Test AS2 Protocol

how to test as2 using active diretory in transfer family write all manual step

Below is a detailed, step-by-step guide on manually testing AS2 using AWS Transfer Family when your identity provider is Active Directory. This guide assumes you have (or will set up) an AWS Managed Microsoft AD (or another Directory Service) and that you've configured your Transfer Family server to use it.

---

1. Set Up Your Active Directory Environment

1. **Deploy an AWS Directory Service**:
   - If you haven't already, create an AWS Managed Microsoft AD.
   - Note the **Directory ID**—you'll need it when creating the Transfer Family server.
2. **Create an AD User for AS2**:
   - In your Active Directory, create (or designate) a user (e.g., `AS2User`).
   - Set a strong password for this user. This account will be used by AWS Transfer Family for authentication.

---

2. Configure Your AWS Transfer Family AS2 Server

1. **Create a Transfer Family Server**:
   - In the AWS Transfer Family console, choose to create a new server.
   - **Select Protocol**: Set protocols to include `"AS2"`.
   - **Set Domain**: Use `"S3"` (if you're storing files in S3).
   - **Identity Provider Type**: Choose **AWS_DIRECTORY_SERVICE**.
   - **Provide Directory ID**: Enter the Directory ID from your AD.
   - **Set Additional Parameters**:

    - For example, configure `security_policy_name` (choose a FIPS-compliant one if needed), pre- and post-authentication banners, and other settings.
- **Endpoint Configuration**:
    - If you need internal-only access (i.e., accessible only within your VPC), select **VPC hosted** (with or without a custom hostname as desired).
    - Choose the correct VPC, subnets, and security groups.

2. **Upload Your Certificate (if applicable)**:
    - For AS2, you'll need a certificate (or multiple) for encrypting/signing messages.
    - In the Transfer Family console (or via Terraform), upload your public certificate as an AWS Transfer Certificate resource.
    - Exchange the certificate with your trading partner if needed.

---

3. Create and Configure a Transfer Family User

1. **Create a Transfer User**:
    - In the AWS Transfer Family console, create a user associated with the server.
    - **Username**: Use the AD username (e.g., `AS2User`).
      This tells AWS Transfer Family to authenticate against Active Directory.
    - **Home Directory**: Define the S3 bucket path where files should be delivered.
    - **IAM Role**: Ensure the role attached has permissions to access the S3 bucket (or EFS) where files are stored.
    - **Mapping**: AWS Transfer Family will use the AD credentials from your Directory Service to authenticate this user.

---

4. Set Up AS2 Profiles, Connector, and Agreement

1. **Create an AS2 Profile for Your Server (Local Profile)**:
    - Define an AS2 ID (e.g., `MyAS2ID`).

- Associate the certificate you uploaded to this profile.

2. **Create an AS2 Partner Profile**:
   - Define your partner's AS2 ID and attach their public certificate.
   - This simulates a trading partner.
3. **Create a Transfer Connector (AS2 Configuration)**:
   - Configure the connector with parameters like:
     - **AS2 Transports** (usually HTTP),
     - **Signing/Encryption Algorithms**,
     - **Message Subject**, and so on.
   - Ensure the connector references your local and partner profiles.
4. **Create a Transfer Agreement**:
   - Link your local AS2 profile with the partner profile using the agreement.
   - Specify the **access role** and **base directory** (this is the S3 bucket folder where files are delivered).
   - Add any tags as needed.
   - This agreement is what the Transfer Family server uses to process and route incoming AS2 messages.

---

5. Test the AS2 Transfer Using a Client

1. **Choose an AS2 Client**:
   - **Mendelson AS2** is a popular GUI-based tool.
   - Alternatively, you can use **OpenAS2** or another AS2 client.
2. **Configure the AS2 Client**:
   - **AS2 IDs**:
     - **Local AS2 ID**: Must match your server's local profile (e.g., `MyAS2ID`).
     - **Partner AS2 ID**: Must match the partner profile you created.
   - **Endpoint URL**:

- Use your Transfer Family server's AS2 endpoint URL.
  (For internal testing, you may need to run the AS2 client from an EC2 instance inside your VPC or use a VPN.)

- **Certificates**:
  - Load your certificate (for encryption/signing) as required by the client.
  - Ensure the partner's certificate is imported as well.
- **Additional AS2 Headers**:
  - Set headers such as `AS2-Version`, `Subject`, and `Disposition-Notification-To` as needed.

3. **Send a Test AS2 Message**:
   - Prepare a simple test file (like a plain text file or EDI file).
   - In the AS2 client, configure the message with the proper headers.
   - **Send the message** to your Transfer Family server.
4. **Verify the Transaction**:
   - **Check for MDN (Message Disposition Notification)**:
     - The client should receive an MDN confirming successful processing (look for status like `processed`).
   - **Confirm File Delivery**:
     - Log in to the S3 console and verify that the file has been delivered to the correct bucket and path as defined in the Transfer Agreement.
   - **Review Logs**:
     - Use **CloudWatch Logs** for your Transfer Family server and Lambda (if used for identity) to debug any issues.

---

6. Troubleshooting

- **Authentication Issues**:
  - Verify that the AD user credentials are correct.

    - Confirm that the Transfer Family server is correctly integrated with your Directory Service.
- **Certificate Errors**:
    - Ensure that the correct certificates are uploaded and associated with the proper AS2 profiles.
- **MDN Errors**:
    - Check the MDN message for error details (e.g., mismatched AS2 IDs or signature issues).
- **Network Issues (Internal Access)**:
    - For internal endpoints, make sure your AS2 client is running within the VPC (e.g., via an EC2 instance) or connected via VPN.

Final Notes

- **For internal testing**, if your Transfer Family server is not internet-accessible, you may need to run your AS2 client from an EC2 instance inside the VPC or via a VPN connection.
- The manual steps above cover all aspects—from AD integration and server/user setup to sending an AS2 message and verifying delivery to S3.

If you need additional details on any step (such as configuring your AS2 client or troubleshooting MDN responses), let me know!