HTTP Connector Demo

Introduction to Streams in Mule 4 Runtime

What are Streams?

1. Streams are used to handle large datasets efficiently in Mule 4.
2. Prevents OutOfMemoryError by processing data one row at a time instead of all at once.
3. Data is retrieved on demand, as needed.

Why Use Streams in Mule 4?

Problems with Collections:

- **Small data:** Fine to use collections (arrays, ArrayLists).
- **Large data:** Can cause OutOfMemoryError as all data is loaded into memory.

Problems with Pagination:

- Load data in chunks (pages) but if many requests access the same page, memory overload can occur.

Streams:

- Efficient way to handle large datasets without memory issues.
- Data is processed row-by-row using a cursor.

Types of Streams in Mule 4

1. Non-Repeatable Stream:
    - Data is read once and then discarded.
    - Memory-efficient as it removes data after use.

2. Repeatable In-Memory Stream:
    - Data is stored in memory (heap).
    - Suitable for small file sizes.
    - Buffer settings include:
        - Initial buffer size
        - Buffer size increment
        - Max buffer size

3. Repeatable File Store Stream:
    - Data is stored in a temporary file when the buffer is full.
    - Data is read from the temp file as needed.

Response Streaming Mode

What is Response Streaming Mode?

- Controls how data is sent back to the client.
- **AUTO (default):** Sends data in chunks or with Content-Length, depending on the response size.
- **ALWAYS:** Always sends data in chunks.
- **NEVER:** Always uses Content-Length, even for unknown sizes.

Reject Invalid Transfer Encoding Headers

Purpose: Ensures only valid transfer encoding headers are accepted, improving security.

Valid Headers:

- Chunked: Sends data in small pieces.
- Deflate: Compresses data.
- Compress: Another compression method.
- Identity: Sends uncompressed data.
- Gzip: Common compression method.

Cross-Origin Resource Sharing (CORS)

What is CORS?

- Allows sharing data between websites with different origins (e.g., different domains, subdomains, ports, or protocols).
- Uses HTTP headers to control access between websites.
- Ensures secure and controlled communication across sites.

Redelivery Policy in HTTP Listener

What is Redelivery Policy?

- Controls retries for failed message processing.
- Max Redelivery Count: Number of retries before failure.
- Use Secure Hash: Ensures secure tracking of retries.
- Object Store: Keeps track of the retry count.

HTTP Polling Source

- Acts as a timer to regularly check a website or API.
- Combines HTTP request and scheduler for event-based processing.

HTTP Basic Security Filter

Ensures only authorized users with correct credentials (username & password) can access the API.

HTTP Request & Listener

- **HTTP Request Connector:** Used to make requests to external services over the internet.
- **Listener:** Acts as a receiver for incoming requests from other systems or users.

Set up TLS (for secure communication):

Keystore: A file that holds the server's security certificates and private keys. It helps the server prove its identity.

Truststore: A file that holds certificates for trusted servers or clients. It's needed if both sides (client and server) must verify each other.

Choose how to log in (authentication):

Basic authentication: Use a username and password.

Digest authentication: Similar to Basic, but passwords are sent in a more secure, encrypted way.

NTLM authentication: A Microsoft method for logging in, often used in Windows systems.

Client Socket Properties

This tells us about how your Mule application communicates with another system over a TCP (Transmission Control Protocol) connection.

Proxy

A proxy in HTTP requests is like a middleman and it sits between your Mule app and the server. Instead of talking directly to the server, your app sends the request to the proxy, and the proxy passes it along to the server.

NTLM Proxy is when a proxy server requires a username and password (using the NTLM security system) to allow your Mule app to connect to a server. It's like the proxy asking for permission before it lets the connection happen.

Preserve Headers Case

If Preserve Headers Case is false, MuleSoft automatically changes all HTTP header names to lowercase when sending the request.

If Preserve Headers Case is true, MuleSoft keeps the exact capitalization of HTTP header names as you define them, without converting them to lowercase.

Load Static Resource

Loads specific files (e.g., webpages, scripts) from the server using HTTP Connector.

Thank You