

Azure Backup “Need to Know” Exam Information



Michael Bender

AUTHOR EVANGELIST - PLURALSIGHT

@michaelbender



Exam Breakdown of Objective Domain

Monitor and Backup Up Azure Resources (10-15%)

- Monitor resources by using Azure Monitor
- Implement backup and recovery



Objectives

Configure and review backup reports

Perform backup and restore operations by using Azure Backup

Create a Recovery Services Vault

- use soft delete to recover Azure VMs

Create and configure backup policy

Perform site-to-site recovery by using Azure Site Recovery



Configure and Review Backup Reports



Configure Backup Reports

Support multiple backup sources

Requires a Log Analytics workspace

Configure diagnostic settings in Recovery Services Vault

Know the Azure Backup log events for Resource specific diagnostics

View Reports in the Recovery Services Vault



Log Events for Resource Specific Diagnostic Logs

Microsoft Azure Search resources, services, and docs (G+/)

mbender@bentech.net BENDER TECHNOLOGY CONSULT...

Home > demovault >

Diagnostic setting

Save Discard Delete Provide feedback

log

- ☐ AzureBackupReport
- ☐ CoreAzureBackup
- ☐ AddonAzureBackupJobs
- ☐ AddonAzureBackupAlerts
- ☐ AddonAzureBackupPolicy
- ☐ AddonAzureBackupStorage
- ☐ AddonAzureBackupProtectedInstance
- ☐ AzureSiteRecoveryJobs
- ☐ AzureSiteRecoveryEvents

☒ Send to Log Analytics workspace

Subscription
Visual Studio Enterprise

Log Analytics workspace
DefaultWorkspace-afab04a1-b389-446a-9228-ad4d59680dc6-EUS (eas...

Destination table

Azure diagnostics Resource specific

i You need to create separate diagnostic settings for Azure Backup and Azure Site Recovery events to prevent potential data loss. For Azure Backup events, if you choose the 'Resource specific' mode, you must select the following events only - CoreAzureBackup, AddonAzureBackupJobs, AddonAzureBackupAlerts, AddonAzureBackupPolicy, AddonAzureBackupStorage, AddonAzureBackupProtectedInstance. The AzureBackupReport event works only in 'Azure diagnostics' mode. [Learn more](#)

☐ Archive to a storage account

☐ Stream to an event hub



Create and Configure Backup Policy



Create a Backup Policy



Stored in Recovery Services Vault in region of resources

Defines how a backup plan is implemented

Setup asks for backup configuration

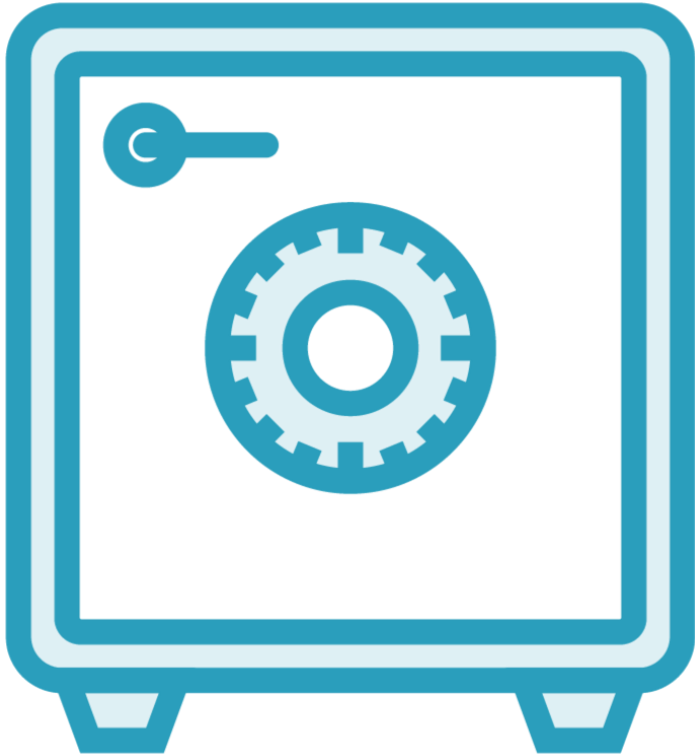
Multiple retention periods

Policy for each resource type

Create a Recovery Services Vault



Recovery Service Vault



Storage Entity for backup and recovery resources

Centralized management

Work with on-premises and cloud-based workloads.

Backup resources in same region as RSV

- RSV and VMs in East US

Site recovery resources in different region

- RSV in East US
- Source VMs in West US



Understand what you can
and can't protect based on
Azure region



Perform Backup and Restore Operations by using Azure Backup



Performing Backup Operations

Supports on-premises and Azure workloads

App-consistent backups

Require resources and vault in same region

Initiate backup manually or scheduled



You can only backup
resources in the SAME
region as your Recovery
Services Vault



Restoring VM Backups

Point-In-time Restores

VM Restore Options

- Entire VM
- Individual disks
- Files

Mount Files in VM Backup via Script



Restoring File Shares

Based on Snapshots

Incorporates Soft Delete for 14 days of retention by default

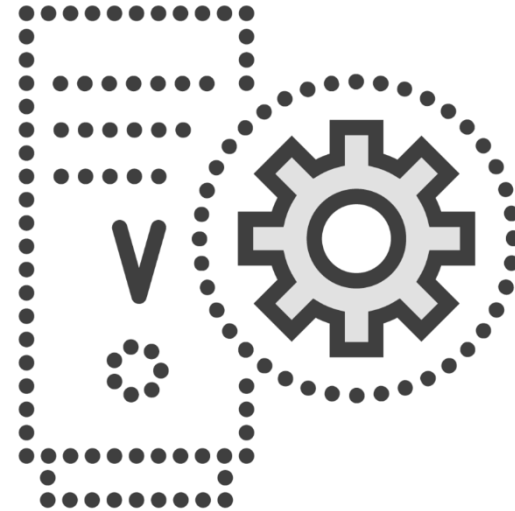
File Share backup data is in storage account



Backup Agents



Azure Backup extension
For all Azure VMs



Microsoft Azure Recovery Services
agent (MARS)
For On-premises servers or AWS
VMs

Virtual Machine Soft Delete

Protects against unintended VM deletions

Stored for up to 14 days

Requires a backup to have been completed

Multiple tools for completing



Perform Site-to-site Recovery by Using Azure Site Recovery



Perform Site-to-site Recovery by Using Azure Site Recovery

Set up site recovery at VM level or in recovery services vault

RSV and VM resources for replication must be in different regions

Example:

- VMs in East US and West US Regions
- Existing RSV in West US Region
- Only East US VMs can be protected

You can perform test failovers or production failovers.



Site-Recovery Protected
VMs must be in a different
Azure region from your
Recovery Services Vault.



Exam Strategy

Know how services fit together

- For example, how would you backup up VMs and Azure Files
- Creating Alerts in Azure Monitor

Be familiar with implementations in portal and with code

Weight your study time based on exam percent

- Monitor and Backup will be approximately 5-8 questions



Exam Strategy

Build on your weaknesses

Make sure to check the AZ-104 exam guide regularly

Remember this is an Administrator Associate Exam

Get hands-on experience



Best of Luck on the Exam!!!



Michael Bender

AUTHOR EVANGELIST - PLURALSIGHT

@michaelbender

bender@Pluralsight.com

