

Architecting Hybrid Cloud Environments

**Publication Date**: January, 2016

**Authors**: Victor Arzate, Shawn Gibbs; Michael Greene, Ian Lucas; Wagner Mota; Bala Natarajan; Uday Pandya

**Editor**: Glenn Minch

**Summary**: Hybrid cloud environments combine traditional on-premises IT with the consumption of cloud-based capacity (IaaS) and other cloud-based services. When carefully planned and executed, hybrid cloud models can deliver much of the best of both on-premises and cloud services. This paper focuses on understanding the different design approaches for architecting hybrid cloud environments, using technologies available from Microsoft, Microsoft Partner Solutions, and the Open Source community. Its objective is to enable IT architects to develop the right infrastructure strategies to deliver more of the potential promised by hybrid cloud-enabled scenarios.

*© 2015 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.*

*Some examples are for illustration only and are fictitious. No real association is intended or inferred.*

*This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.*

*Some information relates to pre-released product which may be substantially modified before it’s commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.*

Table of Contents

[Overview 4](#_Toc439249244)

[Hybrid Cloud Foundations 8](#_Toc439249245)

[Connecting Clouds 8](#_Toc439249246)

[Exploring the options 9](#_Toc439249247)

[Virtual Private Networks (VPN) using Internet Gateways 9](#_Toc439249248)

[Dedicated connections using ExpressRoute 9](#_Toc439249249)

[Choosing among the options 10](#_Toc439249250)

[Integrating Identity 12](#_Toc439249251)

[Terminology 13](#_Toc439249252)

[Connecting an on-premises identity to the cloud 13](#_Toc439249253)

[Directory synchronization 14](#_Toc439249254)

[Directory federation 14](#_Toc439249255)

[Managing IAM in hybrid environments 16](#_Toc439249256)

[Self-service management scenarios 16](#_Toc439249257)

[Additional IAM scenarios 18](#_Toc439249258)

[Managing in Hybrid Environments 22](#_Toc439249259)

[Deployment 23](#_Toc439249260)

[Operating system installation 23](#_Toc439249261)

[Optimizing server footprint 24](#_Toc439249262)

[Offline servicing 24](#_Toc439249263)

[Baseline server configuration 24](#_Toc439249264)

[Image management in hybrid environments 25](#_Toc439249265)

[Configuration management 26](#_Toc439249266)

[Monitoring 27](#_Toc439249267)

[Data flow topology 28](#_Toc439249268)

[Real-time alerting 28](#_Toc439249269)

[Data sensitivity 28](#_Toc439249270)

[Self-healing service management 29](#_Toc439249271)

[Examples 30](#_Toc439249272)

[Business Continuity and Disaster Recovery 31](#_Toc439249273)

[Azure Site Recovery 31](#_Toc439249274)

[Using ASR as a cloud-based management plane for DR 31](#_Toc439249275)

[Leveraging Azure as a DR site 32](#_Toc439249276)

[Designing a disaster recovery strategy with ASR 33](#_Toc439249277)

[Choosing your recovery site 33](#_Toc439249278)

[Network address space in a DR environment 37](#_Toc439249279)

[Hybrid Applications and Workloads 38](#_Toc439249280)

[Data placement 38](#_Toc439249281)

[Application architecture 39](#_Toc439249282)

[Application refactoring and cloud-born design 40](#_Toc439249283)

[Revision history 41](#_Toc439249284)

[Appendix 1: WAP and AADAP Comparison 42](#_Toc439249285)

# Overview

IT is experiencing a rapid sea change towards greater consumption of capacity and services through public cloud providers. Enterprises are increasingly feeling pressured to leverage the cost economies and flexibility of cloud-based IT strategies. For most, the reality of current on-premises investments will dictate a gradual transformation from existing on-premises datacenters to cloud-based solutions. Even in the most aggressive pivot toward cloud-based IT, enterprises will continue to leverage their existing IT infrastructure, business applications, and IT processes. Hybrid cloud models, which combine traditional on-premises IT with the consumption of cloud-based capacity (IaaS) and other cloud-based services, play a critical role in bridging from traditional IT approaches to cloud-centric IT strategies.

When carefully planned and executed, hybrid cloud models can deliver much of the best of both on-premises and cloud services. This paper focuses on understanding the different design approaches for architecting hybrid cloud environments, using technologies available from Microsoft and Microsoft Solution Partners. The Open Source community has contributed a number of useful tools that can help with management, automation, and testing in hybrid clouds. Our objective is to enable IT architects to develop the right infrastructure strategies to deliver more of the potential promised by hybrid cloud-enabled scenarios.

After reading this paper, you will understand how to:

* Make strong design choices between the options available to connect your on-premises environment with Azure.
* Understand the options for integrating identity and access management systems between cloud-based services and on-premises datacenters.
* Understand effective approaches to managing hybrid clouds, including how to take advantage of opportunities to enhance the operational management of existing on-premises systems with cloud-based capabilities.
* Work through the design challenges that could otherwise limit your ability to fully leverage the promises of cloud-based infrastructure.
* Understand how to approach the design decisions associated with shifting existing multi-tiered on-premises applications to a hybrid cloud world.

# Hybrid Cloud Foundations

The goal of the following sections is to explain the key choices available when designing hybrid environments, and the criteria driving architectural decisions. For most companies, driving towards a cloud-based IT service model will be a journey. IT architects must be able to balance short term needs with longer term strategies.

This paper focuses on the systems architecture, but bear in mind that shifting technologies can also bring changes to the traditional division of responsibilities in IT operations. When designing your hybrid cloud environment, it is important to consider the value of separating the roles that manage and operate the environment from the provisioning of new services and applications which can be provided through self-service portals. This can influence overall design, but is not covered in depth in this paper.

As mentioned above, hybrid cloud models combine traditional on-premises IT with the consumption of cloud-based capacity (IaaS) and other cloud-based services. The paper contains architectural discussions covering five areas that are fundamental to most hybrid clouds:

* Connecting clouds
* Integrating identity
* Managing hybrid environments
* Business continuity and disaster recovery (BCDR)
* Hybrid applications and workloads

The first two sections describe the foundation of a hybrid cloud environment: network connectivity and identity integration. Subsequent sections build on the foundational services to deliver on key scenarios: IT operational management, BCDR, and hybrid applications.

Here is a brief introduction to each of the five hybrid foundation areas:

#### Connecting clouds

Designing the right connectivity between an on-premises environment (private cloud) and a public cloud such as Azure depends largely on the communication requirements imposed by the workloads and applications across the cloud boundaries. Network connectivity characteristics such as data bandwidth and network latency are important to understand, but not always easy to model. Other potential considerations such as cost models, data privacy and security needs, and the agility to modify network configuration to adapt to changing needs, also need to be understood.

This section will help you understand how to choose between different connectivity approaches, which range from simple ‘web browsing over the public internet’ connections, to various kinds of virtual private networks (VPN), to dedicated connection options such as Azure ExpressRoute.

#### Integrating identity

With the shift towards cloud-based applications and services comes a change in the constructs and protocols used for authentication and management of access to cloud-based resources. It is important to understand the role played by new cloud-based identity services like Azure Active Directory in hybrid environments, and how to integrate cloud-based identity services with traditional on-premises identity and access management (IAM) systems.

This section aims to give an IT architect a view of the possibilities and choices needed to design an IAM system for a hybrid cloud infrastructure, using either an all-Microsoft or a heterogeneous stack. It outlines important considerations when extending a traditional on-premises identity to the cloud, comparing on-premises, cloud, and hybrid cloud practices and technologies. It also looks at self-service scenarios for identity management, single sign-on, self-governance, and access management. It positions cloud-based services like Azure Active Directory (AAD) with on-premises Active Directory (AD) and AD Federation Services (ADFS).

This section is an adaptation of the entire paper [Identity in Hybrid Clouds](https://gallery.technet.microsoft.com/Identity-in-Hybrid-Clouds-f4ff797e).[[1]](#footnote-1)

#### Managing in hybrid environments

Most companies have a significant investment in the management of existing IT environments, including management tools, operational processes, and the expertise of IT professionals. Understanding how to move these investments forwards is an important component of a ‘shift to cloud’ strategy.

Managing hybrid environments, where applications and workloads are spread across on-premises datacenters and public clouds (Azure), poses some interesting choices and opens up some exciting new opportunities.

This section will help you understand how to architect effective management topologies in a hybrid world, supporting scenarios such as provisioning, configuration and patch management, monitoring and alerting, and change visibility. It will help identify how well traditional multi-datacenter design approaches translate to a hybrid, on-premises + Azure environment, and how to choose between managing from on-premises versus managing from Azure. It will discuss important considerations such as security, performance consequences, and automation approaches.

In addition to exploring traditional management scenarios in the context of hybrid environments, this section also introduces new options for leveraging Azure-based management capabilities using [Microsoft Operations Management Suite](http://www.microsoft.com/oms)[[2]](#footnote-2) (OMS). The “pay only for what you use” model of Azure makes new capabilities such as advanced analytics more viable, providing deeper insights into operational health of both on-premises and Azure based workloads.

#### Business continuity and disaster recovery

Until recently, ensuring the business continuity and disaster recovery (BCDR) of IT operations during or after a regional disaster or a major service disruption commonly involved complex and expensive investments in redundant capacity. Public clouds such as Microsoft Azure have evolved to provide a practical, cost-effective alternative to capital investments to provide the failover capacity that is needed for a robust BCDR program.

The BCDR section will help you understand how to design effective BCDR and backup scenarios in a hybrid environment, using technologies such as Azure Site Recovery (ASR), Azure Backup, and storage replication technologies in Windows Server. The discussion includes considerations relating to network design, capacity planning, and automation approaches to achieve recovery point objectives (RPO) and recovery time objectives (RTO) in disaster recovery design. While the focus of this section is primarily on DR, the same approaches apply when leveraging replication technologies for data back-up and other cloud backed storage scenarios, looking at performance and network utilization implications, security, and operational considerations.

#### Hybrid applications and workloads

There are many motivations driving the shift towards consuming IT applications from public cloud capacity. Changing the cost profile to a consumption model is a leading driver, leveraging the elasticity of ‘capacity on demand’ for dynamic or seasonal workloads, removing the cost of reserve capacity in on-premises data centers. Security has also shifted from being a potential adoption concern, to an adoption accelerator as corporations realize that the huge investments and expertize public clouds like Azure expend on counter-intrusion far exceeds what is feasible for individual companies.

Regardless of the motivation for driving to cloud-based workloads, ensuring a successful transition of traditional on-premises applications to either fully-cloud or hybrid-cloud operational models requires a strong understanding of the application architecture to fully realize the intended value of moving to cloud, and to avoid common pitfalls.

This paper will help you understand some of the considerations when mapping existing applications into a hybrid cloud model. Performance profiling, cost analysis, and security modelling are all important considerations when assessing how to migrate a traditional tiered application in whole or in part to the cloud. It looks at the challenges of the application refactoring that is sometimes necessary to fully realize the promise of cloud-based workloads.

# Connecting Clouds

Designing the communication channels between traditional on-premises infrastructure and public clouds is fundamental to being able to successfully enable hybrid cloud scenarios. There are several approaches to extend an on-premises network to public clouds (such as Microsoft Azure), each with different strengths and weaknesses. The more seamless the interconnectivity in hybrid cloud environments, the better the ability for hybrid applications and workloads to take advantage of the respective strengths of different clouds. For example, well-designed and well-executed hybrid connectivity enables the following:

* Optimizing application performance based on placement of individual components
* Minimizing cost by leveraging low cost public cloud storage, and capacity on demand
* Reducing operational risk by cloud-based backup and/or disaster recovery strategies
* Leveraging public cloud-based services to extend management capabilities

Key considerations when choosing between the different connectivity options described in this section include understanding bandwidth and latency needs, security implications, reliability goals, and ensuring that you have the operational agility to quickly adapt network configurations to meet changing needs. When analyzing the needs of specific applications and workloads you need to support in your hybrid environment, the following questions will help map these needs back to the network design choices you will need to make:

* What are the inter-cloud data bandwidth requirements of the application and/or workload?
* Are there any specific security and/or compliance requirements that would exclude networking approaches that route communications over the public Internet?
* Is your hybrid solution likely to be susceptible to issues due to any latencies in cross-cloud network connections?
* What are the network reliability needs of the applications, to meet service continuity requirements?
* Are multiple (primary/backup) connection types needed to eliminate single points of failure?
* Some approaches will require multiple public IP addresses; are they available?
* Does your VPN impose compatibility requirements between the software gateways and VPN appliances used?

## Exploring the options

There are several choices to evaluate when designing connectivity from your on-premises environments to public clouds such as Azure.

### Virtual Private Networks (VPN) using Internet Gateways

The decision to use VPNs to connect on-premises environments to a public cloud is subject to considerations similar to connecting multiple on-premises sites. The key benefits of using VPN connections to public clouds include the familiarity of the technology and the (relatively) low cost compared to more dedicated connections.

There are two key VPN variations to consider:

#### Point-to-site connection

This is an individually configured connection between an on-premises client and a virtual network in a public cloud. It imposes no requirement on the client side for a dedicated VPN device. Connection is established manually over the public Internet. When connecting from an on-premises client to Azure, the connection is secured using Secure Sockets Tunneling Protocol (SSTP).

#### Site-to-site connection

This is a secure connection between an on-premises site and a virtual network in a public cloud. It requires a VPN device to be configured at your on-premises site, which creates a connection to a VPN gateway running in the cloud, secured using Internet Protocol Security (IPsec). Once the connection is established, resources in both the on-premises site and the cloud virtual network are able to communicate seamlessly with each other.

### Dedicated connections using ExpressRoute

Azure ExpressRoute enables a dedicated Layer 3 connection between an on-premises environment and the Azure public cloud. The key benefits of dedicated connections include the improved traffic isolation and increased predictability of performance of a private connection. Network traffic is not as exposed to the potential risks of flowing over the public Internet, or to the potential performance impact of noisy neighbors. ExpressRoute connections provide built-in redundancy to help ensure high availability, and they include a number of controls to manage quality-of-service (QoS) for different traffic types. Microsoft uses an industry standard BGP routing protocol to exchange routes between your network, your private VNETs in Azure, and Microsoft public cloud addresses.

There are three key dedicated connection topologies to consider:

#### Colocation at a cloud exchange

If your on-premises infrastructure is located in an ExpressRoute provider’s edge (typically referred to as an Exchange Provider), then they can provide a Layer 2 or managed Layer 3 connection between your on-premises network edge and the Microsoft Azure cloud.

#### Point-to-point Ethernet connection

This is a Layer 2 or Layer 3 connection provided by your service provider, directly from your on-premises edge to the Microsoft Azure cloud.

#### Any-to-any connection

This is a dedicated IPVPN (MPLS VPN), providing site-to-site connection between on-premises datacenters and the Microsoft Azure cloud. In this configuration, the Microsoft Azure cloud is like any other WAN connection between your on-premises environment and a remote site.

## Choosing among the options

As mentioned previously, a good design decision on a connectivity approach depends on its alignment to the needs of your applications and workloads. Consideration of how these needs may change over time is also important.

The following list contains descriptions and recommendations for ten design considerations that are common to hybrid network designs:

1. **Security** **Considerations**: For some applications that communicate over a site-to-site VPN, routing traffic over the shared, public Internet is a security concern even though that traffic is encrypted. A dedicated connection using ExpressRoute can provide greater traffic isolation than can be achieved over the shared Internet, however, traffic over ExpressRoute is not encrypted. You will need to take additional steps to encrypt traffic if you want to combine traffic isolation with encryption to leverage the full security potential of your dedicated connection.

Encryption over an ExpressRoute connection can be done using 3rd party firewall VMs to perform tunnel-mode IPsec over the connection. In this approach, the processing cost of encryption is incurred by the two firewall VMs, one on each end of the ExpressRoute circuit. An alternative approach that distributes the cost of encryption is to use transport-mode IPsec policy for all traffic between the VMs in the public cloud and the on-premises end points. This option spreads the cost of encryption across all VMs in the cloud, but it needs careful planning for deploying transport-mode IPsec policies.

1. **Performance Predictability**: In scenarios where performance characteristics of the network connection between on-premises environment and Microsoft Azure cloud are critical to application’s operation, a dedicated connection approach provides a degree of separation from the risk of sometimes unpredictable performance variations over public Internet-based connections (VPN). For example, a distributed application with high bandwidth and/or frequent (“chatty”) communication between components distributed across clouds will benefit from the reliably consistent bandwidth of a dedicated connection.
2. **Cost**: While the costs for a given connectivity approach will vary depending on circumstances, VPN solutions will typically be less expensive to establish than dedicated connections. When comparing costs, the cost of high bandwidth ExpressRoute connections should be amortized across multiple applications for a fair assessment, along with other cost factors including the value of built-in redundancy (ExpressRoute) and the operational agility of having a Layer 3 connection stretched across environments.
3. **Bandwidth Needs**: Point-to-site VPN connections will typically meet peak bandwidth requirements of ≤ 100Mbps. For site-to-site VPN connections, you will need to ensure your VPN device and matching public cloud gateway, will provide the aggregated throughput needed for your needs. Dedicated connections offer predictable bandwidth, better management controls, and improved SLAs which will become necessary as your overall bandwidth requirements grow beyond 100Mbps. Applications that have specific bandwidth and latency requirements in order to maintain adequate performance during periods of peak activity will generally benefit from the predictable bandwidth provided by a dedicated connection.
4. **Redundancy**: ExpressRoute connections automatically provide redundancy across peering sites. Where high availability is critical for specific hybrid applications, eliminating single failure points will be a key consideration in design. Combining different types of connection in primary or backup configurations, or providing parallel connections using different service providers, are viable approaches to minimize single point of failure risks.
5. **Client Connections**: Where only a small number of well-defined connections from specific clients to cloud based applications is required, a point-to-site VPN connection will provide a simple solution. A drawback to this type of VPN connection is the manual configuration that is required. As the number of clients increases, or when clients change often, manually configuring clients adds operational costs and complexity that is difficult to scale elastically. This drawback can be mitigated by using a site-to-site VPN connection or a dedicated connection, both of which incur higher upfront configuration costs, but they do not require per-client configuration.
6. **Remote Locations**: When clients need to connect from remote (or mobile) locations, point-to-site VPN connections that have no dependencies on VPN devices provide a simple solution. If the enterprise has multiple locations and different virtual networks in the public cloud for each location, a site-to-site VPN connection is needed from each of the locations to the respective virtual networks. Similarly, for ExpressRoute, a dedicated circuit is needed to reach the respective cloud end point from the nearest on-premises location. There are two ExpressRoute offerings: ExpressRoute Standard and [ExpressRoute Premium](https://azure.microsoft.com/en-us/pricing/details/expressroute/)[[3]](#footnote-3). The ExpressRoute premium offer covers global connectivity to access resources in the public cloud across multiple geo political locations, increased limits for the number routes exchanged and the number of virtual networks supported per express route circuit.
7. **Persistent Connections**: In some applications or workloads, having a persistent connection will be critical to the continuous operation. In these scenarios, point-to-site VPN connections may not provide the continuous connectivity needed. A site-to-site VPN or a dedicated connection will provide the persistent connectivity required.
8. **Complex Applications**: Where you are deploying complex applications with many interconnected components across a hybrid environment, point to site solutions will be overly complex to configure and maintain. Site-to -site solutions will simplify the deployment and ongoing network management associated with complex distributed workloads.
9. **Technical Complexity**: VPN based approaches are likely to leverage existing skills, knowledge and experience of your IT team. In comparison, dedicated connections are more commonly provided as a managed service with a service level agreement, where the technical skills and support are provided by your network provider. The extent to which this becomes a factor in choosing a connectivity approach will vary between organizations.

In addition to the above, here are some specific considerations for VPNs and ExpressRoute:

#### Point-to-site VPN

* Requires manual configuration or configuration through a mobile device management solution for each client connection
* Only the configured client has access to the public cloud resources.

#### Site-to-site VPN

* The on-premises VPN device must have an Internet-facing IPv4 IP address. This address cannot be behind a NAT.
* Site-to-site VPN requires a VPN device that is compatible with the public cloud gateway that it will connect to.
* There are two gateway types: static routing (also known as policy-based VPN), and dynamic routing (also known as route-based VPN). It is important to ensure that your VPN device works with the specific routing type you want to use. To learn more about VPN Gateways and routing types, please visit the [Microsoft Azure VPN Gateway](https://azure.microsoft.com/en-us/documentation/services/vpn-gateway/)[[4]](#footnote-4) documentation.

#### ExpressRoute

* ExpressRoute providers are strategically located around the world, allowing you to establish an ExpressRoute connection from virtually anywhere. Typically, your existing carrier will be able to peer with an ExpressRoute provider, but in some locations it may be necessary to extend your network by peering with an intermediate carrier to reach the nearest provider. For a list of ExpressRoute providers in your region, see [ExpressRoute Connectivity Providers](https://azure.microsoft.com/en-us/documentation/articles/expressroute-locations/)[[5]](#footnote-5) in the Microsoft Azure documentation.
* The premium SKU of ExpressRoute allows a user to access resources across global geopolitical regions from a peering location closer to them by allowing traffic to be routed over the Azure backbone network.
* A single ExpressRoute circuit can connect to your resources in Azure IaaS, PaaS, and O365.

# Integrating Identity

The aim of this section is to give the IT architect the information needed to establish a strategy for delivering well integrated Identity and Access Management (IAM) services in hybrid environments, where on-premises and public cloud environments have differing IAM needs, and consequently depend on different IAM technologies. Establishing an integrated IAM model across hybrid environment is key to enabling several key scenarios and desirable user experiences, such as single sign-on across applications irrespective of where they are hosted, and self-service management (e.g., password reset).

It is important to understand the differences in IAM practices and technologies between on-premises and cloud environments, to inform the hybrid design choices needed to support a number of important objectives. Some of the key IAM goals in hybrid environments include the following:

* Establish and maintain the right connections between traditional on-premises and cloud identities, to simplify users’ authentication and authorization experiences.
* Ensure hybrid applications, distributed across on-premises and cloud environments, can access necessary identity information stored in IAM directories.
* Enable key identity management scenarios, such as self-service, governance, and application access management.

## Terminology

In this section, these definitions will be used for the following terms:

* ***Identity*** is a user property that uniquely identifies the user to a computing platform. Identity is a fundamental property and it is a foundation for other infrastructure.
* ***Directory*** is a storage mechanism to securely store identity information. In this paper, directory refers to any construct for storing identity information as an authoritative source for validating a user’s identity.

## Connecting an on-premises identity to the cloud

Modern application design and architecture patterns have evolved rapidly in the past few years. Modern applications do not rely on traditional constructs and protocols to authenticate and authorize users for access management. For example, ASP.Net Web API doesn’t utilize a directory searcher or traditional Windows authentication protocol like Kerberos or NTLM for authentication and authorization; instead it relies on a lightweight protocol such as OAuth. Modern devices don’t utilize existing directory services in the same way as a workstation joined to a domain. Devices running Windows RT, Apple iOS, and Android do not use Kerberos and NTLM to authenticate with Active Directory.

In hybrid environments it is necessary to meet the requirements for authentication and authorization of both modern and traditional devices and applications. The concept of a directory needs to be extended so organizations can continue to use authentication in the traditional way, and also be able to use the new features and functionality associated with mobile devices. Traditionally, all authentication and authorization for Windows users and devices is in Active Directory, but that is not the case for other applications and services that have their own identity store. For example, a software as a service (SaaS) cloud application may store identity information in a custom LDAP-enabled directory store. We have to be able to unify these identity stores to enable seamless connectivity to multiple various identity sources.



Figure : Connected identity

There are two main approaches for unifying on-premises identity stored in Active Directory (AD) with Azure cloud based identity stored in Azure Active Directory (AAD):

* Directory synchronization: uses replication technology between identity stores to keep separate identity records belonging to a single user in synch between the two stores.
* Directory federation: creates a link between a user’s identity records across multiple directories, such that once authenticated in one system the user is trusted in all systems that are federated with the authentication authority.

The following sections describe each of these approaches in more detail, to help inform a choice between them.

### Directory synchronization

A valuable feature of Azure Active Directory (AAD) is its ability to consolidate identity sources. When synchronized with an existing on-premises identity source using Azure AD Connect, a cloud based identity is created as a projection of a user’s on-premises identity. A user (or application) can authenticate with either using common credentials (username/password), which are kept synchronized. In this approach, a user does not need to keep track of separate credentials, but still needs to sign-on separately to both to access applications in both environments.

The Azure Active Directory Sync tool keeps your on-premises Active Directory continuously synchronized with Azure Active Directory. Directory synchronization is relatively simple to configure, is intended as an ongoing relationship between your on-premises environment and Azure Active Directory and should be considered a long-term commitment to coexistence scenarios between your on-premises Active Directory and cloud directory.

The design of directory synchronization requires a choice between which environment, on-premises (AD) or cloud (AAD), should be the *authoritative* source of identity. If AAD is the authoritative source, then user credentials can be directly validated in the Azure. If AAD is a non-authoritative source, then users will be redirected to an on-premises authoritative source for credential validation.

Some of the key factors in choosing where your authoritative source should reside are:

* On-premises AD provides a level of granular functionality which is currently not available in AAD. Retaining an authoritative on-premises identity directory may be necessary for continued operation of some existing on-premises applications.
* Moving to an authoritative AAD identity directory simplifies the set of components needed to maintain synchronization across environments.

### Directory federation

Active Directory Federation Services (ADFS) is an on-premises, standards-based Microsoft solution that can be used to connect directories using WS-Federation, WS-Trust, SAML, and OAuth. Federation of on-premises AD with AAD provides a level of integration that goes beyond what can be achieved with just Directory Synchronization, to fully facilitate scenarios including single-sign on and the seamless exchange of identity related information between selected trusted partners. For more information about ADFS, see the [AD FS Design Guide in Windows Server 2012 R2](https://technet.microsoft.com/en-us/library/dn554245.aspx).[[6]](#footnote-6)

The key benefit of a hybrid environment with federated identity directories, is that once users (or applications) have authenticated in one environment, their credential token can be used across the hybrid environment to access applications and resources in either on-premises or public Azure. This concept underpins experiences like Single Sign On (SSO), and creating other user experiences that seamlessly span hybrid environments – for example, a single store that presents a user with a set of applications they are authorized to access, spanning both on-premises and cloud based applications.

Some of the key considerations in choosing a directory federation approach over directory synchronization are:

* The importance to your organization of enabling the more seamless user experiences (like SSO) provided by federation.
* Distributed applications with components running across environments, may require trusted access between environments.
* Federation incurs additional costs related to the installation and operation of an ADFS instance to coordinate the federation between your on-premises AD environment and AAD.

When federating identities between AD and AAD, while the federated identity conceptually has the full set of properties of the individual objects in both AD and AAD, applications will only be truly portable across environments where the object properties they depend upon are supported by both. Many existing on-premises solutions are likely to leverage the extended support in AD for computers and group policy, which are not (today) supported in AAD. This does not reduce the desirability of federating identities across the AD and AAD realms, but it has implications when looking at application migration scenarios.

While AD and AAD are designed and architected for different needs, there are similarities as outlined in the table below:

|  |  |  |
| --- | --- | --- |
|  | AD | AAD |
| Location | On-premises | Cloud |
| Support for Users | Yes | Yes |
| Support for Groups | Yes | Yes |
| Support for Devices | Active Directory Domain Join | Azure AD Join |
| Support for Management | Group Policy | Mobile Device Management Policies |
| Primary Interaction | NetLogon API, LDAP, Directory Service API | REST |
| Authentication Protocol | NTLM and Kerberos | WS-Fed, SAML, OAuth, OpenID Connect |
| Administration Tools | Active Directory Administrative tools and PowerShell, | PowerShell, Portal |

Table : Comparing Active Directory to Azure Active Directory

## Managing IAM in hybrid environments

In a hybrid environment, you can choose to manage IAM either from Azure AD experience provided as a service from the cloud, or from on-premises management tools. Azure AD offers a broad range of management solutions tailored for enterprise and users’ personal needs. On-premises management capabilities are provided using AD, ADFS, and Microsoft Identity Manager (MIM).

Some key differences between the two approaches include:

* Using on-premises management tools incurs ongoing cost associated with maintaining on-premises components to provide management experiences, compared to the simplicity of consuming IAM management services from Azure.
* There are (currently) some differences in management capabilities available between the two different approaches. These are described in more detail below.

There is a middle ground between these approaches, where an enterprise can utilize on-premises management where necessary in the immediate short term, while also starting a journey towards identity management-as-a-service using AAD. Prioritizing which management experiences are important and selecting the right combination of management experiences is a key part of IAM design.

The following sections describe several management scenarios often seen as providing high value in hybrid environments, and details on how they can be enabled through AAD or on-premises management experiences (or both).

### Self-service management scenarios

The ability to offer self-service capabilities for users greatly reduces the overall cost of managing within an IT environment. Even a simple ability for users to reset their own password can result in significantly lower help desk costs. Microsoft’s on-premises IAM solutions empower users to manage some of their own identity attributes through a self-service capability, and AAD is no different in this regard. AAD offers self-service password reset and account lockout, group management, and a customizable portal for users to access all resources.

**Note** Self-service user management features are available in the Azure Active Directory Basic and Premium editions. For more information about the differing capabilities of the free and paid editions, see [Azure Active Directory editions](https://msdn.microsoft.com/en-us/library/azure/dn532272.aspx).[[7]](#footnote-7)

Some common self-service features in the context of hybrid environments are:

* Self-service password reset

Self-service password reset allows users in your organization to reset their passwords without calling on an administrator or helpdesk for support. In a hybrid environment, directory replication (password synchronization) or the directory federation service (ADFS) will ensure the user only needs to reset their password once. The user experience is provided either through AAD or by implementing MIM on-premises.

* Self-service group management and role-based access control

Self-service group management enables users to create and manage security groups. Users can request security group memberships, which can subsequently be approved or denied by the owner of the group. By using self-service group management features, the day-to-day control of group membership can be delegated to people who understand the business context for that group. The user experience is provided either through AAD or by implementing MIM on-premises.

* Multi-Factor Authentication (MFA)

MFA provides a more stringent authentication by making users pass through multiple separate authentication processes. Use of MFA is often mandated by corporate policy or regulation compliance, especially for high privilege accounts with access to sensitive data or administrative control. MFA can be enabled and managed through either on-premises or AAD based management.

* Access Panel

The Windows Azure Active Directory Access Panel is a web-based portal that allows an end user with an organizational account in AAD to view and launch cloud-based applications to which they have been granted access by the AAD administrator. When using Premium editions of AAD, users can also utilize self-service group management through the Access Panel. The Access Panel allows users to edit some of their profile settings, including the ability to:

* + Change the password associated with their organizational account.
  + Edit password reset settings.
  + Edit multi-factor authentication-related contact and preference settings (for those accounts that have been required to use it by an administrator).
  + View account details, such as their User ID, alternate email, mobile, and office phone numbers.
  + View and launch cloud-based applications to which they have been granted access by the AAD administrator.
  + They can create and manage security groups, and request security group memberships in AAD.

Similar capabilities can be provided on-premises through ADFS with some minimal customization, or through a custom portal.

### Additional IAM scenarios

There are many other scenarios dependent on IAM systems that provide significant value to corporations. Generally, these scenarios are important regardless of whether their IT infrastructure is predominately cloud based, on-premises, or a hybrid combination of the two. When designing hybrid environments, it is important to assess which scenarios built on IAM infrastructure are most important, and then understand how hybrid IAM design choices impact the ability to deliver those scenarios.

This section introduces a number of features available in either AAD or on-premises tools (AD, ADFS, MIM) which enable IAM scenarios. In hybrid environments, many of these depend on identity federation, but can be managed either from AAD or on-premises management tools. Links to more detailed implementation documents are provided, to help assess any design implications of enabling these scenarios.

#### Integrating Microsoft and third-party applications with federation-based SSO

When using federated SSO, an administrator can restrict the set of applications visible to a user. Administrators can configure applications for federation-based SSO by adding them into the Active Directory section of the Azure Management Portal and setting the single sign-on mode to Azure AD Single Sign-On (SSO). Users will only see applications that they have been explicitly granted access to. The following types of applications with SSO enabled can be included:

* Password-based SSO without identity provisioning
* Password-based SSO with identity provisioning
* Applications with existing SSO solutions

For more information, see [Active Directory Federation Services](https://technet.microsoft.com/en-us/library/dn554245.aspx).[[8]](#footnote-8)

#### Managing users from other directories in your AAD directory

It is often useful for a user to be a member of more than one directory. For example, where production environments are separated from development, each may have its own IAM directory, with a subset of users from production populated in the development directory. A directory administrator can add users to one directory from another directory provided the administrator is a member of both. Any individual user can be a member of up to 20 directories.

In this scenario, the display name and user name is copied from the user's "home directory" and stamped into the second directory as an external user resource. Subsequently, the properties of the external user object are entirely independent of the original user record. Any changes to the user in the home directory, for example changing the user’s name or adding a job title, will not be propagated to the external user account in the other directory.

The only durable link between the two objects is that the user always authenticates against the home directory. There is no ability to reset the password or enable multi factor authentication for an external user account, and currently, the authentication policy of the home directory is the only one that's evaluated when the user signs in.

For more information, see [Create and use external users](https://msdn.microsoft.com/en-us/library/azure/hh967632.aspx#BKMK_5)[[9]](#footnote-9) in the Azure AD documentation.

#### Device management

In today’s security conscious but increasingly mobile world, controlling access to resources by authenticating only the user is not enough to provide the level of confidence most organizations demand. In environments where users can provide their own mobile devices which are outside of the organization’s direct control, it becomes desirable to create access policies in which authentication and access is based on multiple interrelated criteria:

* User identity
* The type of device that is attempting to access a resource
* The location from which the user or device is attempting to connect—Intranet i.e. connected to network in office, extranet i.e. connected from outside of the office network, or a home network

Using a combination of the above criteria to create access policies to specific applications, provides for higher scrutiny on user access to applications dealing with sensitive corporate data, especially from mobile devices. Traditionally, where a PC is joined to a domain, permission to access corporate resources could be controlled through group policy and other mechanisms. This approach allows a middle ground between all or nothing access for non-domain joined devices, allowing a user to work on the device of their choice and still have access to corporate resources.

For more information about protecting corporate resources in the context of mobile devices, see [Information Protection](http://www.microsoft.com/en-us/server-cloud/solutions/information-protection.aspx)[[10]](#footnote-10) on the Microsoft web site.

#### Workplace Join

Workplace Join is a feature introduced in Windows Server 2012 R2, which allows users to register devices (both Windows, and non-Windows such as iOS) and enable Single Sign-On (SSO) for access to corporate data. Workplace Join works in conjunction with AD and ADFS, and it requires an Enterprise Certificate Authority to work properly. With Workplace Join, we have the ability to offer granular control over access to corporate resources from a wide variety of devices. After a user registers their device, IT can grant that device and user access to corporate resources while still enforcing governance parameters on the device. You can think of Workplace Join as being a light form of Domain Join, but for mobile devices. Registered devices are recorded in the Active Directory and they are issued credentials. However, they don’t support Group Policy or scripting. Instead, you can manage the device from the cloud by enrolling it for mobile device management. The act of registering the device to Active Directory does not allow IT to control the device in any manner; that is covered by enrollment, and it is beyond the scope of this document. Workplace Join is only used to govern access to corporate resources and to enable SSO.

Devices registered using WJ can also be used as a seamless second factor of authentication. This means that users do not need to supply anything beyond their normal credentials to confirm their identity when using registered device to access resources. Device registration can be done on-premises using ADFS, or in the cloud using Azure Device Registration Service. As of this writing, the supported devices are:

* Windows 7 domain joined devices
* Windows 8.1 personal and domain joined devices
* iOS 6 and 7

For more information about Workplace Join, see the following resources:

* [Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications](https://technet.microsoft.com/en-us/library/dn280945.aspx)[[11]](#footnote-11)
* [Why Windows Server 2012 R2: Step-by-Step Workplace Join, Bringing Peace of Mind for BYOD](http://blogs.technet.com/b/matthewms/archive/2013/11/01/why-windows-server-2012-r2-step-by-step-workplace-join-bringing-peace-of-mind-for-byod.aspx)[[12]](#footnote-12)

#### Integrating cloud applications

Azure Active Directory (AAD) enables easy integration with many of today’s popular SaaS applications. AAD provides identity and access management and provides an Access Panel for users where they can discover which applications they have access to and which of those applications can use SSO. Once you have user identities connected to the external world via ADFS or AAD, existing applications can utilize these identities for authentication and access control. If an application is natively aware of this modern identity type, the application can use AAD or ADFS natively as depicted below. Examples of applications that can use modern IAM include SharePoint, CRM, various web applications, and Web API.

If an application relies on traditional forms of IAM, such as basic authentication or Windows authentication, the application can be published through a reverse-proxy solution if the transport protocol is based on HTTP payload. If an on-premises solution is used, Web Application Proxy (WAP) can be used, as shown in Figure 2: Traditional application authentication, below.



Figure : Traditional application authentication

If the application relies on AAD for IAM, Azure Active Directory Application Proxy (AADAP) can be used as shown in Figure 3: Modern application.

For more information see [Application Proxy Prerequisites](https://msdn.microsoft.com/en-us/library/azure/dn768214.aspx#BKMK_1).[[13]](#footnote-13)



Figure : Modern application authentication

For a comparison of the functionality available in WAP and AADP, see

Appendix 1: WAP and AADAP Comparison.

For more information about managing identity in a hybrid environment, see [Identity + Access Management](http://www.microsoft.com/en-us/server-cloud/solutions/identity-management.aspx).[[14]](#footnote-14)

# Managing in Hybrid Environments

As companies shift to leverage the on-demand, highly available, and low cost capacity from public clouds, there are similar shifts happening to take advantage of these same cloud characteristics in IT management approaches. Management capabilities consumed as cloud services enable tasks that were not practical in the past. At the same time, IT management is also adopting practices from agile developer paradigms to reduce the costs of supporting the applications and services required by business. The driving motivation behind these shifts is the quest to simplify the challenge of maintaining a healthy server environment.

Traditionally, administrators have deployed servers with the intent to use the same deployed operating system instance for the greatest duration of time possible, often providing uninterrupted service for multiple years. To facilitate this approach, management systems have been designed to retain detailed knowledge of each deployed node, and to identify when conditions indicate a possible failure.

In cloud operating models, administrators look at servers collectively as simple compute capacity. Each individual node is expected to perform a portion of the work to support a service. The business need for continuous availability has not changed, but the approach to how the service is delivered and maintained is to spend less time resolving unexpected errors on individual nodes and focus on the quality of the service. Capacity to host the service is considered to be a disposable resource that is always in the intended state. If the application or service is not in its intended state, the simple answer is to redeploy the current application build to recycle the server nodes to the desired operational state. This shift represents a significant change to management processes and thus management tools.

Another shift in management tools is to move from a solution deployed and maintained locally (the traditional software model) to a service hosted in a public cloud and consumed on-premises. Cloud-hosted management offers numerous benefits compared to running a solution entirely on premises. First, there is no longer a need to deploy and support the management tools that provide services to support operations, and second, cloud-hosted environments offer the opportunity to use massive amounts of compute capacity for short periods of time at a low cost. The bountiful, low-cost resources of a public cloud bring sophisticated capabilities within reach of organizations that would otherwise be unable to justify the cost of maintaining those capabilities on-premises. introduce capabilities such as storing more log data than would have been possible in an on-premises monitoring solution, and then performing Big Data analysis of the data to identify trends and patterns, using cloud resources that would be prohibitively expensive for many organizations to maintain on-premises. that would have required very expensive hardware to analyze on premises.

Microsoft offers a combination both traditional on-premises management tools through its System Center (SC) products, and a growing set of cloud based management services through the Microsoft Operations Management Suite (OMS). Both SC and OMS offer the ability to manage across on-premises and public cloud resources. OMS provides a number of capabilities which take advantage of the benefits (described above) of the Software as a Service (SaaS) model. Current OMS capabilities include Log Analytics, Security Analysis, Business Continuity and Disaster Recovery, and Azure Automation. Enhancing management functions through cloud service-based solutions signals a shift towards a more balanced hybrid approach to management tools and services.

In reality, a full shift to management as an IT Service (sometimes referred to as ITMaaS) cannot happen overnight. Many organizations will find that their suite of applications and services includes new services that are specifically designed for agile approaches to management, but many of their existing applications will likely be difficult to manage using the same concepts.

This section describes some of the new approaches to different stages of the management lifecycle, to help clarify some of the management tools and approaches that can be leveraged in the design of hybrid cloud environments.

## Deployment

Shifting to a management model where infrastructure can truly be treated as a collection of easily recyclable assets, depends on achieving high agility and predictability in deployment processes. While IT administrators have always had a vested interest in streamlining the process for deploying new server capacity, moving to a model where redeploying a server or application is the default remediation approach, elevates the importance of minimizing the time required to flatten and rebuild an individual server back to a known state.

In addition, the predictability of deployment processes become hugely important. Completely rebuilding a server to remediate an issue with only partial impact to services exposes a risk of more significant business impact if the rebuild fails. Ensuring that the process to rebuild a server is highly repeatable, and ideally completely automated to remove the opportunity for human error, will minimize the risk. The payoff for developing a simple, repeatable model is high, reducing the dependence on manual troubleshooting of individual issues, thus reducing the overall cost and time traditionally invested in manually maintaining individual server health.

Many of the traditional approaches and tools used by administrators today to manage deployment of on-premises systems, both physical and virtual, continue to be important to achieve these shifts in agility and predictability. These include the following:

### Operating system installation

The key components of an OS deployment platform include the following concepts, which should already be familiar to most administrators.

Installation Sources

* Install from media (example: Windows Server 2012 R2 DVD)
* Install from captured image (example: Windows Image File)
* Boot to image (example: Windows Preinstall Environment)

Delivery Tools

* PXE service (example: Windows Deployment Service)
* Virtual Disk template (example: Virtual Hard Disk file)
* Storage volume provisioning (example: NetApp Thin Provisioning)

In a hybrid cloud environment, the images used on-premises can also be used when provisioning virtual machines in a public cloud environment. Value can be achieved through standardizing the images and tools used for deployment across both environments, as well as streamlining the tools used in the task of image creation and management.

### Optimizing server footprint

Reducing the footprint of the server image deployed can significantly reduce the time to deploy a new server. Different application services could have dependencies on different OS components, so it is important to analyze the requirements to determine the minimal OS installation type per application. Favoring the smallest footprint available for a given server role reduces the time to deploy, and also delivers other benefits such as reducing the total attack surface and servicing requirements. For more details on the OS installation options available, refer to the following documents.

* Minimal footprint OS environments (example, Windows Server Core, Nano)
* Desktop footprint OS environments (example, Windows Server Full)
* When required by application support requirements, deploy a server OS that includes a desktop environment

### Offline servicing

Another deployment optimization technique is to design for automated offline servicing of the images that will be used throughout the environment. Ensuring images are fully patched removes the need for updates and reboots after deployment. This capability has improved in Windows Server 2008 R2 and later, through the latest DISM tool set. OS images in WIM or VHD(X) format can be mounted to a workstation and modified “offline” without the need to deploy and recapture an image. Some of the capabilities in this solution include:

* Apply security updates
* Add additional drivers, including storage drivers required for deployment
* Add and remove features and components of the OS, especially those that require the source media to install
* Add and remove files, including [answer files](https://technet.microsoft.com/en-us/library/cc749113(v=ws.10).aspx)[[15]](#footnote-15) and automation scripts
* Add and remove MOF[[16]](#footnote-16) files for the local configuration manager
* Add and remove registry settings

### Baseline server configuration

Administrators will already familiar with using server images to deliver server configuration, defined during the image capture process. Using the modern OS deployment toolset, instead of “capturing” these configuration changes they can be integrated into the image using the answer file. This adds a level of agility by decoupling the settings, which are applied during the OOBE (“out-of-box experience”) phase of Windows Setup or executed as part of a custom script that will run as soon as setup completes.

Examples of work that might be integrated into an answer file:

* Set the username, password, and status for built-in accounts
* Default computer name
* Product Key

Examples of tasks that might be executed by a script (%WINDIR%\Setup\Scripts\SetupComplete.cmd):

* Configure firewall rules that are needed during the deployment process or as operational requirements
* Install agents that will connect the machine to operational services, such as public cloud automation and monitoring
* Deliver the default meta-configuration that connects the local configuration manager to a public cloud service

An exception to consider is the installation of very large applications. For example, Microsoft SQL Server offers the ability to pre-install the setup files in to an image and generalize the environment as part of a sysprep operation. In this case, an image capture process might be the best solution.

## Image management in hybrid environments

Once you have a set of optimized server images, there is an opportunity to automate the process for image creation and maintaining consistency between the on premises environment and the nodes deployed in public clouds.

Azure Automation offers the [Hybrid Runbook Worker](https://azure.microsoft.com/en-us/documentation/articles/automation-hybrid-runbook-worker/)[[17]](#footnote-17) so that PowerShell workflows and scripts can be stored in a public service, together with important assets such as credentials, keys, paths to install files, etc., and then executed on premises.

Examples of tasks that could be automated using a Hybrid Runbook Worker to automate image creation and management across a hybrid environment:

* Automatically create VHD files from ISO media after the ISO is added to a folder.
* Check for security updates that are applicable to VHD images and apply them to the image mounted offline. For more information, see <http://blogs.technet.com/b/privatecloud/archive/2013/12/07/orchestrated-vm-patching.aspx>.
* Update username, password, and status of built-in accounts for the image based on credential assets stored in the service.
* Obtain the latest copies of scripts from source control and insert them in to the image to be executed when setup completes.
* Synchronize the images to cloud storage for use in deployments.
* Automate test procedures in cloud VMs to verify health of images used across private/public.

## Configuration management

Designing hybrid cloud environments offers an opportunity for architects to create a solution where the configuration of servers is consistent regardless of whether nodes are deployed to a public cloud or a private cloud. This approach provides an increased level of predictability of configuration, and can be used regardless of whether the applications on each server node will be managed using a change management philosophy that is based on long term deployment or continuous deployment. The vision that will need to be defined is how a *release management pipeline* will be constructed to handle *configuration as code*.

To enable a *Configuration as Code* strategy in a hybrid environment, Azure Automation offers a [Desired State Configuration](https://azure.microsoft.com/en-us/documentation/articles/automation-dsc-overview/)[[18]](#footnote-18) (DSC) service. Servers that are registered and configured to connect to the service can receive configuration details defined by server role.

Additional service roles that should be considered part of the design:

* A repository to store configuration scripts and PowerShell DSC modules where multiple authors can contribute.
* A build service to run PowerShell Pester[[19]](#footnote-19) tests against the scripts at check-in, and publish to Azure Automation when no errors are discovered.

In this strategy, the configuration of a server role should be defined before production deployment. The current configuration script that is checked in to source control should be considered the authority for how each server role will be configured. This can also be considered part of the documentation effort for the environment. When changes will be introduced to the environment, they should only be introduced to the configurations scripts. Using this approach, all changes will automatically be documented with contributor, description, and a time signature, as each change is submitted to the repository.

Consider the following approaches based on application requirements:

* If an application includes complex state information and the expectation is that each server will be deployed and maintained for an extended period of time, the service would provide incremental changes in server configuration. (Example: implementing configuration change to modify an application due to issues raised with the local help desk)
* If an application is stateless and can be redeployed without interrupting the production service, as each new node is deployed it can receive the latest configuration changes based on the configuration name. (Example: web servers)

Azure Automation service is available to any server; they do not have to be hosted as virtual machines on Azure. This means that servers hosted in other public cloud environments such as Amazon AWS and physical or virtual servers running on premises can be configured to retrieve configuration details from the online service. This offers an opportunity to uniformly deploy server roles regardless of location, which reduces complexity in troubleshooting.

## Monitoring

The approach to monitoring a hybrid cloud environment must take into consideration both the need to understand the health of cloud infrastructure and the services (resource capacity) it provides to applications, and the health of the application services delivering business value to users. This is a subtle change from traditional IT environments, where the health of an application included the health of the underlying servers as a component. When monitoring cloud environments, the health of the underlying infrastructure is separated out as a service in its own right. When this service is provided by a public cloud provider such as Azure, this is provided with specific SLAs around availability, resilience, cost and scale agility.

Monitoring typically refers to collecting information, representing this information through instrumentation dashboards, and automatically responding to prescribed conditions through alerting systems and/or remediation tasks. In the simplest of examples monitoring refers to a task such as highlighting in an operations dashboard when a server node has not responded to an ICMP request for some threshold number of seconds, and then sending an SMS alert to operations personnel. Monitoring information typically includes a spectrum of data from service performance and reliability to server state and security compliance.

As we think about infrastructure consisting of recyclable compute capacity, a service health approach requires a greater level of integrated service monitoring. An example of service monitoring is aggregating information across many nodes, and then sending an alert when application code returns an error, a sudden change in the number of connected users, or a fewer number of active connections than is expected for a day and time given historical trending.

Traditional on-premises monitoring solutions have been expensive to deploy and maintain at scale. As the number of servers being monitored increases, the amount of data being collected also increases as does the server, networking, and storage infrastructure needed to collect and maintain monitoring data. If historical trend analysis of the data collected is a requirement, then a Big Data platform is also required, which can add significant cost to IT operations.

Microsoft Azure provides the [Log Analytics](https://azure.microsoft.com/en-us/services/operational-insights/)[[20]](#footnote-20) solution as part of the Operations Management Suite (OMS) to address these needs. The [Microsoft Monitoring Agent](https://technet.microsoft.com/en-us/library/dn465153.aspx)[[21]](#footnote-21) is deployed to server nodes to collect information, and results are loaded to the service. The monitored nodes can be located either on-premises or in a public cloud, and are configured directly to send log data to OMS. Alternatively, in on-premises environments System Center Operations Manager (SCOM) can be used as a point of control to configure multiple nodes for data collection, rather than configuring each node individually. After data is collected, Microsoft Azure provides the computing power to analyze log data. As a consumer of the online service, customers avoid the capital cost of deploying a Big Data platform but are able to customize the rules in regards to which queries should be run against data, customize reporting, and set alert thresholds for notifications.

While cloud based management services provide some powerful new approaches to monitoring, designing for monitoring in a mixed cloud environment involves establishing a balance with traditional on-premises capabilities. Some of the design influences will include:

### Data flow topology

Big Data approaches require large amounts of data to identify meaningful patterns and trends. While public cloud-based services can provide the on-demand computing resources necessary to provide great analytic experiences, they will be constrained by any filtering imposed on the data logs collected from the services (servers, applications) being analyzed. In large hybrid environments, the scale of unfiltered data has the potential to incur unwanted costs, in network utilization, service costs, or latencies in the collection process.

Log filtering to fine tune monitoring systems is not a new concept, and users of System Center Operations Manager (SCOM) today are familiar with the need to target the set of logs and alerts being collected. When extending this to a public cloud services, the implications on the network connectivity from the on-premises site(s) to the public cloud service must be assessed, to ensure the network connections have the needed capacity to deal with unfiltered data logs (refer to Networking section).

In addition, all the implications on internal network capacity within the on-premises sites need to be understood. The agents used to collect and compress data for cloud services like OMS, are based on the proven technologies used in on-premises systems like SCOM today and are highly effective at minimizing network load, so network implications should be minimal even with large increases in collected data. OMS service scales out as needed to consume and unpack this data real time at scale.

### Real-time alerting

The capabilities in monitoring services such as OMS are continually expanding, and recently new “close to real time” solutions, such as performance counter collection, have been enabled. These utilize polling cycles as frequent as every 10 seconds, which is (typically) more than adequate for user-monitored dashboards.

When looking at automated remediation of detected issues, the impact of the sum of latencies in detecting the problem and executing the remediation task need to be considered. To this end, it is likely that in some scenarios, an on-premises solution will provide a more agile response than a cloud based service.

### Data sensitivity

As with many aspects of the shift to public cloud computing, the implications of sensitive data leaving the boundaries of a corporate datacenter need to be assessed. IT metadata, especially machine identifying information like server names and IP addresses, is often considered sensitive. Using a cloud-based service for IT management may drive other design requirements such as use of dedicated network connections (e.g. ExpressRoute).

## Self-healing service management

After data about server nodes has been collected and analyzed to identify health issues, actions can be automatically taken to notify operations personnel or, by combining the service with Azure Automation, actions can be taken automatically. Azure Automation executes PowerShell scripts, which could then call any other endpoint ranging from a web service API to making an SSH connection and executing some other embedded code/script language. With PowerShell as the foundation, there is a lot of flexibility about the types of downstream actions that could potentially be taken. Examples:

* Create a new record in a help desk platform
* Restart a service, daemon, or operating systems
* Remove nodes from a load balancing service
* Verify configuration state and notify operators via Email regarding configuration drift
* Create a new item in a database or collaboration platform such as a SharePoint list or a Slack[[22]](#footnote-22) channel

In a traditional on-premises environment this role might have been provided by a server node configured with scheduled tasks to run scripts at a given frequency, or by an automation platform such as System Center Orchestrator or System Center [Service Management Automation](https://technet.microsoft.com/en-us/library/dn469260.aspx).[[23]](#footnote-23)

In a hybrid environment, Azure Automation provides an online service for executing PowerShell without the need to host a complicated on premises solution. Scripts can be written either in the form of runbooks or scripts.

* ***Runbooks*** leverage PowerShell Workflow so that activities can be broken in to smaller stages and restarted from checkpoints throughout a long running process.
* ***Scripts*** provide an easier authoring experience than runbooks for short jobs where checkpoint restarts are less of a concern.

Azure Automation provides an [Automation Assets](https://azure.microsoft.com/en-us/blog/getting-started-with-azure-automation-automation-assets-2/) storefor maintaining important data securely. This could include general information such as service endpoint addresses, server names, or Email addresses for operations contacts, or secure information including usernames and passwords for service accounts required throughout the environment.

Activities can be authored using a graphical authoring interface where common script actions are combined using a “drag and drop” interface. To accelerate authoring, examples can be pulled from the online [PowerShell Gallery](https://www.powershellgallery.com/) and [TechNet Script Center](https://technet.microsoft.com/en-us/scriptcenter/bb410849.aspx).

In public cloud environments, the online service typically will make direct network connections to managed servers. For servers deployed on premises, the Hybrid Runbook Worker can be installed on a server within the local infrastructure. Hybrid Runbook Worker will retrieve jobs from the online service that are queued for execution on premises so required connections to managed servers can reach across a local network. This allows administrators to use the online asset store, graphical authoring, script examples, and ensures the same automation activities are run across servers in both public and private clouds.

Designing how a service will maintain “run state” in different failure situations is important in driving towards self-healing services. For traditional applications this might include managing planned configuration changes, and making unplanned changes visible to operations personnel. For applications deployed as a service across many disposable server nodes, this might mean continually deploying service updates or even replacing server nodes entirely, on a frequent cadence.

## Examples

Below are two contrasting examples of applications with different run state maintenance process models in a hybrid environment, combining multiple application models:

#### Virtual machines are deployed to a private cloud environment to store information due to a regulatory boundary.

This application is purchased and deployed to a fixed number of servers. The deployment is delivered as a configuration end state. The servers are monitored for health, performance, and security related information. Configuration changes are introduced as published changes to the configuration state. Maintenance activities occur during a standard change window by running scripts to perform work such as installing security updates or resetting service account passwords.

Hybrid services include:

* Azure Automation Desired State Configuration for initial deployment to a known end state, publishing planned configuration changes, and reporting on configuration drift
* OMS Log Analytics for monitoring and reporting
* Azure Automation for activities based on OMS Log Analytics data to interact with other services and maintenance activities using a Hybrid Runbook Worker

#### Virtual machines in a public cloud host a custom web application.

Aggregate information from the data set does not have the same regulatory requirements so it can be safely stored in a public cloud environment where capacity bursts are deployed based on business requirements. Information collected by the web application is processed as transactions and output is returned either to on premises servers or to online storage services based on the data type and requirements.

The web front end is updated several times per day to respond to changing user interests. The servers must meet baseline security requirements, and to reduce service troubleshooting in outage events, the server nodes should have operating system configurations consistent with servers deployed on premises. Changes are introduced as application releases. New servers are deployed with the latest code and old servers are retired by modifying load balancer settings. No data is stored on individual server nodes.

Hybrid services include:

* VM Image consistency across on premises and public cloud deployment templates so server baselines are not unique to any one environment.
* Azure Automation Desired State Configuration for deployment to a known end state. As application requirements change, new versions of the server end state configuration are published to the online service and referenced in the Azure Resource Manager deployment template.
* OMS Log Analytics is used to monitor and report on the state of the service and provides analysis of log information long after individual server nodes are deprovisioned.
* Azure Automation for activities based on OMS Log Analytics data to interact with other services such as publishing notice of new deployment activities in to a Slack communications channel or SharePoint list.

# Business Continuity and Disaster Recovery

Most businesses today are critically dependent on the continued availability of their IT environments to support business operations. Business Continuity and Disaster Recovery (BCDR) allows organizations to resume operations as soon as possible when components fail, which can be due to catastrophic natural disasters (flooding, earthquakes, fire, hurricanes), or sometimes even caused by human component errors during operations. Traditional BCDR solutions tend to require expensive secondary datacenters, with complex and time consuming processes to validate the protection and recovery SLAs, which includes the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

When a disaster occurs, RTO is used to measure the amount of time that takes a business to resume operations, while RPO measures the period of time in which data might be lost. Businesses’ BCDR strategies aim to minimize RTO (get back to operations as soon as possible) and RPO (minimize data lost) at the minimal possible cost.

In hybrid IT environments, new approaches to traditional BCDR solutions are possible, leveraging benefits of the public cloud such as the relatively inexpensive capacity. The pay-as-you-go model of public clouds changes the cost equation for BCDR by removing the cost of maintaining stand-by failover capacity, but at the same time, knowing that the capacity will be there in case it is needed. In addition, cloud based BCDR services gives businesses the flexibility to leverage the cloud as best suits their needs leveraging existing investments, in other words, you only consume what you need.

## Azure Site Recovery

[Azure Site Recovery (ASR)](https://azure.microsoft.com/en-us/documentation/learning-paths/site-recovery/) is a cloud service of Microsoft Azure that is part of the [Microsoft Operations Management Suite](http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx) (OMS) which provides a Disaster Recovery as a Service (DRaaS) solution for applications running on Windows and Linux servers. ASR facilitates DR to and from Azure (also called *failback*), or between on-premises datacenters. ASR relies on the Azure infrastructure to provide site recovery to (or from) cloud-based storage and compute resources, or it can act as the management plane for your on-premises or datacenter-to-datacenter DR plans. You can failover individual servers and/or failover applications spanning multiple servers across your datacenter. The rest of this section is a detailed look at the failover scenarios available at the time of this writing.

### Using ASR as a cloud-based management plane for DR

Some organizations already have infrastructure investments on-premises, such as having secondary datacenters for DR purposes, high-speed network connectivity between sites, and even SAN replication across sites to support their DR strategy. In such cases, ASR offers the flexibility to leverage existing on-premises investments, managing the recovery plans from Azure, but all the customer data remains on-premises. Data is replicated between sites, and ASR handles the orchestration to failover virtual machines to the recovery site when required. ASR acts as the management plane for the DR plans, and no customer data is replicated to Azure. For this scenario, ASR supports the following protection:

* Between two System Center Virtual Machine Manager (SCVMM) sites
* Between a site with physical servers and VMware VMs, and between two VMware sites

In these two scenarios, ASR acts as the management plane running on Azure to orchestrate the disaster recovery of your applications between two on-premises datacenters. Although you are leveraging a public cloud-based Azure service to manage your DR, all of your data remains on-premises. Customer data is not replicated to Azure. The only data shared with Azure is metadata that is required to orchestrate the DR, such as source and target sites, and the virtual machines to protect.

### Leveraging Azure as a DR site

Some organizations do not have secondary datacenters, or perhaps they are consolidating datacenters and want to make use of the capacity available in the public cloud to support their DR strategy. For these scenarios, ASR supports the following protection:

* Between an on-premises SCVMM site and Microsoft Azure
* Between an on-premises Hyper-V site and Microsoft Azure
* Between an on-premises site with VMware/physical servers and Microsoft Azure

In these scenarios, while ASR also acts as the management plane to orchestrate the disaster recovery of your applications, Microsoft Azure is the recovery site for your applications. When you use Microsoft Azure as your recovery site, you get the benefits of off-site storage with the redundancy and economy of scale of cloud capacity.

Figure 4 graphically illustrates the difference between using ASR as the cloud-based DR orchestration service for recovery to an on-premises datacenter, and using ASR in conjunction with Microsoft Azure as the recovery site:



Figure : ASR datacenter-to-datacenter compared to ASR datacenter to Azure.

## Designing a disaster recovery strategy with ASR

ASR offers flexibility to protect customer’s applications running on supported Windows and Linux servers, but you may be wondering which scenario(s) to choose. There are different facts that can influence your decision if you implement a DR solution based in ASR between two on-premises datacenters or between an on-premises datacenter and Microsoft Azure. In this section we will review some typical factors and we will provide guidance that can help you design the DR strategy that best fits your organizational needs.

### Choosing your recovery site

There are several factors that you should take into consideration when deciding if your DR strategy should be implemented between two on-premises datacenters or between an on-premises datacenter and Azure. Among the factors that might incline you to implement an on-premises to on-premises DR strategy include:

* You already have investments in a secondary datacenter with available capacity to failover your applications to the secondary site.
* Excellent network connectivity between sites.
* A Storage Area Network (SAN) is deployed at both primary and secondary sites with SAN replication enabled.
* You have applications running on hardware configurations that are not currently compatible with Microsoft Azure, such as guest clusters or servers with disks larger than 1TB.
* Poor connection links to the internet and to Microsoft Azure.
* In some scenarios, regulations may restrict the ability to use an out-of-country public cloud as a replication target for sensitive applications.

Some factors that might incline you to implement an on-premises to Microsoft Azure DR strategy include:

* Your organization has only one on-premises datacenter
* Your organization has a dedicated site-to-site (S2S) VPN connection to Azure or has leased an ExpressRoute circuit
* Your organization is consolidating datacenters
* You have branch offices with good connectivity to the Internet and an Azure datacenter, but slow access to corporate sites

These are some common factors you may have to take into consideration when deciding if your DR strategy is better off using on-premises datacenters, or if you should leverage Microsoft Azure as your recovery site. The next section goes into more details on currently supported scenarios for both approaches.

When designing your DR protection either between two on-premises datacenters or between an on-premises data center and Microsoft Azure, you need to consider the following factors:

* Platforms supported by ASR
* How the data can be replicated between the primary and the recovery site
* Network address space in a DR environment

The following section describes in detail these considerations for both scenarios, on-premises to on-premises protection and on-premises to Microsoft Azure protection with ASR.

#### On-premises to on-premises protection with ASR

When designing your protection model between two on-premises datacenters, you need to understand which environments can be protected by ASR, and how the data can be replicated between the primary and the recovery site. At the time of this writing, the supported scenarios for on-premises to on-premises DR with ASR are:

* You have SCVMM managing Hyper-V hosts on your primary and recovery site, and the data replication can be done via:
  + Hyper-V Replica (host-based replication)
  + SAN Replication (storage-based replication) – see the list of our [SAN storage partners](http://social.technet.microsoft.com/wiki/contents/articles/28317.deploying-azure-site-recovery-with-vmm-and-san-supported-storage-arrays.aspx)[[24]](#footnote-24)
* You have VMware or physical servers on your primary site, and VMware on your recovery site. In this case the replication is done via InMage Scout[[25]](#footnote-25)(guest-based replication).

Figure 5 below depicts the scenarios supported for on-premises to on-premises DR protection with ASR:



Figure : On-premises to on-premises protection with ASR

#### On-premises to Microsoft Azure protection with ASR

When you are designing protection model to leverage Azure as your disaster recovery site, you need to understand which environments can be protected by ASR, how the data is replicated between the on-premises site and Microsoft Azure, and the networking options that you have to connect the on-premises site with Microsoft Azure. At the time of this writing, the supported scenarios for on-premises to Microsoft Azure DR with ASR are:

* SCVMM is managing Hyper-V hosts on your on-premises datacenter and the data replication to Azure is done via Hyper-V Replica (host-based replication).
* You have a Hyper-V server(s) on your on-premises site without SCVMM managing it (for example, a branch office) and the data replication to Azure is done via Hyper-V Replica (host-based replication).
* You have VMware or physical servers on your on-premises datacenter and the data replication to Azure is done via InMage Scout (guest-based replication).

These scenarios are depicted in the following picture:

**

Figure : On-premises to Microsoft Azure

In these cases, as there is a need to replicate data from your on-premises datacenter to Microsoft Azure (and potentially from Microsoft Azure to your on-premises datacenter in case of a failback), the connectivity between your on-premises datacenter and Azure becomes important. You can refer to the Connecting Clouds section in this whitepaper for more details on these connectivity options to Azure. You can leverage any of the data replication channels discussed in the Connecting Clouds section of this whitepaper (site to site VPN or ExpressRoute) or also you could replicate directly over the internet where traffic will be encrypted.

Besides the factors already discussed previously in this whitepaper that will help you to select the right replication channel to Microsoft Azure, you should also bear in mind the following considerations when protecting on-premises servers with ASR having Microsoft Azure as the recovery site:

* **Network bandwidth to Microsoft Azure**—this is a key factor that can have a direct impact on your overall DR strategy to Azure. Consider the following key factors when planning the network bandwidth requirements to Azure:
  + Bandwidth required for the initial replication (IR). Initial replication can transfer large amounts of data to Azure per virtual machine. Depending on the available bandwidth and the number and size of virtual machines you are protecting, the IR window (time you have to wait for IR to complete) can be low (you don’t have to wait too long for IR) or it can be very high (something you might not want).
  + Average network bandwidth for delta replication. This will be the result of the number of virtual machines you are protecting and the average churn rate (daily delta replication).
  + You can enable protection in batches (to reduce IR window) and control networking traffic using ASR agent.
  + When replicating large amounts of virtual machines to Azure, consider ExpressRoute or WAN optimizers. For more information about ExpressRoute + ASR, see the Virtualization Blog post [here](http://blogs.technet.com/b/virtualization/archive/2014/07/20/expressroute-and-azure-site-recovery.aspx)[[26]](#footnote-26).
* **Azure IaaS constraints**—for example:
  + Disks must be < 1TB
  + No support for guest clusters
  + Other limits imposed by Microsoft Azure per subscription. For more information, see footnote 26.
* **Security considerations**—data replication using direct connection over the Internet, site-to-site VPN and ExpressRoute provide different levels of security. These factors may help you to choose the right approach for your environment:
  + Directly over the Internet – traffic is encrypted.
  + Site to site VPN – traffic is also encrypted, and you have a direct private connection Azure Virtual Networks in your Azure subscription. This will enable you not only to replicate ASR traffic securely over the VPN tunnel, but also application traffic could be replicated using this channel, for example AD DS or SQL Server AlwaysOn traffic.
  + ExpressRoute – traffic bypasses the Internet, and you’ve a direct connection to Microsoft datacenters via an ExpressRoute circuit. This will give you not only a secure private channel to your Azure subscription, but also, you’ll have a predictable performance, secure and high throughput connection to Azure.

You can leverage the Azure Site Recovery Capacity Planner tool (available [here](https://gallery.technet.microsoft.com/Azure-Recovery-Capacity-d01dc40e)[[27]](#footnote-27)) to help you analyze your source environment and plan for your DR solution requirements.

Also, it’s important to know that Azure imposes some limits by default (which can be raised up to the maximum limit) on services offered. For more information about service limits, see [Azure Subscription and Service Limits](https://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/)[[28]](#footnote-28) in the Microsoft Azure documentation. You should familiarize with these limits when designing your DR strategy that targets Azure as your recovery site.

### Network address space in a DR environment

One key factor that you must plan carefully when designing your DR strategy is how users and customers will connect to the applications when the servers they run into are failed over to the recovery site, whether on-premises or in Microsoft Azure. Basically, this implies if you’re planning to retain existing IP addresses when failing over to the recovery site, or if you will change IP addresses to the ones that are used in the recovery site. This is a topic that falls out of the scope of this document. For more information about designing and implementing a DR strategy, see “Designing Your Network Infrastructure For Disaster Recovery”[[29]](#footnote-29)

# Hybrid Applications and Workloads

Ultimately, the purpose of any IT infrastructure is to support the running of applications and workloads which provide value to the business. For existing business applications, the decision to shift an application to run in a public cloud should be driven by tangible improvements in operational characteristics such as cost, performance, reliability, and agility.

In hybrid environments where choices exist between hosting applications in traditional datacenters or using public cloud capacity, decisions around individual workloads or applications tend to fall into one of the following cases:

* Choosing between running the application solely using either on-premises or cloud capacity
* Choosing to split the existing components (layers) of the application between on-premises and cloud capacity
* Choosing to refactor the application, optimizing different components to run on either on-premises or cloud capacity
* Developing an application from scratch (greenfield), architecting the application specifically to take full advantage of cloud based capabilities (cloud-born) or both on-premises and cloud capabilities (hybrid-born)

This section will work through a few of the factors influencing the above choices, and look at the implications of application deployment choices may have on the design of your hybrid environment. For example, when an application spans both on-premises and public cloud worlds, the demands of that application on the connectivity between on-premises data centers and the public cloud influence network connectivity design choices.

## Data placement

Some of the biggest factors influencing the placement of applications, or components of applications, between on-premises datacenters or public cloud, are those surrounding the application data. Data sovereignty, privacy, and/or security concerns will in some countries favor on-premises placement, either of the full application or the key application components storing application data. Often these concerns can be more perception than actual, and undermine the opportunity to take advantage of the real benefits of cloud hosting, so due diligence is required.

Some of the important considerations in placing application data in a public cloud include:

* **Cost advantages**: The cost of storage in public clouds such as Azure can be significantly lower than the cost of maintaining storage with similar characteristics in an on-premises datacenter. Of course, many companies will have existing investments in high-end SANs, so these cost advantages may not reach full fruition until existing hardware ages out.
* **Scale agility**: Planning for and managing data capacity growth in an on-premises environment can be challenging, particularly for applications where data growth is difficult to predict. For these applications, cloud-based placement can take advantage of the capacity-on-demand and virtually unlimited storage available. In contrast, applications which consist of relatively static sized datasets are equally suitable for placement on-premises or in public cloud (on this dimension).
* **Data assurance**: When placing applications in public clouds such as Azure, protection of data through redundancy is provided automatically with multiple copies of data placed across disks, racks, and even geographic regions. Similar levels of protection can be provided in on-premises infrastructures through data replication technologies where multiple datacenters are available. In hybrid environments, these same technologies can be used to replicate between on-premises and cloud based data stores.

## Application architecture

Understanding the component architecture of an application is extremely important when thinking about deploying an application in a distributed (hybrid) way, or refactoring an application to optimize deployment across a hybrid or pure cloud infrastructure.

In a pure migration scenario, where an existing on-premises application is moved (as a whole) to public cloud, the internal dependencies between components will be less important than understanding external factors such as authentication, user scale, and external connectivity demands.

When distributing an application’s components, for example to take advantage of the cost of storage in cloud whilst keeping key processing and user presentation components on-premises, understanding the internal application interdependencies becomes critically important as you decouple application components from each other. These dependency factors include:

* **Internal data transfer patterns**: In particular, the size and frequency of data moved between components that are split between on-premises and cloud locations, places important requirements on the hybrid network connectivity design. When refactoring applications, caching approaches will often provide good solutions to optimize data transfer between components. In addition, it is important to assess any additional data security considerations associate with such inter-component data transfer.
* **Performance**: Understand the impact of added latencies in inter-component communications. The effect of latencies is not limited to pure data transfer. In tightly coupled applications, decoupling components which require ‘high chatter’ among themselves, the cumulative effect of adding even small inter-component latencies can result in significant overall performance degradation, and application instability where tolerance for increased internal latencies is low.
* **Security**: Many applications with components which typically co-exist together, take advantage of implicit trust between components. Distributing components across a hybrid infrastructure can introduce the need for more explicit security mechanisms such as private certificates.

While some of the potential challenges with distributing (or refactoring) and application to work in a hybrid deployment may seem daunting, there are some key benefits that can be gained.

* **Cost and scale**: Taking advantage of the pay-as-consumed characteristics of cloud based hosting can significantly reduce the cost of running an application. Profiling an application to understand which components are used frequently and which components are used rarely, can better inform decisions around placement of individual components from a cost perspective. Similarly, where some components scale based on usage demand, placing these components on public cloud capacity can leverage not only the scale agility of cloud, but also the cost advantages of only paying for what is needed.
* **User access**: Using the common three-tier application model as an example, there can be tangible value in hosting the presentation components in a public cloud to take advantage of global reach and dynamic scaling for peak usage periods. In addition, refactoring presentation components to take advantage of cloud-hosted identity and authorization mechanisms, enables the opportunity to leverage many of the associated cloud based benefits.

### Application refactoring and cloud-born design

Deciding to refactor or develop the applications from scratch can offer opportunities to take advantage of newer architecture and components and receive some of the greatest benefits afforded by the public cloud. It is important also to also consider some of the potential limitations that may result from application designs that depend heavily on cloud based services. If portability between clouds and/or on-premises environments is considered important for an application, then both the availability of the cloud services and the consistency of service APIs across environments will be important to assess, to prevent lock-in to a single cloud. Moving from on-premises to a public cloud (lift and shift) will likely be easier than the return path after refactoring the application to take advantage of public cloud services.

A look towards the future technologies such as Windows Service Fabric, Windows Containers, and Azure Stack which are coming soon can alleviate these concerns and continue to achieve the highest possible benefits from the cloud but still offer portability. Windows Service Fabric and Windows Containers offer an application design and packaging pattern, respectively, that can natively enable portability while Azure Stack will offer a consistent resource management model as Azure public cloud.

# Revision history

|  |  |  |
| --- | --- | --- |
| Publication Date | Version | Comments |
| January, 2016 | 1.0 | Initial publication. |
|  |  |  |

# Appendix 1: WAP and AADAP Comparison

The table below summarizes the available functionality in WAP and AADAP to help you make a decision on whether to use AADAP in the cloud, or WAP on-premises. This table is reproduced from “Identity in Hybrid Clouds” whitepaper, which goes into the details in more depth than the discussion in this document. To download the paper, see <https://gallery.technet.microsoft.com/Identity-in-Hybrid-Clouds-f4ff797e> (http://bit.ly/1OXJ2IN).

| Feature | On-premises | Cloud |
| --- | --- | --- |
| Identity store | AD | AAD |
| Multi-factor authentication | Yes | Yes |
| Support for HTTPS publishing | Yes | Yes |
| Single sign-on to backend applications using Kerberos Constrained Delegation (KCD) | Yes | Yes |
| Support for SharePoint | Yes | Yes |
|  | On-premises (ADFS + MIM) | Azure Active Directory (AAD) |
| Replicating password hash from on-premises directory | Not required | Not required but can be enabled. |
| Identity synchronisation | Not required | Not required but recommended when you have existing identities. |
| On-premises infrastructure requirement | Required | Not required but when synchronising identities, existing infrastructure can be utilised. |
| Impact of Outage or unavailability of on premise infrastructure for user logins and application access | High | Low when password hash synchronization enabled. |
| Federating with partner identities | Point-to-point trust link managed by ADFS administrators | Seamless provisioning and no partner directories trusts to manage |
| Support for multi-tenancy and managing external/partner identities | No | Yes |
| Self-service password reset | Provided by implementing MIM on-premises | Provided natively in AAD |
| Self-service group management | Provided by implementing MIM on-premises | Provided natively in AAD |
| Registering devices in directory | ADFS | AAD – Azure Device Registration Service |
| Fine grain access policy rules based on user, device, and network location | ADFS | Not available |
| Enforce per application authentication policies and multi-factor authentication option | ADFS | Not available |
| Access Panel (web portal) for end user | ADFS (requires minimal customization) or custom portal | Access Panel in AAD including application discovery |
| Adding users from a federated or partnered identity source | ADFS can provide functionally equivalent solution but recommended to manage at application level | Available natively |
| Support for consumer and social identities | Support through AAD only | Available in limited capacity via Access Control Service (ACS) |
| Extending functionality via custom extensions and SDKs | ADFS and MIM SDK | Not available |
| Auditing and reporting functionality for | Custom Solution required | Available Out-Of-Box |
| Multi-factor authentication | Yes | Yes |
| Third party multi-factor authentication providers support | Yes | Yes but in non-authoritative mode only and leveraging on-premises AD FS |
| Connector requirement on application servers | No | Yes (but very light weight) |
| Support for Exchange and ActiveSync | Yes | No |
| Support for Lync | Yes | No |
| Support for external traffic filtering before reaching your network | No | Yes – Azure acts as external sites and traffic filtering can be done in Azure first before it reaches on premise. |

1. Uday Pandya, Microsoft. “Identity in Hybrid Clouds.” Whitepaper. <https://gallery.technet.microsoft.com/Identity-in-Hybrid-Clouds-f4ff797e> (http://bit.ly/1OXJ2IN). [↑](#footnote-ref-1)
2. Microsoft Operations Management Suite (OMS). Microsoft portal for OMS. <http://www.microsoft.com/oms.> [↑](#footnote-ref-2)
3. “ExpressRoute Pricing.” Microsoft Azure product web site; available port speeds, pricing, links to technical requirements. <https://azure.microsoft.com/en-us/pricing/details/expressroute/> (http://bit.ly/1Nt5Lfk). [↑](#footnote-ref-3)
4. VPN Gateway documentation. Microsoft Azure documentation. <https://azure.microsoft.com/en-us/documentation/services/vpn-gateway/> (http://bit.ly/1PGZBfa). [↑](#footnote-ref-4)
5. “ExpressRoute partners and peering locations.” Product documentation. <https://azure.microsoft.com/en-us/documentation/articles/expressroute-locations/> (http://bit.ly/1LaSMQY). [↑](#footnote-ref-5)
6. AD FS Design Guide in Windows Server 2012 R2. Product documentation. <https://technet.microsoft.com/en-us/library/dn554245.aspx> (http://bit.ly/1Oq8tlT). [↑](#footnote-ref-6)
7. Azure Active Directory editions. Comparison of basic and paid editions; also lists new features currently in public preview. Microsoft Azure product documentation. <https://msdn.microsoft.com/en-us/library/azure/dn532272.aspx> (http://bit.ly/1cbDtKJ). [↑](#footnote-ref-7)
8. See note 5. [↑](#footnote-ref-8)
9. Create or edit users in Azure AD: Create and use external users. Microsoft Azure product documentation. [https://msdn.microsoft.com/en-us/library/azure/hh967632.aspx#BKMK\_5](https://msdn.microsoft.com/en-us/library/azure/hh967632.aspx%23BKMK_5) (http://bit.ly/1mnxCqQ). [↑](#footnote-ref-9)
10. Information Protection. Azure Rights Management services and information protection overview. Microsoft Azure product documentation. <http://www.microsoft.com/en-us/server-cloud/solutions/information-protection.aspx> (http://bit.ly/1C5K7Zx). [↑](#footnote-ref-10)
11. Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications. Windows Server, Getting Started with AD FS product documentation. <https://technet.microsoft.com/en-us/library/dn280945.aspx> (http://bit.ly/1IjZJQn). [↑](#footnote-ref-11)
12. Matt Hester, Microsoft. “Why Windows Server 2012 R2: Step-by-Step Workplace Join, Bringing Peace of Mind for BYOD.” TechNet Blogs post. <http://blogs.technet.com/b/matthewms/archive/2013/11/01/why-windows-server-2012-r2-step-by-step-workplace-join-bringing-peace-of-mind-for-byod.aspx> (http://bit.ly/1rvP0tj). [↑](#footnote-ref-12)
13. Enabling Azure AD Application Proxy. Microsoft Azure product documentation. <https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-proxy-enable/> (http://bit.ly/1NTAzGF). [↑](#footnote-ref-13)
14. Identity + Access Management. Microsoft solution portal; hybrid identity, Azure Active Directory. <https://www.microsoft.com/en-us/server-cloud/solutions/identity-management.aspx> (http://bit.ly/1Pu1bki). [↑](#footnote-ref-14)
15. Understanding Answer Files. Windows System Image Manager Technical Reference. <https://technet.microsoft.com/en-us/library/cc749113(v=ws.10).aspx> (http://bit.ly/1OjaZP7). [↑](#footnote-ref-15)
16. Managed Object Format file, used by Windows Management Instrumentation and System Center Configuration Manager, among others, to define configurations and custom actions during deployment. [↑](#footnote-ref-16)
17. Azure Automation Hybrid Runbook Workers. Microsoft Azure product documentation. <https://azure.microsoft.com/en-us/documentation/articles/automation-hybrid-runbook-worker/> (http://bit.ly/1kqOjjQ). [↑](#footnote-ref-17)
18. Azure Automation DSC Overview. Microsoft Azure product documentation. <https://azure.microsoft.com/en-us/documentation/articles/automation-dsc-overview/> (http://bit.ly/1RQ8V3x). [↑](#footnote-ref-18)
19. Pester is an open-source testing framework for PowerShell. You can find it at <https://github.com/pester/Pester>. [↑](#footnote-ref-19)
20. Operational Insights (part of Microsoft Operations Management Suite). Collect, store, and analyse log data. Microsoft Azure product page. <https://azure.microsoft.com/en-us/services/operational-insights/> (http://bit.ly/1VomINF). [↑](#footnote-ref-20)
21. Monitoring with Microsoft Monitoring Agent. Operations Guide for System Center 2012 - Operations Manager. <https://technet.microsoft.com/en-us/library/dn465153.aspx> (http://bit.ly/1YMwAX4). [↑](#footnote-ref-21)
22. Slack is a team collaboration tool. For more information, see <https://slack.com/>. [↑](#footnote-ref-22)
23. Service Management Automation. Overview and comparison to other automation tools. Microsoft System Center Orchestrator; Windows Azure Pack. <https://technet.microsoft.com/en-us/library/dn469260.aspx>. [↑](#footnote-ref-23)
24. Deploying Azure Site Recovery with VMM and SAN - supported storage arrays. TechNet Wiki article. <http://social.technet.microsoft.com/wiki/contents/articles/28317.deploying-azure-site-recovery-with-vmm-and-san-supported-storage-arrays.aspx> (http://bit.ly/1NOYyJv). [↑](#footnote-ref-24)
25. Praveen Vijajaraghavan, Microsoft. “Azure Site Recovery adds InMage Scout to Its Portfolio for Any Virtual and Physical Workload Disaster Recovery.” Virtualization Blog post. <http://blogs.technet.com/b/virtualization/archive/2014/07/17/azure-site-recovery-adds-inmage-scout-to-its-portfolio-for-any-virtual-and-physical-workload-disaster-recovery.aspx> (http://bit.ly/1YQP9nK). [↑](#footnote-ref-25)
26. Praveen Vijajaraghavan, Microsoft. “ExpressRoute + ASR = Efficient DR solution.” Virtualization Blog post. <http://blogs.technet.com/b/virtualization/archive/2014/07/20/expressroute-and-azure-site-recovery.aspx> (http://bit.ly/1VorgUd). [↑](#footnote-ref-26)
27. Azure Site Recovery Capacity Planner. Microsoft Excel-based planning tool for estimating capacity requirements. <https://gallery.technet.microsoft.com/Azure-Recovery-Capacity-d01dc40e> (http://bit.ly/1VKB777). [↑](#footnote-ref-27)
28. Azure Subscription and Service Limits, Quotas, and Constraints. Microsoft Azure product documentation. <https://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/> (http://bit.ly/1LjBORA). [↑](#footnote-ref-28)
29. Nader Benmessaoud, Microsoft. “Designing Your Network Infrastructure for Disaster Recovery.” Whitepaper. <http://blogs.technet.com/b/privatecloud/archive/2015/07/05/whitepaper-designing-your-network-infrastructure-for-disaster-recovery.aspx> (http://bit.ly/1NJI9Fb). [↑](#footnote-ref-29)