



- [🏠 \(https://www.whizlabs.com/learn\)](https://www.whizlabs.com/learn) > [My Courses \(https://www.whizlabs.com/learn/my-courses\)](https://www.whizlabs.com/learn/my-courses)
- > [AWS Certified Solutions Architect Associate \(https://www.whizlabs.com/learn/course/aws-csaa-practice-tests#section-1\)](https://www.whizlabs.com/learn/course/aws-csaa-practice-tests#section-1)
 - > [Amazon Elastic File System \(EFS\) - Quiz \(https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14791\)](https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14791)
 - > **Report**

AMAZON ELASTIC FILE SYSTEM (EFS) - QUIZ

Attempt	4	Completed on	Sunday , 03 February 2019 , 02:32 PM
Marks Obtained	9 / 10	Time Taken	00 H 05 M 45 S
Your score is	90%	Result	Pass

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Other	10	9	1	0

10 Questions	9 Correct	1 Incorrect	0 Unattempted	Show Answers	All	▼
------------------------	---------------------	-----------------------	-------------------------	--------------	-----	---

QUESTION 1 CORRECT

Your organization has an existing VPC in us-east-1 with two subnets in us-east-1b. They are running few EC2 instances each in both subnets and would need a low latency common File

Store for all instances to share files for heavy work loads. They have created an EFS, mounted on all the EC2 instances and able to share files across all the EC2 instances. You were tasked to increase the number of instances due to the increase in work load. You created a new subnet in us-east-1c and launched few instances. When you tried to mount the previously created EFS on new EC2 instances, operation getting failed. What could be the reason?

- ☐ A. AWS EFS does not support cross availability zone mounting.
- ☐ B. By default EFS is only available in one availability zone. Create a case with AWS support to increase EFS availability zones.
- ☐ C. EFS created with mount targets in us-east-1b availability zone. Instances in us-east-1c cannot use EFS mount target in us-east-1b.
- ☒ D. EFS mount target security group inbound rules does not allow traffic from new EC2 instances. ✓

Explanation :

Answer: D

Amazon EFS provides scalable file storage for use with Amazon EC2. You can create an EFS file system and configure your instances to mount the file system. You can use an EFS file system as a common data source for workloads and applications running on multiple instances

Creating or Deleting Mount Targets in a VPC

To access an Amazon EFS file system in a VPC, you need mount targets. For an Amazon EFS file system, the following is true:

- You can create one mount target in each Availability Zone.
- If the VPC has multiple subnets in an Availability Zone, you can create a mount target in only one of those subnets. All EC2 instances in the Availability Zone can share the single mount target.

Note

We recommend that you create a mount target in each of the Availability Zones. There are cost considerations for mounting a file system on an EC2 instance in an Availability Zone through a mount target created in another Availability Zone. For more information, see [Amazon EFS](#). In addition, by always using a mount target local to the instance's Availability Zone, you eliminate a partial failure scenario. If the mount target's zone goes down, you can't access your file system through that mount target.

For options A, B, C EFS mount targets from one availability zone can be mounted on another availability zone although this approach is not recommended. However, this approach will not cause operations to fail.



Creating or Deleting Mount Targets in a VPC

A *VPC peering connection* is a networking connection between two VPCs that enables you to route traffic between them using private Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) addresses. For more information on VPC peering, see [What is VPC Peering?](https://docs.aws.amazon.com/vpc/latest/peering/Welcome.html) (<https://docs.aws.amazon.com/vpc/latest/peering/Welcome.html>) in the *Amazon VPC Peering Guide*.

You can mount Amazon EFS file systems over VPC connections by using VPC peering within a single AWS Region when using the Amazon EC2 instance types T3, C5, C5d, I3.metal, M5, M5d, R5, R5d, and z1d. However, other VPC private connectivity mechanisms such as inter-region VPC peering and VPC peering within an AWS Region using other instance types are not supported.

Note the following restrictions:

- You can mount an Amazon EFS file system on instances in only one VPC at a time.
- Both the file system and VPC must be in the same AWS Region.

For option D, when using Amazon EFS, you specify Amazon EC2 security groups for the EFS mount targets associated with the file system. Security groups act as a firewall, and the rules you add define the traffic flow.

You can authorize inbound and outbound access to your EFS file system. To do so, you add rules that allow your EC2 instance to connect to your Amazon EFS file system through the mount target using the Network File System (NFS) port.

Ask our Experts



QUESTION 2 CORRECT

You have an AWS setup with an existing VPC in us-east-1. You have a fleet of 20 EC2 instances which are attached to EFS with mount targets on all existing VPC's availability zones. Your organization had requested you to replicate the same setup in another VPC within us-east-1 keeping same EFS volume. How will you achieve this?

- ☐ A. Attach new VPC to existing EFS, create new mount targets for new VPC and mount EFS on EC2 instances within new VPC
- ☒ B. Peer both VPCs, launch C5 or M5 EC2 instances on new VPC and mount existing EFS on new EC2 instances. ✓
- ☐ C. EFS is available for all VPCs within a region by default. Mount EFS on new EC2 instances and configure EFS security group to allow inbound traffic.



- ☐ D. EFS can be used only within one VPC at a time. You need to launch EC2 instances in existing VPC.

Explanation :

Answer: B

Working with VPC Peering in Amazon EFS

A *VPC peering connection* is a networking connection between two VPCs that enables you to route traffic between them using private Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) addresses. For more information on VPC peering, see *What is VPC Peering?* (<https://docs.aws.amazon.com/vpc/latest/peering/Welcome.html>) in the *Amazon VPC Peering Guide*.

You can mount Amazon EFS file systems over VPC connections by using VPC peering within a single AWS Region when using the Amazon EC2 instance types T3, C5, C5d, I3.metal, M5, M5d, R5, R5d, and z1d. However, other VPC private connectivity mechanisms such as inter-region VPC peering and VPC peering within an AWS Region using other instance types are not supported.

<https://docs.aws.amazon.com/efs/latest/ug/manage-fs-access-change-vpc.html#manage-fs-access-vpc-peering> (<https://docs.aws.amazon.com/efs/latest/ug/manage-fs-access-change-vpc.html#manage-fs-access-vpc-peering>)

For options A and C, you can use an Amazon EFS file system in one VPC at a time. That is, you create mount targets in a VPC for your file system, and use those mount targets to provide access to the file system from EC2 instances in that VPC.

Note the following restrictions:

- You can mount an Amazon EFS file system on instances in only one VPC at a time.
- Both the file system and VPC must be in the same AWS Region.

For option D, although the statement is correct, launching EC2 instances within same VPC is not a solution when you were asked to do in a new VPC. Correct answer from given options would be to peer the VPC and use appropriate instance types.

Ask our Experts



Which of the following statements is correct in terms of the newly created security group to allow Secure Shell (SSH) to connect to instances and communication between EC2 instance and EFS?

- ☒ A. Open port 22(SSH) on EC2 security group and port 2049(NFS) on EFS security group. ✓
- ☐ B. Open port 22(SSH) on EC2 security group and ports 111(NFS) & 2049(NFS) on EFS security group.
- ☐ C. Open port 2049(NFS) on EC2 security group and ports 111(NFS) & 2049(NFS) on EFS security group.
- ☐ D. Open port 111(NFS) on EC2 security group and ports 111(NFS) & 2049(NFS) on EFS security group.

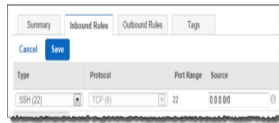
Explanation :

Answer: A



3. You need to authorize additional access to the security groups as follows:

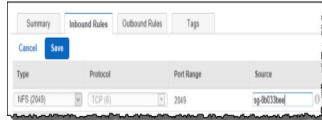
- a. Add a rule to the EC2 security group to allow inbound access, as shown following. Optionally, you can restrict the **Source** address.



Type	Protocol	Port Range	Source
SSH (22)	TCP (8)	22	0.0.0.0/0

For instructions, see [Adding and Removing Rules](#) in the *Amazon VPC User Guide*.

- b. Add a rule to the mount target security group to allow inbound access from the EC2 security group, as shown following (where the EC2 security group is identified as the source):



Type	Protocol	Port Range	Source
NFS (2049)	TCP (8)	2049	sg-80330ee1

Note

You don't need to add an outbound rule because the default outbound rule allows all traffic to leave (otherwise, you will need to add an outbound rule to open TCP connection on the NFS port, identifying the mount target security group as the destination).

- <https://docs.aws.amazon.com/efs/latest/ug/accessing-fs-create-security-groups.html#create-security-groups-console>
(<https://docs.aws.amazon.com/efs/latest/ug/accessing-fs-create-security-groups.html#create-security-groups-console>)

AWS EFS does not require any other port to be open except NFS (2049) on its security group.





QUESTION 4 CORRECT

You have two VPCs (VPC A and VPC B) peered with each other. You have created an EFS for VPC A. When you tried to mount the EFS on EC2 instances on VPC B, you are getting connection timed out. What can cause this?(choose 2 options)

- ☐ A. AWS EFS takes upto an hour after creation to make mount targets available.
- ☐ B. VPC B could be in different region than VPC A.
- ☒ C. Security group on mount targets does not have NFS port open to VPC B's EC2 instances. ✓
- ☒ D. VPC B's EC2 instance types are not M5 or C5. ✓
- ☐ E. EFS cannot be mounted through VPC peering.

Explanation :

Answer: C, D

- Option A is not true. Usually, EFS and its mount targets get created within a few moments.

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
us-east-1a	us-east-1a	us-east-1a	10.0.1.1	mtg-1a1a1a1a	eni-1a1a1a1a	sg-1a1a1a1a	Available
us-east-1b	us-east-1b	us-east-1b	10.0.1.2	mtg-1b1b1b1b	eni-1b1b1b1b	sg-1b1b1b1b	Available

The console shows the newly created file system on the **File Systems** page. Verify that all mount targets show the **Life Cycle State** as **Available**. It might take a few moments before the mount targets become available (you can expand/collapse the file system in the EFS console to force it to refresh).

- Option B is not true. You can now connect to Amazon EFS (<https://aws.amazon.com/efs/>) file systems from EC2 instances in other AWS regions using an inter-region VPC peering connection, and from on-premises servers using an AWS VPN connection.
- Option C is true. Inbound rule for NFS port must be added on mount target's security group for the EC2 instances which will mount the EFS.



Working with VPC Peering in Amazon EFS

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) addresses. For more information on VPC peering, see [What is VPC Peering?](#) in the *Amazon VPC Peering Guide*.

For Amazon EFS, you can work with VPC peering within a single AWS Region when using C5 or M5 instances. However, other VPC private connectivity mechanisms such as a VPN connection, interregion VPC peering, and intraregion VPC peering using other instance types are not supported.

- Option D is true.

Working with VPC Peering in Amazon EFS

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) addresses. For more information on VPC peering, see [What is VPC Peering?](#) in the *Amazon VPC Peering Guide*.

For Amazon EFS, you can work with VPC peering within a single AWS Region when using C5 or M5 instances. However, other VPC private connectivity mechanisms such as a VPN connection, interregion VPC peering, and intraregion VPC peering using other instance types are not supported.

- Option E is false. Refer above screen shot.
- Please find the below AWS docs link:
 - <https://docs.aws.amazon.com/efs/latest/ug/manage-fs-access-vpc-peering.html>
(<https://docs.aws.amazon.com/efs/latest/ug/manage-fs-access-vpc-peering.html>)
 - <https://aws.amazon.com/about-aws/whats-new/2018/10/amazon-efs-now-supports-aws-vpn-and-inter-region-vpc-peering/>
(<https://aws.amazon.com/about-aws/whats-new/2018/10/amazon-efs-now-supports-aws-vpn-and-inter-region-vpc-peering/>)

Note:

Below is the list of EC2 instances that are supported when working with EFS.

Mounting an EFS file system from an EC2 instance in the same AWS Region over a VPC peering connection is supported with only the following EC2 instance types:

- T3
- C5
- C5d
- I3.metal
- M5
- M5d
- R5
- R5d
- z1d



- For reference check this link
- <https://docs.aws.amazon.com/efs/latest/ug/manage-fs-access-vpc-peering.html>
(<https://docs.aws.amazon.com/efs/latest/ug/manage-fs-access-vpc-peering.html>)

Ask our Experts



QUESTION 5 CORRECT

You have created AWS EFS with default settings and mounted on an EC2 instance. Due to regulatory policies, your organization had asked you to encrypt data stored on EFS. What would you do to enable encryption?

- ☐ A. Edit EFS volume and enable “encryption at rest” setting. All existing data automatically gets encrypted as a background process. You will be notified once the process is completed.
- ☒ B. Encryption at rest option can only be set during EFS creation. You need to create encryption-at-rest EFS, copy data from old EFS to new EFS and delete old EFS. ✓
- ☐ C. You can enable encryption at rest during mounting of EFS on EC2. To encrypt an existing EFS mount, unmount the EFS and remount with encryption option.
- ☐ D. EFS does not support encryption. Use S3 for encrypting data at rest.

Explanation :

Answer: B

AWS EFS supports encrypting data at rest. It can only be done during EFS creation.

Enable encryption
If you enable encryption for your file system, all data on your file system will be encrypted at rest. You can select a KMS key from your account to protect your file system, or you can provide the ARN of a key from a different account. **Encryption of data at rest can only be enabled during file system creation.** Encryption of data at rest is enabled when mounting your file system. Learn more.

☐ Enable encryption of data at rest

Enforcing Encryption at Rest

Your organization might require the encryption at rest of all data that meets a specific classification or that is associated with a particular application, workload, or environment. You can enforce policies for data encryption at rest for Amazon EFS file systems by using detective controls. These controls detect the creation of a file system and verify that encryption at rest is enabled.

If a file system that doesn't have encryption at rest is detected, you can respond in a number of ways. These range from deleting the file system and mount targets to notifying an administrator.



If you want to delete an unencrypted-at-rest file system but want to retain the data, first create a new encrypted-at-rest file system. Next, copy the data over to the new encrypted-at-rest file system. After the data is copied over, you can delete the unencrypted-at-rest file system.

Option A is incorrect. You cannot enable encryption once EFS is created.

Option C is incorrect. You cannot enable encryption at rest through mounting options. Option D is incorrect. Refer to above screen shots.

Ask our Experts



QUESTION 6 INCORRECT

You have created AWS EFS with default settings and mounted on an EC2 instance. Due to regulatory policies, your organization had asked you to encrypt data during transit to EFS. What would you do to enable encryption during transit?

- ☐ A. AWS EFS uses NFS protocol which encrypts the data in transit by default.
- ☐ B. Edit EFS to enable "encryption during transit" setting.
- ☒ C. Encryption during transit can only be enabled during EFS creation. You need to create encryption during transit EFS, copy data from old EFS to new EFS and delete old EFS. ✕
- ☐ D. Enable encryption during mounting on EC2 using Amazon EFS mount helper. Unmount unencrypted mount and remount using mount helper encryption during transit option. ✓

Explanation :

Answer: D

AWS uses NFS protocol for EFS. NFS is not an encrypted protocol and anyone on the same physical network could sniff the traffic and reassemble the information being passed back and forth.

However, AWS provides an option to encrypt data at transit through NFS to EFS.

For information on how to enable encryption during transit, refer documentation here.

- <https://docs.aws.amazon.com/efs/latest/ug/encryption.html#encryption-in-transit>
(<https://docs.aws.amazon.com/efs/latest/ug/encryption.html#encryption-in-transit>)

Option A is incorrect. Refer above statements.

Option B and C are incorrect. Encryption during transit is not an option on EFS during or after creation.



Step 1: Configure the system access
 Step 2: Configure optional settings
 Step 3: Review and create

Configure optional settings

Add tags

You can add tags to describe your file system. A tag consists of a case-sensitive key-value pair. (For example, you can define a tag with key-value pair with key = Corporate Department and value = Sales and Marketing.) In a minimum, we recommend a tag with key = Name.

Key	Value	Remove
Name	Add New Value	
Add New Key		

Choose performance mode

We recommend **General Purpose** performance mode for most file systems. **Max IO** performance mode is optimized for applications where tens, hundreds, or thousands of EC2 instances are accessing the file system — it enables higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for the operations.

☒ General Purpose
☐ Max IO

Choose throughput mode

We recommend **Bursting** throughput mode for most file systems. Use **Provisioned** throughput mode for applications that require more throughput than allowed by **Bursting** throughput. [Learn more](#)

☒ Bursting
☐ Provisioned

Enable encryption

If you enable encryption for your file system, all data on your file system will be encrypted at rest. You can select a KMS key from your account to protect your file system, or you can provide the ARN of a key from a different account. Encryption of data at rest can only be enabled during the system creation. Encryption of data in transit is configured when mounting your file system. [Learn more](#)

☐ Enable encryption of data at rest

File systems

Create file system Actions

Name	
	Manage file system access Manage tags Manage throughput mode Delete file system

Other details

Option D is correct. Refer above documentation link for more information on using Amazon EFS mount helper to enable encryption during transit.

Ask our Experts



QUESTION 7 CORRECT

You are building a content serving web application with 20 EC2 instances load balanced. For all the instances, content storage remains the same. You have chosen AWS EFS to act as common storage repository. Your application need to have as low latency as possible when serving content to the web users. Which of the following option would you choose and why?

- ☐ A. Performance mode = General Purpose, AWS can handle performance with general purpose mode till 10s of EC2 instances.
- ☒ B. Performance mode = General Purpose, provides low-latency access to EFS. ✓

- ☐ C. Performance mode = Max I/O, provides better performance when sharing EFS across more than 10 EC2 instances.
- ☐ D. Performance mode = Max I/O, provides low-latency access to EFS.

Explanation :

Answer: B

Although Max I/O is recommended to be used when tens, hundreds or thousands of EC2 instances sharing same EFS, it can slightly increase the latency. In this case, the question states the latency need to be as low as possible.

Choose performance mode

We recommend **General Purpose** performance mode for most file systems. **Max I/O** performance mode is optimized for applications where tens, hundreds, or thousands of EC2 instances are accessing the file system — it scales to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations.

- ☒ General Purpose
- ☐ Max I/O

Performance Modes

To support a wide variety of cloud storage workloads, Amazon EFS offers two performance modes. You select a file system's performance mode when you create it.

The two performance modes have no additional costs, so your Amazon EFS file system is billed and metered the same, regardless of your performance mode. For information about file system limits, see [Limits for Amazon EFS File Systems](#).

Note

An Amazon EFS file system's performance mode can't be changed after the file system has been created.

General Purpose Performance Mode

We recommend the General Purpose performance mode for the majority of your Amazon EFS file systems. General Purpose is ideal for latency-sensitive use cases, like web serving environments, content management systems, home directories, and general file serving. If you don't choose a performance mode when you create your file system, Amazon EFS selects the General Purpose mode for you by default.

Max I/O Performance Mode

File systems in the Max I/O mode can scale to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations. Highly parallelized applications and workloads, such as big data analysis, media processing, and genomics analysis, can benefit from this mode.

Performance Modes

To support a wide variety of cloud storage workloads, Amazon EFS offers two performance modes. You select a file system's performance mode when you create it.

The two performance modes have no additional costs, so your Amazon EFS file system is billed and metered the same, regardless of your performance mode. For information about file system limits, see [Limits for Amazon EFS File Systems](#)

(<https://docs.aws.amazon.com/efs/latest/ug/limits.html#limits-fs-specific>).

Note

An Amazon EFS file system's performance mode can't be changed after the file system has been created.



General Purpose Performance Mode

We recommend the General Purpose performance mode for the majority of your Amazon EFS file systems. General Purpose is ideal for latency-sensitive use cases, like web serving environments, content management systems, home directories, and general file serving. If you don't choose a performance mode when you create your file system, Amazon EFS selects the General Purpose mode for you by default.

Max I/O Performance Mode

File systems in the Max I/O mode can scale to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations. Highly parallelized applications and workloads, such as big data analysis, media processing, and genomics analysis, can benefit from this mode.

- <https://docs.aws.amazon.com/efs/latest/ug/performance.html#performancemodes>
(<https://docs.aws.amazon.com/efs/latest/ug/performance.html#performancemodes>)

From above explanation, only option B is a correct statement

Ask our Experts



QUESTION 8 CORRECT

You are building a content serving web application on 5 EC2 instances load balanced. Total content size stored may not exceed 25 GB. You have chosen EFS for content storage. The content is accessed frequently by large number of users. Which throughput mode would you choose in order to make sure that application on EC2 instances to EFS data transfer will not have performance bottleneck?

- ☐ A. Throughput mode = Bursting, provides a consistent high throughput for smaller data sizes.
- ☐ B. Throughput mode = Bursting, automatically bursts throughput based on the requests irrespective of EFS data size
- ☒ C.
Throughput mode = Provisioned, you can configure specific throughput irrespective of EFS data size ✓
- ☐ D. Throughput mode = Provisioned, AWS provisions high throughput for smaller data sizes and vice versa.

Explanation :

Answer: C

With Bursting Throughput mode, throughput on Amazon EFS scales as a file system grows.



File System Size	Aggregate Read/Write Throughput
A 100-GiB file system can...	<ul style="list-style-type: none"> Burst to 100 MiB/s for up to 72 minutes each day, or Drive up to 5 MiB/s continuously
A 1-TiB file system can...	<ul style="list-style-type: none"> Burst to 100 MiB/s for 12 hours each day, or Drive 50 MiB/s continuously
A 10-TiB file system can...	<ul style="list-style-type: none"> Burst to 1 GiB/s for 12 hours each day, or Drive 500 MiB/s continuously
Generally, a larger file system can...	<ul style="list-style-type: none"> Burst to 100MiB/s per TiB of storage for 12 hours each day, or Drive 50 MiB/s per TiB of storage continuously

The following table provides more detailed examples of bursting behavior for file systems of different sizes.

File System Size (GiB)	Baseline Aggregate Throughput (MiB/s)	Burst Aggregate Throughput (MiB/s)	Maximum Burst Duration (Min/Day)	% of Time File System Can Burst (Per Day)
10	0.5	100	7.2	0.5%
256	12.5	100	180	12.5%
512	25.0	100	360	25.0%
1024	50.0	100	720	50.0%
1536	75.0	150	720	50.0%
2048	100.0	200	720	50.0%
3072	150.0	300	720	50.0%
4096	200.0	400	720	50.0%

In this case, data size is 25 GB can burst through 100 MiB/s only for 18 mins/day. Rest of the day, it uses baseline aggregate throughput and gives 1.25 MiB/s throughput. The baseline rate is 50

MiB/s per TiB of storage (equivalently, 50 KiB/s per GiB of storage).

Specifying Throughput with Provisioned Mode

"Provisioned Throughput mode is available for applications with high throughput to storage (MiB/s per TiB) ratios, or with requirements greater than those allowed by the Bursting Throughput mode. For example, say you're using Amazon EFS for development tools, web serving, or content management applications where the amount of data in your file system is low relative to throughput demands. Your file system can now get the high levels of throughput your applications require without having to pad your file system".

- <https://docs.aws.amazon.com/efs/latest/ug/performance.html#throughput-modes>
(<https://docs.aws.amazon.com/efs/latest/ug/performance.html#throughput-modes>)

For this case, since the data is low compared to the throughput demand, provisioned mode is the right choice for throughput mode.

Ask our Experts



Your organization is planning to use AWS for BigData analysis. Total data is expected to be 400

TB. They were planning to use 150 EC2 instances with EFS because of better performance needs for the analysis. They have reached out to you asking for recommendation on performance mode. What would you suggest?

- ☐ A. Performance mode = General Purpose, AWS can handle performance with general purpose mode till 10s of EC2 instances.
- ☐ B. Performance mode = General Purpose, provides low-latency access to EFS.
- ☐ C. Performance mode = General Purpose, provides higher levels of aggregate throughput and operations per second.
- ☒ D. Performance mode = Max I/O, provides higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies. ✓

Explanation :

Answer: D

Max I/O Performance Mode

"File systems in the Max I/O mode can scale to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations. Highly parallelized applications and workloads, such as big data analysis, media processing, and genomics analysis, can benefit from this mode".

For more information, Please check following AWS Docs:

- <https://docs.aws.amazon.com/efs/latest/ug/performance.html>
(<https://docs.aws.amazon.com/efs/latest/ug/performance.html>)

Ask our Experts



Which of the following are characteristics of EFS? (choose 2 options)

- ☐ A. Data is stored redundantly in a single AZ.
- ☒ B. Up to thousands of Amazon EC2 instances, from multiple AZs, can connect concurrently to a file system. ✓



- ☐ C. Boot volumes, transactional and NoSQL databases, data warehousing, and ETL.
- ☒ D. Big data and analytics, media processing workflows, content management, web serving, and home directories. ✓
- ☐ E. Cross region replication.

Explanation :

Answer: B, D

Following table shows the characteristics of EFS vs EBS.

	Amazon EFS	Amazon EBS Provisioned IOPS
Availability and durability	Data is stored redundantly across multiple AZs.	Data is stored redundantly in a single AZ.
Access	Up to thousands of Amazon EC2 instances, from multiple AZs, can connect concurrently to a file system.	A single Amazon EC2 instance in a single AZ can connect to a file system.
Use cases	Big data and analytics, media processing workflows, content management, web serving, and home directories.	Boot volumes, transactional and NoSQL databases, data warehousing, and ETL.

Option A is characteristic of EBS. Option B is characteristic of EFS. Option C is characteristic of EBS.

Option D is characteristic of EFS. Option E is characteristic of S3.

For more information on AWS EFS use cases, refer documentation here.

- <https://docs.aws.amazon.com/efs/latest/ug/performance.html#performance-usecases>
(<https://docs.aws.amazon.com/efs/latest/ug/performance.html#performance-usecases>)

Ask our Experts



Finish Review (<https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14791>)

Certification

- ➔ Cloud Certification
(<https://www.whizlabs.com/cloud-certification-training-courses/>)
- ➔ Java Certification
(<https://www.whizlabs.com/oracle-java-certifications/>)
- ➔ PM Certification
(<https://www.whizlabs.com/project-management-certifications/>)

Company

- ➔ Support
(<https://help.whizlabs.com/hc/en-us>)
- ➔ Discussions (<http://ask.whizlabs.com/>)
- ➔ Blog (<https://www.whizlabs.com/blog/>)



🔗 Big Data Certification
(<https://www.whizlabs.com/big-data-certifications/>)

Mobile App

 Android Coming Soon

 iOS Coming Soon

Follow us



(<https://www.facebook.com/whizlabs.software/>)



(<https://in.linkedin.com/company/whizlabs-software>)



(<https://twitter.com/whizlabs?lang=en>)



(<https://plus.google.com/+WhizlabsSoftware>)

