**QUESTION 5**

A company has more than 5 TB of file data on Windows file servers that run on-premises.

Users and applications interact with the data each day.

The company is moving its Windows workloads to AWS.

As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency.

The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns.

The company uses an AWS Site-to-Site VPN connection for connectivity to AWS.

What should a solutions architect do to meet these requirements?

1. Deploy and configure Amazon FSx for Windows File Server on AWS.

Move the on-premises file data to FSx for Windows File Server.

Reconfigure the workloads to use FSx for Windows File Server on AWS.

1. Deploy and configure an Amazon S3 File Gateway on-premises.

Move the on-premises file data to the S3 File Gateway.

Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway.

1. Deploy and configure an Amazon S3 File Gateway on premises.

Move the on-premises file data to Amazon S3.

Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway, depending on each workload's location.

1. Deploy and configure Amazon FSx for Windows File Server on AWS.

Deploy and configure an Amazon FSx File Gateway on premises.

Move the on-premises file data to the FSx File Gateway.

Configure the cloud workloads to use FSx for Windows File Server on AWS.

Configure the on-premises workloads to use the FSx File Gateway.

**Answer:** A

**QUESTION 127**

A company runs multiple Windows workloads on AWS.

The company's employees use Windows file shares that are hosted on two Amazon EC2 instances.

The file shares synchronize data between themselves and maintain duplicate copies.

The company wants a highly available and durable storage solution that preserves how users currently access the files.

What should a solutions architect do to meet these requirements?

1. Migrate all the data to Amazon S3.

Set up IAM authentication for users to access files.

1. Set up an Amazon S3 File Gateway.

Mount the S3 File Gateway on the existing EC2 Instances.

1. Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration.

Migrate all the data to FSx for Windows File Server.

1. Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration.

Migrate all the data to Amazon EFS.

**Answer:** C

**Explanation:**

Security groups are stateful. All inbound traffic is blocked by default. If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again. You cannot block specific IP address using Security groups (instead use Network Access Control Lists).

"You can specify allow rules, but not deny rules." "When you first create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group."

Source: <https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#VPCSecurityGroups>

**QUESTION 157**

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage.

The company wants to migrate this workload to the AWS Cloud and is considering various storage options.

The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

1. Configure Amazon EFS storage and set the Active Directory domain for authentication.
2. Create an SMB Me share on an AWS Storage Gateway tile gateway in two Availability Zones.
3. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
4. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

**Answer:** D

**QUESTION 176**

A company is migrating applications to AWS.

The applications are deployed in different accounts.

The company manages the accounts centrally by using AWS Organizations.

The company's security team needs a single sign-on (SSO) solution across all the company's accounts.

The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory.

Which solution will meet these requirements?

1. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

Create a one-way forest trust or a one-way domain trust to connect the company's selfmanaged Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.

1. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.

1. Use AWS Directory Service.

Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.

1. Deploy an identity provider (IdP) on premises.

Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

**Answer:** A

**QUESTION 188**

A company has no existing file share services.

A new project requires access to file storage that is mountable as a drive for on-premises desktops.

The file server must authenticate usrs to an Activ Directory domain before they are able to access the storage.

Which service will allow Active Directory users to mount storage as a drive on their desktops?

1. AWS S3 Glacier.
2. AWS DataSync.
3. AWS Snowball Edge.
4. AWS Storage Gateway.

**Answer:** D

**Explanation:**

Before you create an SMB file share, make sure that you configure SMB security settings for your file gateway.

You also configure either Microsoft Active Directory (AD) or guest access for authentication. <https://docs.aws.amazon.com/storagegateway/latest/userguide/CreatingAnSMBFileShare.html>

**QUESTION 233**

A company has a Windows-based application that must be migrated to AWS.

The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zones.

What should a solutions architect do to meet this requirement?

1. Configure AWS Storage Gateway in volume gateway mode.

Mount the volume to each Windows instance.

1. Configure Amazon FSx for Windows File Server.

Mount the Amazon FSx file system to each Windows instance.

1. Configure a file system by using Amazon Elastic File System (Amazon EFS).

Mount the EFS file system to each Windows instance.

1. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size.

Attach each EC2 instance to the volume.

Mount the file system within the volume to each Windows instance.

**Answer:** B