

CAF Governance Phase for SQL Migration

**List of Contents**

[1. Governance in Landing Zone 3](#_Toc43725137)

[1.1 Organize Resources 3](#_Toc43725138)

[1.1.1 Azure management groups and hierarchy 3](#_Toc43725139)

[1.1.2 Naming standards 4](#_Toc43725140)

[1.1.3 Resource tags 5](#_Toc43725141)

[1.2 Manage access 5](#_Toc43725142)

[1.3 Manage costs 6](#_Toc43725143)

[1.3.1 Analyze cloud costs 6](#_Toc43725144)

[1.3.2 Monitor with budgets 7](#_Toc43725145)

[1.3.3 Optimize with recommendations 9](#_Toc43725146)

[1.3.4 Manage invoices and payments 9](#_Toc43725147)

[1.4 Governance, security and compliance 9](#_Toc43725148)

[1.4.1 Azure Policy 9](#_Toc43725149)

[1.4.2 Azure Blueprints 11](#_Toc43725150)

[1.4.3 Azure Security Center 13](#_Toc43725151)

[1.5 Monitoring and reporting 13](#_Toc43725152)

[1.5.1 Azure Monitor 13](#_Toc43725153)

[1.5.2 Azure Service Health 14](#_Toc43725154)

[1.5.3 Azure Advisor 15](#_Toc43725155)

[1.5.4 Azure Security Center 15](#_Toc43725156)

[1.6 Manage 15](#_Toc43725157)

[1.6.1 Inventory and visibility 16](#_Toc43725158)

[1.6.2 Operational compliance 17](#_Toc43725159)

[1.6.3 Protect and recover 17](#_Toc43725160)

# Governance in Landing Zone

An enterprise that has a standard Microsoft BI platform comprising of on-premise Windows server, SQL Server database, jobs, cubes and PowerBI reports. There are separate VMs to host SQL server instances for prod and dev environments. Each SQL server instance has multiple databases. The enterprise is now looking to migrate from on-premise to Azure Cloud. Following are Azure options that can be chosen to migrate the databases.

* Azure SQL PaaS
* IaaS VM with SQL Server
* Managed Instance PaaS

Let us now look at how to implement governance to migrate the databases from on-premise to Azure Cloud

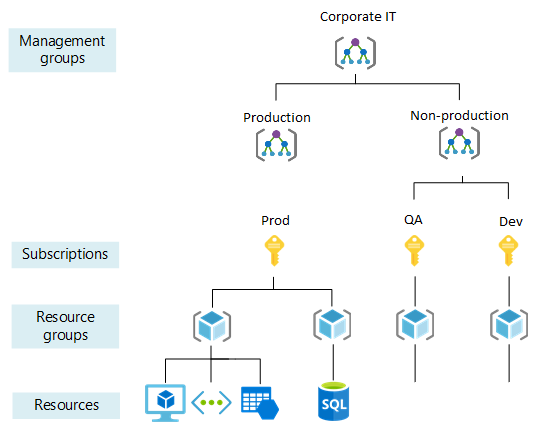
## Organize Resources

Organizing cloud-based resources is critical to securing, managing, and tracking the costs related to the workloads. To organize resources below points, need to be applied

* Define a management group hierarchy,
* Follow a well-considered naming convention, and
* Resource tagging

### Azure management groups and hierarchy

Azure provides four levels of management scope: management groups, subscriptions, resource groups, and resources. Refer to this [link](https://docs.microsoft.com/en-in/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources?tabs=AzureManagementGroupsAndHierarchy%23create-a-management-level) for steps to create management levels. Below hierarchy is suited to the use case.



**Management groups:**

These groups are containers that help to manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group. Management groups can be nested.

For the use case, parent group for Corporate IT is created and then separate child groups for production and non-production environment are formed.

**Subscriptions:**

A subscription logically associates user accounts and the resources that were created by those user accounts. Each subscription has limits/ quotas on the amount of resources that can be created and used. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.

For the use case, subscription per environment is created. i.e. prod, dev and QA. This gives a better control over the environments.

**Resource groups:**

A resource group is a logical container, into which Azure resources like web apps, databases, and storage accounts are deployed and managed. For this use case, below resource groups are created.

* rg-corpit-p-westus-vm: Contains VM, VNet etc in West US region to process the BI workloads.
* rg-corpit-p-eastus-sql: Contains reporting DBs in East US region to help in load balancing user queries.

**Resources:**

Resources are instances of services that are created, like virtual machines, storage, or SQL databases. For the use case, following are some resources based on the chosen Azure destination.

* Azure SQL PaaS: SQL, Active Directory
* IaaS VM with SQL Server: VM, Storage, VNet, subnet, Active Directory, ExpressRoute
* Managed Instance PaaS: Managed Instance, Active Directory

### Naming standards

A good naming standard helps to identify resources in the Azure portal, on a billing statement, and in automation scripts. The naming strategy should include business and operational details as components of resource names:

* The business-side of this strategy should ensure that resource names include the organizational information that is needed to identify the teams. Resource should be used along with the business owners who are responsible for resource costs.
* The operational side should ensure that names include information that is needed by IT teams. Use the details that identify the workload, application, environment, criticality, and other information that is useful to manage resources.

The following table lists naming patterns for a few Azure resources in the use case.

|  |  |  |  |
| --- | --- | --- | --- |
| Entity | Scope | Suggested pattern | Example |
| Resource group | Subscription | rg-<team>-<environment>-<region>-<category> | rg-corpit-p-westus-vm |
| Virtual machine | Resource group | vm-<team>-<environment>-<region>-<number> | vm-corpit-p-westus-01 |
| SQL | Resource group | sql-<team>-<environment>-<region>-<number> | sql-corpit-p-westus-01 |
| Tag | Associated entity | "key": "value" | "department": "Central IT" |

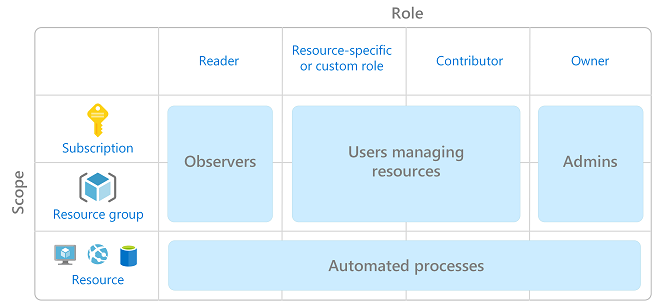
### Resource tags

Tags are applied to Azure resources to logically organize them by categories. Each tag consists of a name and a value. Refer to this [link](https://docs.microsoft.com/en-in/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources?tabs=ResourceTags#tabpanel_CeZOj-G++Q_ResourceTags) for steps to apply a resource tag. Tags can be used for the following purposes in the use case.

* Metadata and documentation: Administrators can easily see detail about the resources they're working on by applying a tag like ‘ProjectOwner’ and ‘Department’.
* Automation: Runbooks can take an action based on tags like ‘ShutdownTime’ and ‘DeprovisionDate’.
* Cost Optimization: Teams responsible for resource costs can be tagged to ‘cost center’. In the Azure cost management, you can apply the cost center tag as a filter to report the charges based on a team or department usage.

## Manage access

Azure role-based access control (RBAC) is the primary method of managing access in Azure. RBAC role definitions list operations that are permitted/ disallowed for users or groups assigned to that role. A role's scope specifies which resources these defined permissions apply to. Scopes can be specified at multiple levels: management group, subscription, resource group, or resource. Scopes are structured in a parent/child relationship.

The following image shows a suggested pattern for assigning RBAC.

Refer to this [link](https://docs.microsoft.com/en-in/azure/cloud-adoption-framework/ready/azure-setup-guide/manage-access#grant-resource-group-access) for steps to grant access to subscription and resource groups.

**RBAC Roles:**

Below table lists few built-in roles to be created for the use case.

|  |  |  |
| --- | --- | --- |
| Role | Resource Type | Access |
| Owner | Core | Manage everything, including access to resources. |
| Contributor | Core | Manage everything except access to resources. |
| Reader | Core | View everything but not make any changes. |
| Virtual Machine Administrator Login | Virtual Machine | View virtual machines in the portal and sign in as administrator. |
| Virtual Machine Contributor | Virtual Machine | Manage virtual machines, but it can't access them or the virtual network or storage account they're connected to. |
| Virtual Machine User Login | Virtual Machine | View virtual machines in the portal and sign in as a regular user. |
| db\_owner | SQL | Perform all configuration and maintenance activities on the database and can also drop the database in SQL Server. |
| db\_securityadmin | SQL | Modify role membership for custom roles only and manage permissions. |
| db\_datawriter | SQL | Add, delete, or change data in all user tables. |
| db\_datareader | SQL | Read all data from all user tables. |

Custom roles can also be created in case the built-in roles do not suffice. For the use case, create a custom role to manage access for a single group of users responsible for managing virtual machines and Azure SQL Database resources.

**Best practice:**

* Avoid resource-specific permissions when possible. Instead, use management groups for enterprise-wide access control and resource groups for access control within subscriptions.
* Avoid user-specific permissions. Instead, assign access to groups in Azure AD.
* Grant users the least privilege required to get their work done.

## Manage costs

Cost management is the process of effectively planning and controlling costs involved in your business. Azure Cost Management provides a few ways to help predict and manage costs. This section will specifically discuss

* Analyze cloud costs
* Monitor with budgets
* Optimize with recommendations
* Manage invoices and payments

Refer to this [link](https://docs.microsoft.com/en-in/azure/cloud-adoption-framework/ready/azure-setup-guide/manage-costs#manage-your-costs-with-azure-cost-management) for steps to view Cost Management to predict and manage costs.

### Analyze cloud costs

Helps to explore and analyze the costs. Aggregated costs can be viewed for the account or view accumulated costs over time. Cost analysis provides few default views. Cost views can also be customized for deeper analysis. The views can also be saved and shared. Data from cost analysis can be exported to be used for analysis elsewhere. Following are the available default views.

**Accumulated cost view:**

This view represents the predefined cost analysis view configuration. Each view includes date range, granularity, group by, and filter settings. The default view shows accumulated costs for the current billing period but can be changed to other built-in views. This view answers questions like: How much is the spent so far this month? Is this within the budget?

**Actual cost:**

This view shows the total usage and purchase costs for the current month, as they're accrued and will show on the bill.

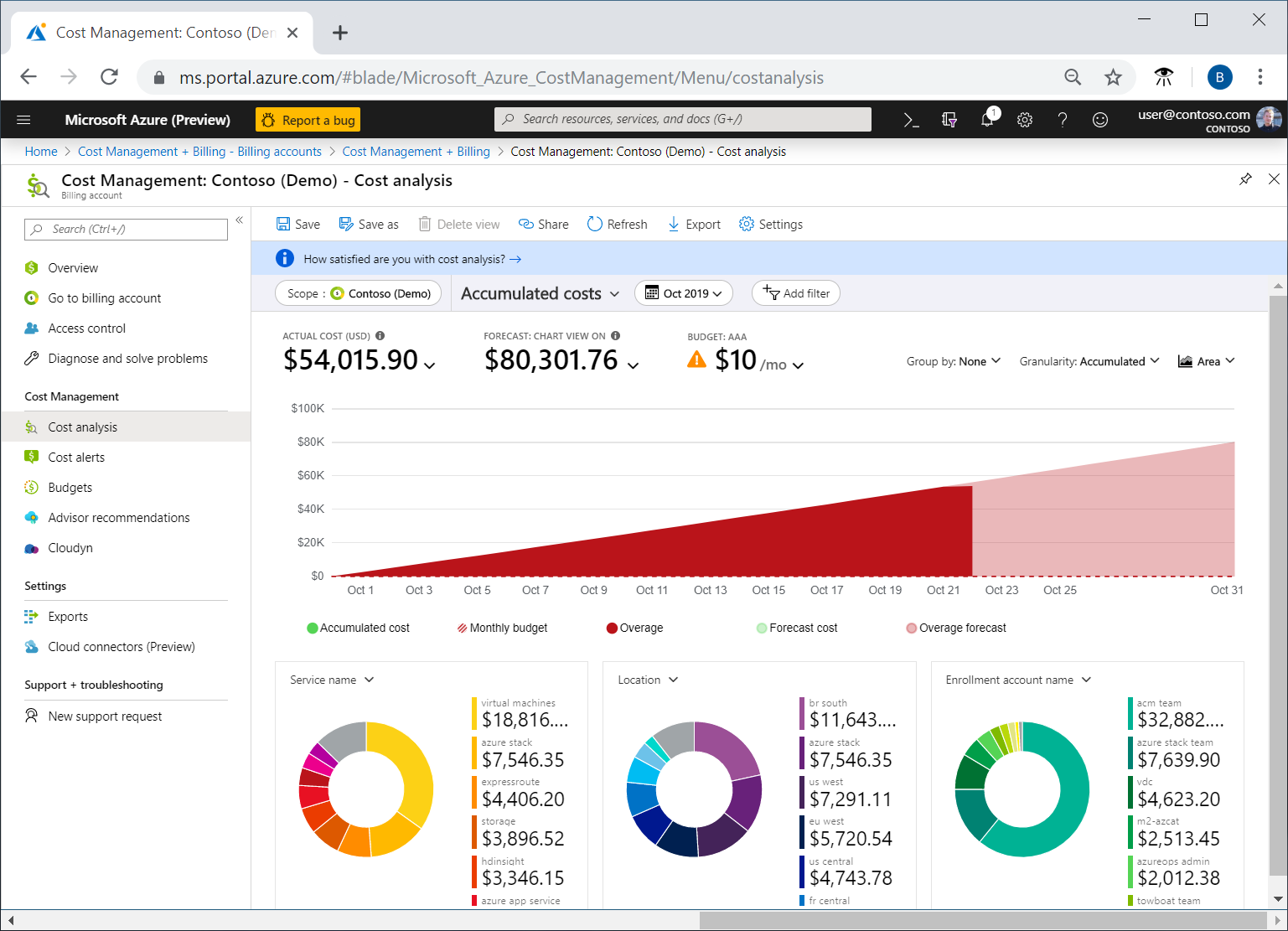
**Forecast:**

This view shows the total forecasted costs for the period chosen. Forecast chart view is used to identify potential budget breaches. When there's a potential budget breach, projected overspending is shown as red area.

**Budget:**

Shows the planned spending limit for the selected scope, if available.

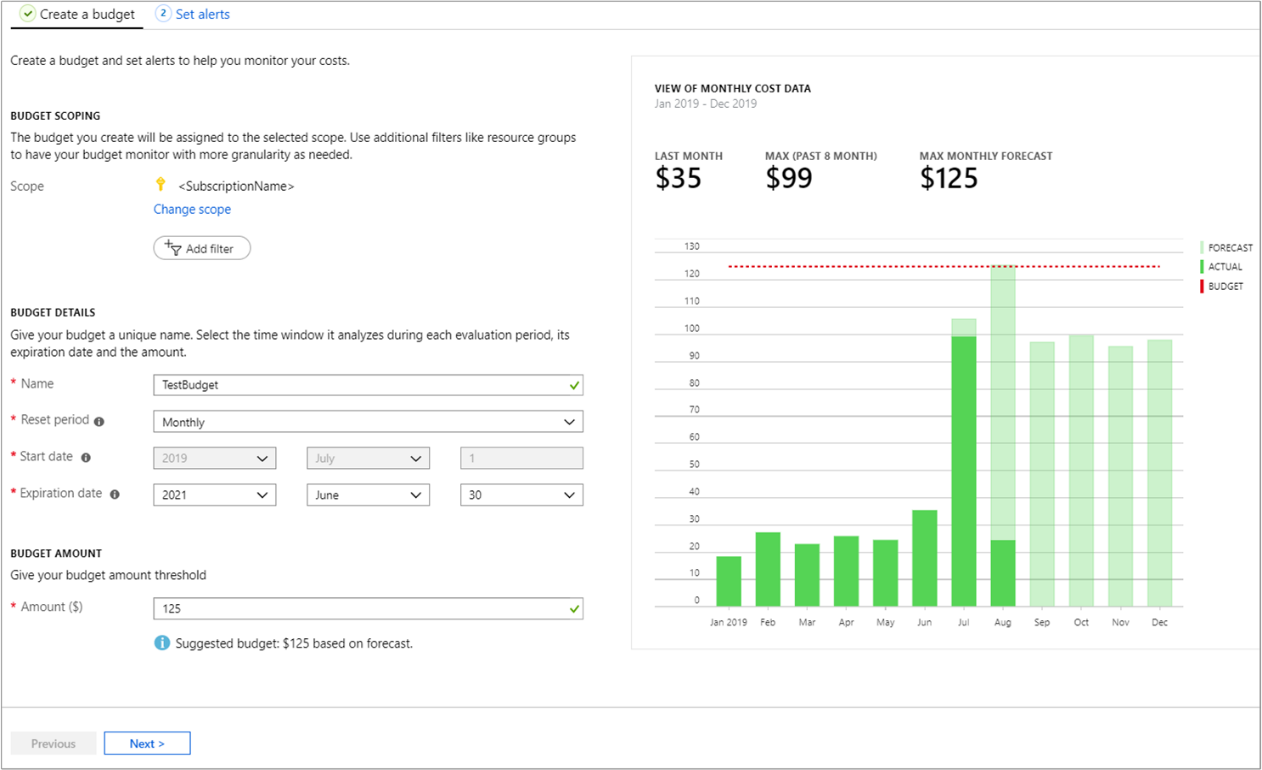
**Pivot (donut) charts:**

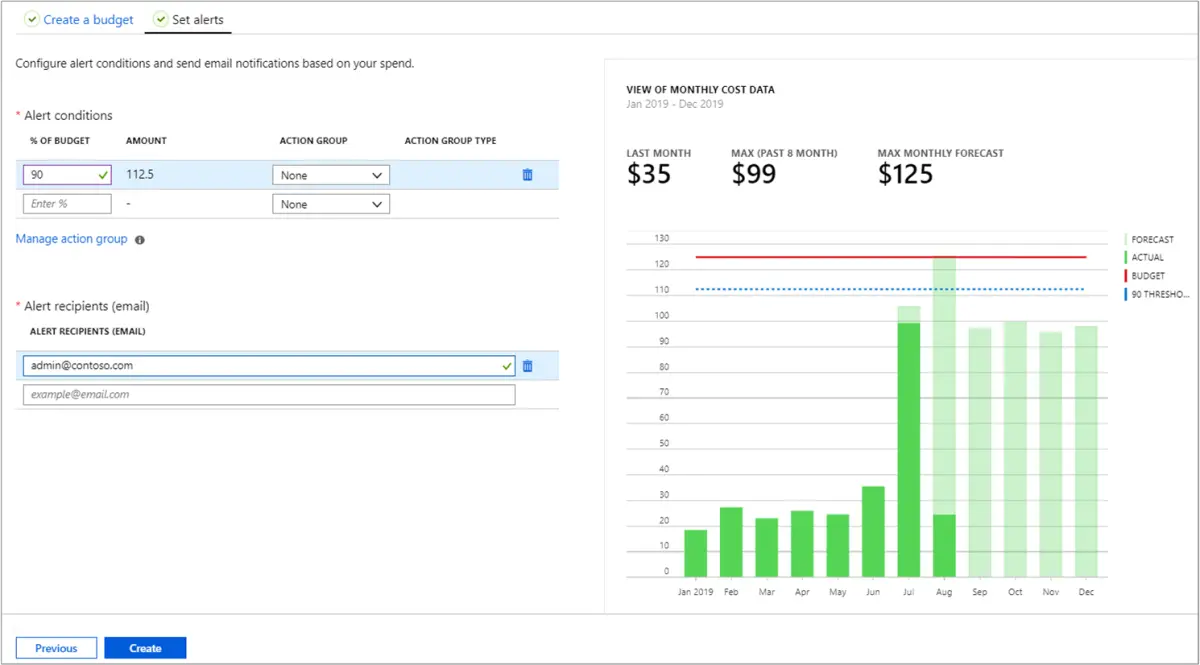
Provide dynamic pivots, breaking down the total cost by a common set of standard properties. Largest to smallest costs for the current month are shown. At any time, pivot charts can be changed by selecting a different pivot. Costs are categorized by service (meter category), location (region), and child scope by default. For example, enrollment accounts are under billing accounts, resource groups are under subscriptions, and resources are under resource groups. Here is an example for Accumulated Costs. The use case would have a similar view based on the resources used in the subscription.

### Monitor with budgets

Allows to create a budget and then configure alerts to warn on when near to exceeding it. Create an Azure subscription budget for a monthly, quarterly, or annual period. Refer to this [link](https://docs.microsoft.com/en-in/azure/cost-management-billing/costs/tutorial-acm-create-budgets?toc=https://docs.microsoft.com/azure/cloud-adoption-framework/toc.json&bc=https://docs.microsoft.com/azure/cloud-adoption-framework/_bread/toc.json#create-a-budget-in-the-azure-portal) for steps to create budgets and alerts. Below is an example for creating budget and alerts. The use case would have following budgets and alerts.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Budget Name | Scope | Reset Period | Budget Amount | Alert Conditions |
| Prod Subscription Monthly budget | Subscription | Monthly | 2000 | 50%, 80% of budget |
| QA Subscription Monthly budget | Subscription | Monthly | 1000 | 50%, 80% of budget |
| Dev Subscription Monthly budget | Subscription | Monthly | 3000 | 50%, 70%, 80%, 90% of budget |





**Cost Alerts**

Cost Management also supports other types of alerts and all active Cost Management and Billing alerts are shown together in one place. Alerts are generated by Cost Management when the consumption reaches a given threshold. There are three types of cost alerts: budget alerts, credit alerts, and department spending quota alerts.

### Optimize with recommendations

Helps identify idle and underused resources to take action to reduce waste. Azure Cost Management works with Azure Advisor to provide cost optimization recommendations. Azure Advisor helps to optimize and improve efficiency by identifying idle and underutilized resources. Below are examples of recommendations that might show up for the use case.

|  |  |
| --- | --- |
| Recommendation | Impact Category |
| Buy reserved virtual machine instances to save money over pay-as-you-go costs | High |
| Optimize virtual machine spend by resizing or shutting down underutilized instances | High |
| Use Standard Storage to store Managed Disks snapshots | High |
| Reduce costs by eliminating un-provisioned ExpressRoute circuits | Medium |
| Reduce costs by deleting or reconfiguring idle virtual network gateways | Medium |

### Manage invoices and payments

Manage invoices and payments gives the visibility for cloud investment.

## Governance, security and compliance

Governance decisions of an organization can be implemented and automated using tools and services like-

* Azure Policy
* Azure Blueprints
* Azure Security Center

### Azure Policy

Azure Policy is a service that is used to create, assign, and manage policies. These policies enforce rules on the resources, so those resources stay compliant with the corporate standards and service level agreements. Azure Policy scans the resources to identify resources that aren't compliant with the policies implemented. For example, a policy is allowed only to a specific virtual machine (VM) size to run in the environment. When this policy is implemented, it evaluates existing VMs in the environment and any new VMs that are deployed. The policy evaluation generates compliance events to use for monitoring and reporting purposes. Following are the compliance events for your perusal.

* Consider common policies to:
* Enforce tagging for resources and resource groups.
* Restrict regions for deployed resources.
* Restrict expensive SKUs for specific resources.
* Audit use of important optional features like Azure-managed disks.

Refer to this [link](https://docs.microsoft.com/en-us/azure/governance/policy/assign-policy-portal) to create policy using Azure portal.

**Azure Policy Objects**

This section will specifically discuss

* Policy definition
* Initiative definition
* Assignments

#### Policy definition

Every policy definition has conditions under which it's enforced. And, it has a defined effect that takes place if the conditions are met. Below table lists the built-in default policies.

|  |  |  |
| --- | --- | --- |
| Policy | Purpose | Value for the use case |
| Allowed Storage Account SKUs | Determines if a storage account being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that don't adhere to the set of defined SKU sizes. | Allow geo redundant storage only in production subscription. Dev and QA can have local redundant storage. |
| Allowed Resource Type | Defines the resource types that you can deploy. Its effect is to deny all resources that aren't part of this defined list. | Allow only VM, storage, managed instance, SQL, VNet in production. Additional resources can be created in dev and QA. |
| Allowed Locations | Restricts the available locations for new resources. Its effect is used to enforce your geo-compliance requirements. | Restrict Dev and QA to West US. Restrict production to US, Canada and Europe. |
| Allowed Virtual Machine SKUs | Specifies a set of virtual machine SKUs that you can deploy. | Allow high performance compute SKUs only to production. |
| Add a tag to resources | Applies a required tag and its default value if it's not specified by the deploy request. | Look for the tag Cost Center in resource group. If it is not present, then create the tag ‘Cost Center’ with value ‘Undefined’. |

#### Initiative definition

An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative defines, simplify managing and assigning policy definitions. They simplify by grouping a set of policies as one single item. For the use case, an initiative titled ‘Enable Monitoring in Azure Security Center’ is a created, with a goal to monitor all the available security recommendations in Azure Security Center. The below policies are added to this initiative.

|  |  |
| --- | --- |
| Policy | Purpose |
| Monitor unencrypted SQL Database in Security Center | For monitoring unencrypted SQL databases and servers. |
| Monitor OS vulnerabilities in Security Center | For monitoring servers that don't satisfy the configured baseline. |
| Monitor missing Endpoint Protection in Security Center | For monitoring servers without an installed endpoint protection agent. |

#### Assignments

An assignment is a policy definition or initiative that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource. The term scope refers to all the resources, resource groups, subscriptions, or management groups that the definition is assigned to. Assignments are inherited by all child resources. However, a sub scope can be excluded from the assignment. For the use case apply the below assignments.

* Assign a definition that prevents the creation of networking resources in subscription scope.
* Networking resource group is excluded from subscription scope. Then access is granted to this networking resource group to networking team.

### Azure Blueprints

Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments and trust that they're building within organizational compliance using a set of built-in components to speed up development and delivery. Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts like:

* Role assignments.
* Policy assignments.
* Azure Resource Manager templates.
* Resource groups.

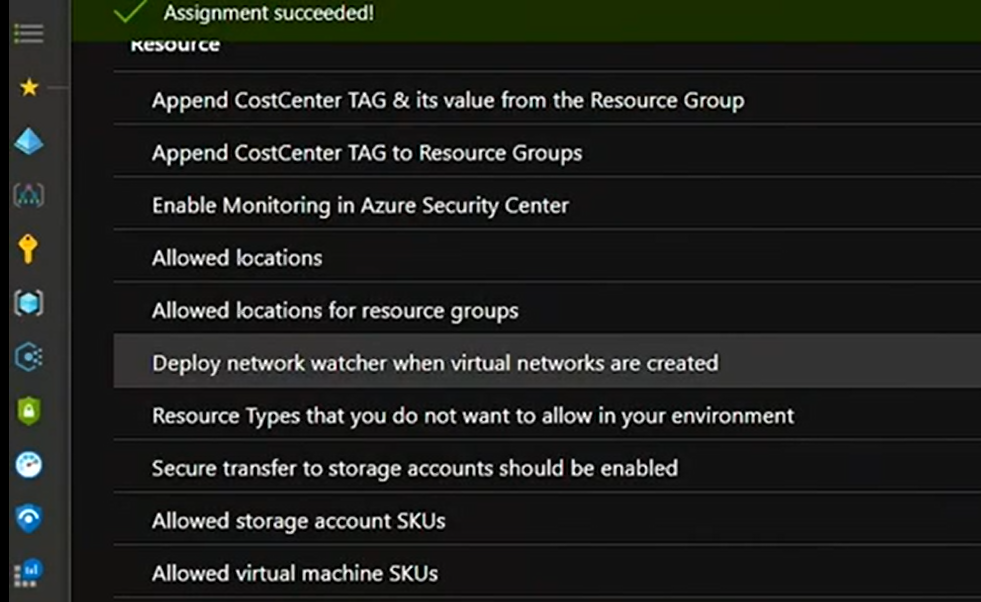
Refer to this [link](https://docs.microsoft.com/en-in/azure/governance/blueprints/create-blueprint-portal) for steps to create and assign blueprint through Azure portal.

Azure Blueprints provides sample blueprints which are production quality and ready to deploy today to assist in meeting various compliance needs. Refer to this [link](https://docs.microsoft.com/en-in/azure/governance/blueprints/samples/#standards-based-blueprint-samples) for the list of all standards-based blueprint samples. For the use case, apply the below standard-based blueprints.

|  |  |
| --- | --- |
| Standard-based blueprint | Purpose |
| [CIS Microsoft Azure Foundations Benchmark](https://docs.microsoft.com/en-in/azure/governance/blueprints/samples/cis-azure-1.1.0/) | Provides a set of policies to help comply with CIS Microsoft Azure Foundations Benchmark recommendations. |
| [CAF Foundation](https://docs.microsoft.com/en-in/azure/governance/blueprints/samples/caf-foundation/) | Provides a set of controls to help you manage your cloud estate in alignment with the [Microsoft Cloud Adoption Framework for Azure (CAF)](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/journeys/index). |
| [ISO 27001 App Service Environment/SQL Database workload](https://docs.microsoft.com/en-in/azure/governance/blueprints/samples/iso27001-ase-sql-workload/) | For monitoring servers without an installed endpoint protection agent. |

The above Three (3) blueprints have lots of steps. Below is a callout to few useful steps from the blueprints that are applicable to the use case.

* An Azure Key Vault instance used to host secrets used for the VMs deployed in the shared services environment
* Deploy Log Analytics is deployed to ensure all actions and services log to a central location from the moment you start your secure deployment in to Storage Accounts for diagnostic logging
* Deploy Azure Security Center (standard version) provides threat protection for your migrated workloads
* Tagging (CostCenter) applied to resources groups
* Append resources in resource group with the CostCenter Tag
* Allowed Azure Region for Resources and Resource Groups
* Allowed Storage Account SKUs (refer to section Policy definition)
* Allowed Azure VM SKUs (refer to section Policy definition)
* Require Network Watch to be deployed
* Require Azure Storage Account Secure Transfer Encryption
* Deny resource types (refer to section Policy definition)
* Audit external accounts with owner permissions on a subscription
* Audit external accounts with write permissions on a subscription
* Audit missing blob encryption for storage accounts
* Transparent Data Encryption on SQL databases should be enabled
* Audit diagnostic setting
* Audit SQL server level Auditing settings
* Auditing should be enabled on advanced data security settings on SQL Server
* Monitor possible app Whitelisting in Azure Security Center
* Monitor missing Endpoint Protection in Azure Security Center
* Monitor missing system updates in Azure Security Center
* Monitor OS vulnerabilities in Azure Security Center
* Monitor SQL vulnerability assessment results in Azure Security Center
* Monitor VM Vulnerabilities in Azure Security Center
* Monitor permissive network access in Azure Security Center
* Monitor unprotected network endpoints in Azure Security Center
* Monitor unprotected web application in Azure Security Center
* Audit unrestricted network access to storage accounts
* Ensure that multi-factor authentication is enabled for all privileged users
* Ensure that no custom subscription owner roles are created
* Ensure that 'Automatic provisioning of monitoring agent' is set to 'On'
* Ensure that standard pricing tier is selected
* Ensure ASC Default policy setting "Monitor OS Vulnerabilities" is not "Disabled"
* Ensure ASC Default policy setting "Monitor Endpoint Protection" is not "Disabled"
* Ensure ASC Default policy setting "Monitor Disk Encryption" is not "Disabled"
* Ensure ASC Default policy setting "Monitor Web Application Firewall" is not "Disabled"
* Ensure ASC Default policy setting "Enable Next Generation Firewall (NGFW) Monitoring" is not "Disabled"
* Ensure ASC Default policy setting "Monitor Storage Blob Encryption" is not "Disabled"
* Ensure ASC Default policy setting "Monitor JIT Network Access" is not "Disabled"
* Ensure ASC Default policy setting "Monitor Adaptive Application Whitelisting" is not "Disabled"
* Ensure ASC Default policy setting "Monitor SQL Encryption" is not "Disabled



### Azure Security Center

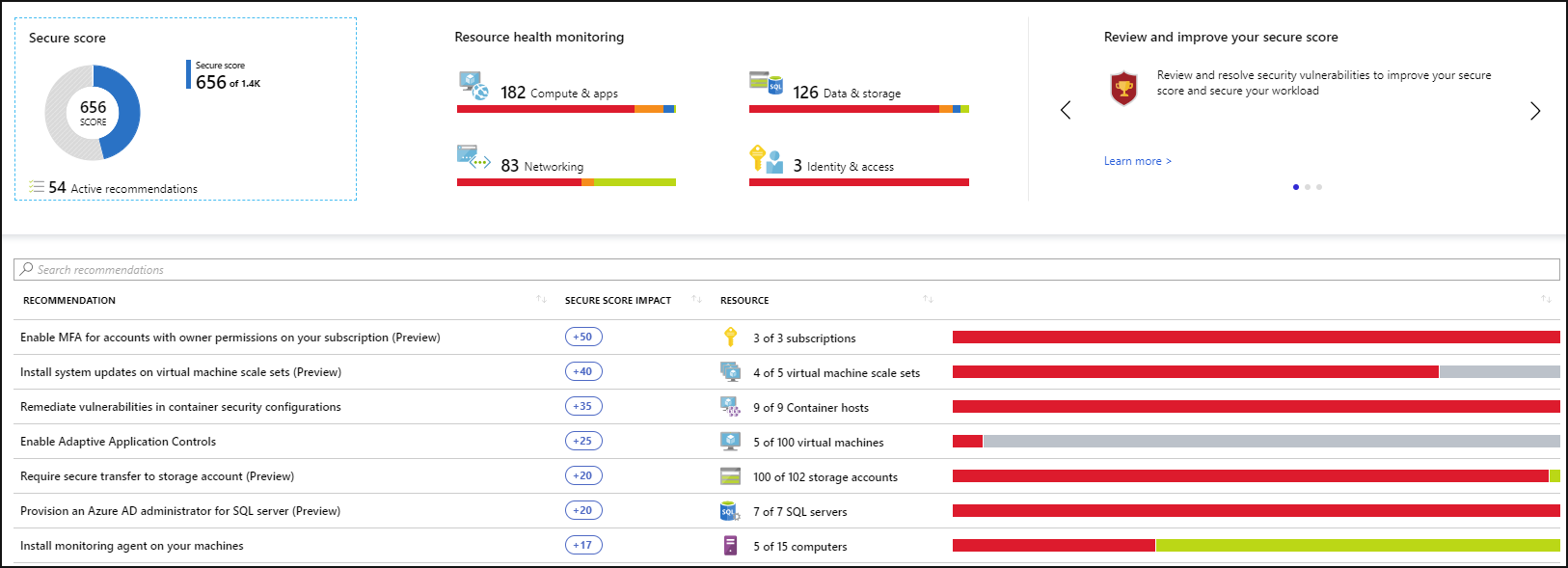
Azure Security Center plays an important part in the governance strategy. It helps to stay on top of security because it:

* Provides a unified view of security across the workloads.
* Collects, searches, and analyzes security data from a variety of sources, which includes firewalls and other partner solutions.
* Provides actionable security recommendations to fix issues before they can be exploited.
* Can be used to apply security policies across the hybrid cloud workloads to ensure compliance with security standards.

Many of the security features, like security policy and recommendations, are available for free. Some of the more advanced features, like just-in-time VM access and hybrid workload support, are available under the Security Center standard tier. Just-in-time VM access can help reduce the network attack surface by controlling access to management ports on Azure VMs.

For the use case, onboard the subscription to Security Center to strengthen security and protect against threats to SQL, VMs, storage, VNets and other resources in the subscription. Refer to this [link](https://docs.microsoft.com/en-us/azure/security-center/security-center-get-started) for steps to onboard a subscription to Security Center.

The Secure Scores are associated with each recommendation received to help understand how important each recommendation is to overall security posture. This is crucial in enabling to prioritize security work.



Security Center's threat protection enables to detect and prevent threats at the Infrastructure as a Service (IaaS) layer, non-Azure servers as well as for Platforms as a Service (PaaS) in Azure.

## Monitoring and Reporting

Azure offers many services that together provide a comprehensive solution for collecting, analyzing, and acting on telemetry from the applications and the Azure resources that support them. In addition, these services can extend to monitoring critical on-premises resources to provide a hybrid monitoring environment. This section will specifically discuss

* Azure Monitor
* Azure Service Health
* Azure Advisor
* Azure Security Center

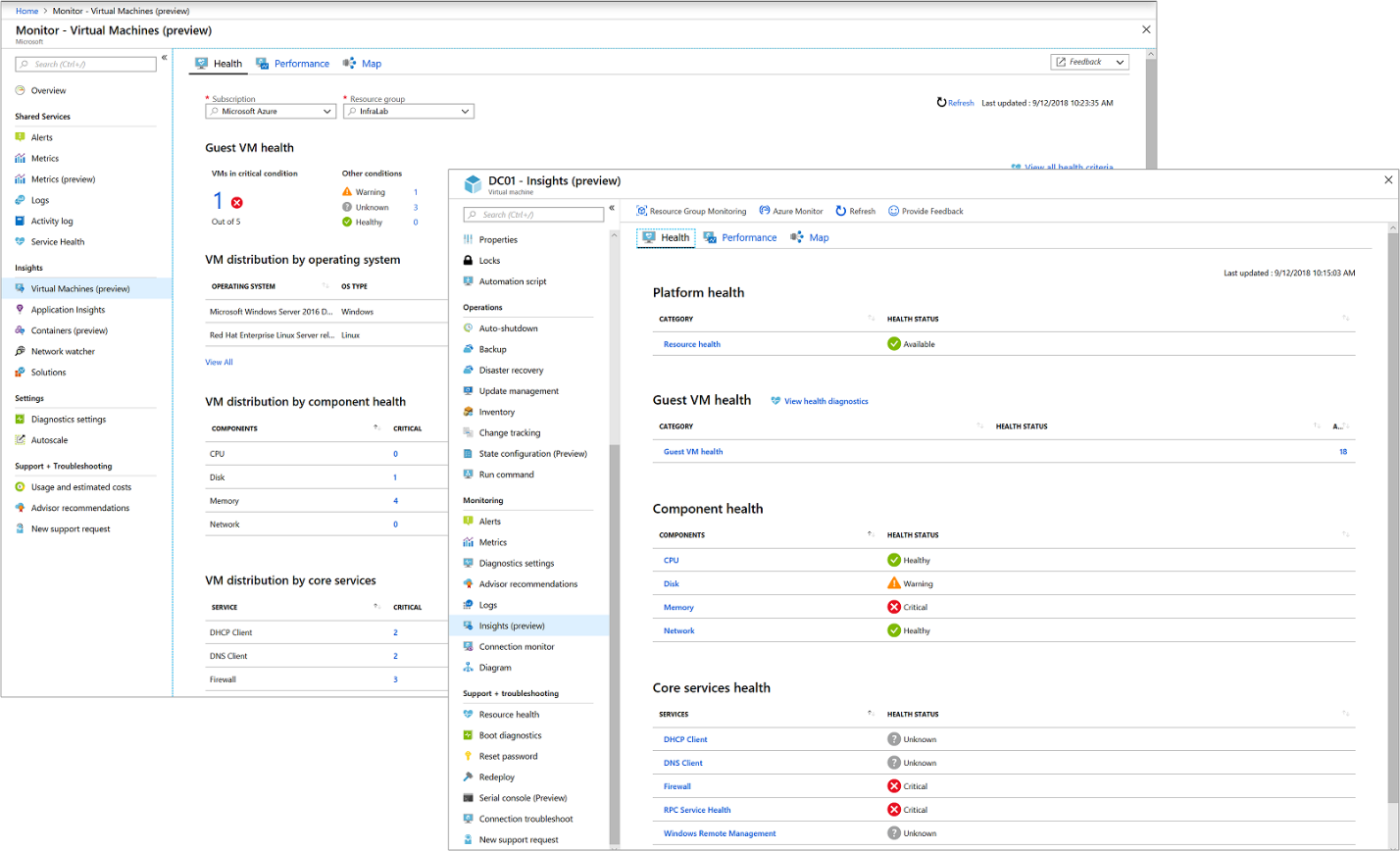
### Azure Monitor

Azure Monitor maximizes the availability and performance of the applications and services by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from the cloud and on-premises environments. It helps to understand how the applications are performing and proactively identifies the issues affecting them and the resources they depend on. Just a few examples of what you can do with Azure Monitor include:

* Detect and diagnose issues across applications and dependencies with [Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview).
* Correlate infrastructure issues with [Azure Monitor for VMs](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-overview) and [Azure Monitor for Containers](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/container-insights-overview).
* Drill into your monitoring data with [Log Analytics](https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview) for troubleshooting and deep diagnostics.
* Support operations at scale with [smart alerts](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-smartgroups-overview) and [automated actions](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules).
* Create visualizations with Azure [dashboards](https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-logs-dashboards) and [workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-workbooks).

For the use case Azure Monitor to monitor VMS, SQL, managed instance etc can be used. Azure Monitor for VMs monitors the Azure virtual machines (VM) at scale by analyzing the performance and health of the Windows and Linux VMs, including their different processes and interconnected dependencies on other resources and external processes. The solution includes support for monitoring performance and application dependencies for VMs hosted on-premises or another cloud provider.

Refer to this [link](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-enable-overview) for steps to enable monitor for VMs.



### Azure Service Health

Azure Service Health provides a personalized view of the health of Azure services and regions used. Information about active issues is posted to Service Health to help understand the impact to the resources. Regular updates helps to keep informed as the issue are resolved.

Planned maintenance events are also published to Service Health so the changes that could affect the availability of resources are known. Set up Service Health alerts to be notified when service issues, planned maintenance, or other changes might affect the Azure services and regions used.

**Azure Service Health includes:**

* Azure status: A global view of the health of Azure services.
* Service health: A personalized view of the health of your Azure services.
* Resource health: A deeper view of the health of each of your individual resources.

### Azure Advisor

Azure Advisor is a free, personalized cloud consultant that helps you follow and implement best practices for Azure deployments. It analyzes your resource configuration and usage telemetry and recommends solutions that can help optimize your environment. The recommendations are divided into the following categories:

* High availability: To improve the continuity of your business-critical applications. Recommendations might include adding virtual machines to an availability set or adding geo-redundant endpoints.
* Security: To detect threats and vulnerabilities that might lead to security breaches. Recommendations might include applying disk encryption or enabling network security groups.
* Performance: To improve the speed of your applications. Recommendations might include boosting SQL query performance by creating indexes or reconfiguring your traffic manager settings.
* Cost: To optimize and reduce your overall Azure spending. Recommendations might include resizing or shutting down underused virtual machines or switching to Azure reservations to lower total cost of ownership.
* Operational excellence: To improve process and workflow efficiency and manageability. Recommendations might include setting up and enforcing Azure Policy rules, repairing invalid log alert rules, and configuring Azure Service Health alerts.

Refer to this [link](https://docs.microsoft.com/en-us/azure/advisor/advisor-get-started) for steps to get starts with Azure Advisor.

### Azure Security Center

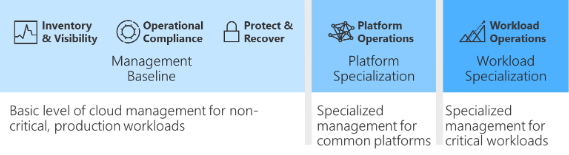
Azure Security Center also plays an important part in monitoring strategy. It helps to monitor the security of machines, networks, storage, data services, and applications. Security Center provides advanced threat detection by using machine learning and behavioral analytics to help identify active threats targeting Azure resources. It also provides threat protection that blocks malware or other unwanted code and reduces the surface area exposed to brute force and other network attacks.

When Security Center identifies a threat, it triggers a security alert with steps that are needed to respond to an attack. It also provides a report with information about the threat that was detected.

Azure Security Center is offered in two tiers: (Free and standard) Features like security recommendations are available for free. The standard tier provides additional protection like advanced threat detection and protection across hybrid cloud workloads.

## Manage

Azure Manage outlines on how to establish tooling for a management baseline. It also outlines ways to extend the baseline or build resiliency beyond the baseline.



**Minimum management baseline**

* Inventory and visibility: Create an inventory of assets across multiple clouds. Develop visibility into the run state of each asset.
* Operational compliance: Establish controls and processes to ensure each state is properly configured and running in a well-governed environment.
* Protect and recover: Ensure all managed assets are protected and can be recovered using baseline management tooling.

**Enhanced management baseline**

* Platform operations: Extend the management baseline with a well-defined service catalog and centrally managed platforms.
* Workload operations: Extend the management baseline to include a focus on mission-critical workloads.

A management baseline is the minimum set of tools and processes that should be applied to every asset in an environment. Several additional options can be included in the management baseline. The next few articles accelerate cloud management capabilities by focusing on the minimum options necessary instead of on all the available options.

### Inventory and visibility

Collecting proper operational data is vital when making decisions about operations. Cloud management teams must understand what is managed and how well those assets are operated. For any enterprise-grade environment, the following table outlines the suggested minimum for a management baseline.

|  |  |  |
| --- | --- | --- |
| Process | Tool | Purpose |
| Monitor health of Azure services | Azure Service Health | Health, performance, and diagnostics for services running in Azure |
| Log centralization | Log Analytics | Central logging for all visibility purposes |
| Monitoring centralization | Azure Monitor | Central monitoring of operational data and trends |
| Virtual machine inventory and change tracking | Azure Change Tracking and Inventory | Inventory VMs and monitor changes for guest OS level |
| Subscription Monitoring | Azure Activity Log | Monitoring change at the subscription level |
| Guest OS monitoring | Azure Monitor for VMs | Monitoring changes and performance of VMs |
| Network monitoring | Azure Network Watcher | Monitoring network changes and performance |
| DNS monitoring | DNS Analytics | Security, performance, and operations of DNS |

### Operational compliance

Improving operational compliance reduces the likelihood of an outage related to configuration drift or vulnerabilities related to systems being improperly patched. For any enterprise-grade environment, this table outlines the suggested minimum for a management baseline.

|  |  |  |
| --- | --- | --- |
| Process | Tool | Purpose |
| Patch management | Update Management | Management and scheduling of updates |
| Policy enforcement | Azure Policy | Policy enforcement to ensure environment and guest compliance |
| Environment configuration | Azure Blueprints | Automated compliance for core services |
| Resource Configuration | Desired State Configuration | Automated configuration on Guest OS and some aspects of the environment |

### Protect and recover

Protect and recover aims to reduce the duration and impact of outages that can't be prevented. For any enterprise-grade environment, this table outlines the suggested minimum for any management baseline.

|  |  |  |
| --- | --- | --- |
| Process | Tool | Purpose |
| Protect data | Azure Backup | Back up data and virtual machines in the cloud. |
| Protect the environment | Azure Security Center | Strengthen security and provide advanced threat protection across your hybrid workloads. |

Refer to Ready section for details on how to use manage tools.