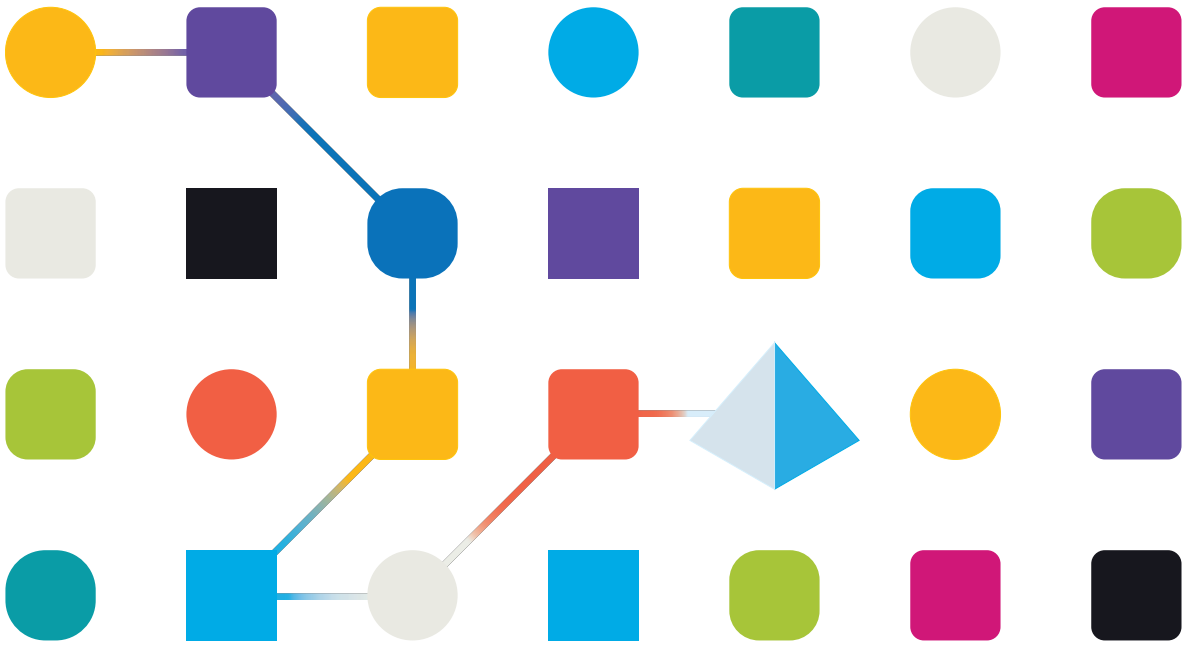
blueprism®

Blue Prism 6

Azure Reference Architecture

Document Revision: 1.0



Trademarks and Copyright

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Registered in England: Reg. No. 4260035. Tel: +44 370 879 3000. Web: www.blueprism.com

Contents

Introduction 4
Intended audience 4
About this document 4
Azure Services and Key Concepts 5
Azure Services 5
Azure SLAs and Impact on Target Architecture 6
Azure SQL PAAS vs SQL IAAS 6
Blue Prism Azure Reference Architectures 7
Small Scale Deployment using SQL PAAS 7
Medium to Large Scale Deployment Using SQL Clustering 9
Supporting Architecture Patterns 10
Authentication 10

Introduction

Intended audience

This reference guide is intended for use by system architects and designers who are seeking to gain an understanding of the options and considerations for deploying a Blue Prism environment in the Microsoft Azure Cloud.

About this document

The document provides an overview of the key considerations for an Azure based deployment of Blue Prism, along with reference architectures for the commonly requested patterns for a Cloud based deployment. The objective of this document is to explain the key considerations for deployment on Azure. A basic understanding of the Azure architecture is expected. The reference architectures contained within this document are based upon generalized assumptions and Azure design best practices and Reference Architectures. The architecture may need to be modified to suit a client deployment.

Azure Services and Key Concepts

The following sections outline some of the relevant services and concepts that are key in designing an Azure based Blue Prism deployment.

Azure Services

The Blue Prism architecture uses several key Azure services and concepts. These are outlined below. Refer to the Azure documentation in the links for further information.

Virtual Network (Vnet) – The Azure Virtual Network service enables you to securely connect Azure resources to each other with virtual networks (VNets). A VNet is a representation of your own network in the cloud. A VNet is a logical isolation of the Azure cloud dedicated to your subscription. You can also connect VNets to your on-premises network.

Availability Set - In Azure, virtual machines (VMs) can be placed in to a logical grouping called an availability set. When you create VMs within an availability set, the Azure platform distributes the placement of those VMs across the underlying infrastructure. Should there be a planned maintenance event to the Azure platform or an underlying hardware / infrastructure fault, the use of availability sets ensures that at least one VM remains running. The Blue Prism design should make use of Availability sets to avoid single points of failure across the environment.

Azure Active Directory - Azure Active Directory (Azure AD) is Microsoft's multi-tenant cloud based directory and identity management service. Importantly for this document, it does not behave in the same way as a standard Windows Active Directory domain controller and Blue Prism cannot be directly integrated with it. If Azure AD will be used, then the Azure AD Domain Services should be deployed, to allow integration of Blue Prism

Azure Active Directory Domain Services – Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, Kerberos/NTLM authentication that are fully compatible with Windows Server Active Directory. This can be deployed as an extension to Azure AD, to enable integration of applications (such as Blue Prism) that depend on standard domain services such as Kerberos or NTLM.

Network Security Group - A network security group (NSG) contains a list of access control list (ACL) rules that allow or deny network traffic to your VM instances in a Virtual Network. NSGs can be associated with either subnets or individual VM instances within that subnet. When a NSG is associated with a subnet, the ACL rules apply to all the VM instances in that subnet. In addition, traffic to an individual VM can be restricted further by associating a NSG directly to that VM. The Blue Prism reference architecture makes some recommendations around the segregation of components within NSGs.

Azure SLAs and Impact on Target Architecture

The impact of the Azure SLAs on each component needs to be assessed against the non-functional requirements of the target architecture. The following may be used as a set of default guiding principles:

- 99.5% availability is guaranteed for at least one instance within an availability set. However, as the Blue Prism Runtimes and Interactive Clients are not aware of multiple application server instances, manual intervention would still be required in the event of an outage of an instance within an availability set
- 99.5% availability is guaranteed for Single Instance VMs with premium storage, therefore these should be used for Application servers (as a minimum) within any production instance. The single instance VMs may still be added to an availability set.
- Azure SQL is guaranteed to 99.99% availability, however there is a possibility of some small data loss in event of a failover between the back-end instances.

Azure SQL PAAS vs SQL IAAS

The selection of an SQL PAAS based architecture is not just dependant on the sizing. The limitations (and advantages) of using a PAAS platform should also be understood. These are detailed fully here, however the main considerations in context of a Blue Prism deployment will be:

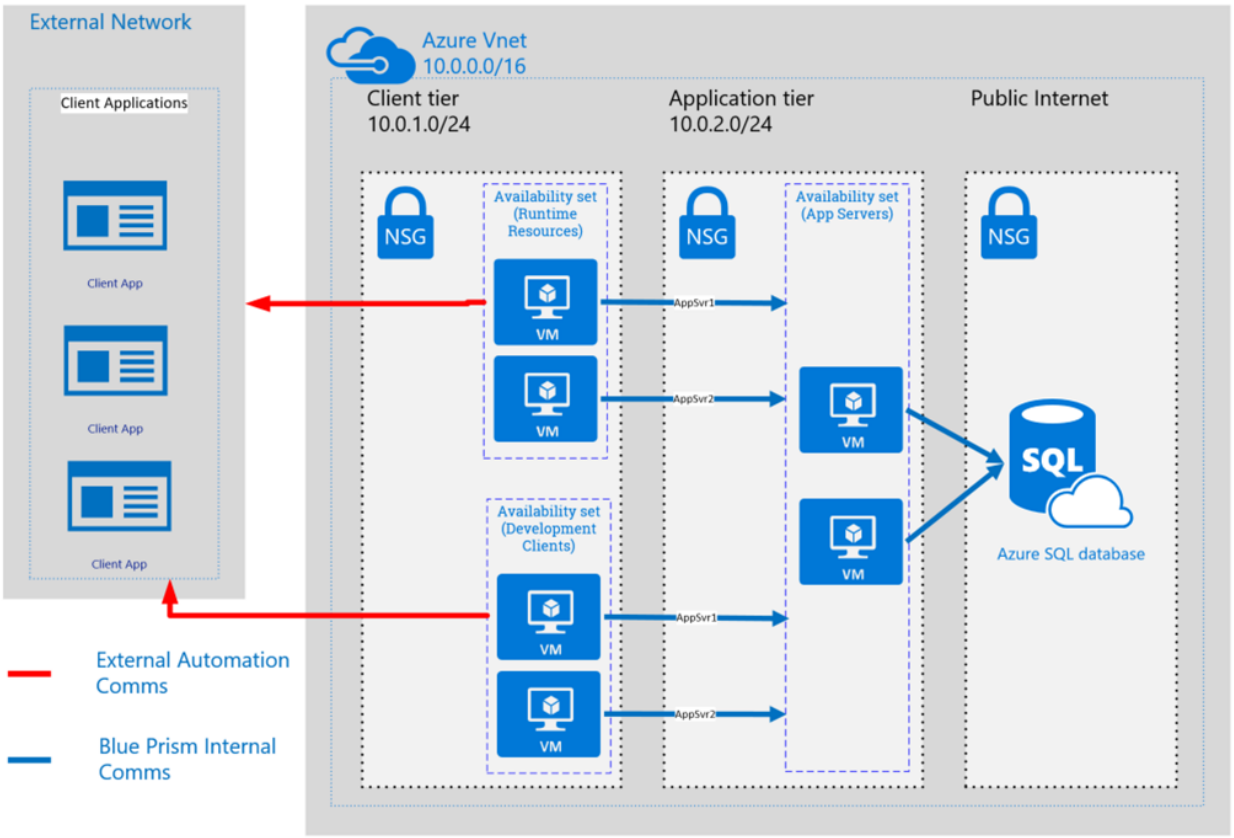
- Size – Primarily limited by the current maximum size of 1TB, as Blue Prism generates a high volume of database logging.
- Speed of deployment – Using PAAS will enable an environment to be initiated more quickly
- Management and Control – Managed platform vs full control over configuration and security
- Cost – Using a PAAS solution is likely to be cheaper overall
- Features – Access to some features is limited in Azure SQL vs a full IAAS installation

Blue Prism Azure Reference Architectures

The following sections outline the core reference architectures for the expected deployment models for Blue Prism on the Azure cloud. These are supplemented by peripheral design considerations and scenarios, such as integration with Single Sign-On (SSO).

Small Scale Deployment using SQL PAAS

This pattern makes use of the Azure SQL Database Platform as a service (PAAS) offering.



Assumptions

- A connection is in place between the Blue Prism network and any external networks where the automated applications reside. This may be via a VPN, internal Vnet Peering (for cloud hosted applications) or Express Route.
- Blue Prism clients and runtimes will need to have all necessary software installed to facilitate the automation of remote applications

The Authentication components are not shown here. See section 4 for considerations.

Key Design Considerations

- The primary limitation on the use of Azure SQL is logging space. The database sizing recommendations for Blue Prism within the Infrastructure Reference Guide should be used as a baseline for selecting the appropriate specification.
- Azure SQL is sized based on "Deployment Transaction Units (DTUs). It is impossible to predict an accurate baseline for DTUs, as this will be highly dependant on workload for the environment. As Azure allows for the easy scaling up or down of DTUs, it is recommended to start with a medium DTU specification and monitor performance and scale up accordingly.
- Multiple application servers are included in this design, to provide some degree of high availability in event of a failure. This may be reduced to 1 for small POC environments.
- Consider splitting the connections between application servers and distributing workload between Runtimes on both, to account for failures or maintenance of one Application Server within the Availability set.

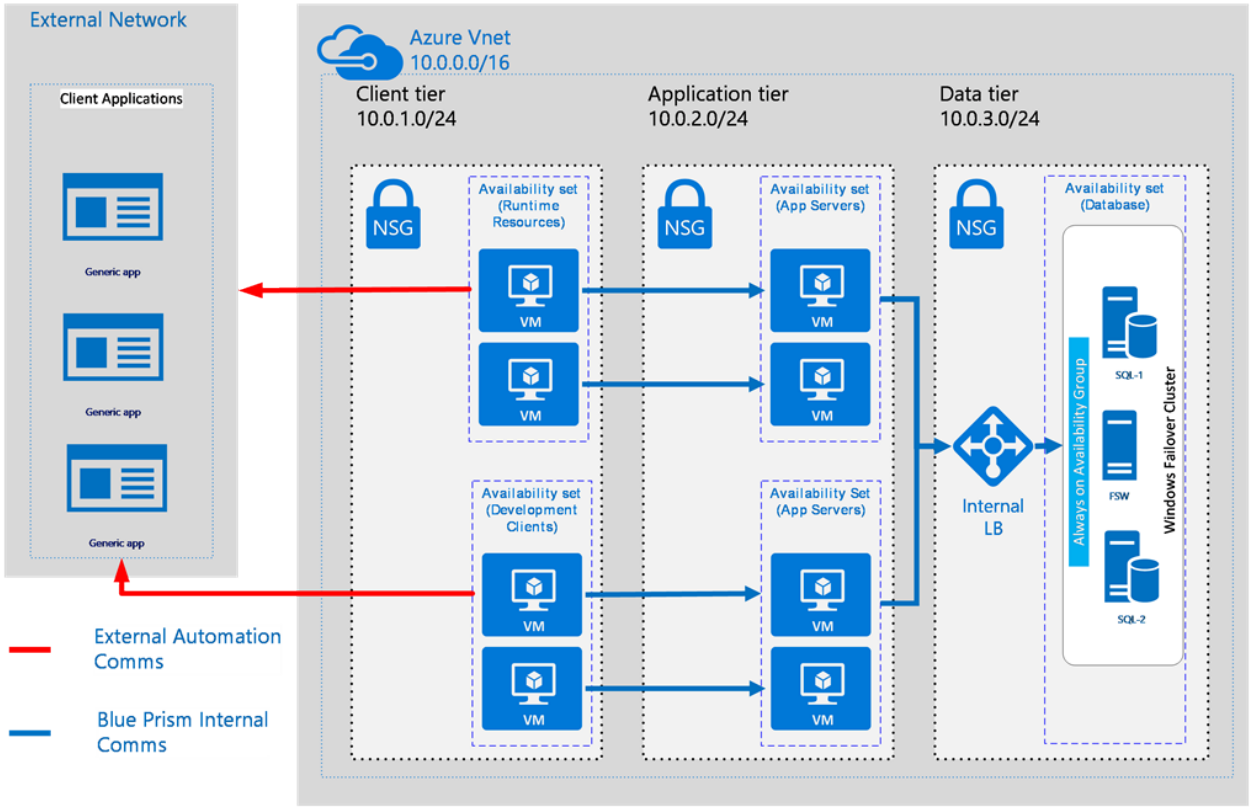
Azure SQL High Availability and Failover

Azure SQL Database maintains multiple copies of all databases in different physical nodes located across fully independent physical sub-systems, such as server racks and network routers. At any one time, Azure SQL Database keeps three replicas of each database – one primary replica and two secondary replicas. Azure SQL Database uses a quorum-based commit scheme where data is written to the primary and one secondary replica before the transaction is considered committed. If any component fails on the primary replica, Azure SQL Database detects the failure and fails over to the secondary replica. In case of a physical loss of the replica, Azure SQL Database creates a new replica automatically. Therefore, there are at least two replicas of each database that have transactional consistency in the data center. Other than the loss of an entire data center all other failures are mitigated by the service.

The replication, failure detection and failover mechanisms of Azure SQL Database are fully automated and operate without human intervention. This architecture is designed to ensure that committed data is never lost and that data durability takes precedence over all else.

Medium to Large Scale Deployment Using SQL Clustering

This pattern involves the deployment of a SQL cluster with Always on Availability Groups (AAG) for HADR.



Assumptions

- A connection is in place between the Blue Prism network and any external networks where the automated applications reside. This may be via a VPN, internal Vnet Peering (for cloud hosted applications) or Express Route.
- Blue Prism clients and runtimes will need to have all necessary software installed to facilitate the automation of remote applications
- The Authentication components are not shown here. See section 4 for considerations.

Key design considerations

- The sizing of the SQL environment (compute and database) should be based on the recommendations within the Infrastructure Reference Guide.
- This design pattern separates the Application servers into 2 separate Availability groups for the Interactive Clients and Runtimes. This is optional and the application servers may be combined for both if desired.
- The number of application servers may be scaled up, according to the size of environment. Refer to the Blue Prism Infrastructure Reference Guide for additional information on sizing.
- If Disaster Recovery is required, it may be necessary to deploy a cross-region scenario. Further information on the options for SQL Server are contained within the following Azure Reference Guide: HADR for SQL Server in Azure VMs

Supporting Architecture Patterns

The following sections outline some of the supporting architecture patterns for peripheral services, such as Authentication and remote connectivity. These are likely to be highly variable, depending on the client's existing Azure usage and strategy.

Authentication

There are multiple options for integration of the Blue Prism environment into a Directory. This section will outline the 2 most common scenarios:

- Cloud only Authentication
- Via Azure AD
- Via dedicated domain controllers deployed on Azure
- Hybrid scenario – primary control provided by Client hosted domain and sync to Azure
- Via Azure AD Connect / Active Directory Domain Services (ADDS)
- Via extension of existing AD Forest into Azure

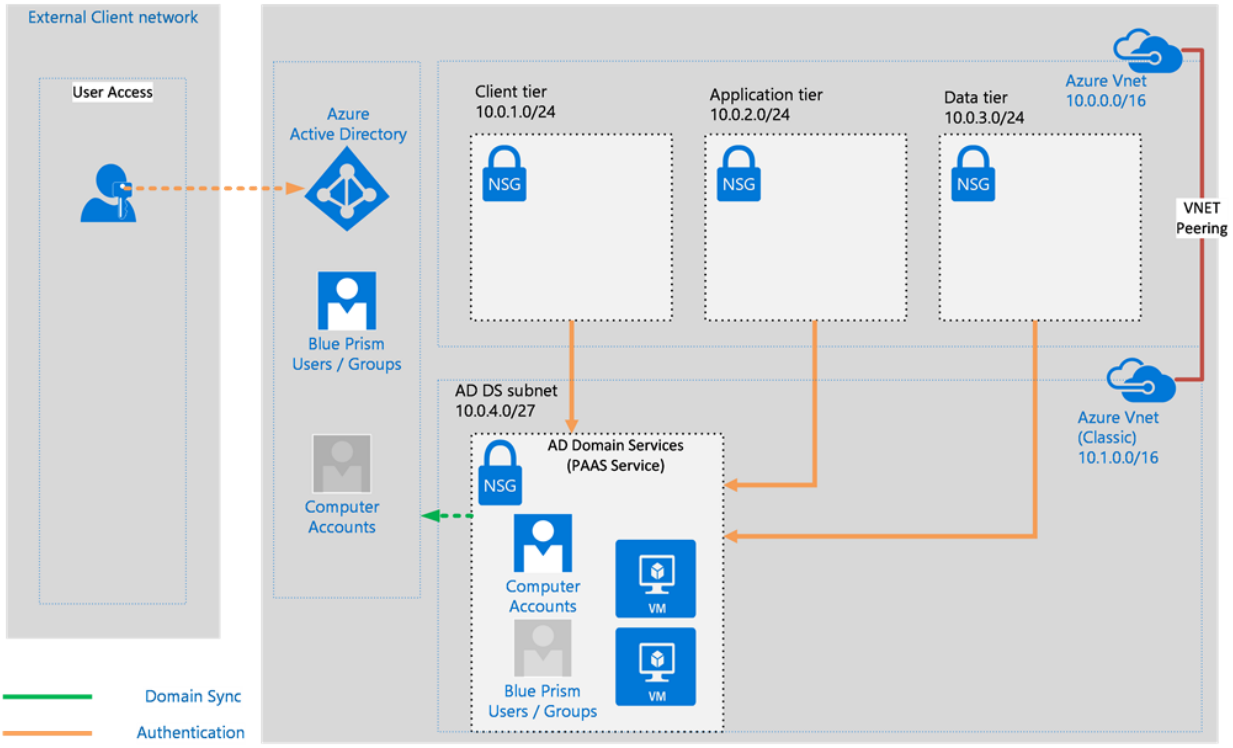
The following scenarios are based on guidance contained within the following Azure documentation:

- Azure AD Domain Services
- Synchronization in an AD Domain Services Managed Domain

The approaches outlined below are documented to indicate the options in which Blue Prism may be integrated with a domain. The overall assessment and selection of an authentication approach is likely to be dependant on many factors and other unrelated client decisions.

Cloud only Authentication (Using Azure AD and Domain Services)

This pattern is applicable in a scenario where authentication for the Blue Prism application will be provided solely from the Azure cloud environment and use of Azure AD is desired.

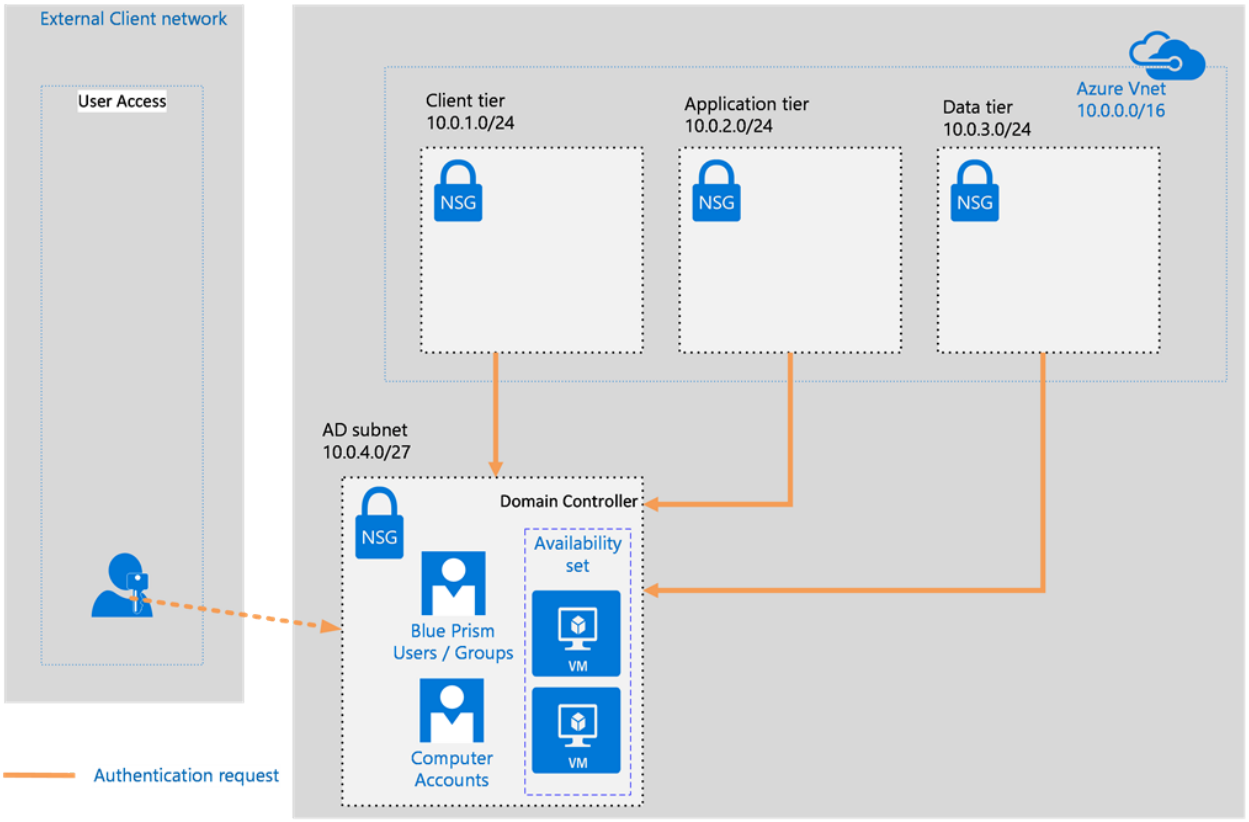


Key considerations

- Blue Prism cannot directly authenticate with Azure AD. The use of AD Domain Services is necessary to enable this.
- Azure ADDS is only supported on a Classic VNet, therefore if using Resource Manager for the primary environment, Vnet peering will need to be established between the Vnets.
- LDAP write access to managed domains provided by Azure AD Domain Services is not supported.
- Schema extensions are not supported in Azure AD Domain Services.
- Certificate/Smartcard based authentication is not supported by Azure AD Domain Services.
- You cannot change passwords directly against the managed domain. End users can change their password either using Azure AD's self-service password change mechanism or against the on-premises directory.

Cloud only Authentication (Using Dedicated Domain Controllers)

This pattern is applicable where authentication for the Blue Prism application will be provided within the Azure Cloud environment, but use of Azure AD is not desired.

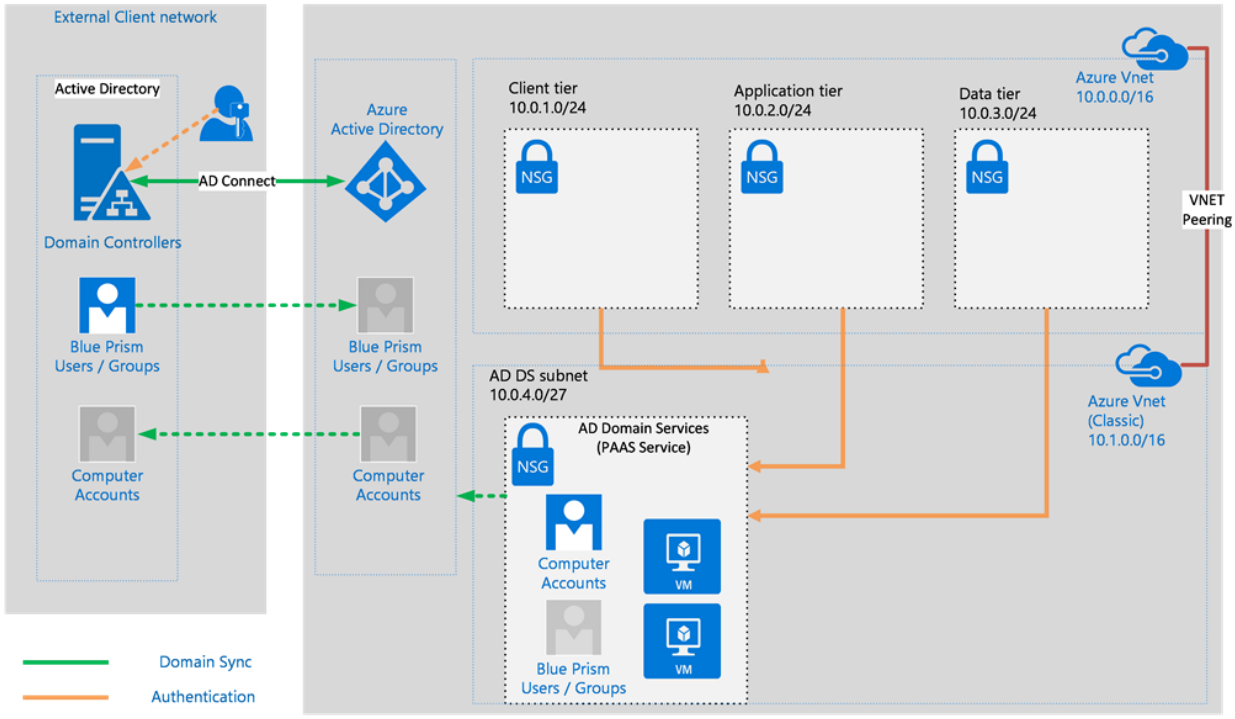


Key Design Considerations

- Integration and management is identical to an on premises integration of Blue Prism with Active Directory.

Hybrid Authentication (using Azure AD)

The following pattern is applicable where authentication for Blue Prism application will be controlled from a remote Active Directory on the client network, but the use of Azure AD is still desirable.

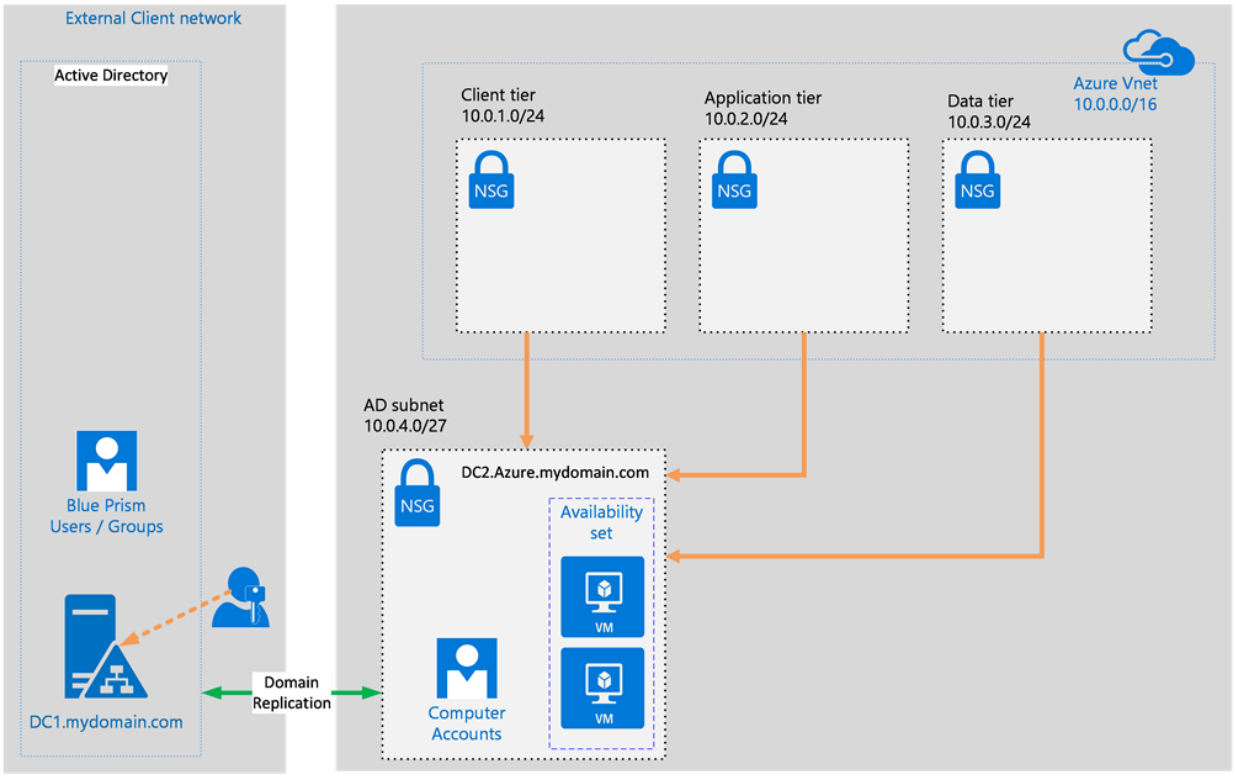


Key considerations

- The computer groups and OUs will be synced from the on-premise domain (i.e. the computer accounts for the cloud VMs will be visible on premise and vice versa for the shadow domain accounts.
- Note that this is a sync relationship, not a trust based setup.
- Refer to the limitations of using AD Domain Services, as documented in section 4.1.1
- ADDS can only be deployed to ONE Azure Vnet subnet – so if a customer is already using ADDS elsewhere this will impact the design

Hybrid Authentication (using extended Domain Forest)

The following pattern is applicable where the existing domain forest will be extended into Azure.



Key considerations

- Refer to the Blue Prism Infrastructure Reference Guide for further guidance on this topic.