Automated and repeatable environment setup in Azure.

Azure Blueprints provides automated and repeatable environment setup in Azure. It is able to implement Role assignments - Policy assignments - Azure Resource Manager templates (ARM templates) - Resource groups

Automated and repeatable resource deployment in Azure.

Is describes ARM templates, which only automate resource deployment. Azure Blueprints, by comparison, is able to deploy multiple ARM templates (resources), plus policies, role assignments, and more.

Monitors and analyses the cost of your current Azure resources

Cost Management is part of subscription billing tools, which breaks down current cost via a variety of filters and can set budgets and alerts

Create accurate estimates of hourly or monthly Azure costs across the entire Azure portfolio

This statement describes the Azure pricing calculator.

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol. Azure file shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS - A File service in a storage account

Q. What types of data does Azure Monitor collect?

Subscription monitoring data

Azure Monitor collects two broad types of data: metrics and logs. Within these data types sits subscription-monitoring data.

Metrics and logs

All data collected by Azure Monitor fits into one of two fundamental types, metrics and logs. Metrics are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios. Logs contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs in addition to performance data so that it can be combined for analysis.

Azure Privileged Identity Management (PIM)

Azure Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization.

Azure Sentinel

Azure Sentinel is Azure's SIEM tool offering that provides visibility and remediation capabilities to manage the security of your Azure environment.

Q. What are the advantages of the Zero Trust security model?

Limits rogue actors from accessing sensitive resources.

Because it requires establishing trust with identities, as well as restricting access to only what is necessary to perform a job (i.e., principle of least privilege), Zero Trust limits the ability of rogue actors or compromised accounts to do damage.

Allows access from any location once identity has been verified.

The Zero Trust security model is necessary for the modern "work from anywhere" workplace, as access can be granted regardless of a user's location.

Azure Disk Storage, Azure Files 🡪 can be used to house the migrated Windows file share data.

Q. Which Azure service can help you collect, analyse, and act on telemetry from your cloud and on-premises environments?

Azure Monitor

ARM templates are Azure's native Infrastructure-as-Code (IaC)

Azure Policy enforces organizational standards and compliance at scale. Examples include restricting a SKU or size of a virtual machine or defining which types of Azure resources are allowed.

Access Control (IAM) can be used to prevent the creation of Azure resources, but improper use could prevent required system access from other administrators. This is not the best selection.