AZ-140 Agenda

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles

Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD

Learning Path 4

10. Implement and manage FSLogix
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Monitor and manage performance and health
14. Plan and implement updates, backups, and disaster recovery

Microsoft

Plan and implement updates, backups, and disaster recovery

Introduction

After completing this module, you'll be able to:

- Plan for disaster recovery for Azure Virtual Desktop
- Design and implement a backup strategy for Azure Virtual Desktop
- Monitor costs by using Azure Cost Management

Disaster recovery for Azure Virtual Desktop

Disaster recovery for Azure Virtual Desktop

Responsibility for components that make up Azure Virtual Desktop are divided between those components that are Microsoft-managed, and those components that are customer-managed, or partner managed.

The following components are customer-managed or partner-managed:

- Session host virtual machines
- Profile management, usually with FSLogix
- Applications
- User data
- User identities

To learn about the Microsoft-managed components and how they're designed to be resilient, see Azure Virtual Desktop service architecture and resilience.

Business continuity and disaster recovery basics

When you design a disaster recovery plan, you should keep the following three things in mind:

- **High availability:** distributed infrastructure so smaller, more localized outages don't interrupt your entire deployment. Designing with high availability in mind can minimize outage impact and avoid the need for a full disaster recovery.
- **Business continuity:** how an organization can keep operating during outages of any size.
- **Disaster recovery:** the process of getting back to operation after a full outage.

Fault tolerance in Azure Virtual Desktop

You can distribute session hosts across multiple Azure regions provides even more geographical distribution, which further reduces outage impact.

The table lists the technology areas you need to consider as part of your disaster recovery strategy and links to other Microsoft documentation that provides guidance for each area:

Technology area	Documentation link
Active-passive vs active-active plans	Active-Active vs. Active-Passive
Session host resiliency	Multiregion Business Continuity and Disaster Recovery
Disaster recovery plans	Multiregion Business Continuity and Disaster Recovery
Azure Site Recovery	Failover and failback
Network connectivity	Multiregion Business Continuity and Disaster Recovery
User profiles	Design recommendations
Files share storage	Storage
Identity provider	Identity
Backup	Backup

Design and implement a backup strategy for Azure Virtual Desktop

Design and implement a backup strategy for Azure Virtual Desktop

Azure Backup provides independent and isolated backups to guard against unintended destruction of the data on your VMs.

As part of the backup process, a snapshot is taken, and the data is transferred to the Recovery Services vault with no impact on production workloads.

The snapshot provides various levels of consistency.

Backup process

Azure Backup starts a job based on the schedule. For application consistent backups, a backup extension is installed. Data is transferred to the vault after a snapshot.

Snapshot creation

Snapshots are taken per the backup schedule. For Windows VMs, Azure Backup uses VSS for app consistent snapshots. Logs can be truncated or preserved based on settings.

Encryption of Azure VM backups

Encryption	Details	Support
SSE	With SSE, Azure Storage provides encryption at rest by automatically encrypting data before storing it. Azure Storage also decrypts data before retrieving it. Azure Backup supports backups of VMs with two types of Storage Service Encryption: SSE with platform-managed keys: This encryption is by default for all disks in your VMs. SSE with customer-managed keys. With CMK, you manage the keys used to encrypt the disks.	Azure Backup uses SSE for at-rest encryption of Azure VMs.
Azure Disk Encryption	Azure Disk Encryption encrypts both OS and data disks for Azure VMs. Azure Disk Encryption integrates with BitLocker encryption keys (BEKs), which are safeguarded in a key vault as secrets. Azure Disk Encryption also integrates with Azure Key Vault key encryption keys (KEKs).	Azure Backup supports backup of managed and unmanaged Azure VMs encrypted with BEKs only, or with BEKs together with KEKs. Both BEKs and KEKs are backed up and encrypted. Encrypted keys and secrets can't be read by unauthorized users or by Azure.

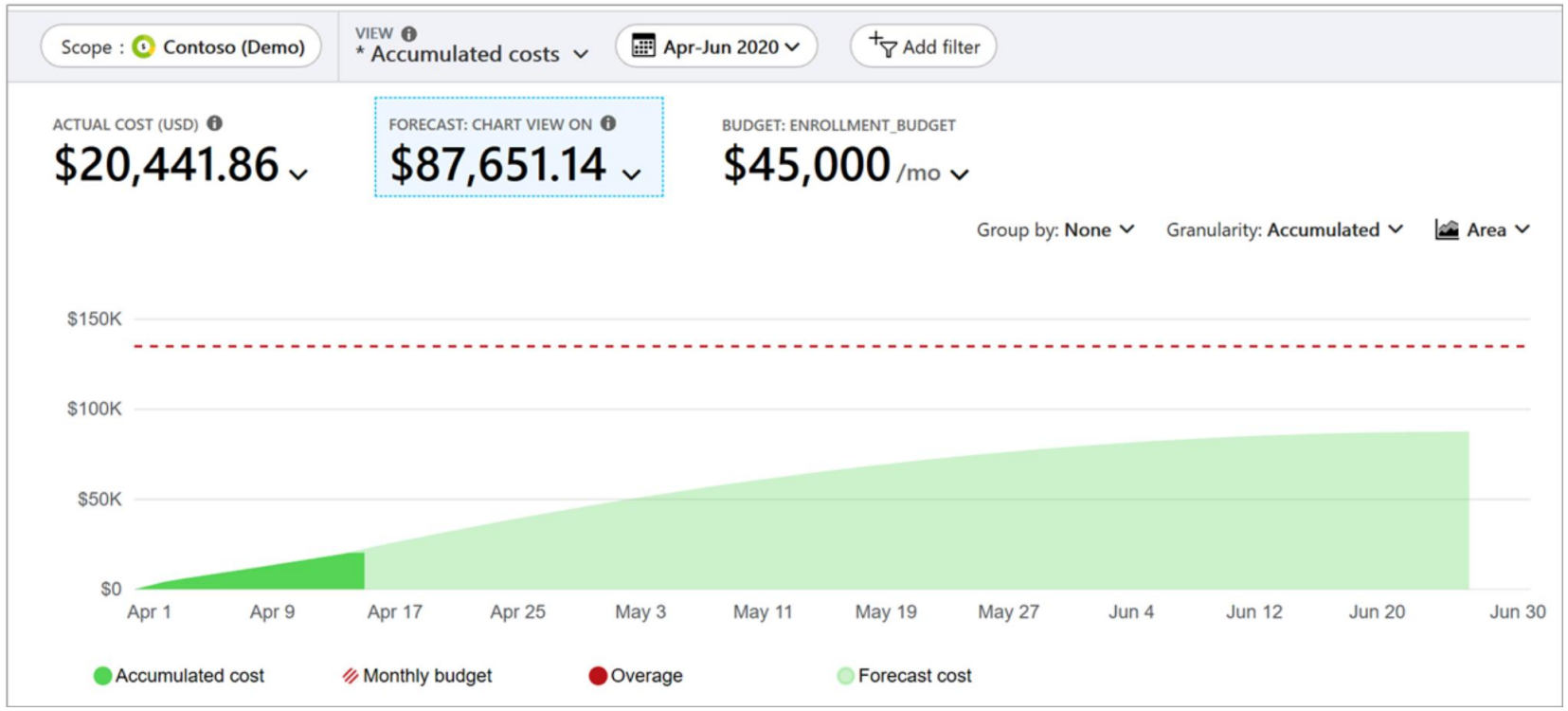
Monitor costs by using Azure Cost Management

View forecast costs

Forecast costs are shown in cost analysis areas for area and stacked column views. The forecast is based on your historical resource use. Changes to your resource use affect forecast costs.

See: **Cost Management + Billing > Cost Management > Cost analysis.**

The solid color of the chart shows your Actual/Amortized cost. The shaded color shows the forecast cost.



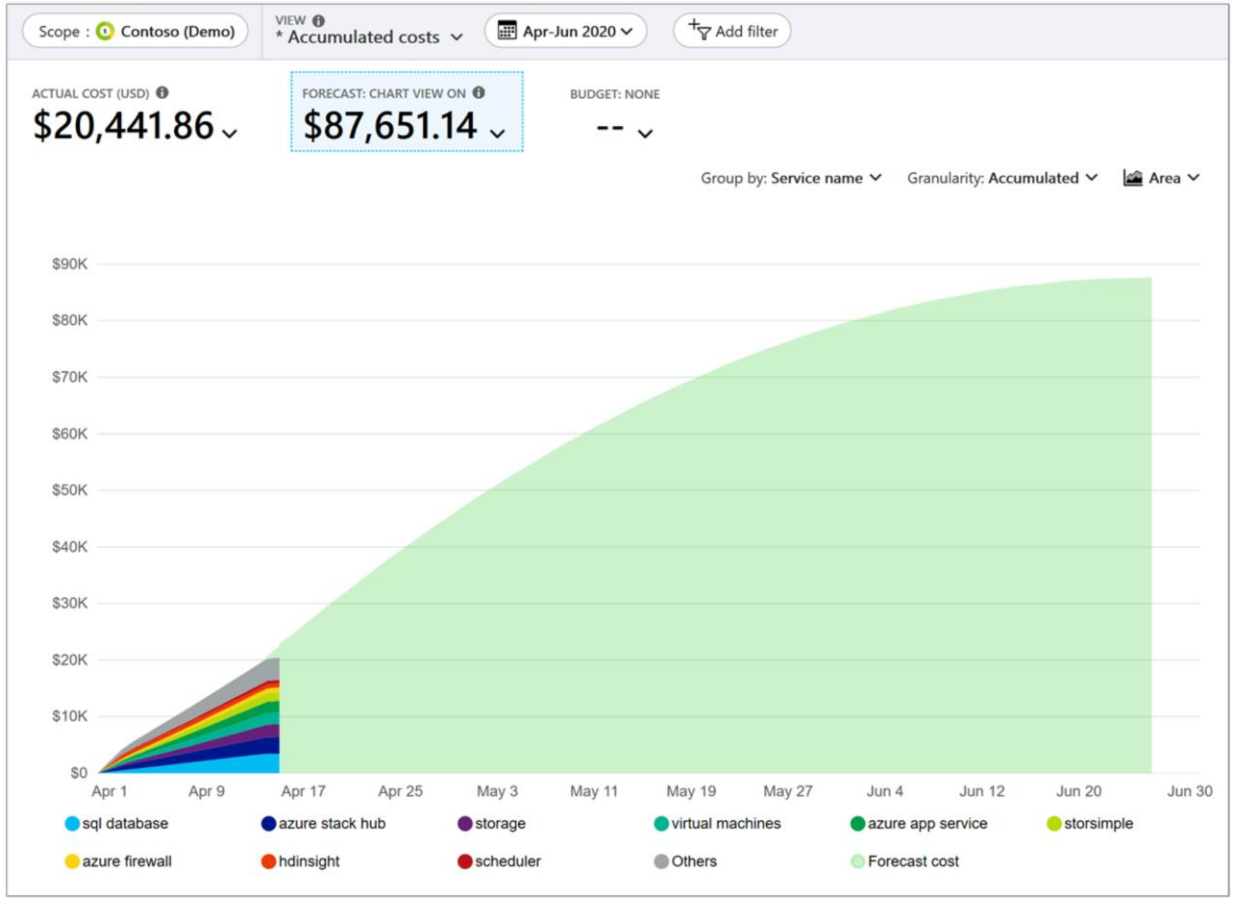
View forecast costs grouped by service vs for a service

View forecast costs grouped by service

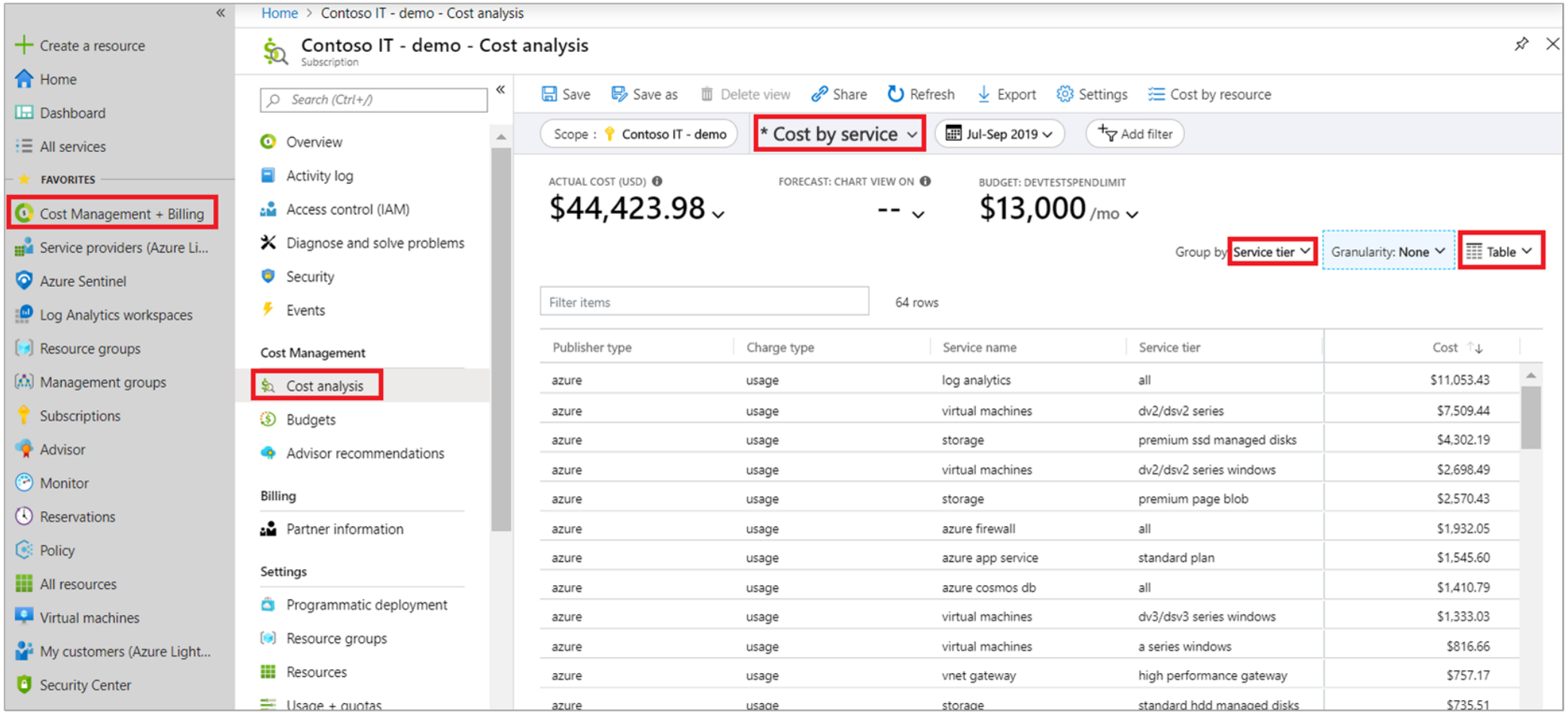
Group by service to see costs for each service. The forecast cost is projected for the total of all services.

View forecast costs for a service

Narrow forecast costs to a single service. For example, view costs for virtual machines.



View cost breakdown by Azure service



Knowledge check

Knowledge check

What should be used to replicate Azure Virtual Desktop virtual machines to the secondary location?

Choices:

1. Deploy Azure Site Recovery
2. Deploy Azure Load Balancer
3. Azure Role-based access control (RBAC)

Knowledge check

A developer is tasked with creating a system that can automatically manage and validate the creation and teardown of environments for application hosting. What technology enables this?

Choices:

1. Identity provider
2. Storage
3. Backup

Knowledge check

A team is planning for disaster recovery for Azure Virtual Desktop. They want to replicate their virtual machines to a secondary location. Which service should they use to manage this replication?

Choices:

1. Azure Cost Management
2. Azure Backup
3. Azure Site Recovery

Knowledge check

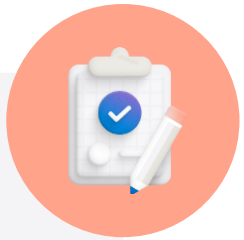
A developer is tasked with creating a system that can automatically manage and validate the creation and teardown of environments for application hosting. What technology enables this?

Choices:

1. Identity provider
2. Storage
3. Backup

Summary

Summary



What you learned:

- Plan for disaster recovery for Azure Virtual Desktop
- Design and implement a backup strategy for Azure Virtual Desktop
- Monitor costs by using Azure Cost Management