Microsoft Hybrid Cloud for Enterprise Architects

What IT architects need to know about hybrid scenarios using Microsoft cloud services and platforms

This topic is 1 of 5 in a series

Hybrid cloud overview

Hybrid cloud uses compute or storage resources on your on-premises network and in the cloud. You can use hybrid cloud as a path to migrate your business and its IT needs to the cloud or integrate cloud platforms and services with your existing on-premises infrastructure as part of your overall IT strategy.

Microsoft hybrid cloud

Microsoft hybrid cloud is a set of business scenarios that combine a Microsoft cloud platform with an on-premises component, such as:

- Getting search results from content both in an on-premises SharePoint farm and in SharePoint Online in Office 365.
- A mobile app running in Azure that queries an on-premises data store.
- An intranet IT workload running on Azure virtual machines.

Because Microsoft has the most complete cloud solution in the marketplace—including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)—you can:

- Leverage your existing on-premises investments as you migrate workloads and applications to the cloud.
- Incorporate hybrid cloud scenarios into your long-term IT plans, for example, when regulations or policies do not permit moving specific data or workloads to the cloud.
- Create additional hybrid scenarios that include multiple Microsoft cloud services and platforms.

Scenarios for hybrid cloud with Microsoft cloud services vary with the platform.

SaaS

Software as a Service

Microsoft SaaS services include Office 365, Microsoft Intune, and Microsoft Dynamics 365. Hybrid cloud scenarios with Microsoft SaaS combine these services with on-premises services or applications. For example, Exchange Online running in Office 365 can be integrated with Skype for Business 2019 that is deployed on-premises.

Azure PaaS

Platform as a Service

Microsoft Azure PaaS services allow you to create cloud-based applications. Hybrid cloud scenarios with Azure PaaS services combine an Azure PaaS app with on-premises resources or applications. For example, an Azure PaaS app could securely query an on-premises data store for information needed to display to mobile app users.

Azure IaaS

Infrastructure as a Service

Azure IaaS services allow you to build and run server-based IT workloads in the cloud, rather than in your on-premises datacenter. Hybrid cloud scenarios with Azure IaaS services typically consist of an IT workload that runs on virtual machines that is transparently connected to your on-premises network. Your on-premises users will not notice the difference.

Elements of hybrid cloud

You must account for the following elements when planning and implementing hybrid cloud scenarios with Microsoft cloud platforms and services.

Networking

Networking for hybrid cloud scenarios includes the connectivity to Microsoft cloud platforms and services and enough bandwidth to be performant under peak loads.

Identity

Identity for SaaS and Azure PaaS hybrid scenarios can include Azure AD as a common identity provider, which can be synchronized with your on-premises Windows Server AD, or federated with Windows Server AD or other identity providers. You can also extend your on-premises Identity infrastructure to Azure IaaS.

Security

Security for hybrid cloud scenarios includes protection and management for your identities, data protection, administrative privilege management, threat awareness, and the implementation of governance and security policies.

Management

Management for hybrid cloud scenarios includes the ability to maintain settings, data, accounts, policies, and permissions and to monitor the ongoing health of the elements of the scenario and its performance. You can also use the same tool set, such as Systems Management Server, for managing virtual machines in Azure IaaS.
Architecture of Microsoft hybrid cloud scenarios

Use an architectural approach to plan and implement hybrid cloud scenarios with Microsoft cloud services and platforms.

<table>
<thead>
<tr>
<th>Category</th>
<th>Microsoft SaaS</th>
<th>Azure PaaS</th>
<th>Azure IaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apps and scenarios</td>
<td>Exchange Online and Skype for Business hybrid</td>
<td>Hybrid search and profiles for SharePoint</td>
<td>Hybrid PaaS apps</td>
</tr>
<tr>
<td></td>
<td>Skype for Business hybrid</td>
<td>Hybrid extranet B2B for SharePoint</td>
<td>Virtual machine (VM)-based IT workloads</td>
</tr>
<tr>
<td></td>
<td>Cloud PBF and Cloud Connector Edition with Skype for Business Server</td>
<td>Hybrid team sites for SharePoint</td>
<td>Extend identity infrastructure to Azure V Nets</td>
</tr>
<tr>
<td></td>
<td>Exchange Server hybrid</td>
<td>Hybrid OneDrive for Business</td>
<td>Site-to-Site VPN or ExpressRoute to Azure IaaS</td>
</tr>
<tr>
<td>Identity</td>
<td>Azure Active Directory integration</td>
<td>Connect to Microsoft cloud services (Internet pipe or ExpressRoute for Office 365, Dynamics 365, and Azure PaaS)</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>On-premises compute, storage, and network environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-premises</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Apps and scenarios layer contains the specific hybrid cloud scenarios that are detailed in topics 3-5 of this model. The Identity, Network, and On-premises layers can be common to the categories of cloud service (SaaS, PaaS, or IaaS).

Hybrid cloud scenarios for the three-phase cloud adoption process

Many enterprises, including Microsoft’s, use a three-phase approach to adopting the cloud. Hybrid cloud scenarios can play a role in each phase.

1. **Move productivity workloads to SaaS**
   For productivity workloads that currently are or must stay on-premises, hybrid scenarios allow them to be integrated with their cloud counterparts.

2. **Develop new and modern applications in Azure PaaS**
   Azure PaaS hybrid applications can securely leverage on-premises server or storage resources.

3. **Move existing applications to Azure IaaS**
   For lift-and-shift and build-in-the-cloud scenarios, server-based applications running on Azure VMs provide easy provisioning and scaling.
Hybrid cloud scenarios for Microsoft SaaS (Office 365)

Combine on-premises deployments of Exchange, SharePoint, or Skype for Business with their counterparts in Office 365 as part of a cloud migration or long-term integration strategy.

Microsoft SaaS hybrid scenario architecture

<table>
<thead>
<tr>
<th>Category</th>
<th>Microsoft SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apps and scenarios</td>
<td>Exchange Online and Skype for Business Server hybrid</td>
</tr>
<tr>
<td></td>
<td>Hybrid search and profiles for SharePoint</td>
</tr>
<tr>
<td></td>
<td>Skype for Business hybrid</td>
</tr>
<tr>
<td></td>
<td>Cloud PBX and Cloud Connector Edition with Skype for Business Server</td>
</tr>
<tr>
<td></td>
<td>Hybrid OneDrive for Business</td>
</tr>
<tr>
<td></td>
<td>Exchange Server hybrid</td>
</tr>
<tr>
<td></td>
<td>On-premises environment</td>
</tr>
<tr>
<td>Identity</td>
<td>Azure Active Directory Integration</td>
</tr>
<tr>
<td>Network</td>
<td>Internet pipe or ExpressRoute for Office 365 or Dynamics 365</td>
</tr>
</tbody>
</table>

The subsequent sections of this topic show the key SaaS-based hybrid cloud scenarios.

Skype for Business Hybrid

Skype for Business Hybrid allows you to combine an existing on-premises deployment with Skype for Business Online.

Some users are homed on-premises and some users are homed online, but the users share the same Session Initiation Protocol (SIP) domain, such as contoso.com.

You can use this hybrid configuration to migrate from on-premises to Office 365 over time, on your schedule. Skype for Business can also be integrated with Exchange Online.

Plan hybrid connectivity between Skype for Business Server and Skype for Business Online

Integration with Exchange and SharePoint

Continued on next page
Cloud PBX with Skype for Business Server

Cloud PBX with Skype for Business Server allows you to transition an existing Skype for Business Server on-premises deployment to a topology with on-premises Public Switched Telephone Network (PSTN) connectivity.

Users in the organization who are homed in the cloud can receive private branch exchange (PBX) services from the Microsoft cloud that include signaling and voicemail, but PSTN connectivity (dial tone) is provided through Enterprise Voice from your on-premises Skype for Business Server deployment.

This is a great example of a hybrid configuration that allows you to gradually migrate to a cloud-based service. You can retain your users’ voice capabilities as you begin to move them to Skype for Business Online. You can move your users at your own pace, knowing that their voice features will continue no matter where they are homed.

SharePoint Hybrid

SharePoint hybrid combines SharePoint Online in Office 365 with your on-premises SharePoint farm for a best of both worlds, connected experience.

Additional SharePoint hybrid scenarios

Hybrid Picker

It is easy to enable hybrid scenarios using the wizards that automate hybrid configuration, available from the SharePoint Online admin center in Office 365.

Extensible hybrid app launcher

Allows users to view and use Office 365 video and Delve apps and experiences within the pages of their on-premises SharePoint farm.

All of these SharePoint hybrid scenarios, except the Extensible hybrid app launcher, are available for both SharePoint 2016 and SharePoint 2013 users.

Exchange Server 2016 Hybrid

With Exchange Server 2016 Hybrid, you can realize the benefits of Exchange Online in Office 365 for online users while on-premises users continue to use existing Exchange Server infrastructure.

Some users have an on-premises email server and some users use Exchange Online, but all users share the same e-mail address space.

This hybrid configuration:

- Leverages your existing Exchange Server infrastructure while you migrate to Exchange Online over time, on your schedule.
- Allows you to support remote sites without investing in branch office infrastructure.
- Allows you to route incoming Internet email through Exchange Online Protection in Office 365.
- Serves the needs of multinational organizations with subsidiaries that require data to reside on-premises.

You can also integrate this hybrid configuration with other Microsoft Office 365 applications, including Skype for Business Online and SharePoint Online.
Hybrid cloud scenarios for Azure PaaS

Combine on-premises data or computing resources with new or converted applications running in Azure PaaS, which can take advantage of cloud performance, reliability, and scale and provide better support for mobile users.

**Azure PaaS hybrid scenario architecture**

<table>
<thead>
<tr>
<th>Apps and scenarios</th>
<th>Hybrid PaaS apps</th>
<th>A hybrid PaaS application runs in Azure and uses on-premises compute or storage resources.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>Azure Active Directory integration</td>
<td>Consists of either directory synchronization or federation with a third-party identity provider.</td>
</tr>
<tr>
<td>Network</td>
<td>Internet pipe or ExpressRoute to Azure PaaS</td>
<td>Consists of either your existing Internet pipe or an ExpressRoute connection with public peering to Azure PaaS. You must include a way for the Azure PaaS application to access the on-premises compute or storage resource.</td>
</tr>
<tr>
<td>On-premises</td>
<td>On-premises environment</td>
<td>Consists of identity and security infrastructure and existing line of business (LOB) applications or database servers, which an Azure PaaS application can securely access.</td>
</tr>
</tbody>
</table>

**Azure PaaS hybrid application**

An organization can make its compute or storage resources available to the Azure PaaS hybrid application by:

- Hosting the resource on servers in the DMZ.
- Hosting a reverse proxy server in the DMZ, which allows authenticated, inbound HTTPS-based requests to the resource that is located on-premises.

The Azure app can use credentials from:

- Azure AD, which can be synchronized with your on-premises identity provider, such as Windows Server AD.
- A third-party identity provider.

**Example Azure PaaS hybrid application**

This example Azure PaaS hybrid application is a custom mobile app that provides up-to-date contact information on employees. The end-to-end hybrid scenario consists of:

- A smartphone app that requires validated, on-premises credentials to run.
- A custom mobile app running in Azure PaaS, which requests information about specific employees based on queries from a user's smartphone app.
- A reverse proxy server in the DMZ that validates the custom mobile app and forwards the request.
- An LOB application server farm that services the contact request, subject to the permissions of the user's account.

Because the on-premises identity provider has been synchronized with Azure AD, both the custom mobile app and the LOB app can validate the requesting user's account name.
Hybrid cloud scenarios for Azure IaaS
Extend your on-premises computing and identity infrastructure into the cloud by hosting IT workloads running in cross-premises Azure virtual networks (VNets).

Azure IaaS hybrid scenario architecture

<table>
<thead>
<tr>
<th>Apps and scenarios</th>
<th>VM-based IT workloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>Extend your identity infrastructure to Azure VNets</td>
</tr>
<tr>
<td>Network</td>
<td>Site-to-Site VPN or ExpressRoute to Azure IaaS</td>
</tr>
<tr>
<td>On-premises</td>
<td>On-premises environment</td>
</tr>
</tbody>
</table>

An IT workload is typically a multi-tier, highly available application composed of Azure virtual machines (VMs).

Add identity servers, such as Windows Server AD domain controllers, to the set of servers running in Azure VNets for local authentication.

Use either a site-to-site VPN connection over the Internet or an ExpressRoute connection with private peering to Azure IaaS.

Contains identity servers that are synchronized with the identity servers running in Azure. Can also contain resources that VMs running in Azure can access, such as storage and systems management infrastructure.

Directory Synchronization server for Office 365
A directory synchronization server for Office 365 synchronizes the list of accounts in Windows Server AD with the Azure AD tenant of an Office 365 subscription.

A directory synchronization server is a Windows-based server that runs Azure AD Connect. For faster provisioning or to reduce the number of on-premises servers in your organization, deploy your directory synchronization in a virtual network (VNet) in Azure IaaS.

You connect your organization network to the Azure VNet with a site-to-site (S2S) VPN or ExpressRoute connection.

The directory synchronization server polls Windows Server AD for changes and then synchronizes them with the Office 365 subscription.

Running your directory synchronization server from an Azure VNet is an example of extending your computing and identity infrastructure to the cloud.

Line of business (LOB) application
You can create LOB applications running on Azure VMs, which reside on subnets of an Azure VNet in an Azure datacenter (also known as a location).

Because you are essentially extending your on-premises infrastructure to Azure, you must assign unique private address space to your VNets and update your on-premises routing tables to ensure reachability to each VNet.

Once connected, these VMs can be managed with remote desktop connections or with your systems management software, just like your on-premises servers.

By configuring publicly-exposed ports, these VMs can also be accessed from the Internet by mobile or remote users.

Continued on next page
Attributes of LOB applications hosted on Azure VMs

Multiple tiers
Typical LOB applications use a tiered approach. Sets of servers provide identity, database processing, application and logic processing, and front-end web servers for employee or customer access.

High availability
Typical LOB applications provide high availability by using multiple servers in each tier. Azure IaaS provides a 99.9% uptime SLA for servers in Azure availability sets.

Load distribution
To distribute the load of network traffic among multiple servers in a tier, you can use an Internet-facing or internal Azure load balancer. Or, you can use a dedicated load balancer appliance available from the Azure marketplace.

Security
To protect servers from unsolicited incoming traffic from the Internet, you can use Azure network security groups. You can define allowed or denied traffic for a subnet or the network interface of an individual virtual machine.

SharePoint Server 2016 farm in Azure

An example of a multi-tier, highly-available LOB application in Azure is an intranet SharePoint Server 2016 farm.

**Tiers:** Servers running different roles within the farm create the tiers and each tier has its own subnet.

**High availability:** Achieved by using more than one server in each tier and placing all the servers of a tier in the same availability set.

**Load distribution:** Internal Azure load balancers distribute the incoming client web traffic to the front-end servers (WEB1 and WEB2) and to the SQL Server cluster (SQL1 and SQL2).

**Security:** Network security groups for each subnet let you to configure allowed inbound and outbound traffic.

Federated identity for Office 365 in Azure

Another example of a multi-tier, highly-available LOB application in Azure is federated identity for Office 365.

**Tiers:** There are tiers for web proxy servers, Active Directory Federation Services (AD FS) servers, and Windows Server AD domain controllers.

**Load distribution:** An external Azure load balancer distributes the incoming client authentication requests to the web proxies and an internal Azure load balancer distributes authentication requests to the AD FS servers.

Evaluate and experiment
Understand the benefits of running SharePoint Server 2016 in Azure and build a simulated dev/test environment.

**SharePoint Server 2016 in Microsoft Azure**

**Intranet SharePoint Server 2016 in Azure dev/test environment**

Design
Step through a process to determine the set of Azure IaaS networking, compute, and storage elements to host your farm and their settings.

**Designing a SharePoint Server 2016 farm in Azure**

Deploy
Step through the end-to-end configuration of the high-availability farm in five phases.

**Deploying SharePoint Server 2016 with SQL Server AlwaysOn Availability Groups in Azure**

Evaluate and experiment
Build a simulated dev/test environment for federated authentication with Office 365.

**Federated identity for your Office 365 dev/test environment**

Deploy
Step through the end-to-end configuration of the high availability AD FS infrastructure in five phases.

**Deploy high availability federated authentication for Office 365 in Azure**

---

November 2019

© 2016 Microsoft Corporation. All rights reserved. To send feedback about this documentation, please write to us at CloudAdopt@microsoft.com.