Module 12: Monitoring & Automating Azure Solutions

Contents:

Module overview

This module covers the monitoring and automation solutions available after an Azure solution has been architected, designed and possibly deployed. The module reviews services that are used to monitor individual applications, the Azure platform, and networked components. This module also covers automation and backup options to enable business-continuity scenarios for solutions hosted in Azure.

Objectives

After completing this module, students will be able to:

- Compare and contrast monitoring services for applications, the Azure platform, and networking.
- Design an alert scheme for a solution hosted in Azure.
- Select the appropriate backup option for infrastructure and data hosted in Azure.
- Automate the deployment of future resources for backup recovery or scaling purposes.

Lesson 1: Monitoring

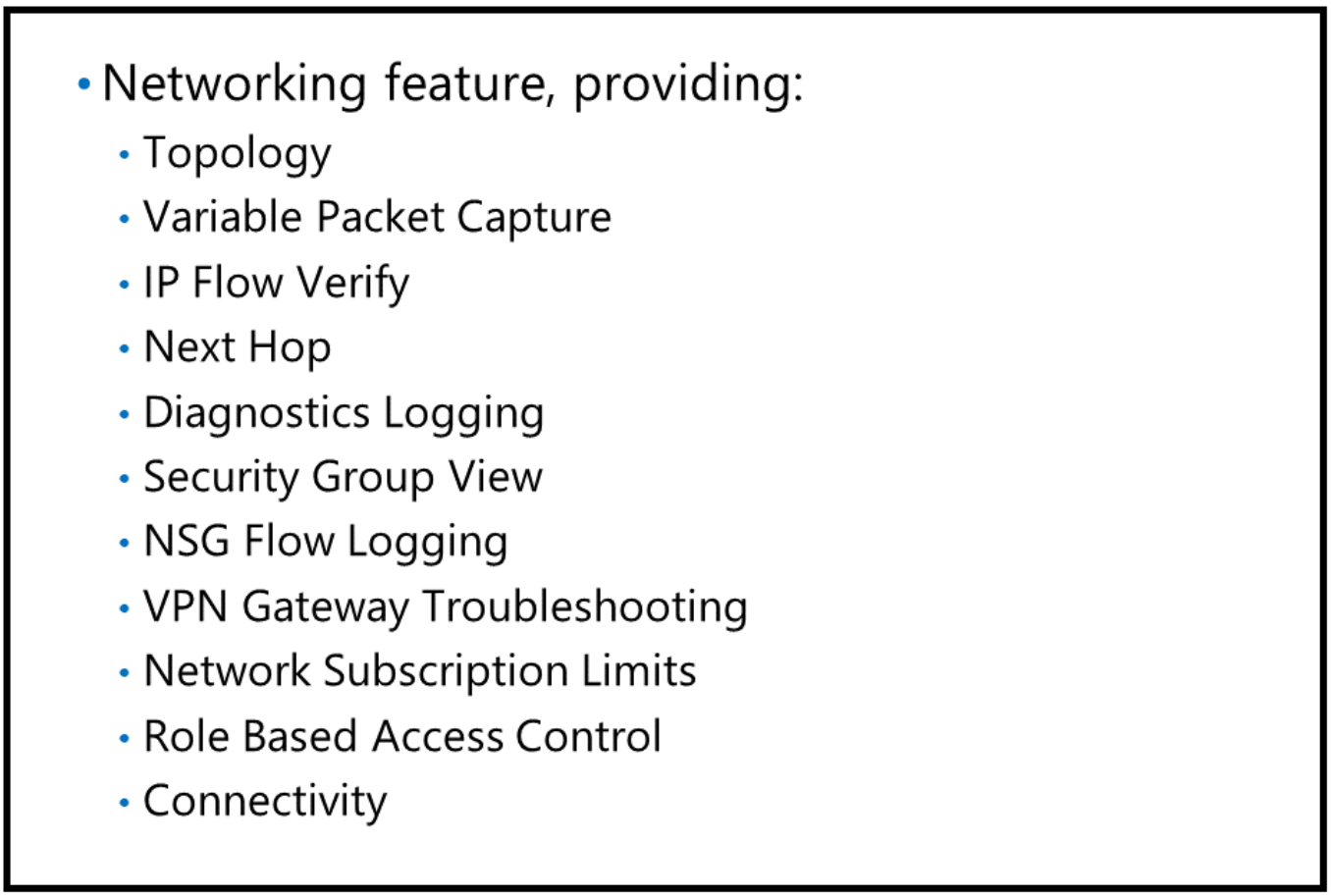
This lesson reviews a variety of services available in Azure to monitor your workloads and applications.

Lesson objectives

After completing this lesson, you will be able to:

- Select between OMS, Network Watcher, Security Center, Azure Monitor, Azure Service Health and Azure Advisors when determining which monitoring solution to use for workloads deployed to Azure.
- Query historical log data using Power BI.
- Integrate Application Insights into a custom software solution hosted on Azure.

Azure Network Watcher



Customers can build an end-to-end network in Azure by orchestrating and composing various individual network resources such as VNet, ExpressRoute, Application Gateway, Load balancers, and more. Monitoring is available on each of the network resources. We refer to this monitoring as resource level monitoring.

The end to end network can have complex configurations and interactions between resources, creating complex scenarios that need scenario-based monitoring through Network Watcher.

Network Watcher provides the following features:

- Topology
- Variable Packet Capture
- IP Flow Verify

- Next Hop
- Diagnostics Logging
- Security Group View
- NSG Flow Logging
- VPN Gateway Troubleshooting
- Network Subscription Limits
- Role Based Access Control
- Connectivity

Network Monitor

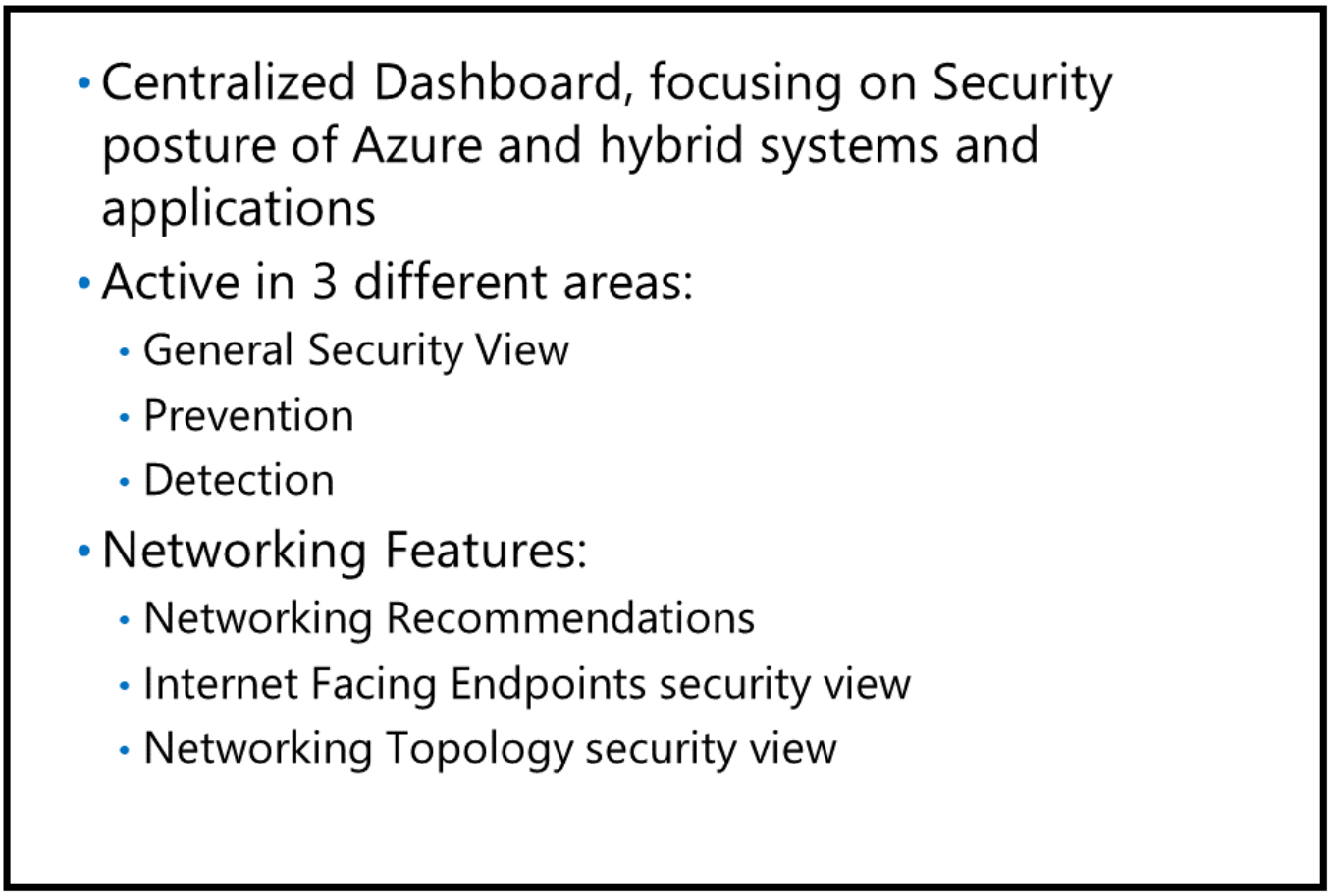
Operations performed as part of the configuration of networks are logged. These logs can be viewed in the Azure portal or retrieved using Microsoft tools such as Power BI or third-party tools. Audit logs are available through the portal, PowerShell, CLI, and Rest API.

Metrics are performance measurements and counters collected over a period of time. Metrics are currently available for Application Gateway. Metrics can be used to trigger alerts based on thresholds.

Periodic and spontaneous events are created by network resources and logged in storage accounts, sent to an Event Hub, or Log Analytics. These logs provide insights into the health of a resource. These logs can be viewed in tools such as Power BI and Log Analytics.

The troubleshooting blade, available in the portal, is provided on network resources today to diagnose common problems associated with an individual resource. This blade is available for the following network resources - ExpressRoute, VPN Gateway, Application Gateway, Network Security Logs, Routes, DNS, Load Balancer, and Traffic Manager.

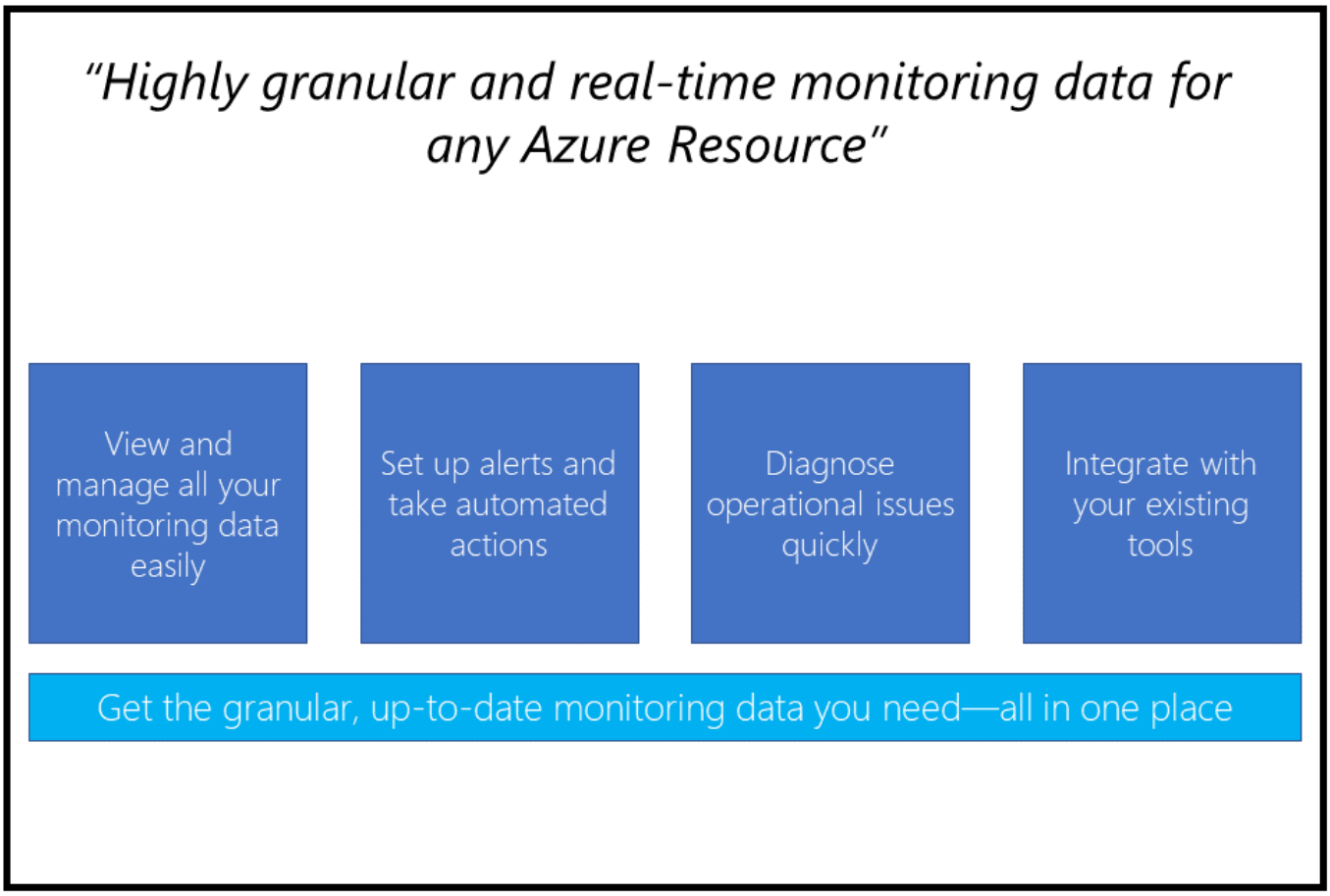
Azure Security Center



Azure Security Center provides unified security management and advanced threat protection for workloads running in Azure, on-premises, and in other clouds. It delivers visibility and control over hybrid cloud workloads, active defenses that reduce your exposure to threats, and intelligent detection to help you keep pace with rapidly evolving cyberattacks.

The Security Center Overview provides a quick view into the security posture of your Azure and non-Azure workloads, enabling you to discover and assess the security of your workloads and to identify and mitigate risk.

Azure Monitor & Diagnostics



Azure Monitor is part of Microsoft Azure's overall monitoring solution. Azure Monitor helps you track performance, maintain security, and identify trends. Learn how to audit, create alerts, and archive data with our quickstarts and tutorials.

Azure Monitor enables you to consume telemetry to gain visibility into the performance and health of your workloads on Azure. The most important type of Azure telemetry data is the metrics (also called performance counters) emitted by most Azure resources. Azure Monitor provides several ways to configure and consume these metrics for monitoring and troubleshooting.

What can you do with metrics?

Metrics are a valuable source of telemetry and enable you to do the following tasks:

- **Track the performance** of your resource (such as a VM, website, or logic app) by plotting its metrics on a portal chart and pinning that chart to a dashboard.
- **Get notified of an issue** that impacts the performance of your resource when a metric crosses a certain threshold.
- **Configure automated actions**, such as autoscaling a resource or firing a runbook when a metric crosses a certain threshold.
- **Perform advanced analytics** or reporting on performance or usage trends of your resource.
- **Archive** the performance or health history of your resource **for compliance or auditing** purposes.

Metrics

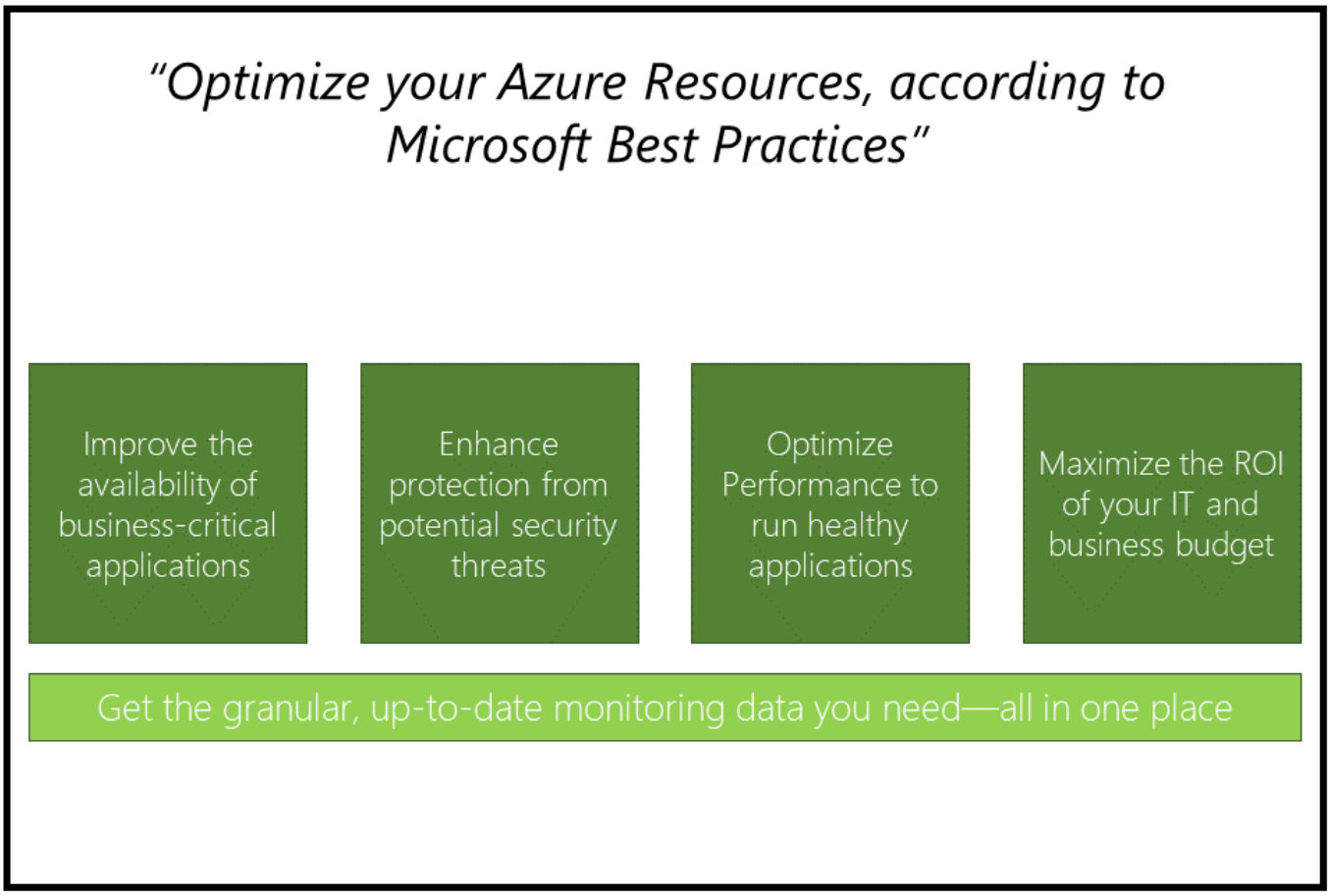
Azure Monitor enables users to obtain telemetry so that the user can gain visibility into the health and performance of workloads on Azure. Metrics is the essential type of Azure telemetry data that can be emitted by most Azure resources. Though Azure Monitor, a user have several ways to consume and configure these metrics for monitoring and troubleshooting.

Metrics have a set of characteristics you can use to identify it. Metrics become available immediately, meaning there is no need to set up additional diagnostics for metrics, nor opt-in for the data. Metrics also have a frequency of one minute. Users receive all metric values every minute from a resource, which allows for expanded visibility into the health and current state of your resource. Some metrics available can also have name-value pair attributes. These are known as dimensions which enable you to further segment and explore a metric. Moreover, Lastly, metrics allow users to access up to 30 days of history for each metric. By doing so, you can explore recent and monthly trends in the health and performance of your resource.

Users can use metrics to complete multiple tasks. These include tracking the performance of a resource by plotting its metrics on a chart. You can get notified of an issue if the issue impacts the performance of a resource. Since metrics have a frequency of one minute, this allows users to become aware of an issue on a near real-time basis. You can report on performance and usage trends on your resource to perform advanced analytics. After, users can choose to achieve health and performance history of a resource for compliance or auditing purposes.

Users can also choose to configure a metric alert rule that takes an automatic action, or even merely sends out a notification whenever the metric achieves a defined threshold. One of those automated actions is known as autoscale, which allows you to scale out your resource to meet incoming loads or requests. You can also route al metrics Log Analytics or Application Insights to enable instant Analytics. You can also choose to stream this information to an event hub. Doing so allows you to route them to Azure Stream Analytics for near-real-time analysis. You can choose to view all metrics, easily accessing them when you select a resource. You can also choose to achieve metrics to storage if you need to retrain them for longer then the archive period. You can choose o also route the metrics to an Azure Blob storage when you configure the settings for your resource.

Azure Advisors



Azure Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry. It then recommends solutions to help improve the performance, security, and high availability of your resources while looking for opportunities to reduce your overall Azure spend.

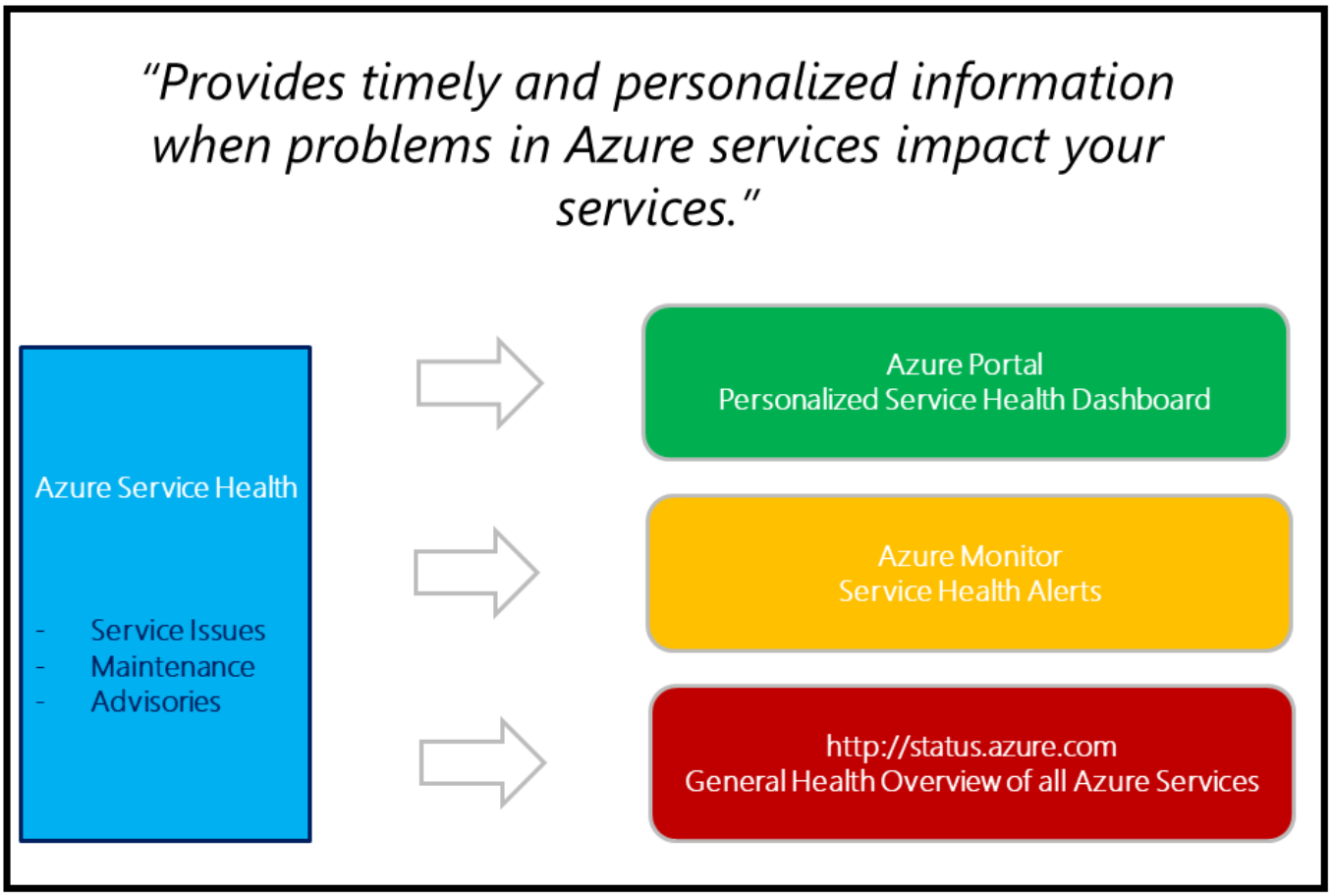
With Advisor, you can:

- Get proactive, actionable, and personalized best practices recommendations.
- Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend.
- Get recommendations with proposed actions inline.

The Advisor dashboard displays personalized recommendations for all your subscriptions. You can apply filters to display recommendations for specific subscriptions and resource types. The recommendations are divided into four categories:

- **High Availability**: To ensure and improve the continuity of your business-critical applications.
- **Security**: To detect threats and vulnerabilities that might lead to security breaches.
- **Performance**: To improve the speed of your applications.
- **Cost**: To optimize and reduce your overall Azure spending.

Azure Service Health



Azure Service Health provides personalized guidance and support when issues in Azure services affect you, and helps you prepare for upcoming planned maintenance. Azure Service Health alerts you and your teams via targeted and flexible notifications.

Service Health tracks three types of health events that may impact your resources:

- **Service issues** - Problems in the Azure services that affect you right now.
- **Planned maintenance** - Upcoming maintenance that can affect the availability of your services in the future.
- **Health advisories** - Changes in Azure services that require your attention. Examples include when Azure features are deprecated or if you exceed a usage quota.

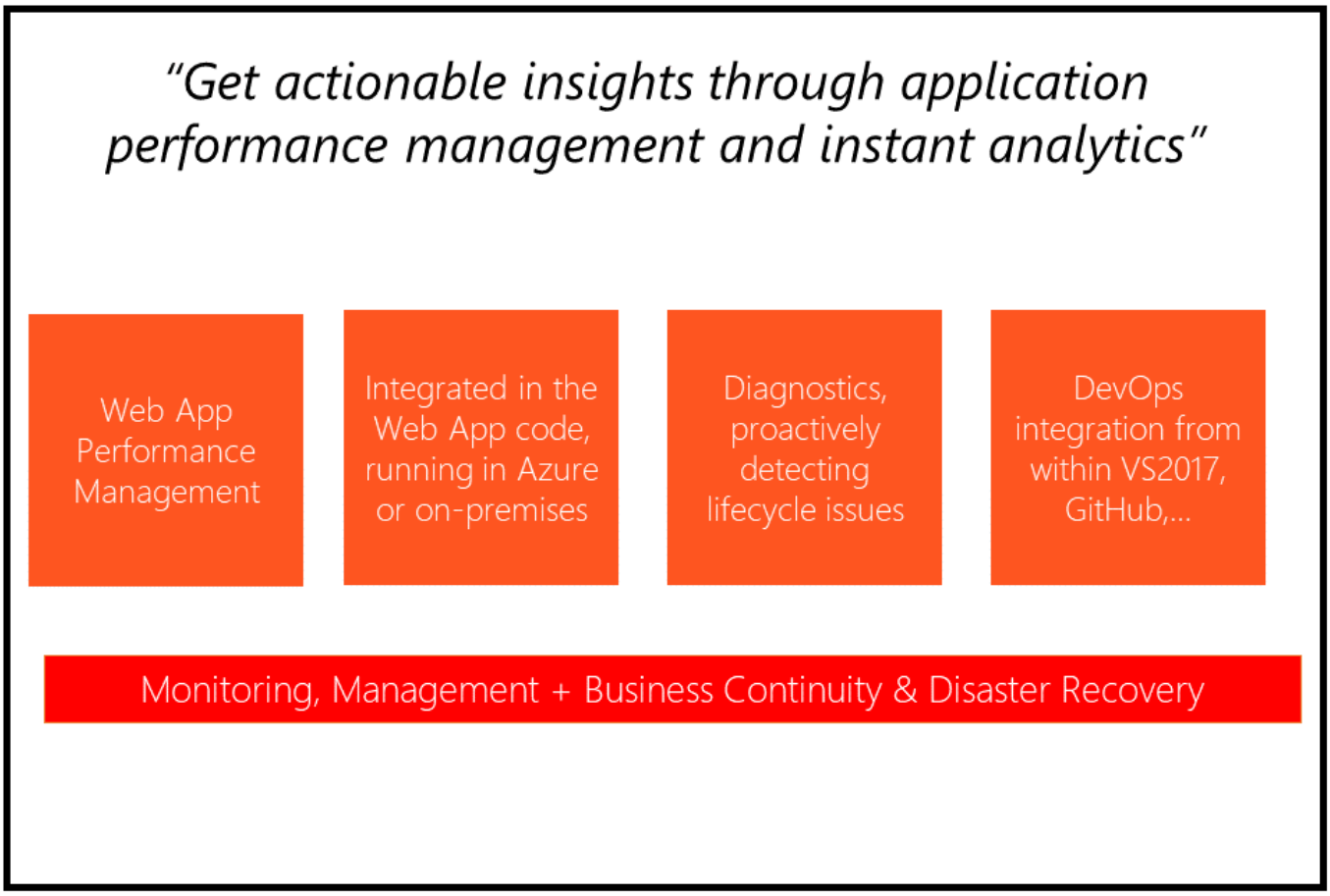
Operations Management Suite – Log Analytics

Log Analytics is part of Microsoft Azure's overall monitoring solution. Log Analytics monitors cloud and on-premises environments to maintain availability and performance. Get insight across workloads and systems to maintain availability and performance.

Log Analytics is a service in Operations Management Suite (OMS) that monitors your cloud and on-premises environments to maintain their availability and performance. It collects data generated by resources in your cloud and on-premises environments and from other monitoring tools to provide analysis across multiple sources. This article provides a brief discussion of the value that Log Analytics provides, an overview of how it operates, and links to more detailed content so you can dig further.

You can access Log Analytics through the OMS portal or the Azure portal which run in any browser and provide you with access to configuration settings and multiple tools to analyze and act on collected data. From the portal you can leverage log searches where you construct queries to analyze collected data, dashboards which you can customize with graphical views of your most valuable searches, and solutions which provide additional functionality and analysis tools.

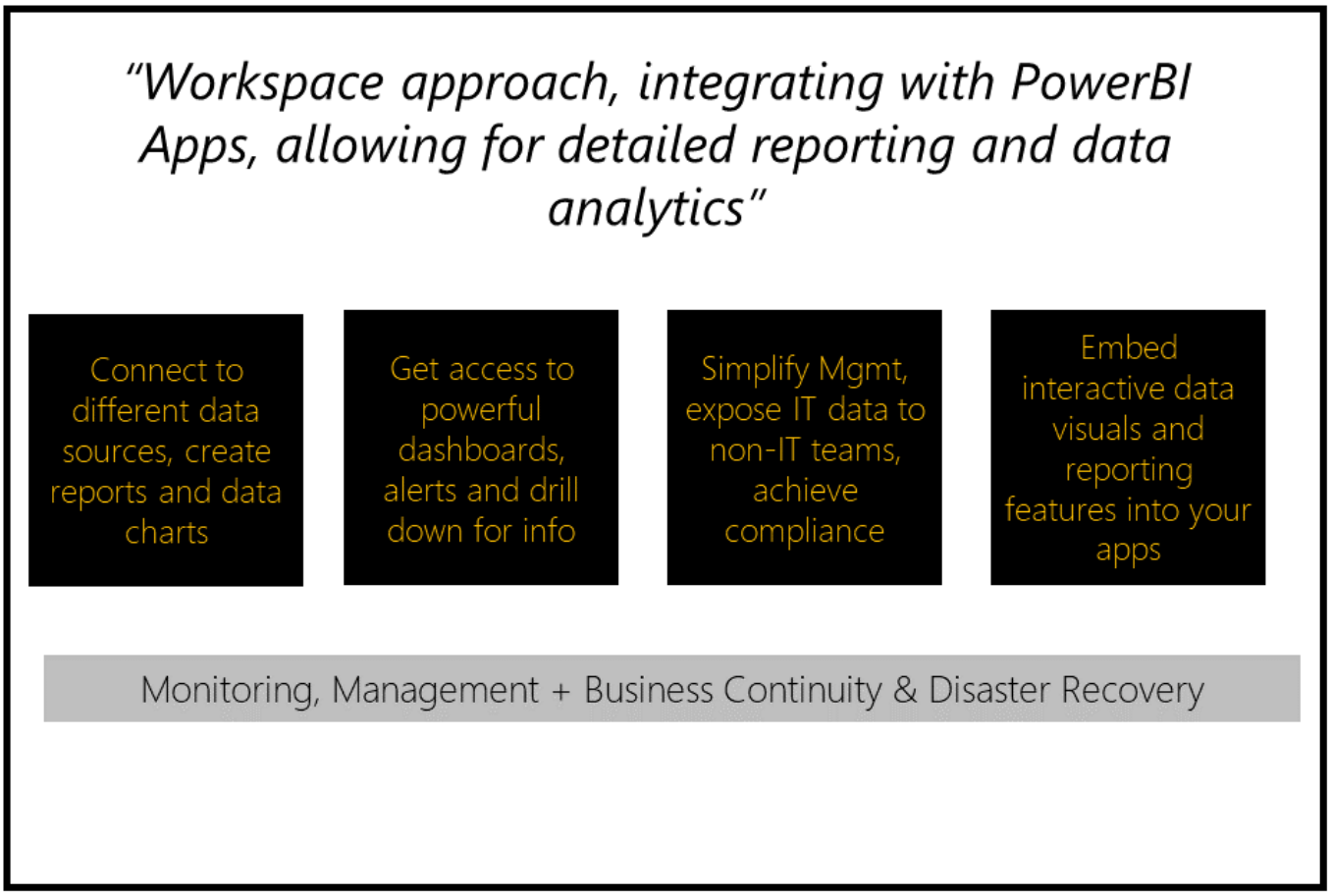
Application Insights



Application Insights is an extensible Application Performance Management (APM) service for web developers building and managing apps on multiple platforms. Learn how to detect & diagnose issues and understand usage for your web apps and services.

Application Insights is an extensible Application Performance Management (APM) service for web developers on multiple platforms. Use it to monitor your live web application. It will automatically detect performance anomalies. It includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app. It's designed to help you continuously improve performance and usability. It works for apps on a wide variety of platforms including .NET, Node.js and J2EE, hosted on-premises or in the cloud. It integrates with your DevOps process, and has connection points to a variety of development tools. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center and HockeyApp.

Power BI



With Azure services and Power BI, you can turn your data processing efforts into analytics and reports that provide real-time insights into your business. Whether your data processing is cloud-based or on-premises, straightforward or complex, single-sourced or massively scaled, warehoused or real-time, Azure and Power BI have the built-in connectivity and integration to bring your business intelligence efforts to life.

Power BI has a multitude of Azure connections available, and the business intelligence solutions you can create with those services are as unique as your business. You can connect as few as one Azure data source, or a handful, then shape and refine your data to build customized reports.

Azure SQL Database and Power BI

You can start with a straightforward connection to an Azure SQL Database, and create reports to monitor the progress of your business. Using the Power BI Desktop, you can create reports that identify trends and key performance indicators that move your business forward.

Do you have more complex data, and all sorts of sources? No problem. With Power BI Desktop and Azure services, connections are just a tap of the Get Data dialog away. Within the same Query you can connect to your Azure SQL Database, your Azure HDInsight data source, and your Azure Blob Storage (or Azure Table Storage), then select only the subsets within each that you need, and refine it from there.

There are all sorts of scenarios where Azure and Power BI can be combined - the possibilities and opportunities are as unique as your business. For more information about Azure services, check out this overview page, which describes Data Analytics Scenarios using Azure, and learn how to transform your data sources into intelligence that drives your business ahead.

Lesson 2: Backup

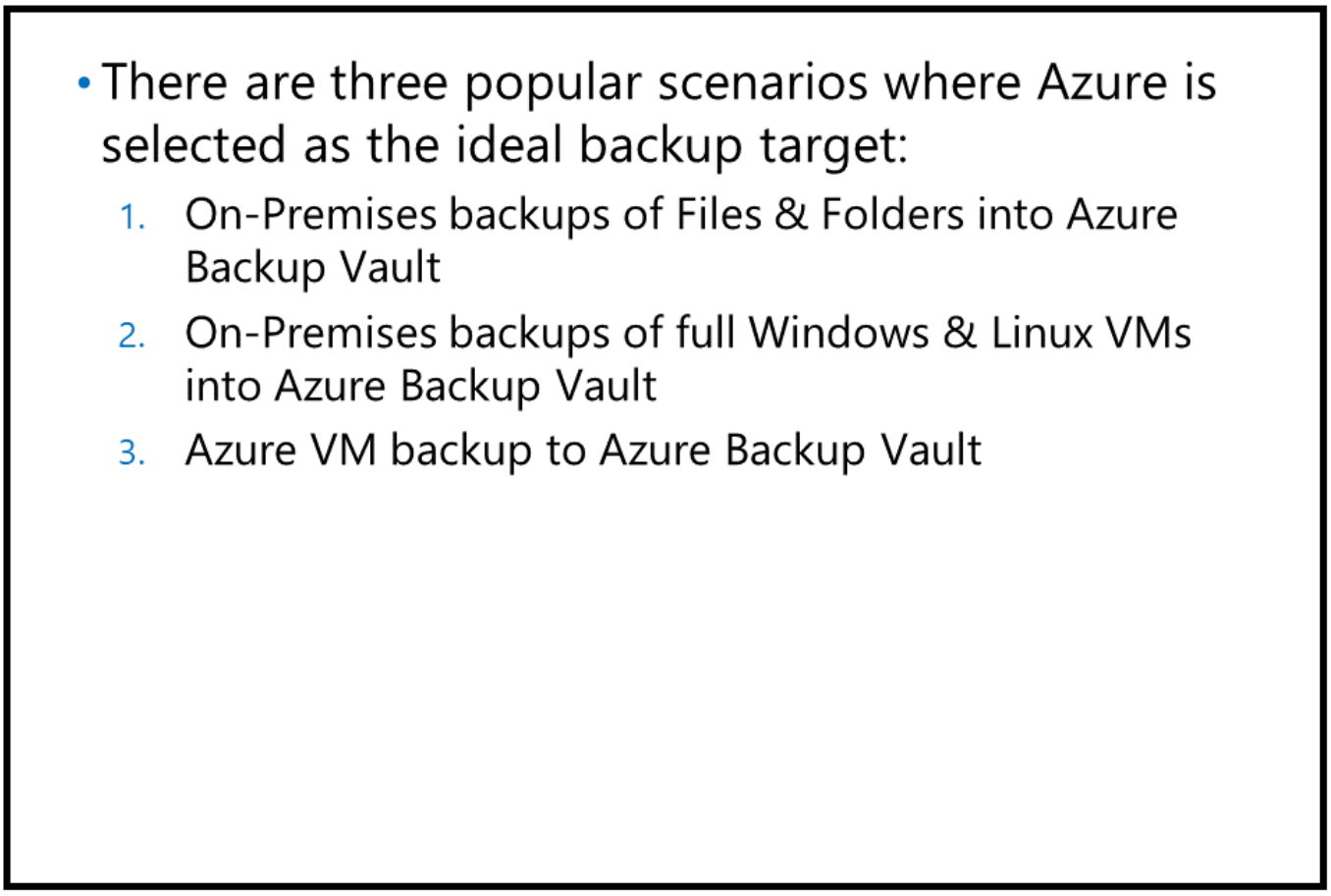
This lesson covers the many possible ways that Azure Backup can be integrated into an infrastructure solution hosted on Azure or in a hybrid-infrastructure scenario.

Lesson objectives

After completing this lesson, you will be able to:

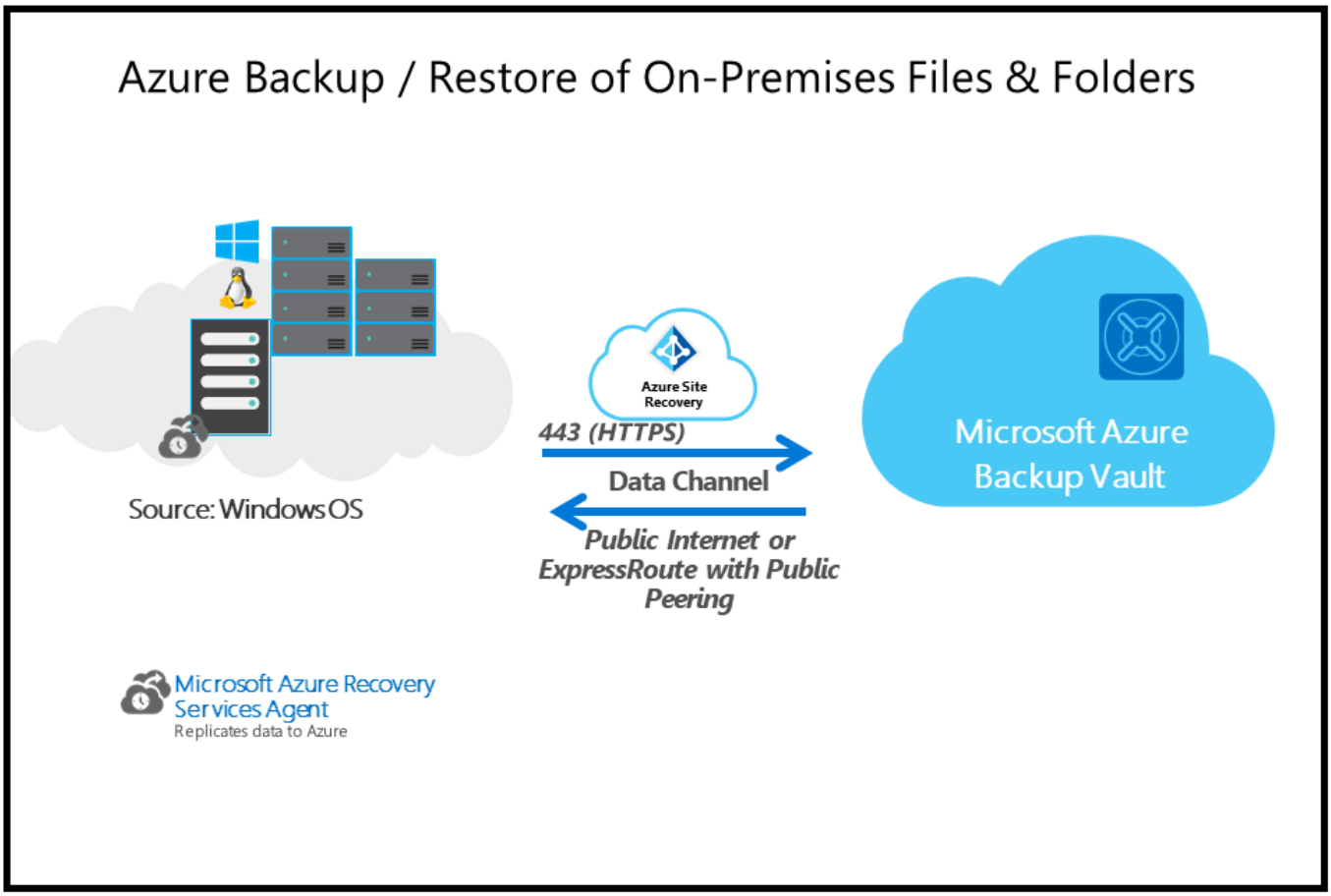
- Detail the architectural components for deploying Azure Backup, using different topologies.
- Recognize the key use cases for implementing the different Azure Backup scenarios.
- Understand the built-in Security features that Azure Backup provides.
- Detail the architectural components for deploying Azure Site Recovery, using different topologies.
- Recognize the key use cases for implementing ASR, whether for DR or as a VM migration tool.

Azure Backup



Azure Backup is a simple and cost-effective backup as a service (BaaS) solution, that gives you trusted tools on-premises with rich and powerful tools in the cloud. It delivers strong protection for customer data wherever it resides —in your enterprise data center, remote and branch offices, or the public cloud—while being sensitive to the unique requirements these scenarios pose. Azure Backup, in a seamless portal experience with Azure Site Recovery, gives you cost-efficiency and minimal maintenance, consistent tools for offsite backups and operational recovery, and unified application availability and data protection.

Backup Options



There are three primary options for backing up to Azure Backup with different characteristics:

1. Azure Backup / Restore of On-Premises Files & Folders

   Ideal for backing up Files & Folders only

   - Deploy the Azure Backup Agent (Azure Recovery Services Agent) on the VM guests running on-premises Hyper-V / SCVMM / Vmware / Physical infrastructure
   - Configure Azure Backup from within the VM guest
   - Configure the integration with Azure Backup Vault
   - Run the Backup job from within the VM guest
   - Files & Folders backup will be stored in Azure Backup Vault, and can be restored from there

2. Azure Backup / Restore of On-premises running full workloads (OS, Sysvol, and Applications)

   Better for backing up full system workloads (OS, system state, applications – consistent)

   - Deploy the Azure Backup Server (or System Center DPM 2012 R2 or 2016) on the on-premises Hyper-V / SCVMM / Vmware / Physical infrastructure

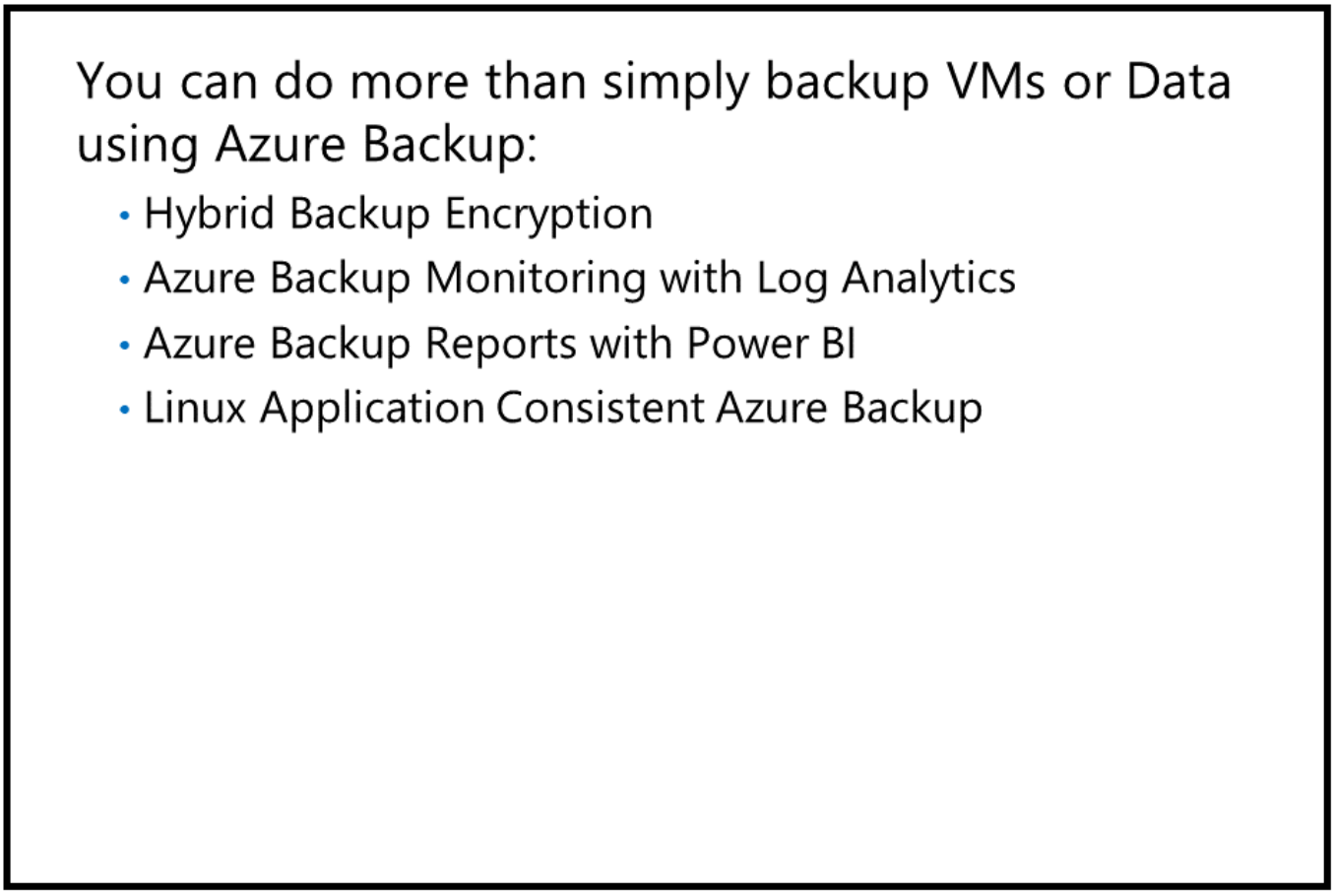
- Configure Azure Backup Server backup policies, backup storage (2-tier) and deploy agents to your workloads
- Configure the integration with Azure Backup Vault
- Run the Backup job from within the Azure Backup Server console
- VM workloads (system state, OS, applications,…) backup will be stored in Azure Backup Vault, and can be restored from there

3. Azure VM Backup / Restore to Azure Backup Vault

   Best for when you want to backup Azure VMs to Azure Backup Vault

   - Deploy the Azure Backup Extension, or select Azure Backup in the VM configuration
   - Configure Azure Backup backup policies, in the Azure platform
   - Configure the integration with Azure Backup Vault
   - Run the Backup job from within the Azure Platform
   - Azure VMs will be backed up as full VM snapshots, and can be restored from within the Azure Portal

Specialized Backup



Hybrid Backup Encryption

Security is an important aspect of any Public Cloud, and particularly in Microsoft Azure.

Azure Backup allows for end-to-end encryption of the backup platform:

1. It starts with a passphrase for the Azure Recovery Services Agent installation;
2. the next layer is the Backup Data itself, which gets encrypted in transit.
3. Once the data is stored in Azure Backup Vault, it gets encrypted at rest as well.

Azure Backup Monitoring with Log Analytics

Azure Backup monitoring is possible from Log Analytics, part of Azure Operations Management Suite.

Out of Log Analytics, one can get a detailed view on the backup statistics, the amount of data that is being consumed, successful and failed jobs and alike.

Azure Backup Reports with Power BI

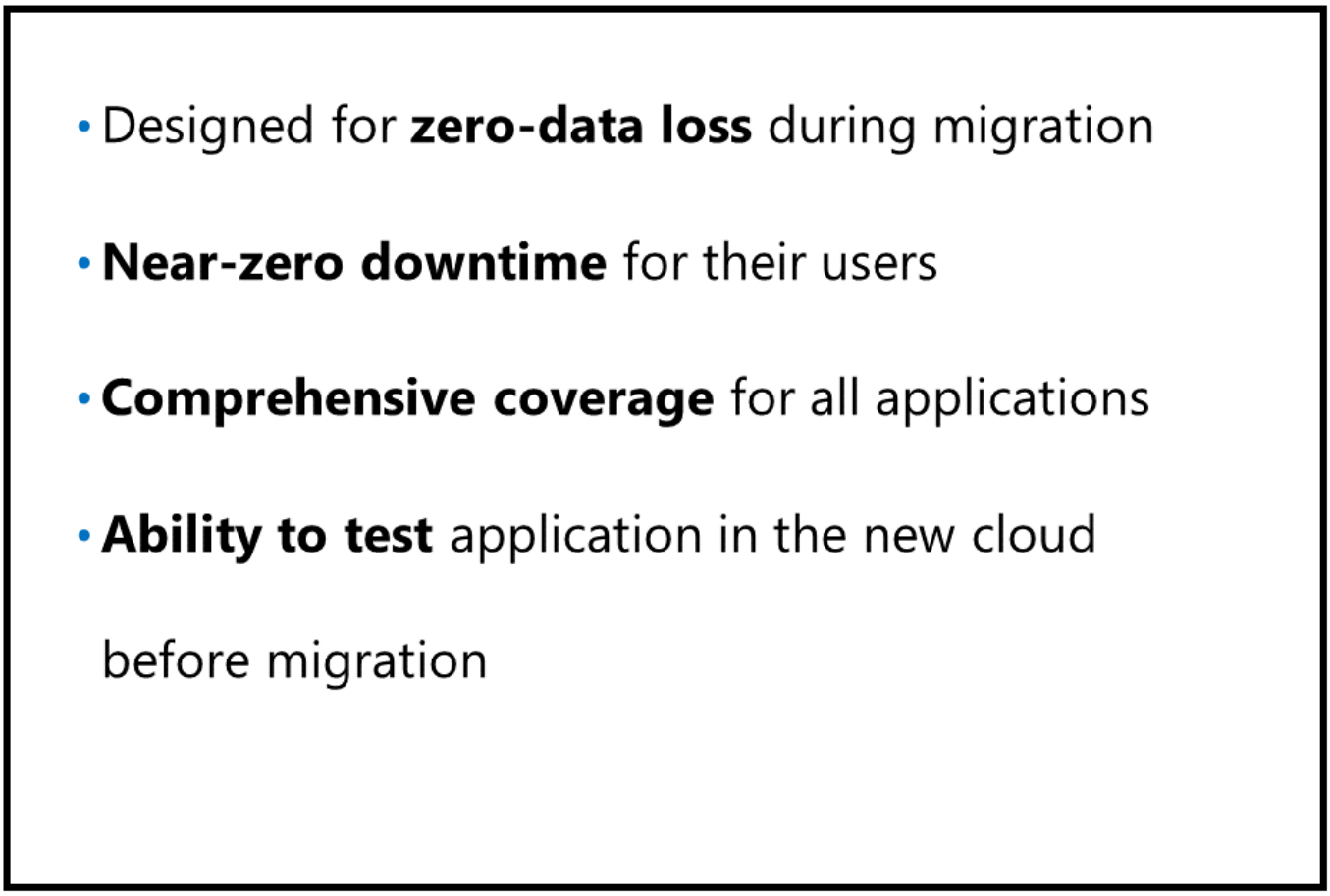
Besides Azure Monitoring capabilities in Operations Management Suite and Log Analytics, Azure Backup also allows for reporting integration with Microsoft Power BI.

Linux Application Consistent Azure Backup

Taking backups of Azure VMs running Linux OS is fully supported, for Azure supported Linux Operating Systems.

To allow for application consistent backups, you need to run a pre- & post- backup script. The VM Snapshot will be your VM Backup, which gets stored in the Backup Vault using an incremental update process.

Site Recovery



Azure Site Recovery is an Azure solution, initially built to provide a datacenter disaster recovery solution for your VM workloads. Whether they were running on-premises on Hyper-V hosts, VMware hosts, running as physical hosts, or as AWS VMs. Next to the core VM disaster recovery aspect of it, Azure Site Recovery is also an ideal tool for performing VM lift & Shift operations of your workloads.

Why Azure Site Recovery?

- Azure as your Disaster/Recovery Datacenter Site
  - Replication-based failover to Azure Virtual Machines
  - Near-zero downtime for your application workloads
  - Application-consistent failover
  - Failover & Failback
  - DR for on-premises Hyper-V, VMware and physical Servers (*), as well as Azure VMs
- Ideal as a Virtual Machine “Lift & Shift” migration tool
  - Full machine-state replication to an Azure VM
  - Perfect for test/dev scenarios
  - Zero-data loss during migration

Lesson 3: Automation

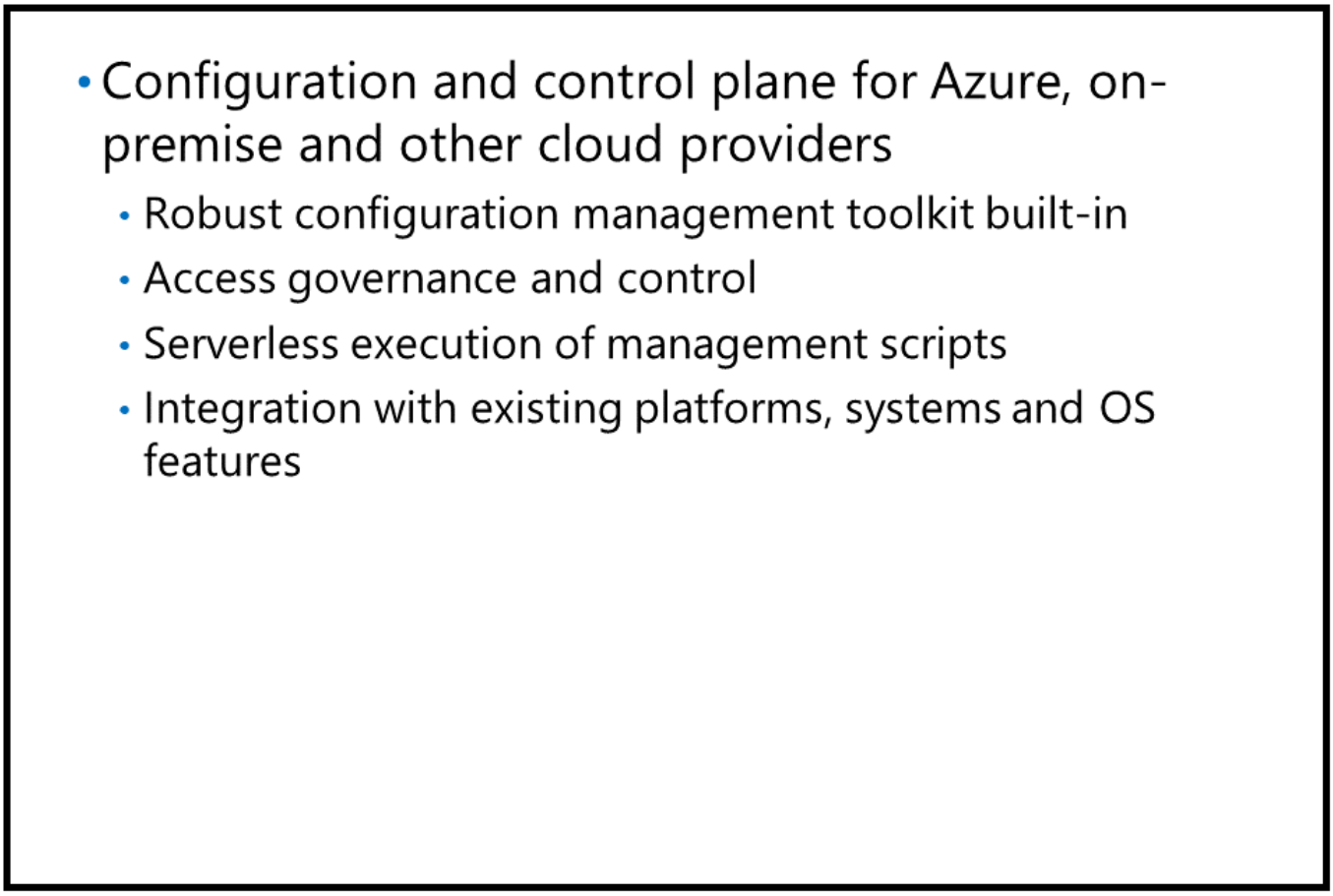
Azure Automation provides a way for users to automate the manual, long-running, error-prone, and frequently repeated tasks that are commonly performed in a cloud and enterprise environment. It saves time and increases the reliability of regular administrative tasks and even schedules them to be automatically performed at regular intervals. You can automate processes using runbooks or automate configuration management using Desired State Configuration. This lesson provides a brief overview of Azure Automation and answers some common questions.

Lesson objectives

After completing this lesson, you will be able to:

- Understand Azure Automation concepts and architecture.
- Recognize and describe Azure Automation capabilities.
- Interact with machines using Azure Automation and Desired State Configuration.

Azure Automation



Microsoft Azure Automation provides a way for users to automate the manual, long-running, error-prone, and frequently repeated tasks that are commonly performed in a cloud and enterprise environment. It saves time and increases the reliability of regular administrative tasks and even schedules them to be automatically performed at regular intervals. You can automate processes using runbooks or automate configuration management using Desired State Configuration.

Azure Automation is a software as a service (SaaS) application that provides a scalable and reliable, multi-tenant environment to automate processes with runbooks and manage configuration changes to Windows and Linux systems using Desired State Configuration (DSC) in Azure, other cloud services, or on-premises. Entities contained within your Automation account, such as runbooks, assets, Run As accounts are isolated from other Automation accounts within your subscription and other subscriptions.

Runbooks that you run in Azure are executed on Automation sandboxes, which are hosted in Azure platform as a service (PaaS) virtual machines. Automation sandboxes provide tenant isolation for all aspects of runbook execution – modules, storage, memory, network communication, job streams, etc. This role is managed by the service and is not accessible from your Azure or Azure Automation account for you to control.

To automate the deployment and management of resources in your local datacenter or other cloud services, after creating an Automation account, you can designate one or more machines to run the Hybrid Runbook Worker (HRW) role. Each HRW requires the Microsoft Management Agent with a connection to a Log Analytics workspace and an Automation account. Log Analytics is used to bootstrap the installation, maintain the Microsoft Management Agent, and monitor the functionality of the HRW. The delivery of runbooks and the instruction to run them are performed by Azure Automation.

Cross-Cloud

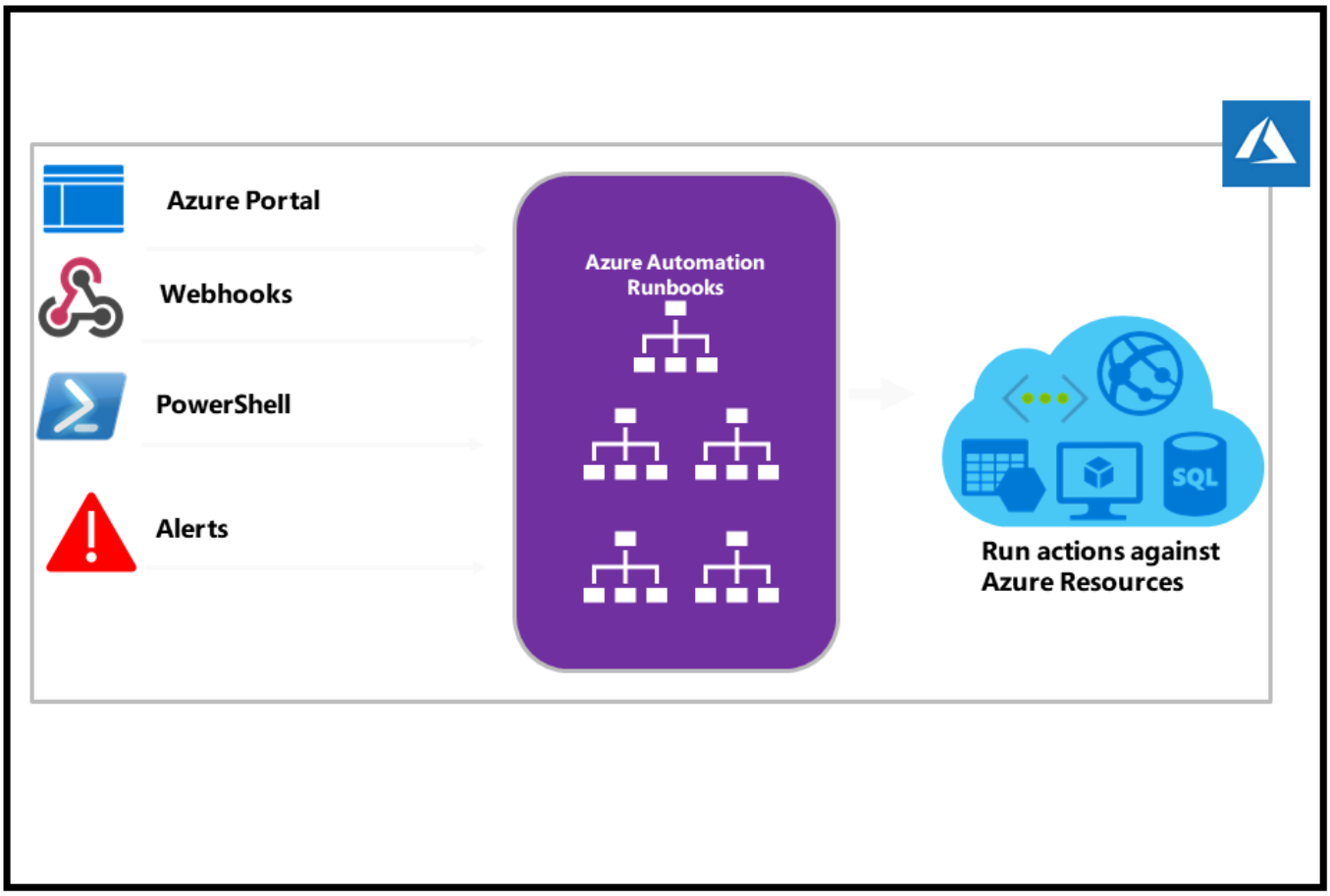
Although Azure Automation lives in the Azure platform, it allows management and configuration of Azure systems, on-premises running systems, systems in AWS, Google Cloud, or any other 3rd party hosting data center.

The core component of Azure Automation is defined and configured in the Azure Platform (cross Regions). From there, you can establish hybrid automation capabilities, by using the Azure Automation Hybrid Worker.

This is similar to running like an Azure Automation agent on your non-Azure cloud platforms, where Amazon Web Services, Google Cloud, your own Private Cloud datacenter, or any third party hosted datacenter if you want, would be a good example.

Latest supportability added to the Azure Automation feature set, is integration with on-premises running Azure Stack.

Automation Flow



An Automation account is separate from the account you use to sign in to the portal to configure and use Azure resources. Automation resources included with an account are the following:

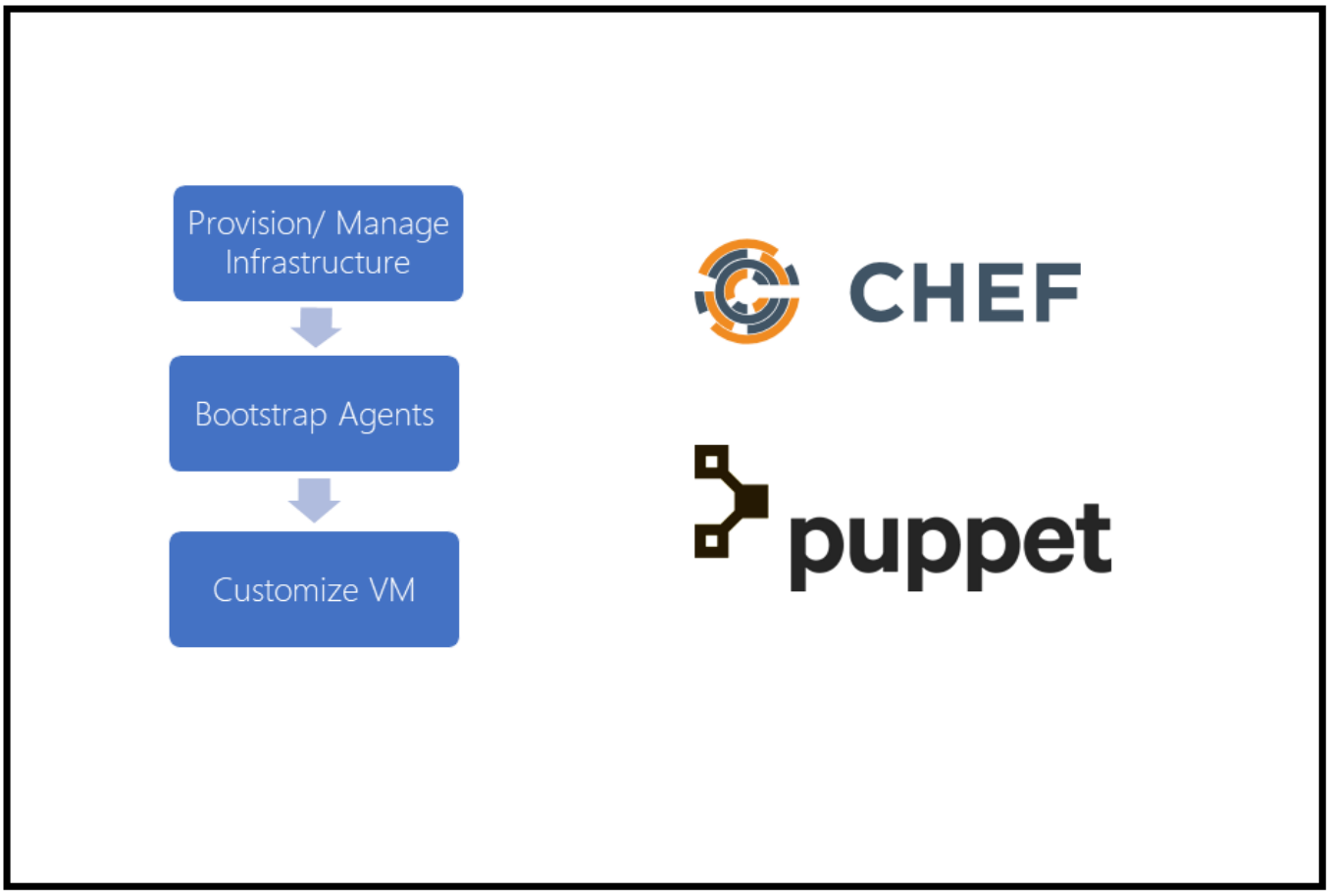
- **Certificates** - contains a certificate used for authentication from a runbook or DSC configuration or add them.
- **Connections** - contains authentication and configuration information required to connect to an external service or application from a runbook or DSC configuration.
- **Credentials** - is a PSCredential object which contains security credentials such as a username and password required to authenticate from a runbook or DSC configuration.
- **Integration modules** - are PowerShell modules included with an Azure Automation account to make use of cmdlets within runbooks and DSC configurations.
- **Schedules** - contains schedules that starts or stops a runbook at a specified time, including recurring frequencies.
- **Variables** - contain values that are available from a runbook or DSC configuration.
- **DSC Configurations** - are PowerShell scripts that describes how to configure an operating system feature or setting or install an application on a Windows or Linux computer.
- **Runbooks** - are a set of tasks that perform some automated process in Azure Automation based on Windows PowerShell.

When you create an Automation account in the Azure portal, you automatically create two authentication entities:

- A **Run Asaccount**. This account creates a service principal in Azure Active Directory (Azure AD) and a certificate. It also assigns the Contributor role-based access control (RBAC), which manages Resource Manager resources by using runbooks.
- A **Classic Run As account**. This account uploads a management certificate, which is used to manage classic resources by using runbooks.

Role-based access control is available with Azure Resource Manager to grant permitted actions to an Azure AD user account and Run As account, and authenticate that service principal. Read **Role-based access control in Azure Automation article** for further information to help develop your model for managing Automation permissions.

Configuration Management



To create and manage Azure virtual machines (VMs) in a consistent manner at scale, some form of automation is typically desired. There are many tools and solutions that allow you to automate the complete Azure infrastructure deployment and management lifecycle. This article introduces some of the infrastructure automation tools that you can use in Azure.

Chef

Chef is an automation platform that helps define how your infrastructure is configured, deployed, and managed. Additional components included Chef Habitat for application lifecycle automation rather than the infrastructure, and Chef InSpec that helps automate compliance with security and policy requirements. Chef Clients are installed on target machines, with one or more central Chef Servers that store and manage the configurations.

Puppet

Puppet is an enterprise-ready automation platform that handles the application delivery and deployment process. Agents are installed on target machines to allow Puppet Master to run manifests that define the desired configuration of the Azure infrastructure and VMs. Puppet can integrate with other solutions such as Jenkins and GitHub for an improved devops workflow.

Lesson 4: Business Continuity Case Study

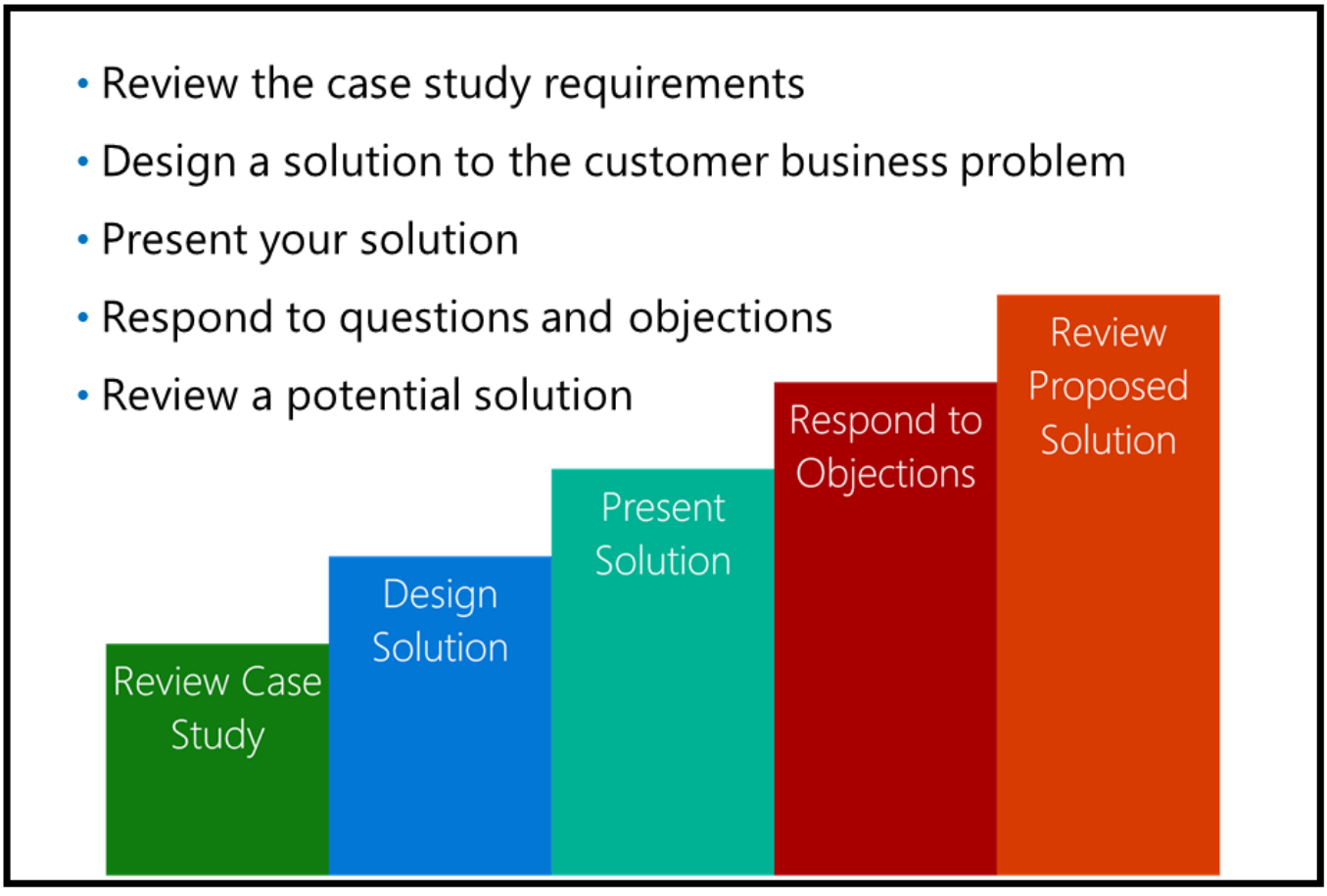
In this case study, we will look at a customer problem that requires an architectural recommendation.

Lesson objectives

After this case study, you should:

- Identify customer problems as they are related to networking.
- Design a solution that will meet the customer's objectives.
- Ensure your designed solution accounts for customer objections.

Case Study Overview



Who is the Customer?

Fabrikam Publishing is a media and publishing company in Seattle, Washington, with approximately 5,000 employees.

What Does the Customer Already Have?

Fabrikam has a single data center that primarily runs Microsoft server software, including Active Directory Domain Services AD DS) and a number of AD-integrated services, including Exchange 2013, as well multi-tier, internal, AD-integrated IIS-based web applications with SQL Server 2014 as the database platform. The services are consumed by client systems hosted in three buildings located in adjacent areas of the city. Buildings are connected to the data center by using site-to-site VPN with the throughput of 100Mbps. Each building has also an independent connection to the Internet.

Server backups are performed by using tape libraries with autoloaders. Tapes are periodically shipped for permanent storage to an offsite location.

If something catastrophic were to happen to the data center, the IT team would have to deploy replacement physical servers by reinstalling the operating system and restoring data from backups in the equipment rooms in small server rooms located in each building.

Fabrikam's IT staff likes to stay current with the latest offerings from Microsoft so that the department functions as cost-effectively as possible. In order to reduce costs, the IT staff has recently started planning the initiative to virtualize majority of its physical servers using the Hyper-V platform and to deploy System Center 2012 R2 Virtual Machine Manager (SCVMM) for managing the resulting virtualized environment.

What is the Customer's Goal?

"We need to greatly improved disaster, server, and application recovery processes," says Anthony Ciske, IT Director for Fabrikam. "We've had some near-disasters in the past that were a real pain to recover from. We needed a real disaster recovery solution for our critical workloads that was compatible with our budget—and our staffing bandwidth." The team had explored building a secondary data center and employing commercial disaster recovery solutions in the past, but both turned out to be too expensive for serious consideration.

What Does the Customer Need?

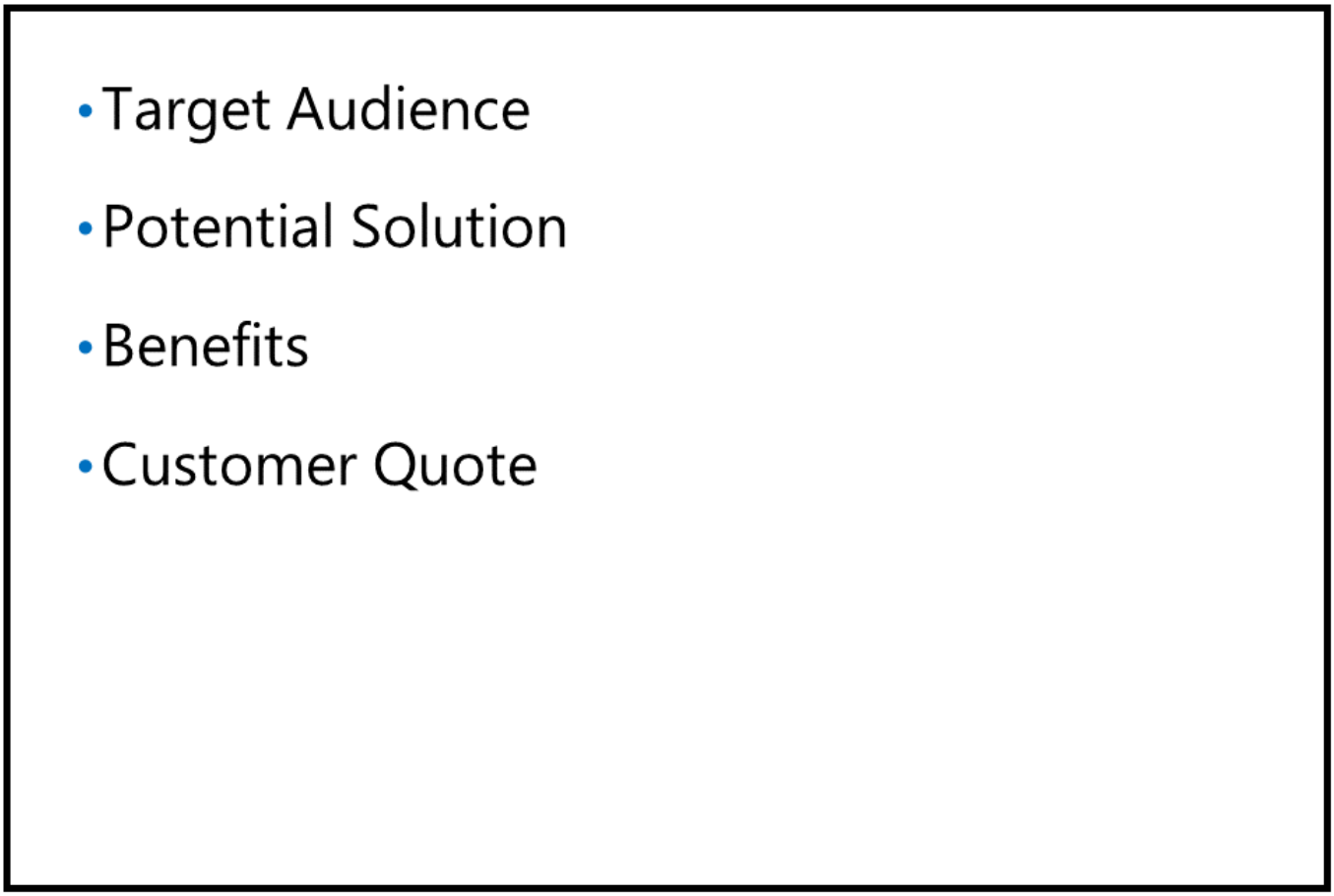
- The ability to perform data-center level recovery for critical workloads that can be executed in the event of a data center failure, with an automated and orderly recovery process so different tiers of the application start in the correct order and remain in a consistent state without manual intervention.
- The ability to perform failback following restoring on-premises data center functionality that can be executed in the automated and orderly manner.
- The ability to perform multi-tier application and individual server-level recovery of critical workloads.
- Support for server-level and application-level high availability whenever possible.
- Quick testing and validation of recovery processes with minimal interruption to the production environment.
- Minimized capital and operational expenses.
- Optimized authentication for AD-integrated services and applications.

- Centralized management of backups and reduced or eliminated dependency on offsite tape storage.
- The level of security and privacy commensurate with highly sensitive and competitive nature of the business.

What Things Worry the Customer?

- Solution must significantly improve their current recovery point/time objectives (which today is a manual process).
- Overall cost of the solution.
- Protecting a diverse environment such as physical servers or other hypervisors.
- The management tools for the solution must be available in the event one of the data centers is unavailable.
- Protect data that is not hosted within a virtual hard disk (VHD/X).
- The protected data must be secure.
- Unsure about which workloads are supported on Azure.

Case Study Solution



Preferred Target Audience

Anthony Ciske, IT Director – Fabrikam Publishing

Network Administrator – Fabrikam Publishing

Application owners (Exchange, SQL, n-tier applications)

Preferred Solution

Fabrikam Publishing decided to complete their deployment of SCVMM and implement two Azure recovery solutions – Azure Site Recovery to provide failover capability of their virtual servers and Azure Backup to replace their existing backup solution and to provide longer term protection of their virtual and physical servers. Azure Site Recovery has been configured to use Microsoft Azure as a disaster recovery site, with protection enabled for virtual machines hosting servers critical from the business continuity standpoint.

For disaster recovery, Fabrikam implemented two separate Azure virtual networks. The first network was for planned/unplanned failover of their server workloads. The second virtual network was configured for testing failover in a non-disruptive manner. As part of the network configuration they implemented site-to-site connectivity between the failover virtual network and the on-premises sites that needed protecting.

Next, they deployed Active Directory in the failover virtual network and configured it to account for the local site to ensure localized authentication in recovery scenarios. In addition, DNS configuration on client systems as well as DNS settings on Azure virtual networks have been modified to ensure that name resolution continues to function during both test and planned/unplanned failover.

The final step for the disaster recovery solution was to address application level recovery on the application servers and high-availability concerns for Exchange 2013, SQL Server 2014, and other Active Directory-integrated applications.

Fabrikam implemented site recovery by configuring cloud recovery settings for the application servers.

Exchange 2013 is not currently supported within Azure IaaS. For an immediate cloud based solution Exchange online is recommended.

For SQL Server deploying an AlwaysOn availability group on-premises with a replica in the failover network is the best solution. The replica should have async commit configured for replication.

Implementing separate recovery plans allows sequencing the failover of various tiers in a multi-tier application, hence, maintaining application consistency. What changes would you recommend to the existing SQL Server 2012 environment to facilitate high availability and recovery?

To address the data security concerns, encryption was enabled so any at rest data is automatically encrypted by Azure Site Recovery.

The second part of the preferred solution was to implement Azure Backup to remove the reliance on tape storage. Fabrikam created an Azure Backup Vault, downloaded and installed vault credentials on the servers that offload backups to tape and configured the Azure Backup Agent to protect the data in Azure instead of tape backup.

Potential Benefits

Fabrikam Publishing is using Microsoft Azure Site Recovery to implement their Disaster Recovery and Business Continuity strategy. By leveraging built-in features of Azure Site Recovery, they are able to accomplish their recovery and resiliency objectives efficiently and with a minimal cost, giving them a competitive advantage.

- **Recovery Objectives**: Azure Site Recovery with a recovery site in Azure offers the ability to perform planned and unplanned recovery and carry out testing with minimal disruption to the production environment. It allows for orchestrated, automated and orderly failover and failback processes, so different tiers of the application can start in the correct order and remain in a consistent state without manual intervention.
- **Cost Effective**: Azure Site Recovery eliminates capital expenses associated with implementing a secondary data center and provides predictable operational expenses. Azure Backup allows for centralized management of backups and eliminates the dependency on offsite tape storage.
- **Security and Privacy**: Data replicated to Azure is encrypted during transit and, if desired, it can be encrypted at rest, while residing in the storage account.
- **Non-Disruptive Testing of their DR Solution**: Site Recovery supports non-disruptive testing. Marquette can validate their disaster recovery solution as their environment changes without disrupting production.

Architecture Example

Using Azure Site Recovery and multiple virtual networks for failover and non-disruptive failover testing:

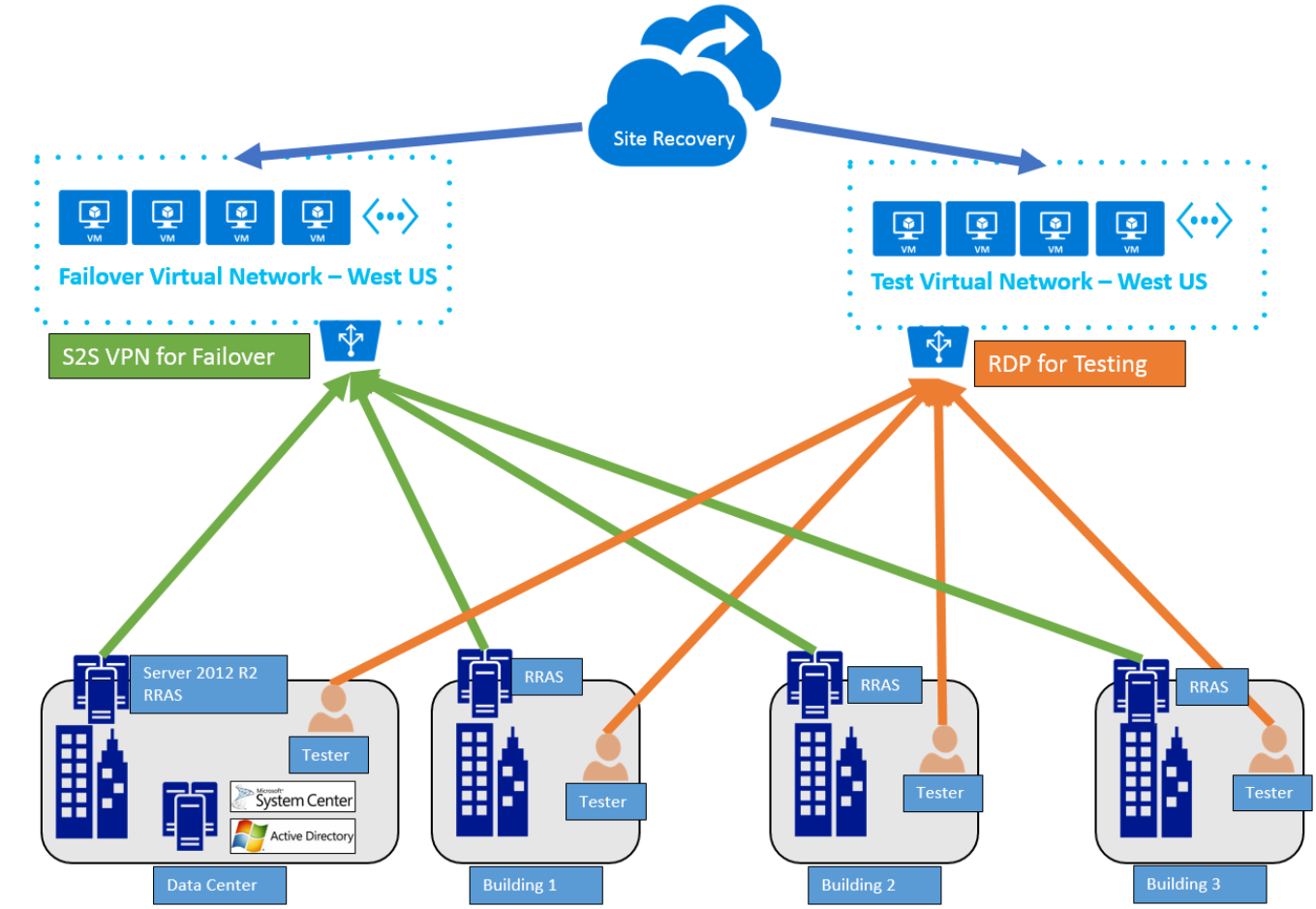


FIGURE 12.1: ARCHITECTURE NETWORKING EXAMPLE

Using Azure Backup to protect servers' on-premises and store the data offsite in Azure:

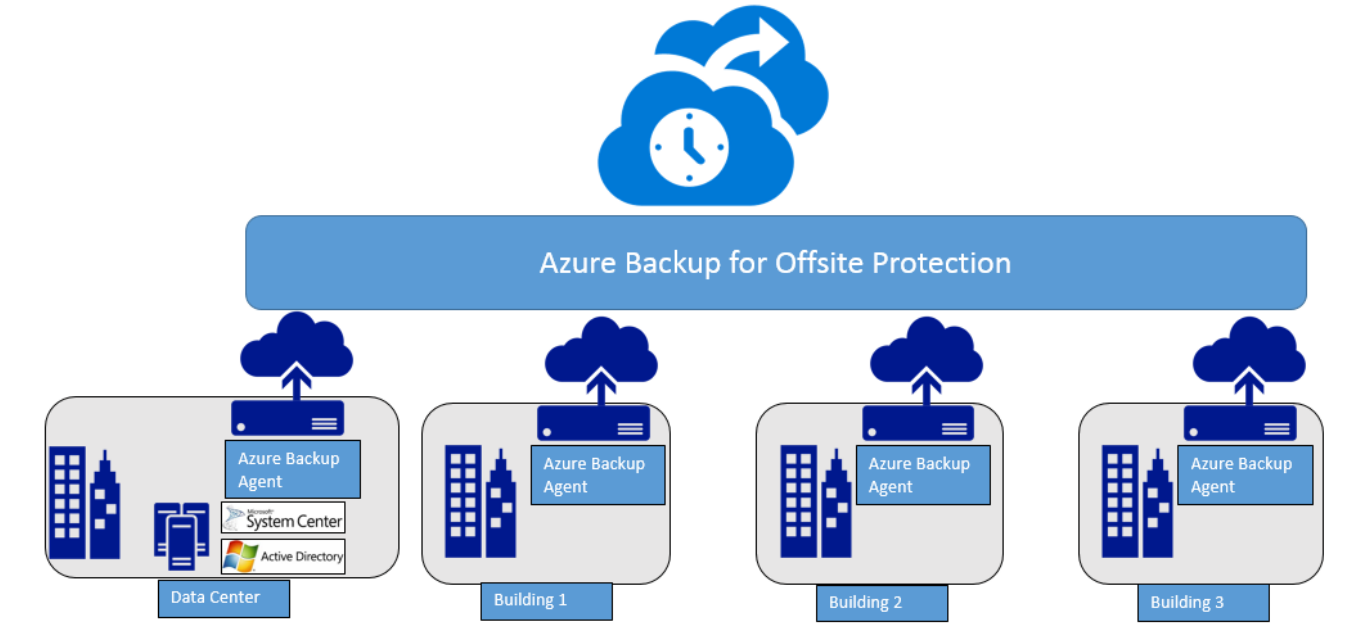


FIGURE 12.2: ARCHITECTURE BACKUP EXAMPLE

Checklist of Potential Benefits

Solution must significantly improve their current recovery point/time objectives (which today is a manual process).

•

With Azure Site Recovery the copy frequency can be configured to as low as 30 seconds. You can also configure additional recovery points to automatically be taken (the default is every hour). Additional recovery points contain one or more snapshots that enable you to recover a snapshot of a virtual machine from an earlier point in time.

Overall cost of the solution.

- Protecting their servers by using Azure as a failover data center is significantly less expensive than implementing a failover solution with secondary data center and hardware.

Protecting a diverse environment such as physical servers or other hypervisors.

- Currently, the Site Recovery service only allows replication to Azure for virtual machines based on Microsoft Hyper-V. Site Recovery can protect VMWare as well but only for on-premises to on-premises scenarios.

Protect data that is not hosted within a virtual hard disk (VHD/X).

- Azure Site Recovery works with Hyper-V based virtual machines and their attached virtual hard disks. In the scenario of restoring to Azure, the source virtual machines can be VHDX. In Azure they will be in the VHD format.

The management tools for the solution must be available if one of the data centers is unavailable.

- Azure Site Recovery is hosted in the cloud so in the event that one of the data centers is down the solution is still available to monitoring and to recover the servers.

Security of protected data.

- Data replicated using Hyper-V Replica/Azure Site Recovery is encrypted while in transit.
- When replicating virtual machines to Azure replicated data can be encrypted even while at rest.

Supported Workloads

- Not all workloads are supported (or fully supported) with Hyper-V replica and Site Recovery.
- We are currently working with the various teams for key workloads such as SharePoint, SQL and Exchange to enable full support for these workloads in Hyper-V replica and site recovery.

Proof of Concept Checklist

- Objectives
  - Identify service recovery point/time objectives for workloads in proof of concept.
  - Identity manual steps needed for a recovery in secondary data center and script those

steps as part of a recovery plan to ensure a fully automated recovery.

- Demonstrate that Azure Site Recovery and Hyper-V replication can replicate and recover virtual machines in the secondary data center within the RPO/RTO objectives.
- Enable backup protection to offsite storage.

- Flow/Scope of the proof of concept (a list of 2-3 bullets)
  - Identify services (Virtual Machines) to configure for replication
  - Implement two separate Azure virtual networks
    - One for planned/unplanned failover
    - The other for testing application and sever-level recovery
    - Configure network connectivity between the on-premises environment and the failover virtual network.
  - Create VMM cloud in the data center (if it does not exist)
  - Configure Active Directory and DNS
  - Configure Azure Site Recovery with on-premises to Azure
    - Create an Azure Site Recovery Vault
    - Install the Provider application on the VMM server
    - If you don't have a storage account create one.
    - Install the Microsoft Azure Recovery Services agent on each Hyper-V host located in VMM clouds you want to protect.
    - Configure cloud protection settings for VMM cloud.
    - Configure network mapping to map source VM network to target Azure network
    - Enable protection for virtual machines located in protected VMM clouds
    - Failover using the test failover method
  - Configure Azure Backup and protect on-premises server backups instead of
- Conditions of satisfaction / success criteria for the proof of concept
  - Demonstrate that Azure Site Recovery does indeed fulfill the customer's recovery requirements of protecting the entire data center.
- Resources / Bill of Materials that you would use

- Online Documentation
- System Center 2012 R2 and Windows Server 2012 R2
- Azure Site Recovery and Azure Storage
- Virtual Private Networks
- Partner / MCS

Customer Quote

“Hopefully we’ll never have to use it, but we have peace of mind in knowing that if something terrible happens, we won’t have to engage in a mad scramble to recover our workloads.” - Anthony Ciske, IT Director – Fabrikam Publishing

Lab: Deploying Configuration Management Solutions to Azure

Scenario

A cutting-edge insurance organization would like to create multiple virtual machines to process insurance claims. Today, those virtual machines are managed in the organization’s datacenter using Chef. The client has reached out to you to create a prototype solution where the machines are created automatically and have the Chef agent and configuration installed as part of the automatic deployment.

Objectives

- Author an ARM Template to deploy single management VM.
- Author an ARM Template to deploy multiple managed VMs.

Lab setup

Estimated Time: 90 minutes

Virtual machine: **20535A-SEA-ARCH**

User name: **Admin**

Password: **Pa55w.rd**

The lab steps for this course change frequently due to updates to Microsoft Azure. Microsoft Learning updates the lab steps frequently, so they are not available in this manual. Your instructor will provide you with the lab documentation.

Exercise 1: Deploy a Chef Management Server using ARM

Exercise 2: Configure Management Server

Exercise 3: Deploy a VM Scale Set using Chef-Configured VMs

Exercise 4: Cleanup Subscription

Review Question(s)

Module review and takeaways

Review Question(s)