

AMAZON FSx

Amazon FSx (File System for Windows/Linux) is a fully managed file storage service provided by Amazon Web Services (AWS). It is designed to simplify the setup and operation of file storage in the AWS Cloud for Windows and Linux workloads.

Here are some key features and points about Amazon FSx:

1. **Managed File Storage:** Amazon FSx is a fully managed service, meaning AWS takes care of routine tasks such as hardware provisioning, software configuration, maintenance, and backups.
2. **Windows and Lustre File Systems:** Amazon FSx supports both Windows File Server (for Windows workloads) and Lustre (for high-performance computing applications) file systems.
3. **Integration with AWS Services:** Amazon FSx integrates with various AWS services, such as Amazon S3 for object storage, AWS Direct Connect for dedicated network connections, and AWS Identity and Access Management (IAM) for access control.
4. **Data Transfer and Backup:** It provides features for data transfer, backup, and recovery. You can create automated daily backups, and the service supports both manual and automatic backups.
5. **High Performance:** Depending on the file system type, Amazon FSx provides high-performance storage with features like Multi-AZ deployment for high availability and SSD-based storage.
6. **Scalability:** It is designed to scale easily to handle growing workloads, and you can adjust the storage capacity and throughput based on your application requirements.
7. **Security:** Amazon FSx provides features such as encryption at rest and in transit, and it integrates with AWS Key Management Service (KMS) for managing encryption keys.

TO BEGIN WITH THE LAB:

STEP 1: CREATE DIRECTORY

1. So, to create a file system for windows server we use a service called Amazon FSx.
2. So, to create FSx you will need a directory.
3. First you have to create that. For that search for directory service.



Directory Service ☆

Host and Manage Active Directory

4. Now click on set up a directory.
5. Here you have to choose AWS managed Microsoft AD.

Directory types

AWS Managed Microsoft AD
 AD Connector
 Amazon Cognito User Pools

AWS Managed Microsoft AD

With AWS Managed Microsoft AD, you can easily enable your Active Directory-aware workloads and AWS resources to use managed actual Microsoft Active Directory in the AWS Cloud. Workload examples include Amazon EC2, Amazon RDS for SQL Server, custom .NET applications, and AWS Enterprise IT applications such as Amazon WorkSpaces.

[Learn more](#) 
[View use cases](#) 

[Cancel](#) [Next](#)

6. Here, you have to choose standard edition.

Directory information [Info](#)

A managed Microsoft Active Directory domain.

Directory type
Microsoft AD

Operating system version
Windows Server 2019

Edition [Info](#)

Microsoft AD is available in the following two editions:

Standard Edition

Best for small to medium sized businesses.

- 1GB of storage for directory objects
- Optimized for up to 30,000 objects

~USD 95.0400/mo (USD 0.1320/hr)*

* includes two domain controllers, USD 47.5200/mo for each additional domain controller.

Enterprise Edition

Best for large businesses.

- 17GB of storage for directory objects
- Optimized for up to 500,000 objects

~USD 308.1600/mo (USD 0.4280/hr)*

* includes two domain controllers, USD 154.0800/mo for each additional domain controller.

7. Then you have to give a DNS name. The DNS name could be anything which you like.
8. Then give it a password.

Directory DNS name

A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable.

Directory NetBIOS name - optional

A short identifier for your domain. If you do not specify a NetBIOS name, it will default to the first part of your Directory DNS name.

Maximum of 15 characters, can't contain spaces or the following characters: `\\/:*?<>|`. It must not start with `\\`.

Directory description - optional

Descriptive text that appears on the details page after the directory has been created.

Maximum of 128 characters, can only contain alphanumerics, and the following characters: `_@#%*+=;?.!\\^-`. It may not start with a special character.

Admin password

The password for the default administrative user named Admin.

Passwords must be between 8 and 64 characters, not contain the word "admin", and include three of these four categories: lowercase, uppercase, numeric, and special characters.

Confirm password

This password must match the Admin password above.

[Cancel](#)[Previous](#)[Next](#)

9. For the networking part, leave VPC to default and choose your Subnets accordingly.

Networking

The VPC that contains your directory. If you do not have a VPC with at least two subnets, you must create one.

VPC Info[Create new VPC](#)**Subnets Info**[Create new subnet](#)

Initial AD site name for this directory [Info](#)

Default-First-Site-Name

[Cancel](#)[Previous](#)[Next](#)

10. Now review your directory and create it.

Review & create [Info](#)

Review

Directory type
Microsoft AD

VPC
vpc-037cc333342fff6f0 (172.31.0.0/16)

Operating system version
Windows Server 2019

Subnets
subnet-02213f094a9f18cbe (172.31.16.0/20, eu-west-2a)
subnet-0beddc528873fe5fe (172.31.32.0/20, eu-west-2b)

Directory DNS name
cloudportalhub.com

Directory NetBIOS name
-

Directory description
-

Pricing

Edition
Standard

Free trial eligible [Learn more](#)

30-day limited trial

Domain controllers charge
~USD 95.0400/mo (USD 0.1320/hr)*

* Includes two domain controllers, USD 47.5200/mo for each additional domain controller.

[Cancel](#)

[Previous](#)

[Create directory](#)



STEP 2: CREATE FSx

1. Now you have to create a FSx. Search FSx and navigate to it.
2. This the dashboard for FSx.
3. Click on create file system.

The screenshot shows the Amazon FSx dashboard. At the top, there's a dark header with the text "Amazon FSx" and a subtext "Launch and run feature-rich and highly performant file systems with just a few clicks". Below this, there's a "Get started" button with an orange background and white text. To the right of the button, there's a "Pricing" section with a table showing options for NetApp ONTAP, OpenZFS, Windows File Server, and Lustre. Each option has a link and a small description. At the bottom, there are two sections: "Amazon FSx for NetApp ONTAP Getting started and documentation" and "Amazon FSx for OpenZFS Getting started and documentation", each with a "Getting started" button and a "Documentation" link.

4. Now here you have to choose Amazon FSx for windows file server. Then move to next page.

The screenshot shows the 'Select file system type' step of the AWS FSx 'Create file system' wizard. On the left, there are three navigation steps: 'Step 1 Select file system type', 'Step 2 Specify file system details', and 'Step 3 Review and create'. The main area is titled 'File system options' and contains four options:

- Amazon FSx for NetApp ONTAP (FSx^N)
- Amazon FSx for OpenZFS (FSx^Z)
- Amazon FSx for Windows File Server (FSx^W)
- Amazon FSx for Lustre (FSx^L)

Below the options, a section titled 'Amazon FSx for Windows File Server' provides a brief description: 'Amazon FSx for Windows File Server provides simple, fully managed, highly reliable file storage that's accessible over the industry-standard Server Message Block (SMB) protocol.' A bulleted list details its features:

- Broadly accessible from Windows, Linux, and macOS compute instances and devices running on AWS or on-premises
- Built on Windows Server, providing full SMB support and a wide range of administrative features like user quotas, data deduplication, and end-user file restore.
- Delivers hundreds of thousands of IOPS with consistent sub-millisecond latencies, and up to 12 GB/s of throughput.
- Offers highly-available and highly-durable single-AZ and multi-AZ deployment options, SSD and HDD storage options, and built-in, fully managed backups.
- Supports dynamic scaling of your file system to fit your storage and throughput needs, and provides cost-efficient HDD storage options.
- Integrates with Microsoft Active Directory (AD) to support Windows-based environments and enterprises.

At the bottom right of the screen are 'Cancel' and 'Next' buttons.

5. Then on the next page for creation method choose Standard create.

The screenshot shows the 'Creation method' step of the AWS FSx wizard. It offers two options:

- Quick create: 'Use recommended best-practice configurations. Most configuration options can be changed after the file system is created.'
- Standard create: 'You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.'

6. Now give a file system name to it.
7. Then select multi-AZ for the deployment.
8. Choose a storage as you wish.

File system details

File system name - optional | [Info](#)

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . _ : /

Deployment type | [Info](#)
 Multi-AZ (Recommended)
Multi-AZ file systems are recommended for most production workloads because they have two file servers in separate Availability Zones (AZ), providing continuous availability to data and helping protect your data against instance failure and AZ disruption.
 Single-AZ 2
Single-AZ 2 is the latest generation of single Availability Zone file systems, and it supports SSD and HDD storage.
 Single-AZ 1

Storage type | [Info](#)
 SSD
 HDD

SSD storage capacity | [Info](#)
 GiB
Minimum 32 GiB; Maximum 65,536 GiB

Provisioned SSD IOPS | [Info](#)
Amazon FSx provides 3 IOPS per GiB of storage capacity. You can also provision additional SSD IOPS as needed.
 Automatic (3 IOPS per GiB of SSD storage)
 User-provisioned
Minimum 96 IOPS; Maximum 80,000 IOPS

Throughput capacity | [Info](#)
The sustained speed at which the file server hosting your file system can serve data. The file server can also burst to higher speeds for periods of time.

9. Now for the network security leave it default. Just match the subnets, they should be same as of your directory.

Network & security

Virtual Private Cloud (VPC) | [Info](#)

Specify the VPC from which your file system is accessible.

vpc-037cc333342fff6f0 (CIDR: 172.31.0.0/16)



VPC Security Groups | [Info](#)

Specify VPC Security Groups to associate with your file system's network interfaces.

Choose VPC security group(s)



sg-0a37ea5df708d1925 (default)

Preferred subnet | [Info](#)

Specify the preferred subnet for your file system.

subnet-02213f094a9f18cbe (eu-west-2a | euw2-az2)



Standby subnet

subnet-0beddc528873fe5fe (eu-west-2b | euw2-az3)



10. Here chooses the directory which you have created.

11. Now directly go to the Review page and create your file system or FSx.

Windows authentication

Choose an Active Directory to provide user authentication and access control for your file system | [Info](#)

- AWS Managed Microsoft Active Directory
- Self-managed Microsoft Active Directory

AWS Managed Microsoft Active Directory | [Info](#)

cloudportalhub.com | d-9c677518ac



Create new directory

12. Remember it might take time to create, until then go and create your EC2 instance.

STEP 3: CREATE EC2 INSTANCE

1. Now navigate to EC2 and create a Windows EC2 instance.
2. While creating the instance you have to add something in the advanced options.
3. Click on the advanced options. Here you will see that you can add your directory.
4. With that you have to add an IAM role too.
5. But you didn't have it. So, you have to create an IAM role and the policies you have to attach are written below the IAM instance profile.
6. So, while you are creating your IAM add these two policies to your role.

▼ Advanced details [Info](#)

Domain join directory | [Info](#)

cloudportalhub.com	d-9c677a2c72	▼	Create new directory
VPC: vpc-037cc333342fff6f0	Shared: No		

IAM instance profile | [Info](#)

Select	▼	Create new IAM profile
Select an IAM role that has read access to Secrets Manager, and that has the following AWS managed policies attached to it: AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess. Learn more		

7. To create an IAM role, navigate to IAM, then click on role, then click on create roles.
8. Now choose AWS service.

Trusted entity type

<input checked="" type="radio"/> AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.	<input type="radio"/> AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.	<input type="radio"/> Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
<input type="radio"/> SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.	<input type="radio"/> Custom trust policy Create a custom trust policy to enable others to perform actions in this account.	

9. Then choose use case as EC2.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

Choose a use case for the specified service.

Use case

- EC2
Allows EC2 instances to call AWS services on your behalf.

10. Now add these two services.
11. Then give your role a name, and then create it.

Step 2: Add permissions

Policy name	Type	Attached as
AmazonSSMDirectoryServiceAccess	AWS managed	Permissions policy
AmazonSSMManagedInstanceCore	AWS managed	Permissions policy

12. Now come to your instance and add your IAM role to it.

▼ Advanced details [Info](#)

Domain join directory [Info](#)

cloudportalhub.com
VPC: vpc-037cc333342fff6f0 Shared: No

d-9c677a2c72



Create new directory



IAM instance profile [Info](#)

FSx-role
arn:aws:iam::463646775279:instance-profile/FSx-role

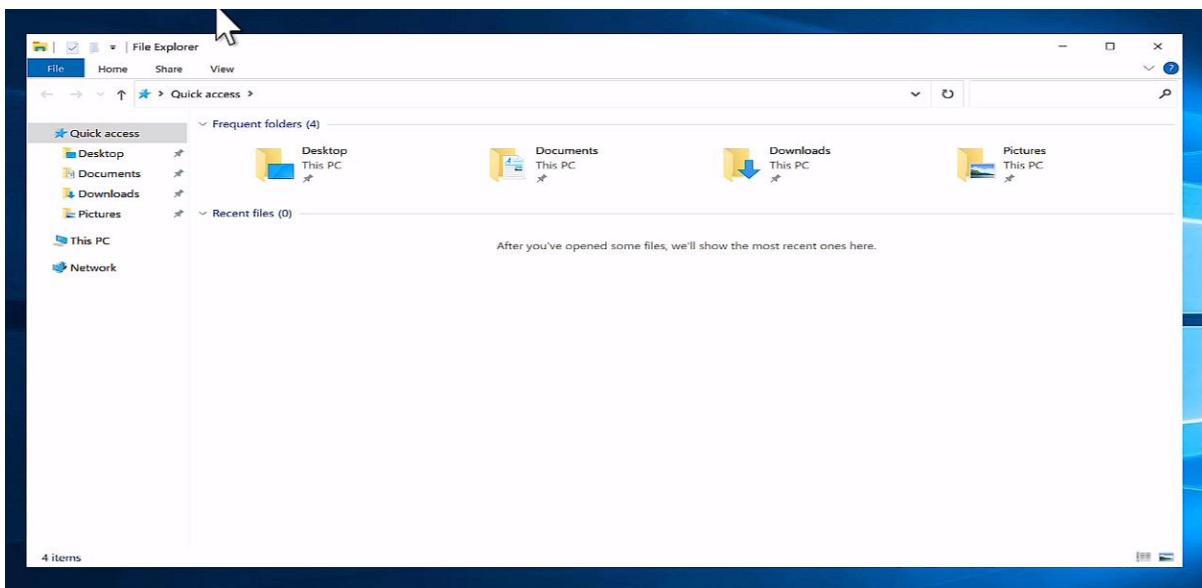


Create new IAM profile

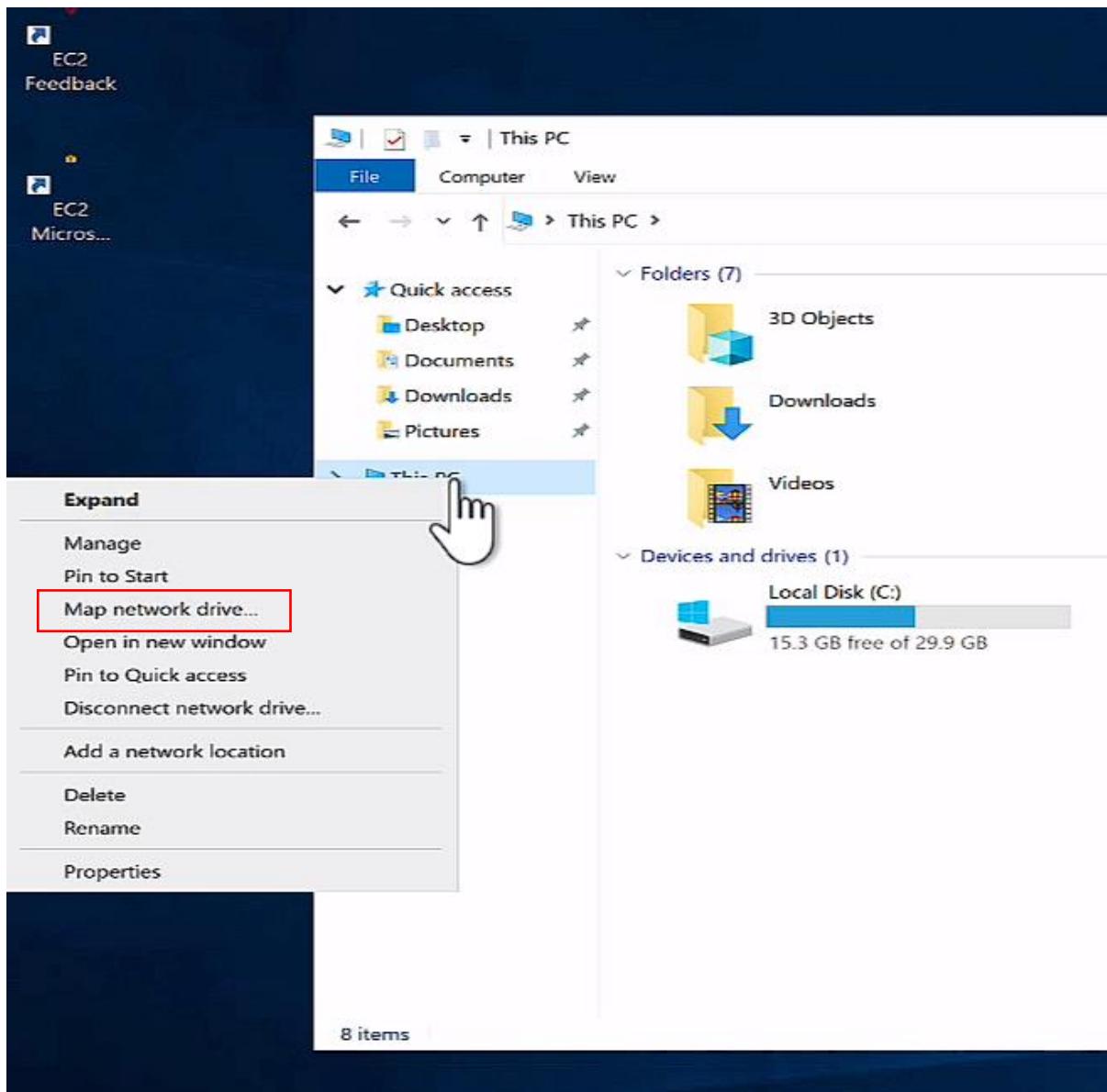


Select an IAM role that has read access to Secrets Manager, and that has the following AWS managed policies attached to it:
[AmazonSSMManagedInstanceCore](#) and [AmazonSSMDirectoryServiceAccess](#). [Learn more](#)

13. Once the role is added then just launch your instance.
14. After the instance is launched successfully, login to your instance. Do a RDP.
15. Once you are in the instance. Open your file explorer.



16. Now you have to right click on **This PC** and **choose map network drive**.



17. Now go back to the console and copy the DNS name from FSx.

DNS name

amznfsxgeym1nui.cloudportalhub.com

DNS aliases

-

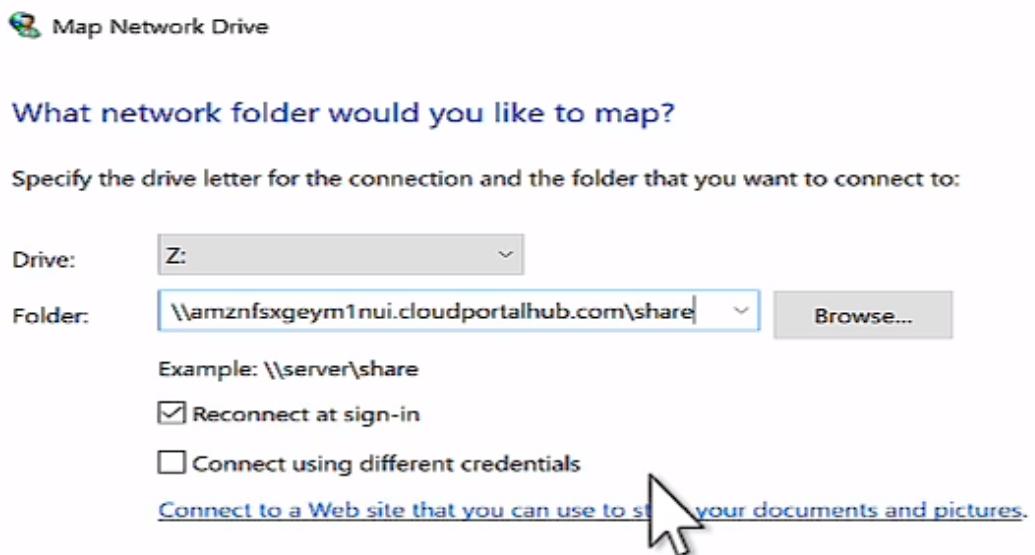
Manage

A screenshot of the AWS FSx console. It shows a message bubble with a checkmark and the word "Copied". Below it, the DNS name "amznfsxgeym1nui.cloudportalhub.com" is listed with a copy icon. There is also a "Manage" button.

18. Then paste that DNS name on the map drive. And click on finish.

19. After you have clicked on finish, it will then ask you for user name and password.

20. This user name and password is of your directory.



21. Once you have entered the user's name and password, then if you will go to This PC.
22. You will see shared file system is here for use.

