Internet Sites in Microsoft Azure using SharePoint Server 2013

Public-facing Internet sites benefit from cloud elasticity and Microsoft Azure AD for customer accounts

1 Design and size the farm topology

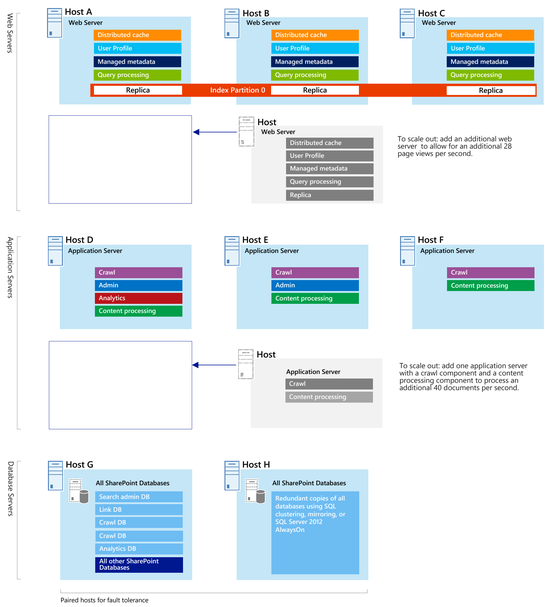
Use the topology, capacity, and performance guidance for SharePoint Server 2013 on TechNet to design the farm topology. See the following technical diagram: Internet Sites Search Architectures for SharePoint Server 2013.

Ensure the farm you design meets the objectives for capacity and performance.

Example: Medium Internet Sites farm (~85 Page views per second)

This farm is intended to provide a fault-tolerant SharePoint Server 2013 search farm topology that is optimized for a corpus that contains 3,400,000 items.

The example farm processes 100-200 documents per second, depending on the language, and it accommodates 85 page views per second and 100 queries per second.



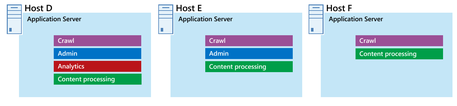
2 Fine-tune for Microsoft Azure

The SharePoint farm might need to be fine-tuned for availability sets in the Microsoft Azure platform. To ensure high availability of all components, ensure that the server roles are all configured identically.

In the example topology above:

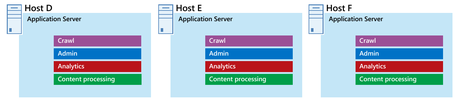
- The web servers and the database servers are configured identically.
- The three application servers are not configured identically. These server roles require fine tuning for availability sets in Microsoft Azure.

Before



The number of components is determined by the performance and capacity targets for the farm.

After



To adapt this architecture for Microsoft Azure, we'll replicate the four components across all three servers. This increases the number of components beyond what is necessary for performance and capacity. The tradeoff is that this design ensures high availability of all four components in the Microsoft Azure platform when these three virtual machines are assigned to an availability set.

3 Choose the Active Directory model

All SharePoint solutions require Windows Active Directory Domain Services. At this time, there are two options for SharePoint solutions in Microsoft Azure.

Option	Description
Dedicated domain	You can deploy a dedicated and isolated domain to Windows Azure to support a SharePoint farm. This is a good choice for public-facing Internet sites.
Extend the on-premises domain through a site-to-site VPN connection	When you extend the on-premises domain through a site-to-site VPN connection, users access the SharePoint farm as if it were hosted on-premises. You can take advantage of your existing Active Directory and DNS implementation.

4 Design for identity management, zones, and authentication

Accounts and authentication

Determine how accounts will be managed and which type of authentication will be used.

Accounts for site developers and authors

- Add accounts to the domain in Microsoft Azure.
- Use ADFS on premises to federate the internal accounts to the domain in Microsoft Azure.
- If the design includes a site-to-site VPN connection, use the internal accounts.

Accounts for customers

- Use Microsoft Azure Active Directory.
- Use a different SAML-based provider.

Zones

In SharePoint 2013, identity management is factored into the configuration of zones and authentication.

This design provides clear separation of customer accounts from all other accounts.

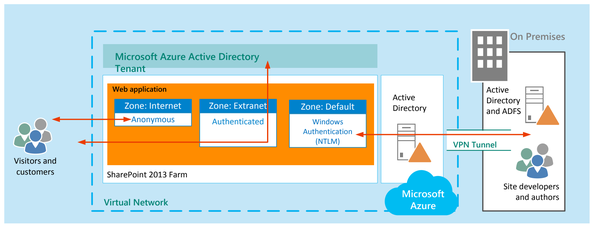
- Use this design if you want customer accounts to be treated entirely different from the internal accounts for authors and site developers.
- This design allows you to use zone policies to limit customer actions within a web application.
- This design results in different URLs for customer accounts and internal accounts.

In this example:

- Configure the default zone for internal accounts.
- Configure the Extranet zone for customer authenticated access. Use Microsoft Azure Active Directory for customer accounts, or use a different SAML-based provider.
- Configure the Internet zone for anonymous access.

At this time, a two-zone design in which all authenticated users are configured to use the default zone is not recommended.

Three-zone design — separation of internal and customer accounts



Connecting to Microsoft Azure Active Directory

Microsoft Azure AD provides identity management and access control capabilities for cloud services. Capabilities include a cloud-based store for directory data and a core set of identity services, including user logon processes, authentication services, and Federation Services. The identity services that are included with Microsoft Azure AD easily integrate with your on-premises Active Directory deployments and fully support third-party identity providers.

See Configure Microsoft Azure Active Directory with SharePoint 2013 in the TechNet library.

When integrating SharePoint 2013 with Microsoft Azure Active Directory, a Microsoft Azure Access Control Service (ACS) serves two purposes:

- AAD uses SAML 2.0, and SharePoint only works with SAML 1.1. ACS understands both formats and serves as the intermediary to transform the token formats between SharePoint and AAD.
- ACS replaces the need for the identity provider security token service (IP-STS) for this SAML scenario.

5 Design sites and URLs for cross-site publishing

A one web-application design is recommended for publishing scenarios.

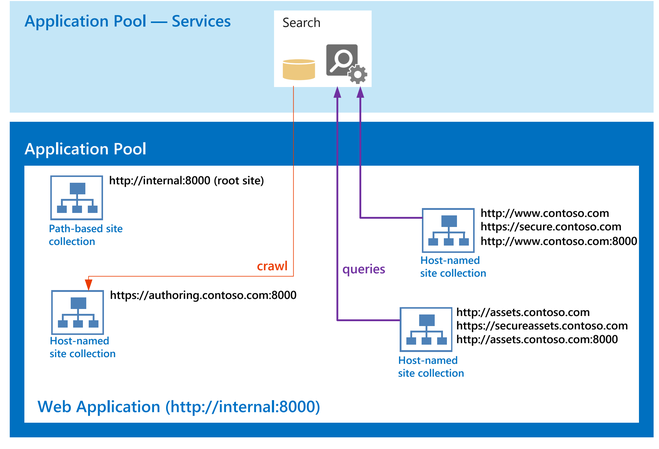
- Both authoring and publishing sites are in the same web application.
- Cross-site publishing is used to publish assets.

Use path-based and host-named site collections.

- A root site collection is a requirement. Create this site as a path-based site.
- Create all other site collections as host-named site collections.

Web application and root site URLs

- Use an internal name for the web application URL. SharePoint uses the local machine name as the default name unless a different name is specified. You can use a domain name that is reserved for the internal network environment.
- SharePoint assigns a non-standard port number when the web application is created. Use this port number instead of port 80 or port 443. Or use a different but non-standard port number.
- Use the same name and port number for the root site collection, which is a path-based site collection.

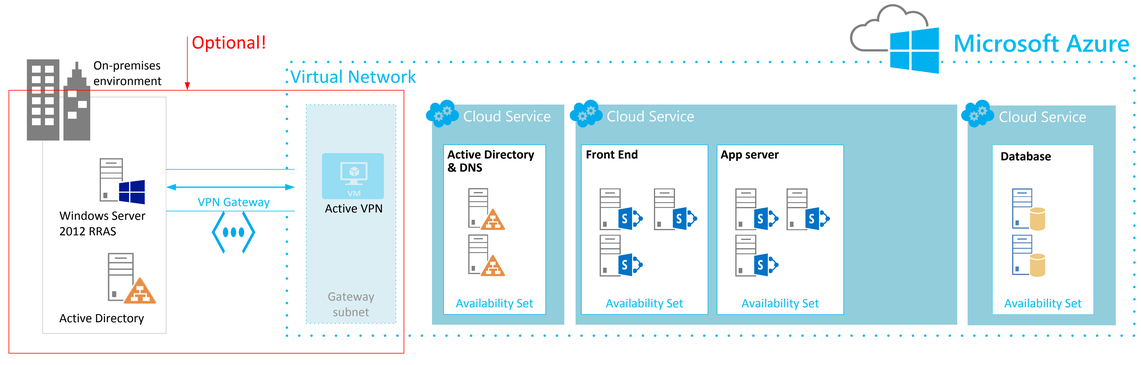


6 Design the Microsoft Azure environment

This example architecture includes the following elements:

- A site-to-site VPN connection is optional and extends the on-premises Windows AD DS and DNS environment to the virtual network in Microsoft Azure.
- Optionally, a dedicated domain can be used in Microsoft Azure to support the SharePoint farm.
- Servers are split across Microsoft Azure cloud services based on role.
- Availability sets ensure high availability of identically configured server roles.

For more information, see the following article on TechNet: Microsoft Azure Architectures for SharePoint Solutions.



SharePoint Microsoft