Microsoft

Welcome

Global Architect Summit 2021

What a Journey!

Microsoft

- Day 1 - Application Architecture Style
- Day 2 - Design Your Cloud Application: Design Principles
- Day 3 - Designing Resilient Applications for Cloud
- Day 4 - Design Your Azure Application
- Day 5 - Catalogue of Patterns

Session 06

Azure Reference Architectures

- Dave Rendón
  - Azure MVP, Solutions Architect
  - 🕮 bit.ly/dr-books
  - 🕮 bit.ly/az-book
  - @DaveRndn

AGENDA

- Identity management
- Hybrid network
- Managed web application
- VM workloads
- IoT
- Data & BI

Reference architectures

- Azure reference architectures are arranged by scenario, with related architectures grouped together.

- Each architecture includes
  - Recommended practices
  - Considerations for scalability, availability, management, and security.

- Intended to provide a footprint for your reference

Identity management

Microsoft

Identity Management Architecture References

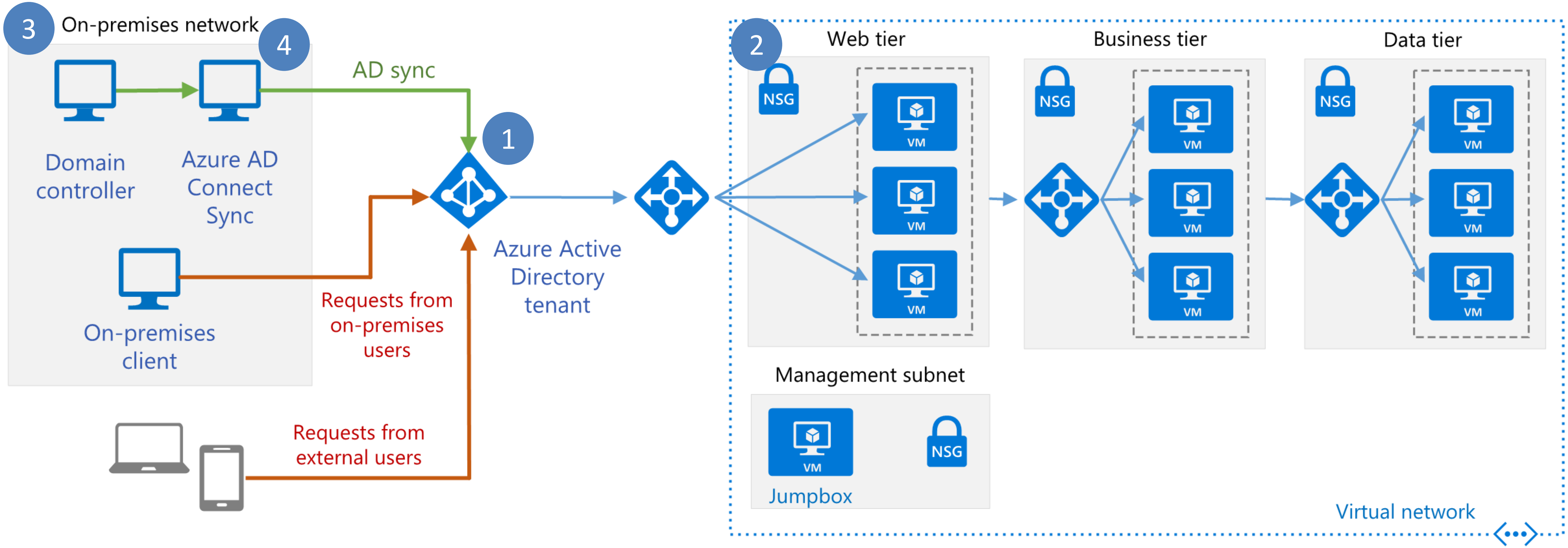
- Integrate on-premises AD domains with Azure AD
- Deploy AD DS in an Azure virtual network
- Create an AD DS resource forest in Azure
- Extend on-premises AD FS to Azure

Integrate on-premises AD domains with Azure AD

- Azure Active Directory (Azure AD) is a cloud-based multi-tenant directory and identity service.

- This reference architecture shows best practices for integrating on-premises Active Directory domains with Azure AD to provide cloud-based identity authentication.

Integrate on-premises AD domains with Azure AD



3 On-premises network

4

Domain controller

Azure AD Connect Sync

On-premises client

AD sync

1

Azure Active Directory tenant

Requests from on-premises users

Requests from external users

2

Web tier

Business tier

Data tier

NSG

NSG

NSG

VM

VM

VM

VM

VM

VM

VM

VM

VM

Management subnet

VM

Jumpbox

NSG

Virtual network

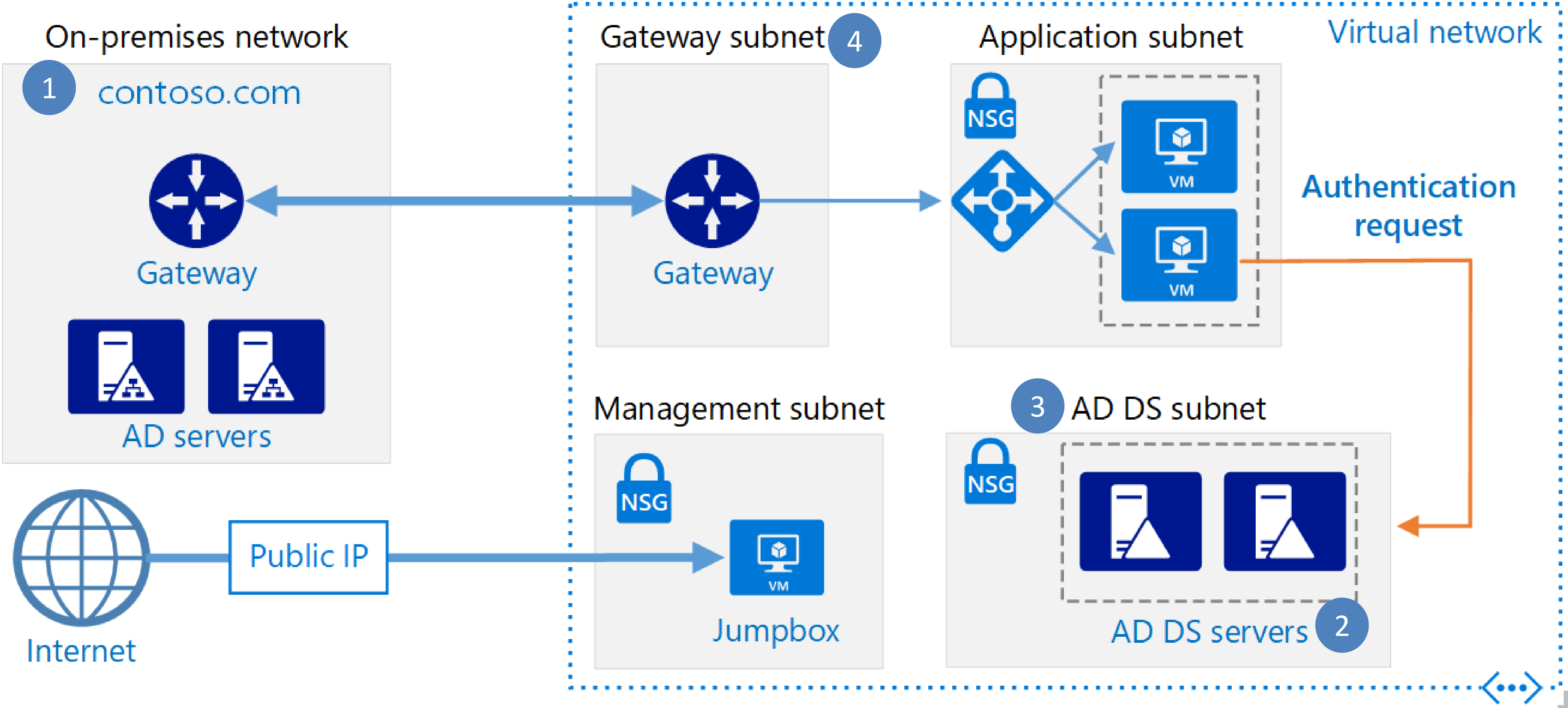
Integrate on-premises AD domains with Azure AD

Typical uses for this reference architecture include:

- Web applications deployed in Azure that provide access to remote users who belong to your organization.
- Implementing self-service capabilities for end-users, such as resetting their passwords, and delegating group management
- Architectures in which the on-premises network and the application's Azure VNet are not connected using a VPN tunnel or ExpressRoute circuit.

Deploy AD DS in an Azure virtual network

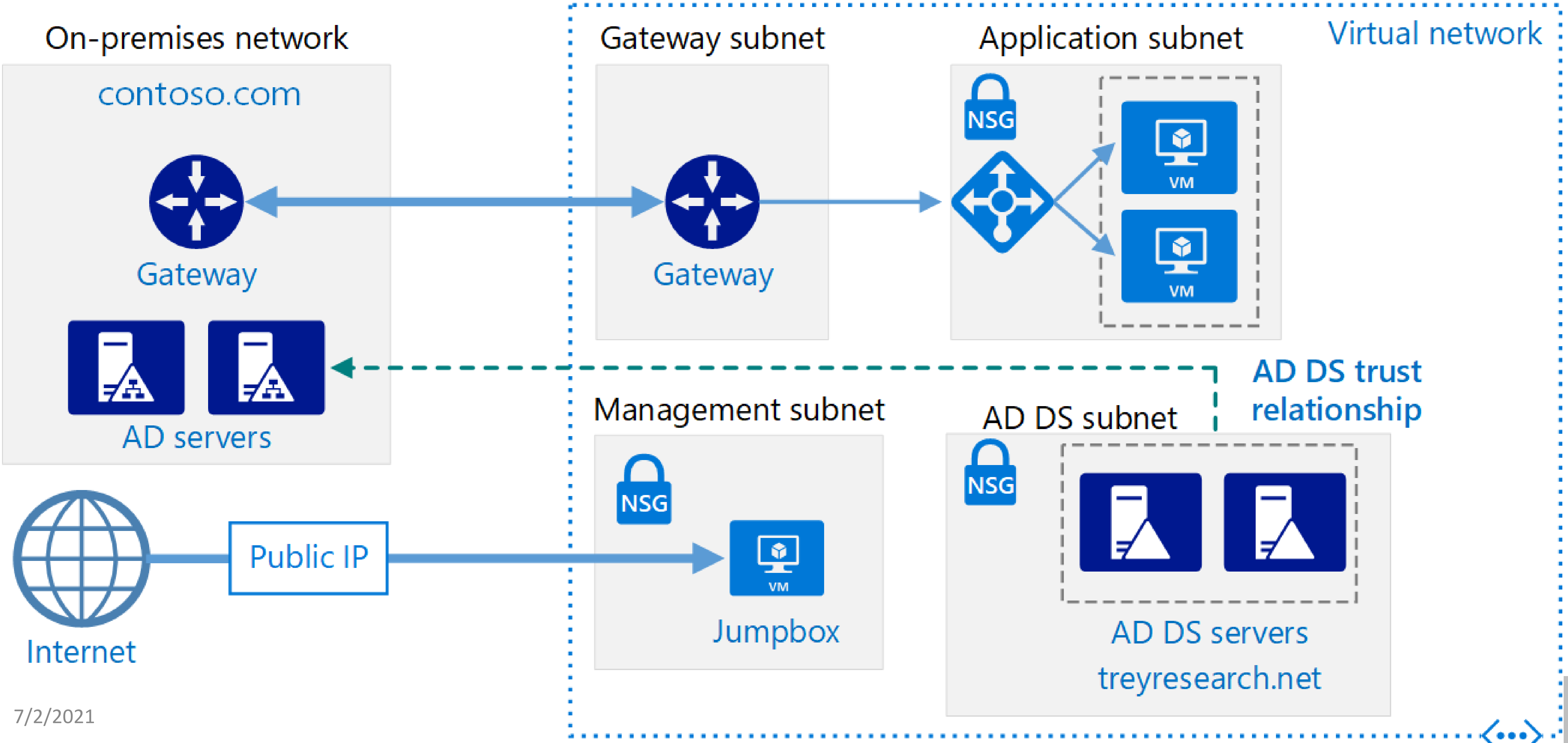
Microsoft



Deploy AD DS in an Azure virtual network

- Typical uses for this architecture include:
  - Hybrid applications in which functionality is distributed between on-premises and Azure
  - Applications and services that perform authentication using Active Directory.

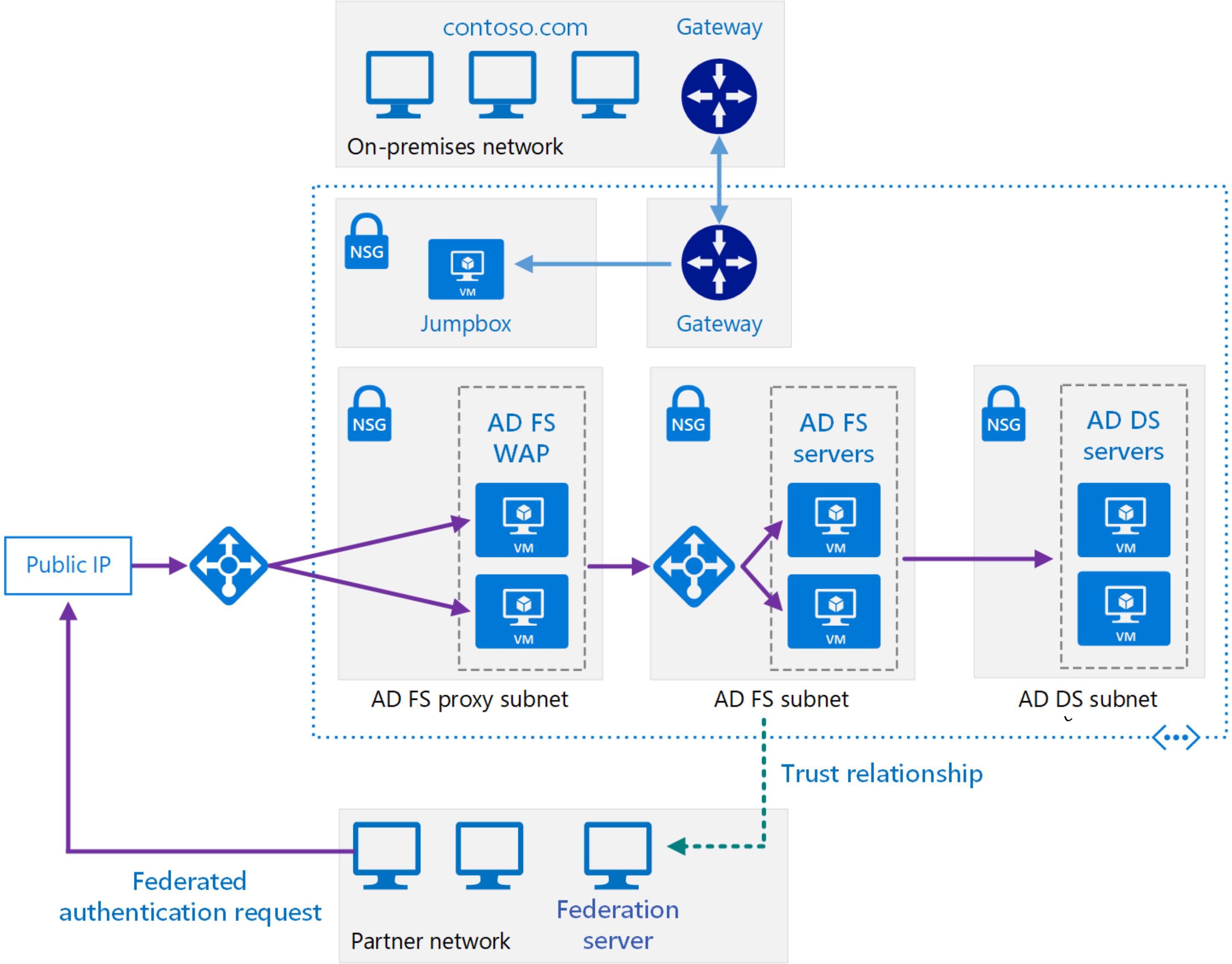
Create an AD DS resource forest in Azure



Create an AD DS resource forest in Azure

- Typical uses for this architecture include maintaining security separation for objects and identities held in the cloud, and migrating individual domains from on-premises to the cloud.

Extend on-premises AD FS to Azure

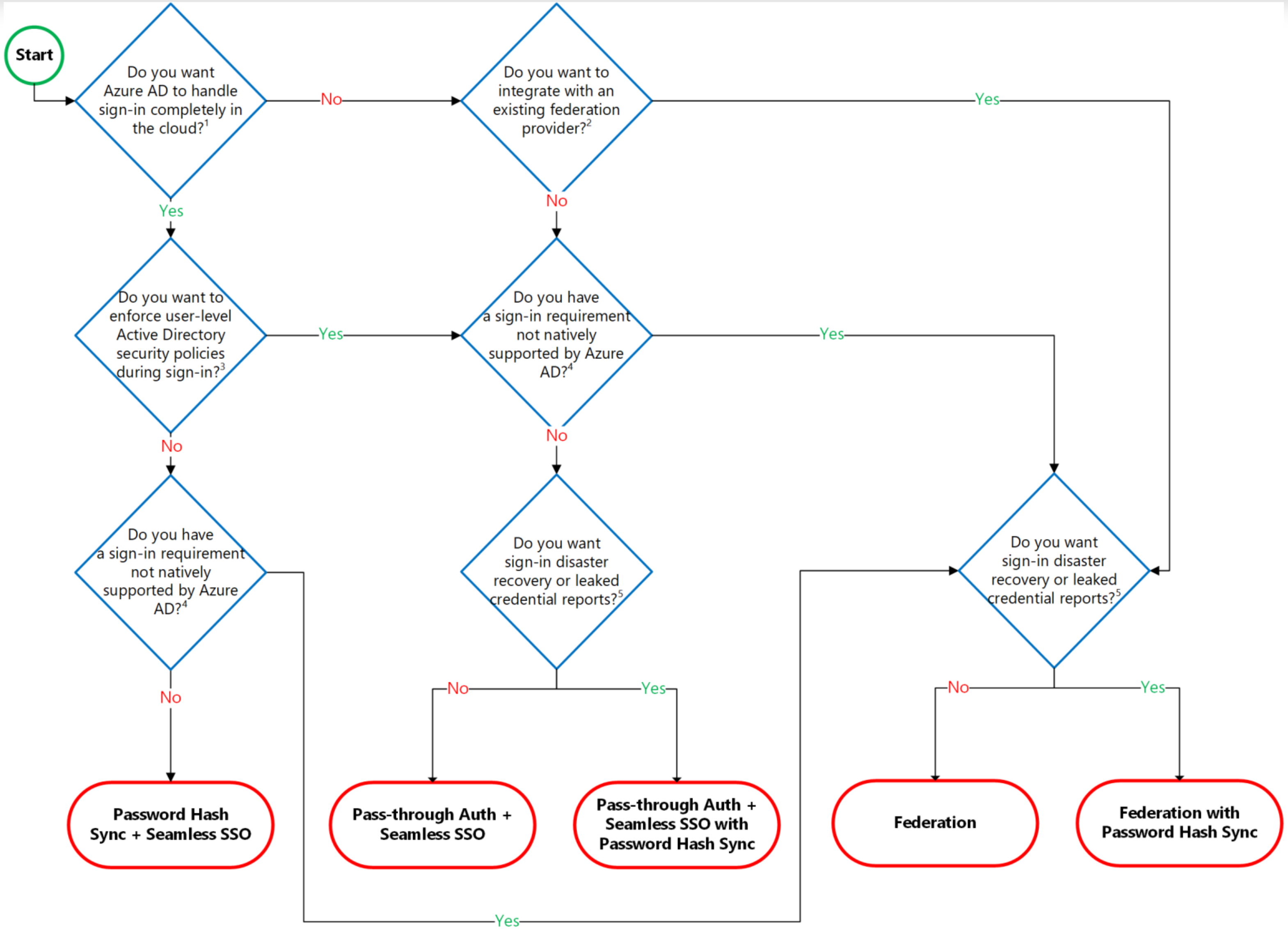


7/2/2021

Extend on-premises AD FS to Azure

- Typical uses for this architecture include:
  - Hybrid applications where workloads run partly on-premises and partly in Azure.
  - Solutions that use federated authorization to expose web applications to partner organizations.
  - Systems that support access from web browsers running outside of the organizational firewall.
  - Systems that enable users to access to web applications by connecting from authorized external devices such as remote computers, notebooks, and other mobile devices.

Hybrid identity auth decision workflow



Start

Do you want Azure AD to handle sign-in completely in the cloud?[1]

No

Do you want to integrate with an existing federation provider?[2]

Yes

Yes

Do you want to enforce user-level Active Directory security policies during sign-in?[3]

Yes

Do you have a sign-in requirement not natively supported by Azure AD?[4]

Yes

No

No

No

Do you have a sign-in requirement not natively supported by Azure AD?[4]

No

Do you want sign-in disaster recovery or leaked credential reports?[5]

No

Yes

Do you want sign-in disaster recovery or leaked credential reports?[5]

No

Yes

Password Hash Sync + Seamless SSO

Pass-through Auth + Seamless SSO

Pass-through Auth + Seamless SSO with Password Hash Sync

Federation

Federation with Password Hash Sync

Yes

Discussion

- How to implement different components of a hybrid identity solution that integrates an Active Directory forest with an Azure Active Directory tenant and leverages additional Azure Active Directory features
  - SSO
  - MFA
  - Self-service password reset
  - Azure AD Password Protection for WinServer AD
  - Hybrid Azure AD join
  - Conditional Access
  - Azure AD proxy
  - Azure AD B2C, B2B

Discussion pt2 – Customer situation -Fabrikam

Microsoft

- Fabrikam, a financial services company with HQ in São Paulo, and a branch office in Spain, looking to enable remote work.
  - Lack of controls to prevent unathorized Access to systems
  - Using traditional VPNs / Direct Access
  - Running on-premises infrastructure on Windows platform
  - Consider implementing policies to allow employees work from home

- 1 AD domain forest was implemented a few years ago
- AD domain uses a non-routable DNS name fabrikam.local
  - Directory Services did not implement domain name
  - Fabrikam owns a publicly routable DNS domain name fabrikam.com
  - AD domain recently upgraded to Windows Server 2016

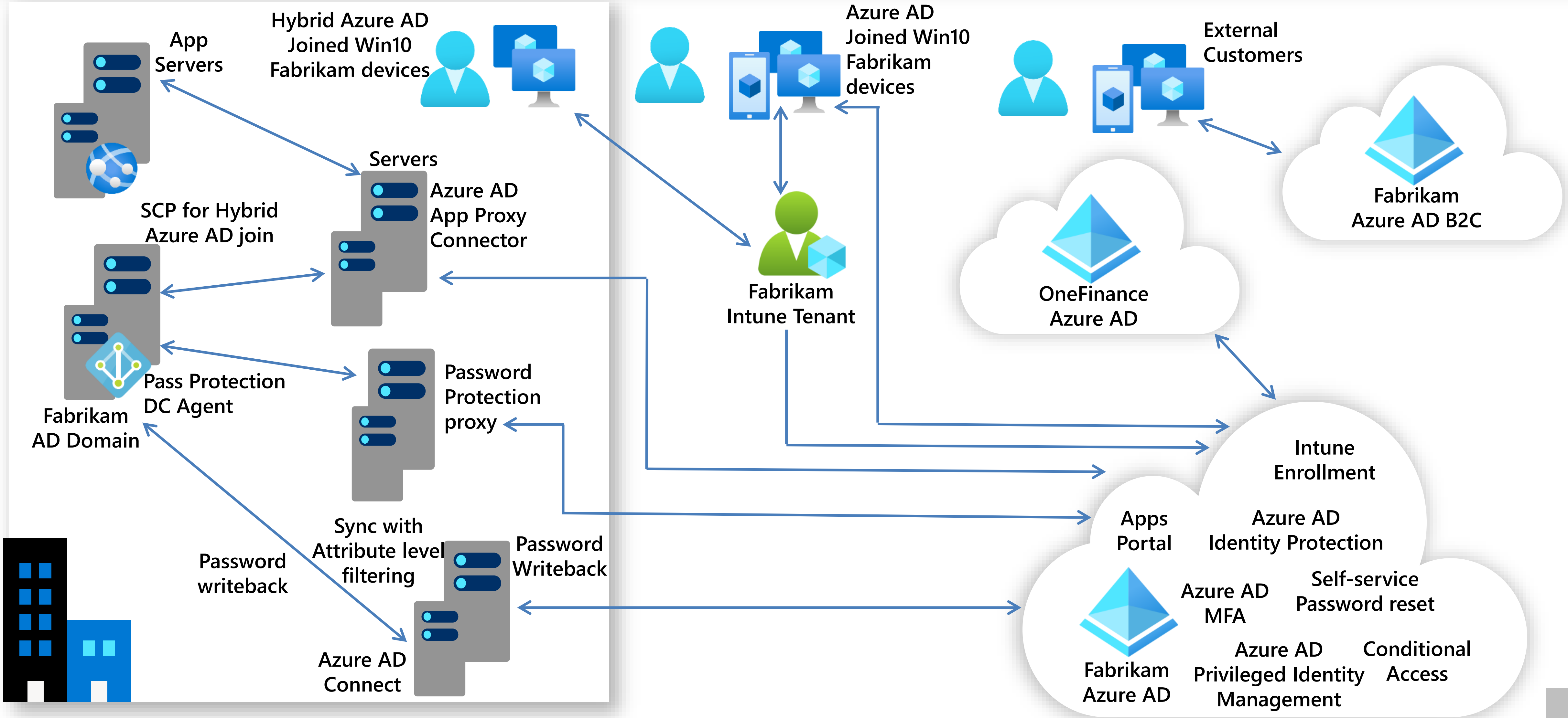
- Most of the servers are running WinServer 2016

Discussion pt. 3 – Customer objectives

- Support for remote workforce and integration with customers and partners
  - Remote uses must be able to sign in using their AD creds to their devices
  - Users must be able to reset their own passwords, prevent use of common terms in passwords
  - Implement new identity capabilities including authentication, per-app permissions.
- Expand partnerships with other organizations:
  - Fabrikam established business relationships with OneFinance
  - OneFinance manages an extensive portfolio of mortgage related products
  - Fabrikam intends to provide OneFinance with access to its internal applications to facilitate integration with the existing OneFinance products
  - OneFinance is running almost entirely to Azure

- Provide Access to services to external clients.
- Critical applications are running on-premises and rely on Kerberos-based auth
- Fabrikam remote users should be able to access on-premises applications
- Fabrikam users should be able to access on-premises applications

Proposed Solution


App Servers
Hybrid Azure AD Joined Win10 Fabrikam devices
Servers
Azure AD App Proxy Connector
SCP for Hybrid Azure AD join
Pass Protection DC Agent
Fabrikam AD Domain
Password Protection proxy
Password writeback
Sync with Attribute level filtering
Password Writeback
Azure AD Connect
Azure AD Joined Win10 Fabrikam devices
Fabrikam Intune Tenant
External Customers
Fabrikam Azure AD B2C
OneFinance Azure AD
Intune Enrollment
Apps Portal
Azure AD Identity Protection
Azure AD MFA
Self-service Password reset
Fabrikam Azure AD
Azure AD Privileged Identity Management
Conditional Access

7/2/2021

Hybrid Network

Microsoft

Hybrid Network Architecture References

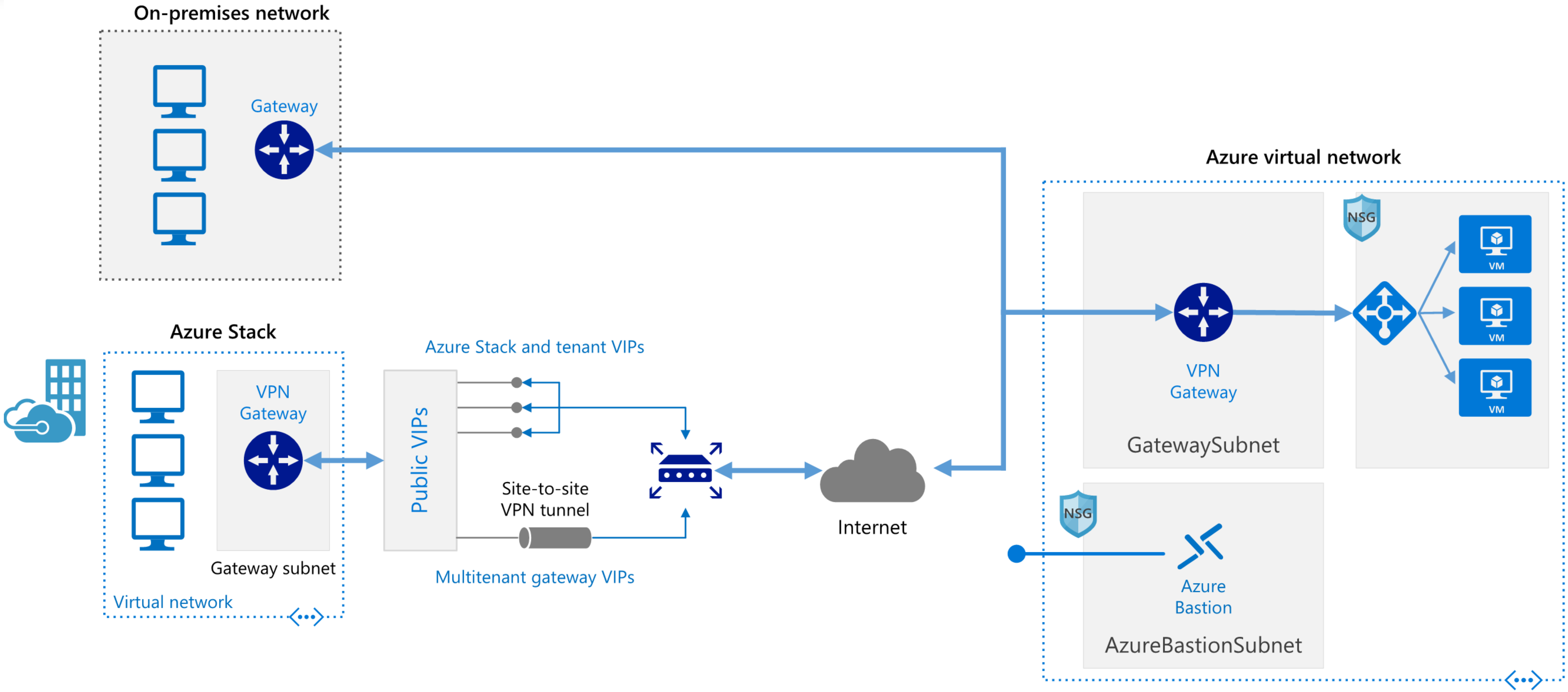
- Extend an on-premises network using VPN
- Extend an on-premises network using ExpressRoute
- ExpressRoute with VPN failover
- Hub-spoke network topology in Azure
- DMZ between Azure and your on-premises datacenter
- Secure Azure Computing Architecture

Extend an on-premises network using VPN

Microsoft

- This reference architecture shows how to extend a network from on premises or from Azure Stack into an Azure virtual network, using a site-to-site virtual private network (VPN).
- Traffic flows between the on-premises network and Azure through an IPSec VPN tunnel or through the Azure Stack multitenant VPN gateway.

Extend an on-premises network using VPN

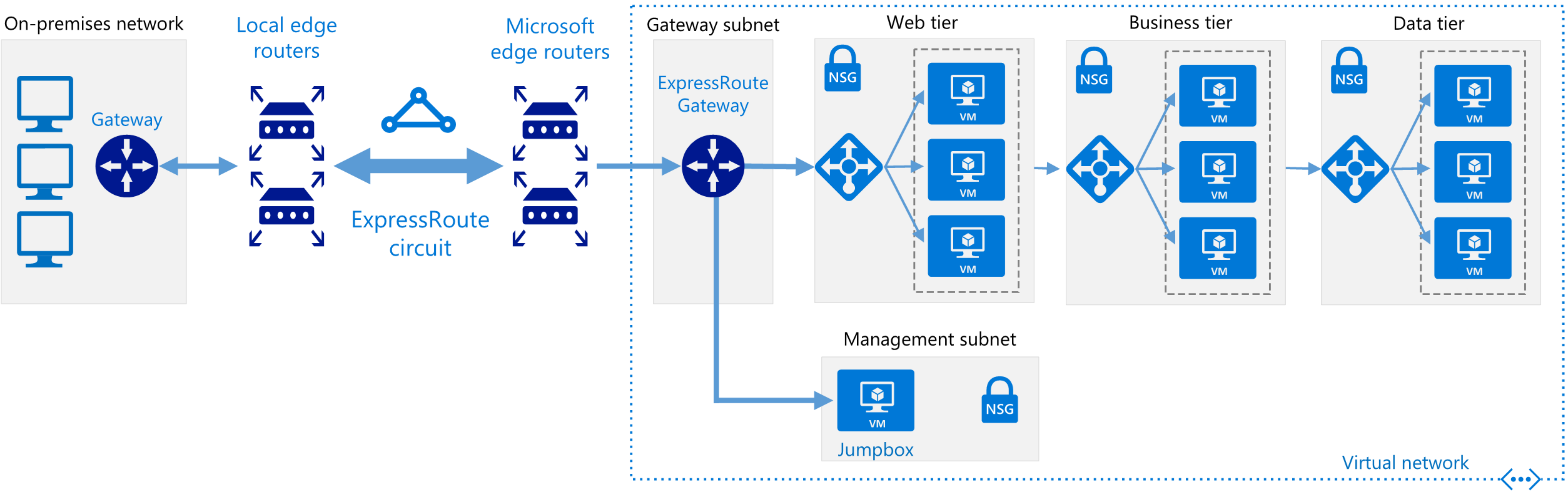


https://github.com/mspnp/reference-architectures/blob/master/hybrid-networking/vpn/README.md

Extend an on-premises network using ExpressRoute

- This reference architecture shows how to connect an on-premises network to virtual networks on Azure, using Azure ExpressRoute.
- ExpressRoute connections use a private, dedicated connection through a third-party connectivity provider.
- The private connection extends your on-premises network into Azure.

Extend an on-premises network using ExpressRoute



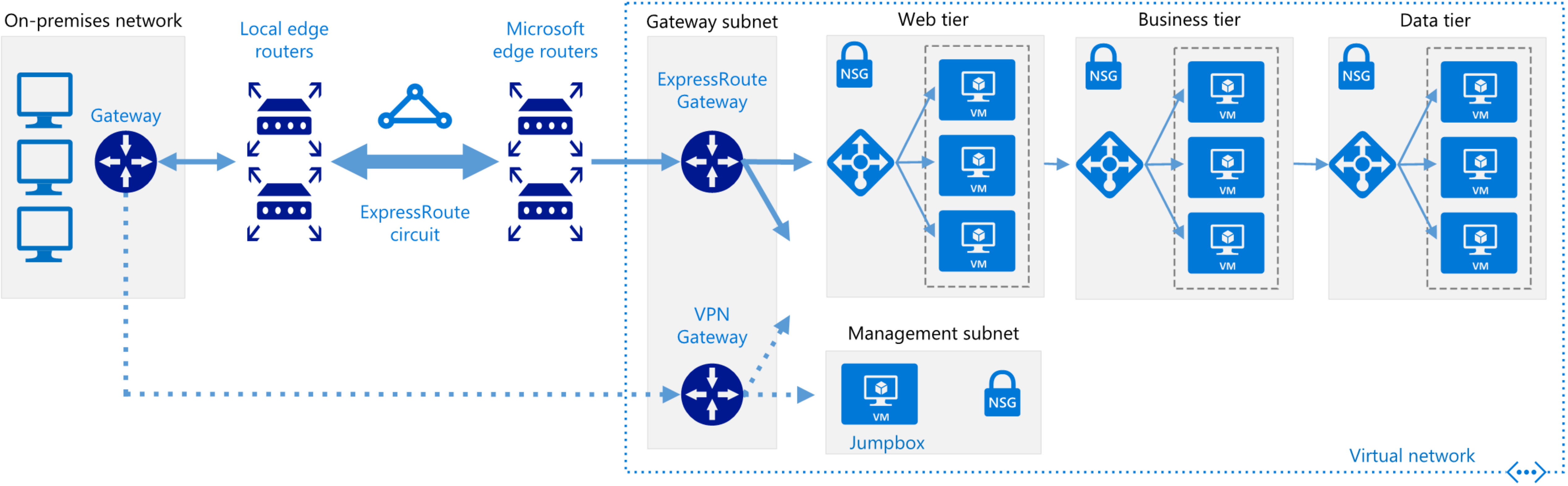
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute#deploy-the-solution

ExpressRoute with VPN failover

- This reference architecture shows how to connect an on-premises network to an Azure virtual network (VNet) using ExpressRoute, with a site-to-site virtual private network (VPN) as a failover connection.
- Traffic flows between the on-premises network and the Azure VNet through an ExpressRoute connection.
- **If there is a loss of connectivity in the ExpressRoute circuit, traffic is routed through an IPSec VPN tunnel**.

ExpressRoute with VPN failover

Microsoft

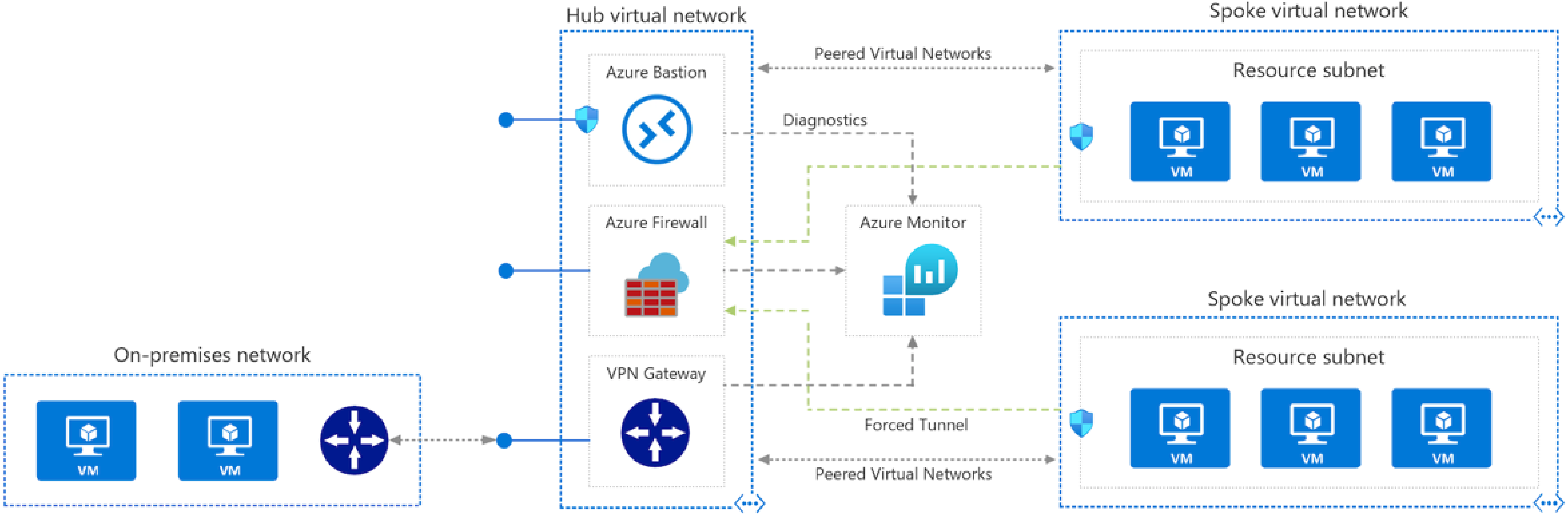


7/2/2021

Hub-spoke network topology in Azure

- This reference architecture details a hub-spoke topology in Azure. The hub virtual network acts as a central point of connectivity to many spoke virtual networks.
- The hub can also be used as the connectivity point to your on-premises networks.
- The spoke virtual networks peer with the hub and can be used to isolate workloads.

Hub-spoke network topology in Azure



https://docs.microsoft.com/en-us/samples/mspnp/samples/hub-and-spoke-deployment/

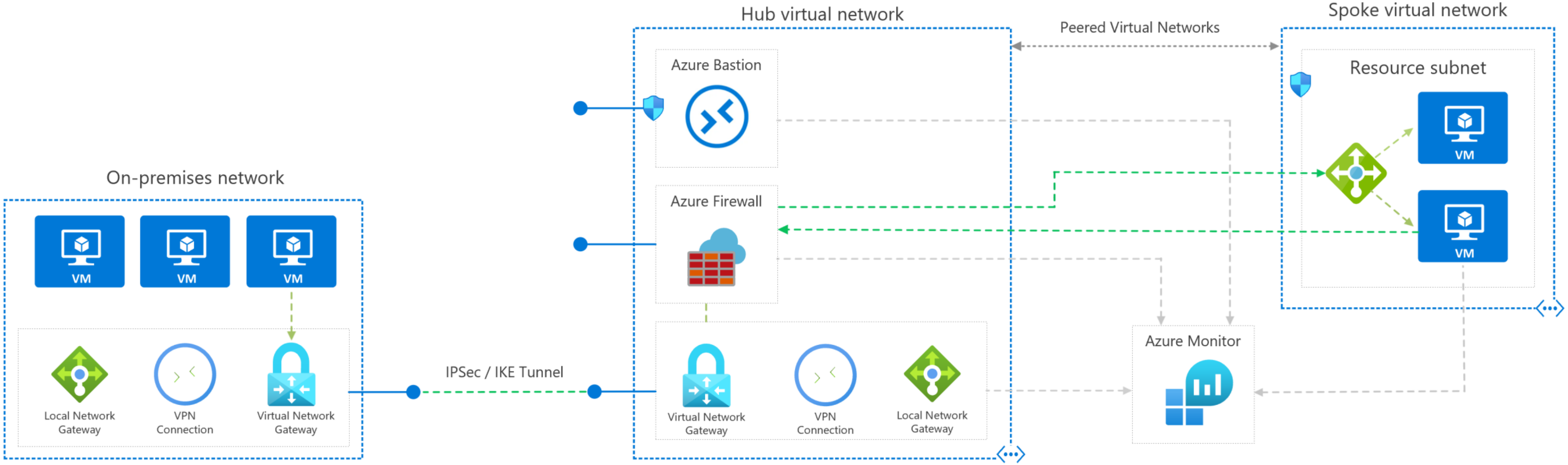
Hub-spoke network topology in Azure

- Typical uses for this architecture include:
  - Workloads deployed in different environments, such as development, testing, and production, that require shared services such as DNS, IDS, NTP, or AD DS. Shared services are placed in the hub virtual network, while each environment is deployed to a spoke to maintain isolation.
  - Workloads that do not require connectivity to each other but require access to shared services.
  - Enterprises that require central control over security aspects, such as a firewall in the hub as a DMZ, and segregated management for the workloads in each spoke.

DMZ between Azure and your on-premises datacenter

- This reference architecture shows a secure hybrid network that extends an on-premises network to Azure.
- The architecture implements a DMZ, also called a *perimeter network*, between the on-premises network and an Azure virtual network.
- All inbound and outbound traffic passes through Azure Firewall.

DMZ between Azure and your on-premises datacenter



7/2/2021

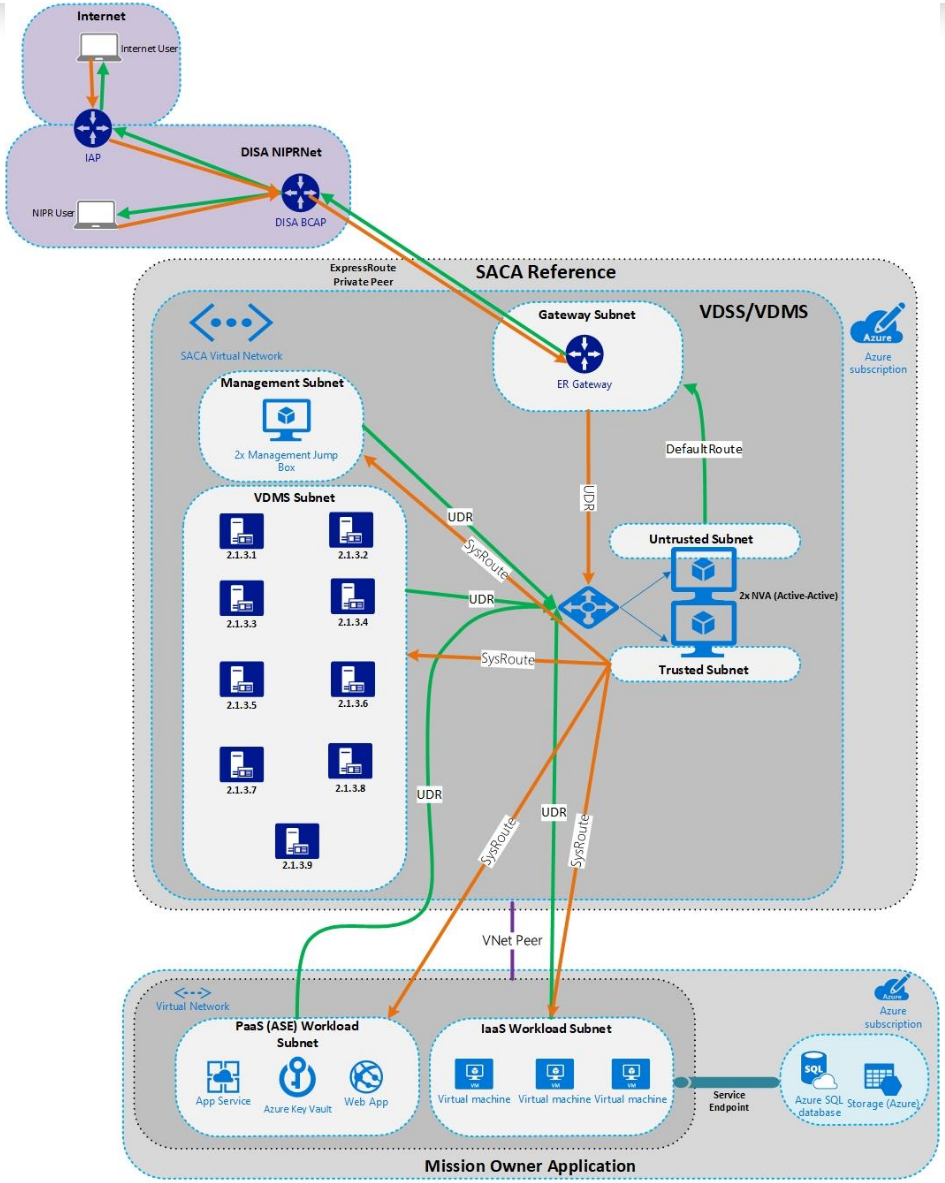
DMZ between Azure and your on-premises datacenter

Use Cases

- Hybrid applications where workloads run partly on-premises and partly in Azure.
- Infrastructure that requires granular control over traffic entering an Azure virtual network from an on-premises datacenter.
- Applications that must audit outgoing traffic. This is often a regulatory requirement of many commercial systems and can help to prevent public disclosure of private information.

Secure Azure Computing Architecture

- Boundary Cloud Access Point (BCAP)
- Virtual Datacenter Security Stack (VDSS)
- Virtual Datacenter Managed Services (VDMS)
- Trusted Cloud Credential Manager (TCCM)



Discussion

- How to configure an enterprise-class network within Azure.

- Consider the technologies to connect multiple virtual networks, as well as using capabilities such as routing to deploy network virtual appliances in Azure and services to secure your deployment.

Discussion pt2 – Customer situation -Fabrikam

- Fabrikam stands at the forefront of technological advancement in the ports industry.
- Headquartered in Miami, FL. 2 separate offices.
- 3 US branches in several states over the south US
- Fabrikam want to run their core application on the cloud.
- Application, Terminal Management System, developed in 2001 by in-house terminal expertise and logistics experts enabling Fabrikam to increase capacity, service and profitability. This app optimises, innovates and collaborates terminals with operations intelligences, execution and control, reporting and inventory.
- Fabrikam is looking for a hybrid solution. Currently, Fabrikam is using NLB in 2 sites to enable access to the applications per site. No redundancy across sites is enabled.

Discussion pt3 – Fabrikam needs

- NetOps team is considering options to redirect traffic using an on-premises gateway for this deployment.
- Fabrikam wants to run a pilot in the cloud
- The core application will be fully running on cloud
- Fabrikam needs to address the virtual networking architecture and support secure data flow between their on-premises infrastructure and the cloud.
- Fabrikam wants to keep their 10gig connectivity between the HQs with 2 sites and the cloud. US branches should also be able to have private connections to the cloud.
- NetOps team requires the ability to analyze traffic flows and detect potential vulnerabilities near real time.

Managed web application

Managed web application Architecture References

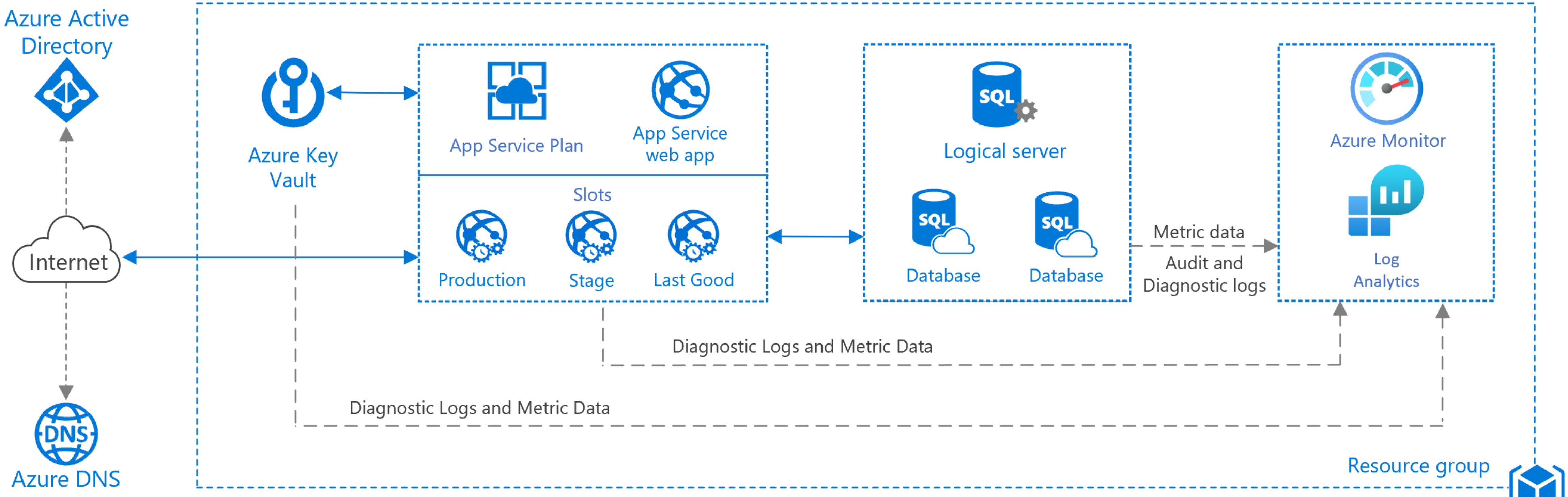
Microsoft

- Basic web application
- Scalable web application
- Serverless web application
- Web application in multiple Azure regions for high availability

Basic web application

- This architecture shows a baseline deployment for a web application that uses Azure App Service and Azure SQL Database.

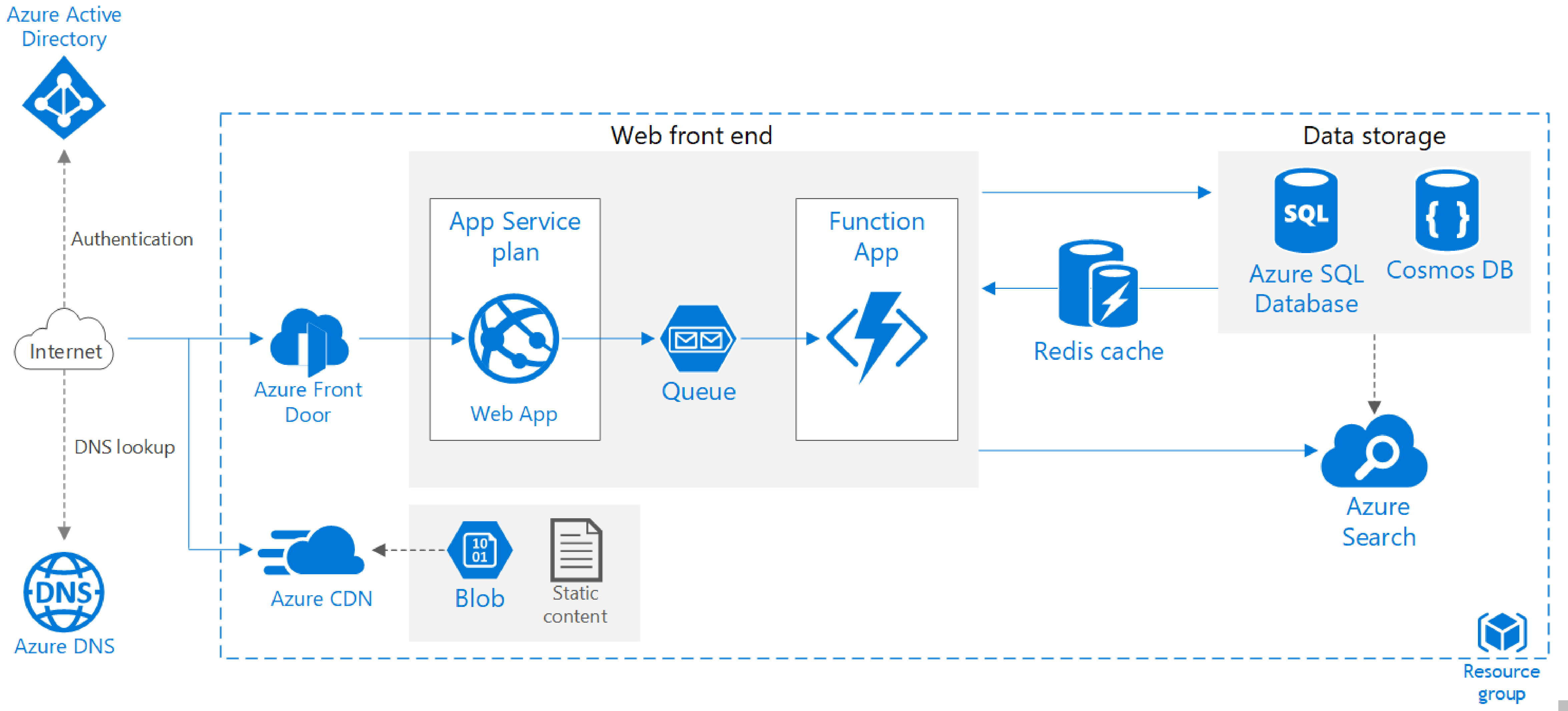
Basic web application



Scalable web application

- This reference architecture shows proven practices for improving scalability and performance in an Azure App Service web application.

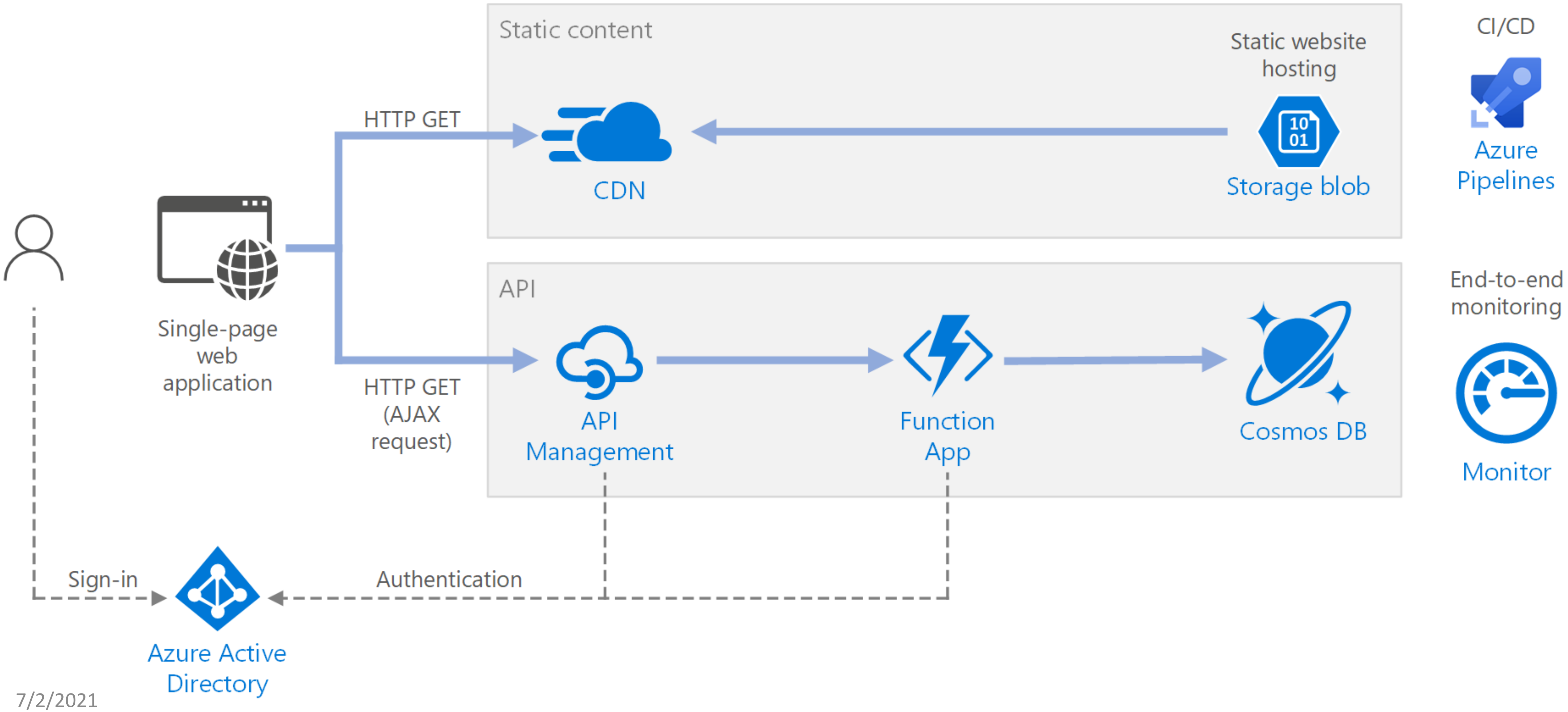
Scalable web application



Serverless web application

- This reference architecture shows a serverless web application. The application serves static content from Azure Blob Storage, and implements an API using Azure Functions.
- The API reads data from Cosmos DB and returns the results to the web app.

Serverless web application



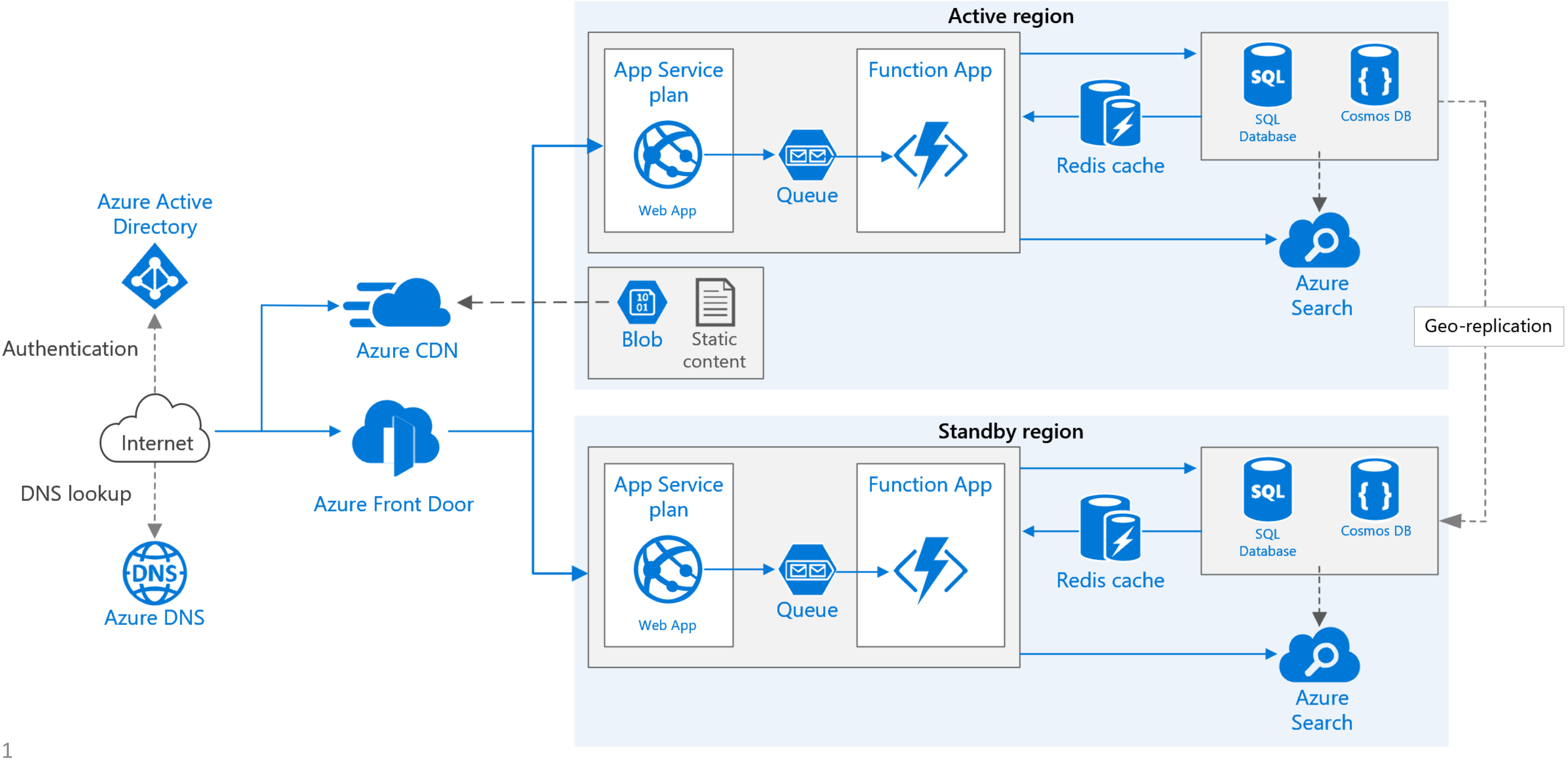
Web application in multiple Azure regions for high availability

Microsoft

- This reference architecture shows how to run an Azure App Service application in multiple regions to achieve high availability.

Web application in multiple Azure regions for high availability

Microsoft



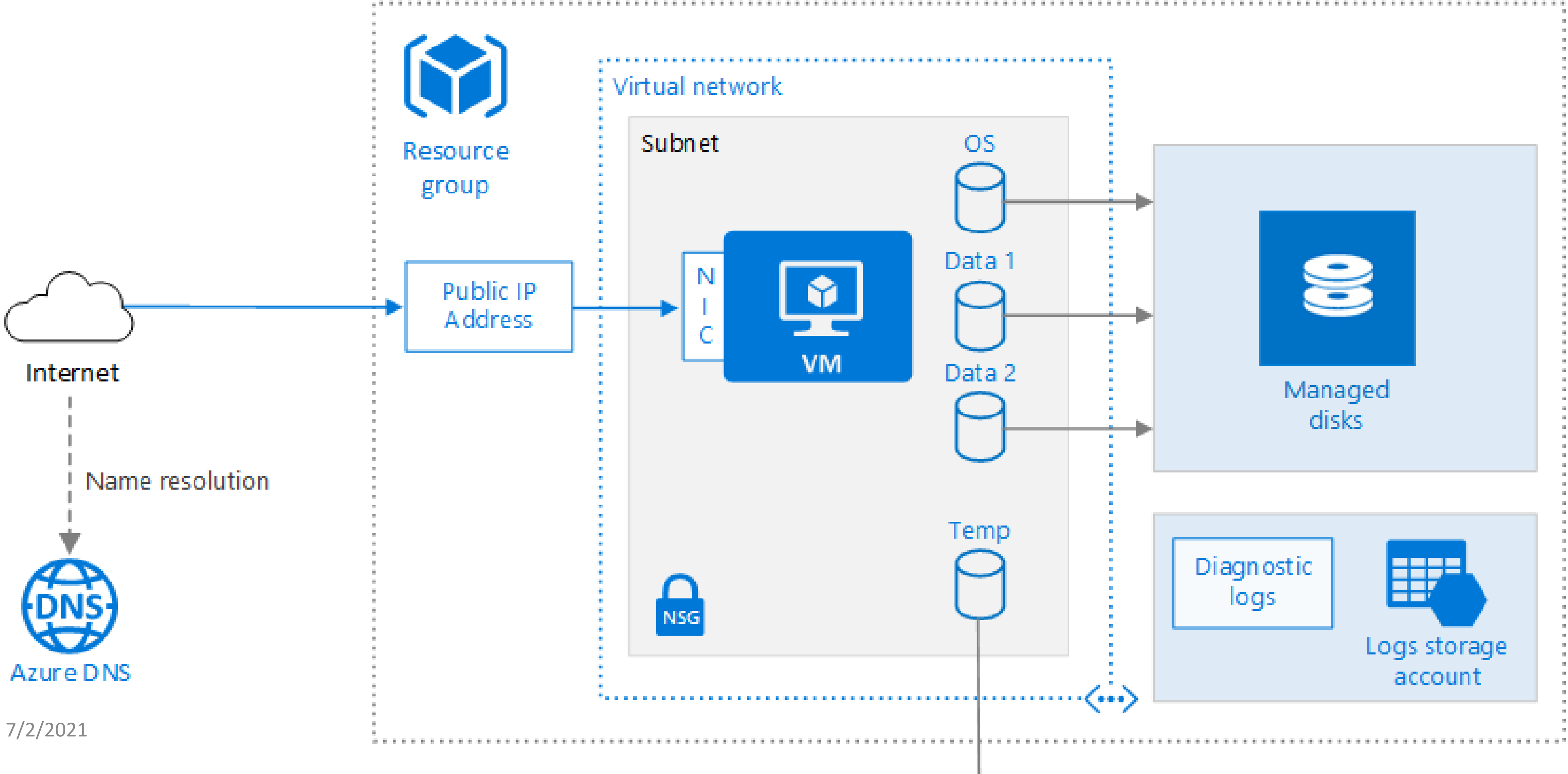
VM workloads

Microsoft

Run a Windows | Linux VM on Azure

- This architecture shows a Linux virtual machine (VM) running on Azure, along with associated networking and storage components.
- This architecture can be used to run a single instance, and is the basis for more complex architectures such as n-tier applications

Run a Windows | Linux VM on Azure



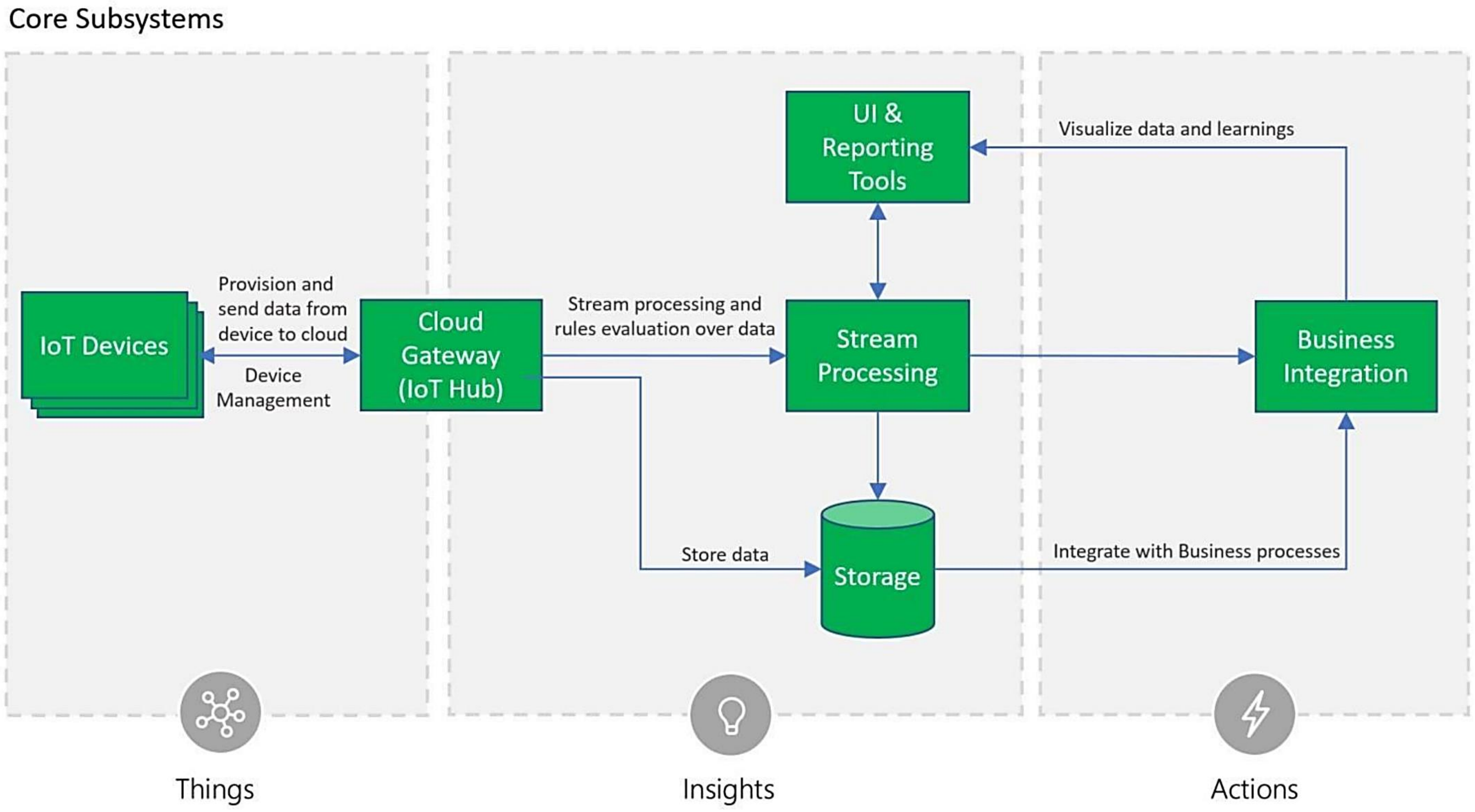
Internet Of Things

Azure IoT reference architecture

Microsoft

- The architecture we recommend for IoT solutions is cloud native, microservice, and serverless-based.
- The IoT solution subsystems should be built as discrete services that are independently deployable, and able to scale independently.
- These attributes enable greater scale, more flexibility in updating individual subsystems, and provide the flexibility to choose appropriate technology on a per-subsystem basis.
- It is critical to have the ability to monitor individual subsystems as well as the IoT application as a whole.

Core Subsystems

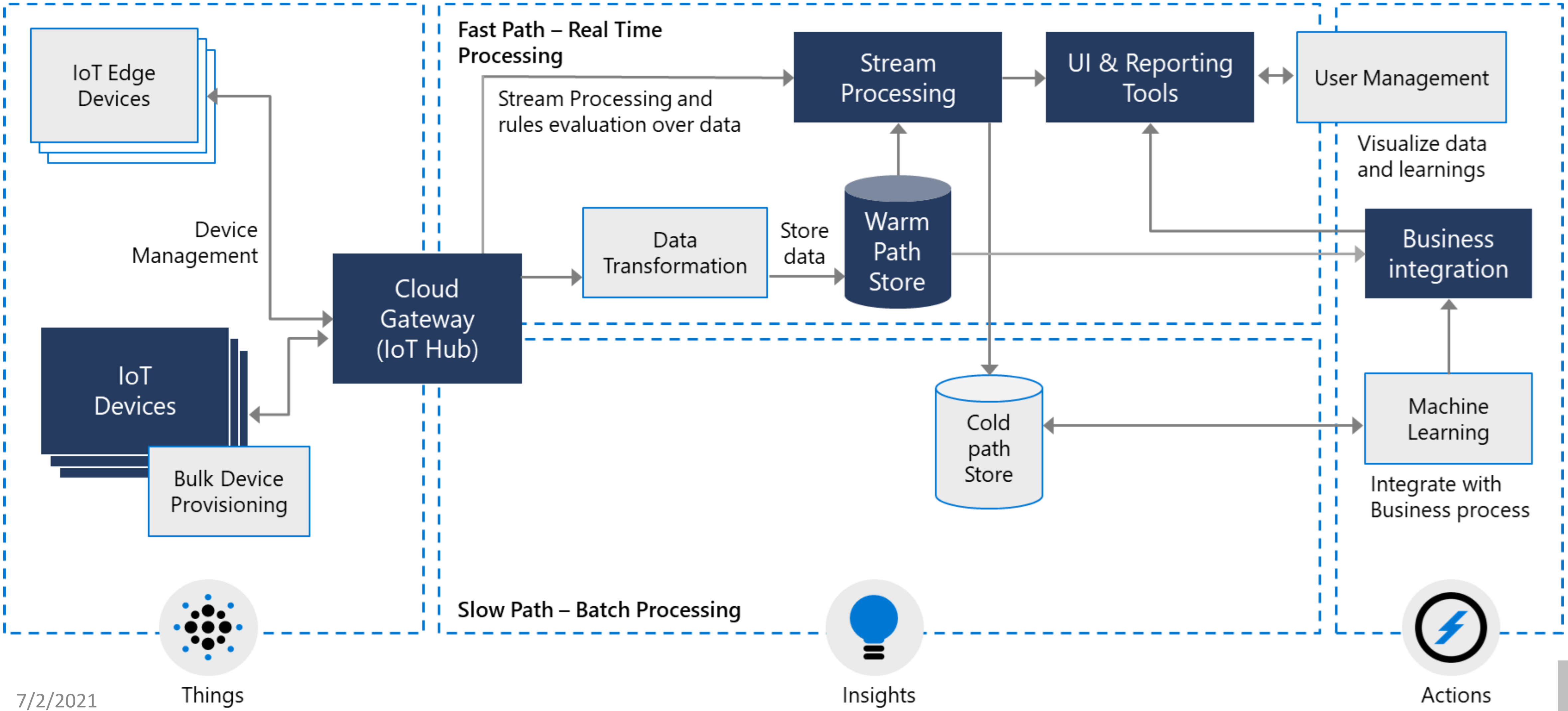


Core Subsystems

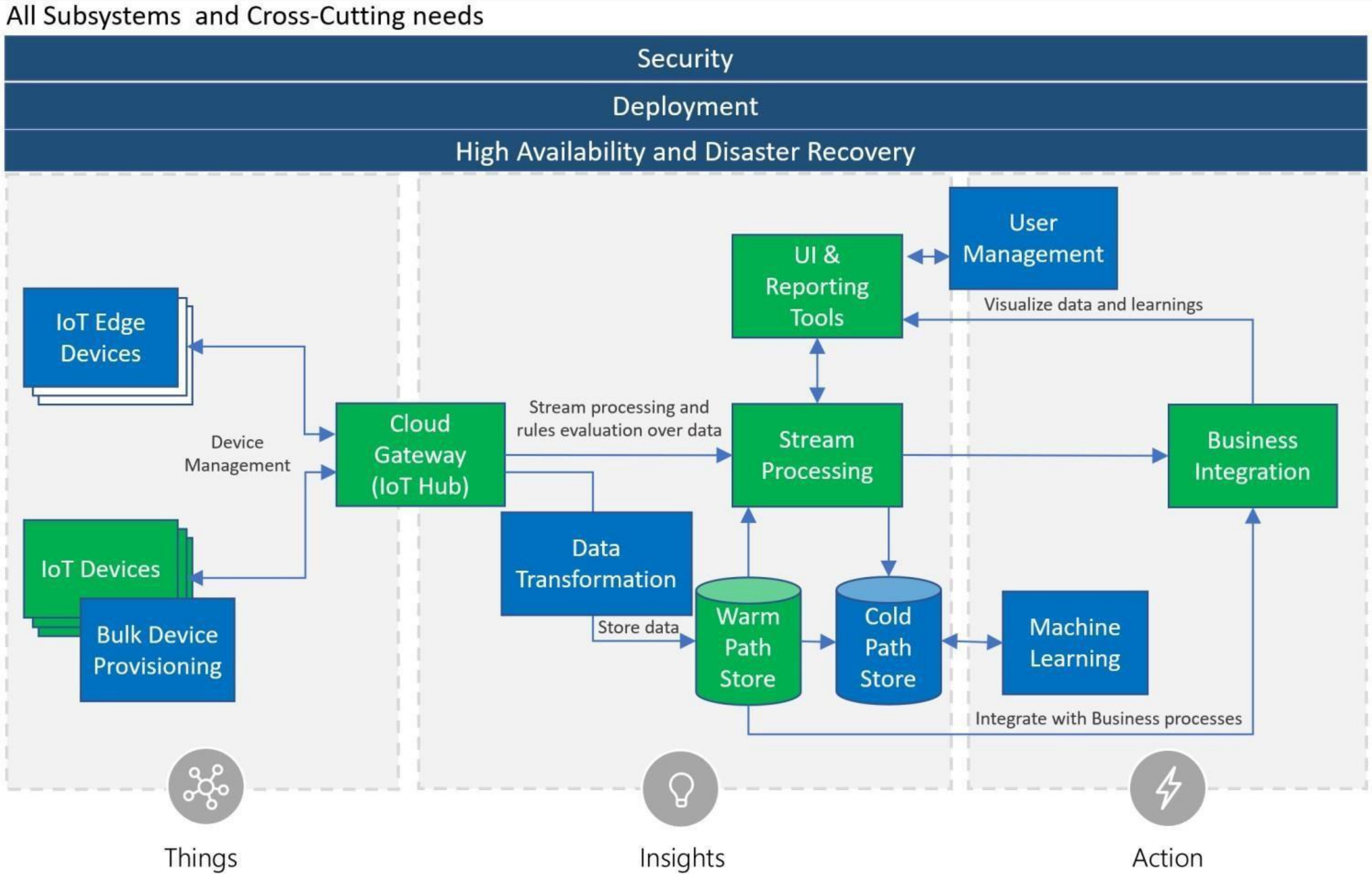
IoT Devices
Provision and send data from device to cloud
Device Management
Cloud Gateway (IoT Hub)
Stream processing and rules evaluation over data
UI & Reporting Tools
Visualize data and learnings
Stream Processing
Business Integration
Store data
Storage
Integrate with Business processes
Things
Insights
Actions

https://azure.microsoft.com/en-us/resources/microsoft-azure-iot-reference-architecture/

Optional Subsystems

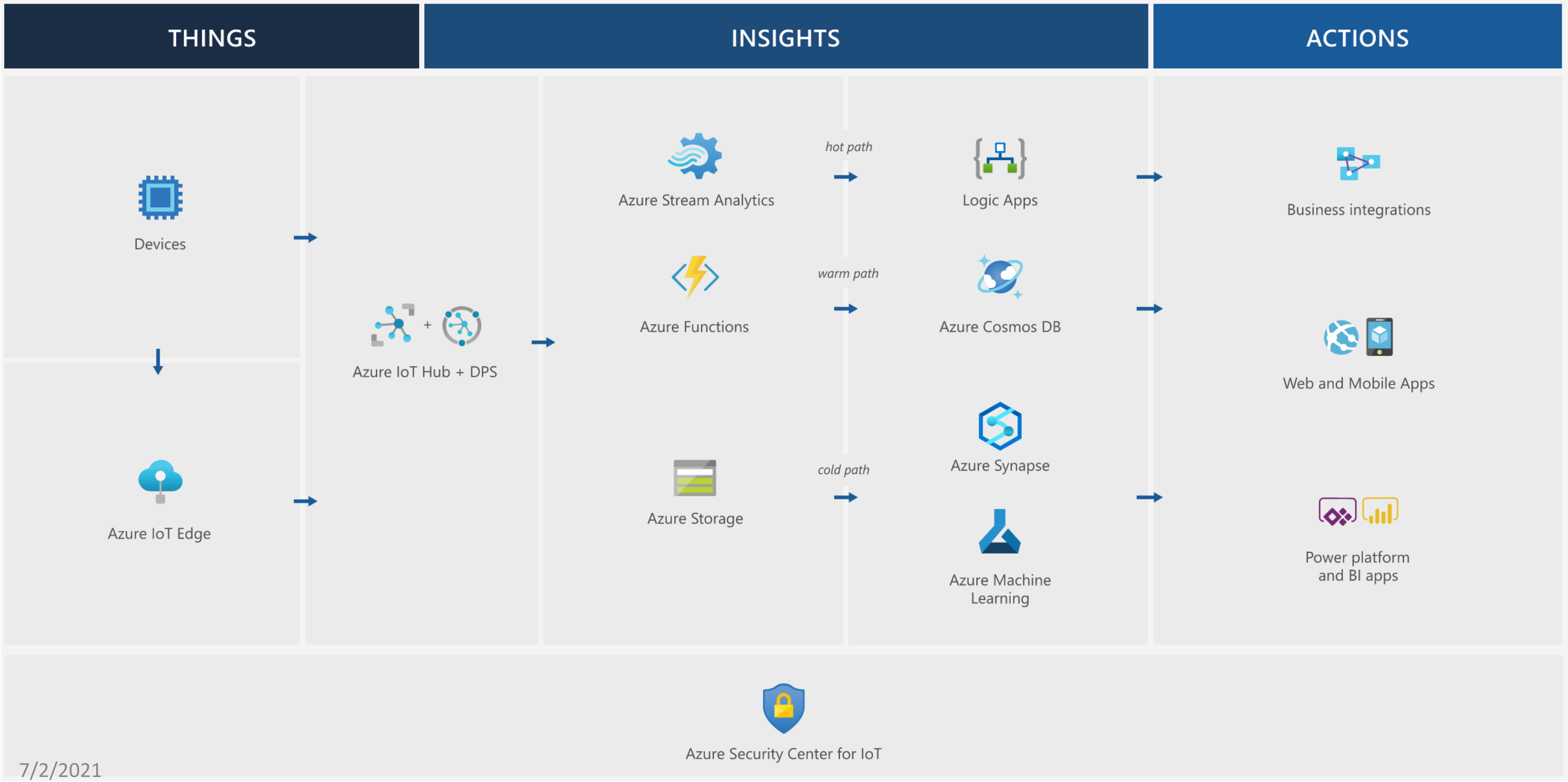


Cross-Cutting IoT application needs



Azure IoT reference architecture

Microsoft



7/2/2021

Data & BI

Data & BI Architecture References

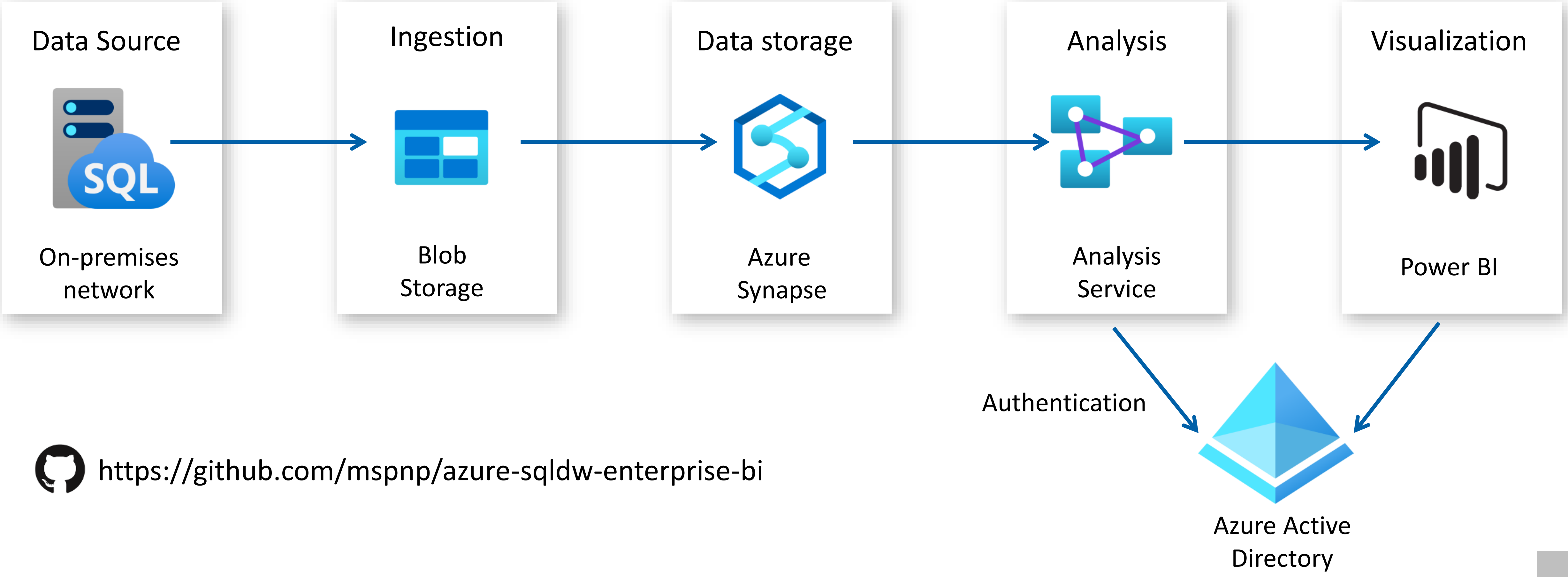
Microsoft

- Enterprise business intelligence
- Advanced Analytics Architecture
- Enterprise Data Warehouse Architecture
- Real Time Analytics on Big Data Architecture

Enterprise business intelligence

- This reference architecture implements an extract, load, and transform (ELT) pipeline that moves data from an on-premises SQL Server database into Azure Synapse and transforms the data for analysis.

Enterprise business intelligence



Data Source

On-premises network

Ingestion

Blob Storage

Data storage

Azure Synapse

Analysis

Analysis Service

Visualization

Power BI

Authentication

Azure Active Directory

https://github.com/mspnp/azure-sqldw-enterprise-bi

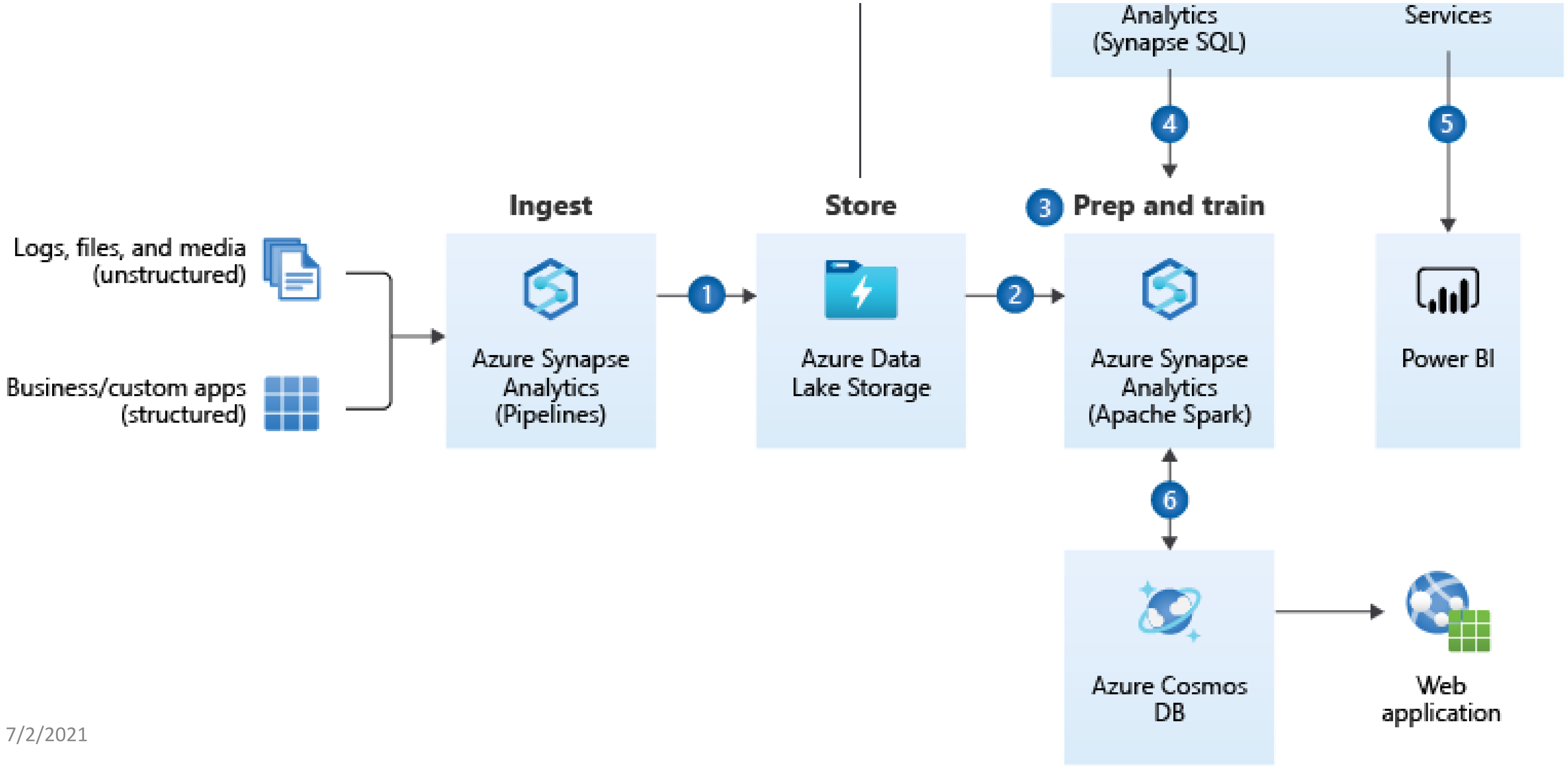
Enterprise business intelligence

- **Scenario**: An organization has a large OLTP data set stored in a SQL Server database on premises.
- The organization wants to use Azure Synapse to perform analysis using Power BI.

Advanced Analytics Architecture

- Transform your data into actionable insights using the best-in-class machine learning tools.
- This architecture allows you to combine any data at any scale, and to build and deploy custom machine learning models at scale.

Advanced Analytics Architecture



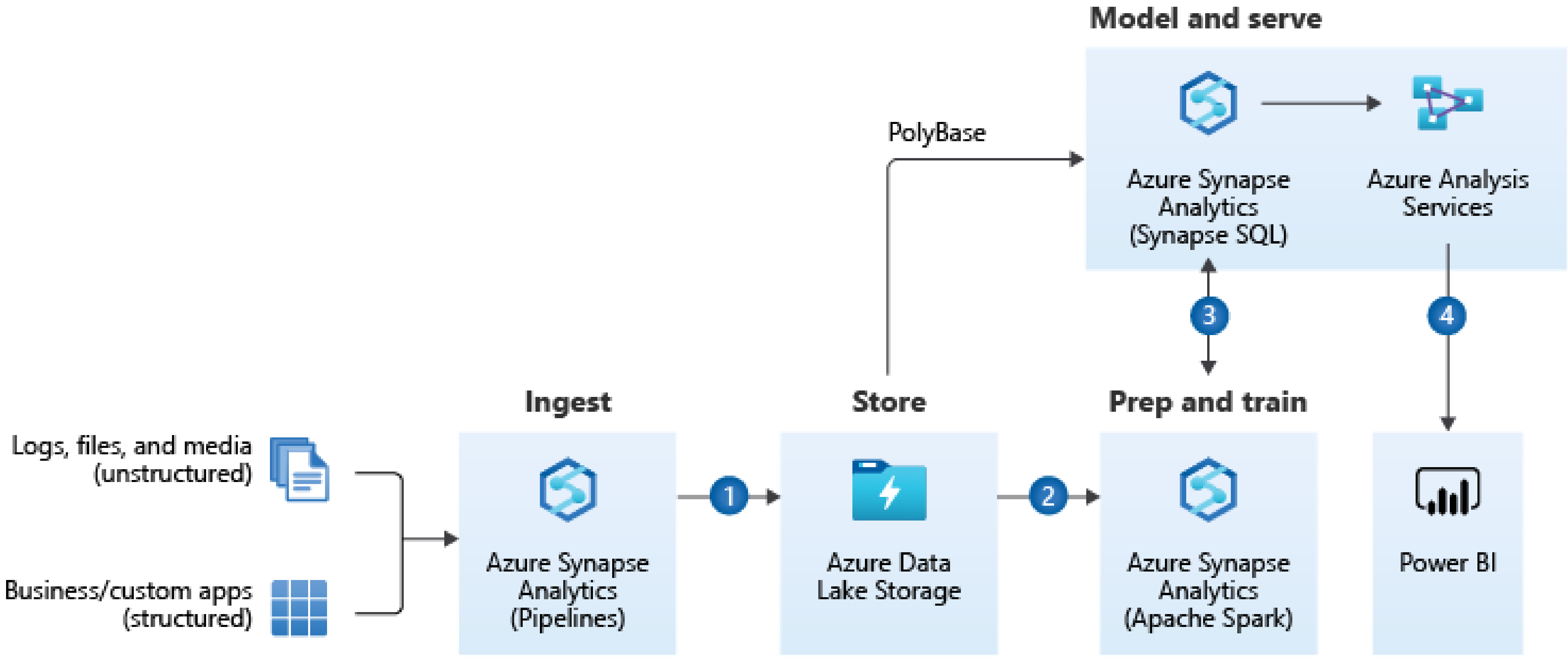
7/2/2021

Enterprise Data Warehouse Architecture

- An enterprise data warehouse lets you bring together all your data at any scale easily, and to get insights through analytical dashboards, operational reports, or advanced analytics for all your users.

Enterprise Data Warehouse Architecture

Microsoft


Model and serve
PolyBase
Azure Synapse Analytics (Synapse SQL)
Azure Analysis Services
3
4
Ingest
Store
Prep and train
Logs, files, and media (unstructured)
Business/custom apps (structured)
Azure Synapse Analytics (Pipelines)
1
Azure Data Lake Storage
2
Azure Synapse Analytics (Apache Spark)
Power BI

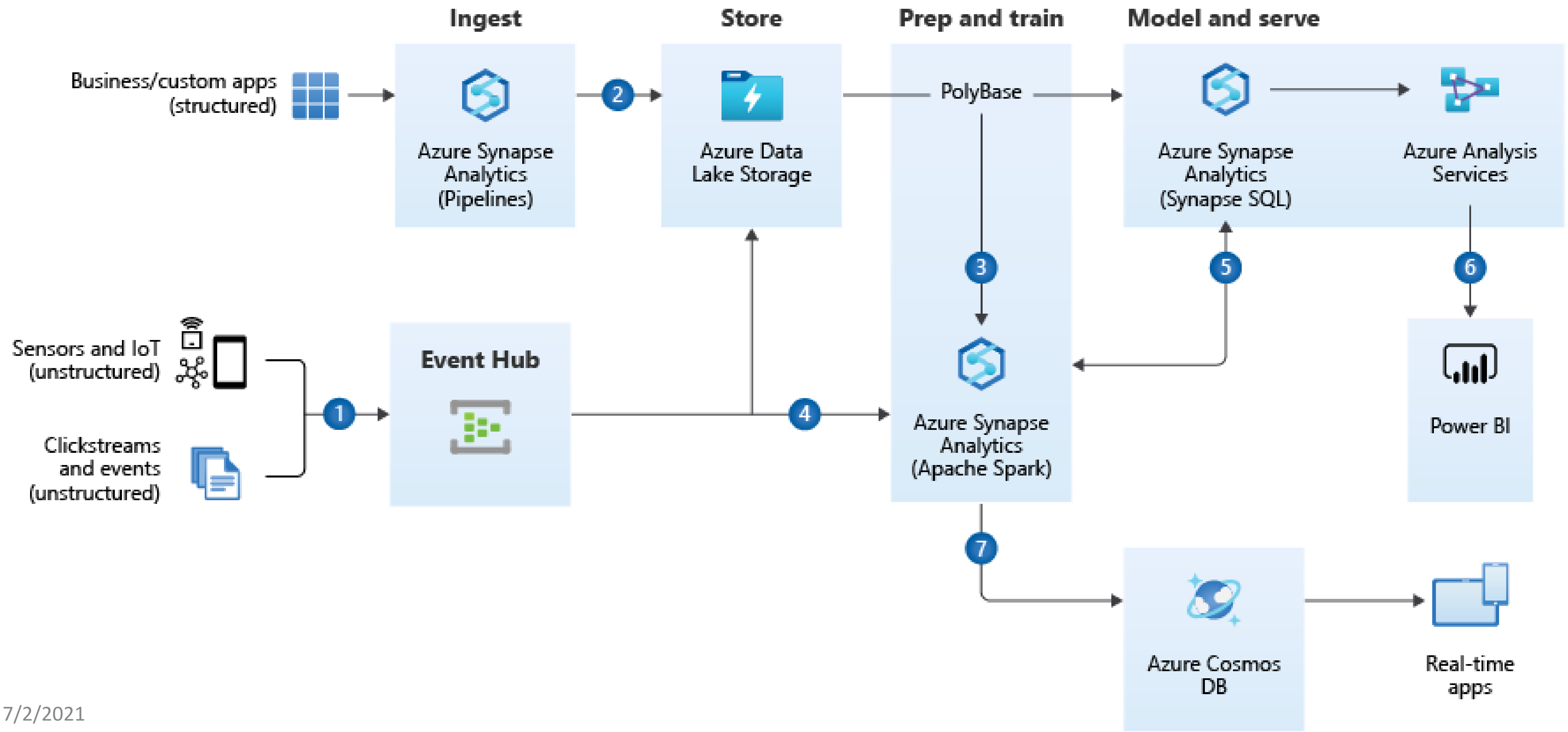
7/2/2021

Real Time Analytics on Big Data Architecture

- Get insights from live streaming data with ease. Capture data continuously from any IoT device, or logs from website clickstreams, and process it in near-real time.

Real Time Analytics on Big Data Architecture

Microsoft



Ingest
Store
Prep and train
Model and serve
Business/custom apps (structured)
Azure Synapse Analytics (Pipelines)
2
Azure Data Lake Storage
PolyBase
Azure Synapse Analytics (Synapse SQL)
Azure Analysis Services
3
5
6
Sensors and IoT (unstructured)
Clickstreams and events (unstructured)
1
Event Hub
4
Azure Synapse Analytics (Apache Spark)
Power BI
7
Azure Cosmos DB
Real-time apps

Resources

- Q & A

Microsoft

Thank You!

Global Architect Summit 2021