing Server Side Object Model applications
  - Making on-premise database content available to SharePoint Online

- **Two-Way:**
  - Everything can be available to both environments
  - Risks over-exposing content or interfering with the user experience
WHAT TOPOLOGY IS RIGHT FOR MY BUSINESS?

- Do your users need to be able to search, find, and use on-premises content and data while they’re in the field or at a branch office?
- Do your remote users need to securely access data from existing on-premises business systems?
- Is it more cost effective to deploy a hybrid environment or to move your SharePoint content and applications to the cloud entirely?
- Are there legal or regulatory considerations that could affect your decision on where to store business data?
- Does your SharePoint Server 2013 farm contain custom code that cannot be easily migrated to SharePoint Online?
WHAT SERVICES CAN INTEGRATE?

SharePoint Search Service
- Provides a single, central location to manage search across both online and on-premises content.
- Integration with search-driven cloud-only services like Delve and Office-Graph.
- Allows query processing and index hosting to be offloaded to the cloud, reducing the on-premise workload.
- Relies on on-premise servers to index on-premise content and supplies the index to cloud-based services.
- Unified relevancy ranking of all indexed content from all locations (including, potentially, multiple on-premise SharePoint farms).

Business Connectivity Services
- Allows users in the cloud to connect to an on-premises ODBC data source for both read and write operations.
- Most effective means of securely surfacing on-premises databases in SharePoint Online without resorting to custom code.
WHAT SERVICES CAN INTEGRATE?

Duet Enterprise Online
- Allows users in the cloud to connect to an on-premises SAP system for both read and write operations.
- Only Microsoft-backed means of connecting SAP content to SharePoint Online.

On-premise Exchange and/or Lync Deployments
- Allows SharePoint Online to fall back on on-premises Office-suite resources rather than the native Office 365 counterparts.
- Allows for additional (potentially legally required) control over the Exchange or Lync configuration.
- Only Microsoft-backed means of integrating Lync-backed phone systems with SharePoint Online.
- Presence information permeates across both environments.
WHAT SERVICES CAN INTEGRATE?

OneDrive for Business

- Allows all OneDrive for business content (i.e. the user’s personal files) to be hosted in the cloud.
- Includes 1TB of storage per user.
- Ensures users can access their files from anywhere.
- Provides secure means of making files available to external users.
- New for 2016: Site Folders provides integrated location for browsing all SharePoint files.

Social and User Profiles

- Allows all user profiles to exist in the cloud (rather than a separate profile for each environment).
- New for 2016: unification of followed sites.
- New for 2016: unification of Delve content.
WHAT ELSE CAN IT DO (NEW FOR 2016)?

- Improved Information Rights Management spanning both pieces of hybrid
  - Search and identify sensitive content across SharePoint Server, SharePoint Online, and OneDrive for Business.
  - Apply IRM policies that persist across the locally synced content divide of One Drive for Business.
  - New Compliance Center and In-Place Policy Hold Center sites provide improved methods for defining, applying, and auditing IRM operations.

- UI Changes bring more consistent experience
  - On-premise document libraries gain the 365 extra buttons.
  - On-premise sites gain the App launcher and can add additional business applications that persist in both environments.
  - Suite bar can be themed in both environments.
WHAT CAN NOT INTEGRATE?

- Web Applications, Site Collections, Sites, Lists/Libraries
- Office Online
- Managed Metadata
  - Managed Metadata based navigation
  - Content Type Hubs
- Server Side Object Model Solutions (sort of)
- Workflow Features (sort of)
OTHER HYBRID CONSIDERATIONS
WHAT DO WE NEED FOR HYBRID?

The Obvious:
- SSL-secured On-Premise deployment of SharePoint Server 2013
- Office 365 subscriptions with SharePoint Online licenses
- On-premise SharePoint Server license

The Technical:
- Common Identity Management:
  - On-Premise deployment of Active Directory
  - On-Premise deployment of DirSync
  - On-Premise deployment of ADFS
- Integrated Services:
  - Reverse Proxy Server
  - Server-to-Server (STS) certificate trust
WHAT IS COMMON IDENTITY MANAGEMENT?

If you have existing user accounts in an on-premises directory, you don’t want to re-create all of those accounts in Office 365 and risk introducing differences or errors between the environments. Directory synchronization helps you mirror those accounts between your online and on-premises environments.

If you want users to be able to log on to Office 365 with their on-premises credentials, you can also configure SSO. With SSO, Office 365 is configured to trust the on-premises environment for user authentication. SSO requires an implementation of ADFS 2.0.
SharePoint 2016 supports Azure Active Directory (AAD) authentication by default.

Azure Active Directory Services Preview allows for cloud-hosted domains.
- On-premise machines are able to join domain.
- Currently the standard implementation for Windows 10 installation when setup with an Office 365 user account.

SharePoint Server 2016 can be installed on Azure VMs or on premise and join an Azure-hosted domain.

All authentication and identity management handled in Azure.

Eliminates the need for on-premise Active Directory deployments.
Reverse proxy devices play a role in the secure configuration of a hybrid SharePoint Server 2013 deployment when inbound traffic from SharePoint Online needs to be relayed to your on-premises SharePoint Server 2013 farm.
WHAT REVERSE PROXIES ARE SUPPORTED?

General Requirements:
- Support client certificate authentication with a wildcard or SAN SSL certificate.
- Support pass-through authentication for OAuth 2.0, including unlimited OAuth bearer token transactions.
- Accept unsolicited inbound traffic on **TCP port 443** (HTTPS).
- Bind a wildcard or SAN SSL certificate to a published endpoint.
- Relay traffic to an on-premises SharePoint Server 2013 farm or load balancer without rewriting any packet headers.

Specific Devices:
- Windows Server 2012 R2 with Web Application Proxy (WA-P)
- Forefront Threat Management Gateway (TMG) 2010
- F5 BIG-IP
- Citrix NetScaler
WHAT ABOUT CERTIFICATE TRUSTS?

When you set up server-to-server authentication for hybrid environments, you create a trust relationship between your on-premises SharePoint farm and your SharePoint Online tenant, which uses Azure Active Directory as a trusted token signing service.
HOW DID WE WANT HYBRID AGAIN?

- Want to move to the cloud in the long term
- Want to maintain existing on-premise applications
- Want to improve off-premise accessibility
- Want to reduce on-premise resource requirements
- Want 1TB of user OneDrive storage without massive hard drive farms
- Want to stay on latest software without major re-investments
WHAT OTHER GOODIES ARE IN SHAREPOINT 2016?

- **MinRoles**
  - Allows each server in the farm to serve a specific role
  - Provides compliance monitoring and enforcement features

- **Improved SMTP handling**
  - Allows for encrypted SMTP traffic
  - Allows for traffic on ports other than 25

- **Zero downtime patching**
  - Patch services individually
  - Install without stopping services

- **Touch-enabled mobile view**

- **Encryption with TLS 1.2**
WHAT OTHER GOODIES ARE IN SHAREPOINT 2016?

- Durable Links with Office Online Server
- Increased boundaries
  - Scale content DBs larger (current best practice is 250GB, this is likely to scale into the TBs)
  - Up to 100,000 site collections per content DB
  - List view threshold changes
  - File size and name handling changes
    - Files up to 10GB (up from 2GB)
    - Removed file naming limitations
  - Doubled search index size to 500 million items per index
- Faster site deployment
- Support for Open Document Format (ODF) files
RESOURCES

Overview of hybrid SharePoint 2013 for technical decision makers

Office 365 integration with on-premises environments

Integrating your on-premises identities with Azure Active Directory

Configure a reverse proxy device

Configure server-to-server authentication

Display hybrid search results

Deploy a Business Connectivity Services hybrid solution in SharePoint 2013

Configure hybrid Duet Enterprise Online