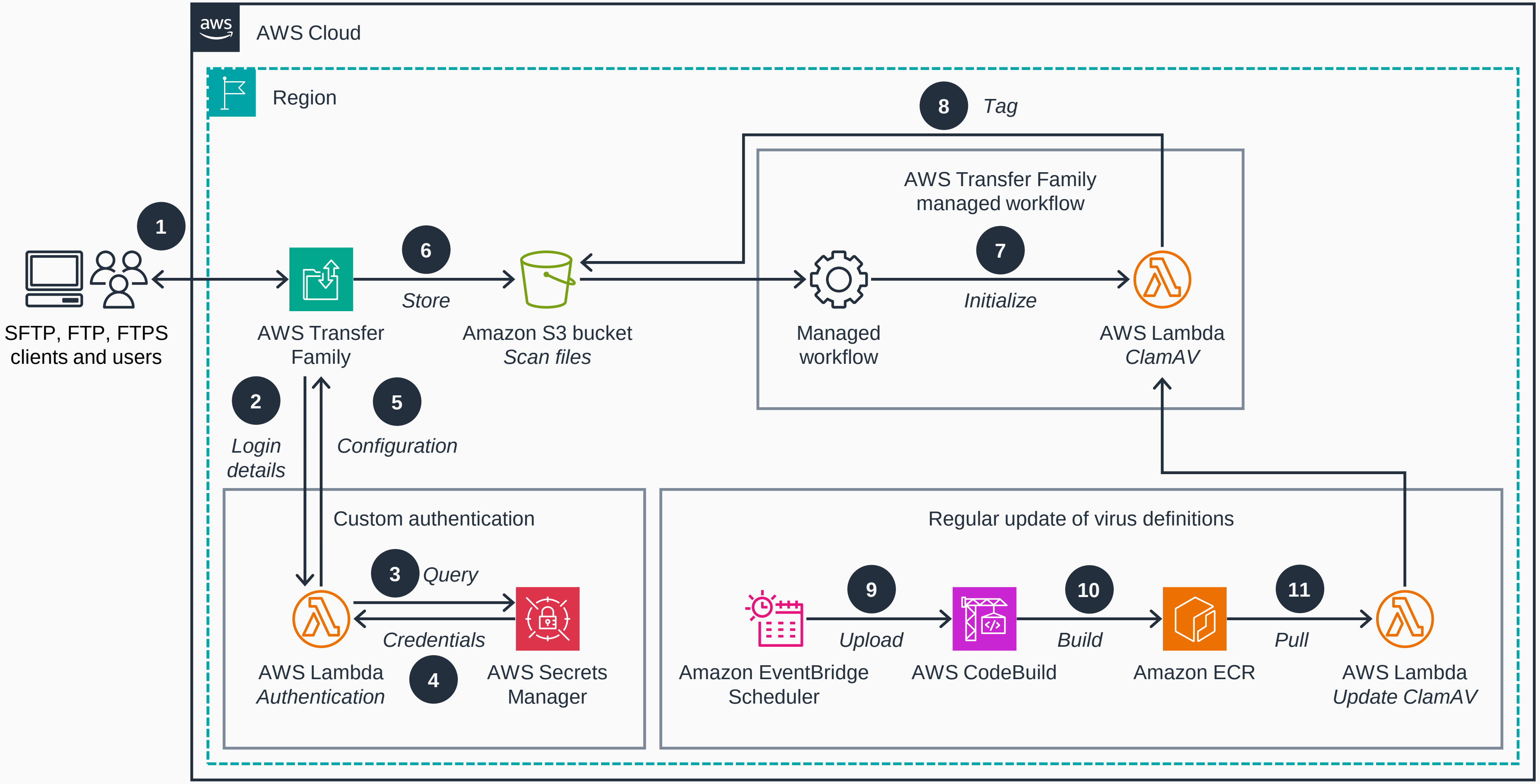
Guidance for Detecting Malware Threats Using AWS Transfer Family

This architecture diagram shows how to securely share files over Secure File Transfer Protocol (SFTP), File Transfer Protocol (FTP), and File Transfer Protocol over SSL (FTPS). It can be configured within a variety of business-to-business (B2B) workflows and industries, including retail, advertising, healthcare, and financial services. This slide details steps 1–7; refer to the next slide for steps 8-11.



1 The user sends an authentication request to the **AWS Transfer Family** server, which forwards it using a custom identity provider.

2 **Transfer Family** sends the user credentials, protocol, and IP address to an **AWS Lambda** authentication function using a password or an SSH key-based authentication (if no password is provided).

3 The authentication function sends a query to **AWS Secrets Manager** for authentication.

4 **Secrets Manager** returns the user credentials, including the stored password, the **AWS Identity and Access Management (IAM)** role mapping, the SSH key data, source IP Classless Inter-Domain Routing, and directory mappings to the authentication function.

5 The Authentication **Lambda** function verifies the login and sends user-specific configurations to **Transfer Family**.

6 The user uploads the files to the **Transfer Family** server. Each file is stored in an **Amazon Simple Storage Service (Amazon S3)** bucket. This event invokes a **Transfer Family** managed workflow implementation.

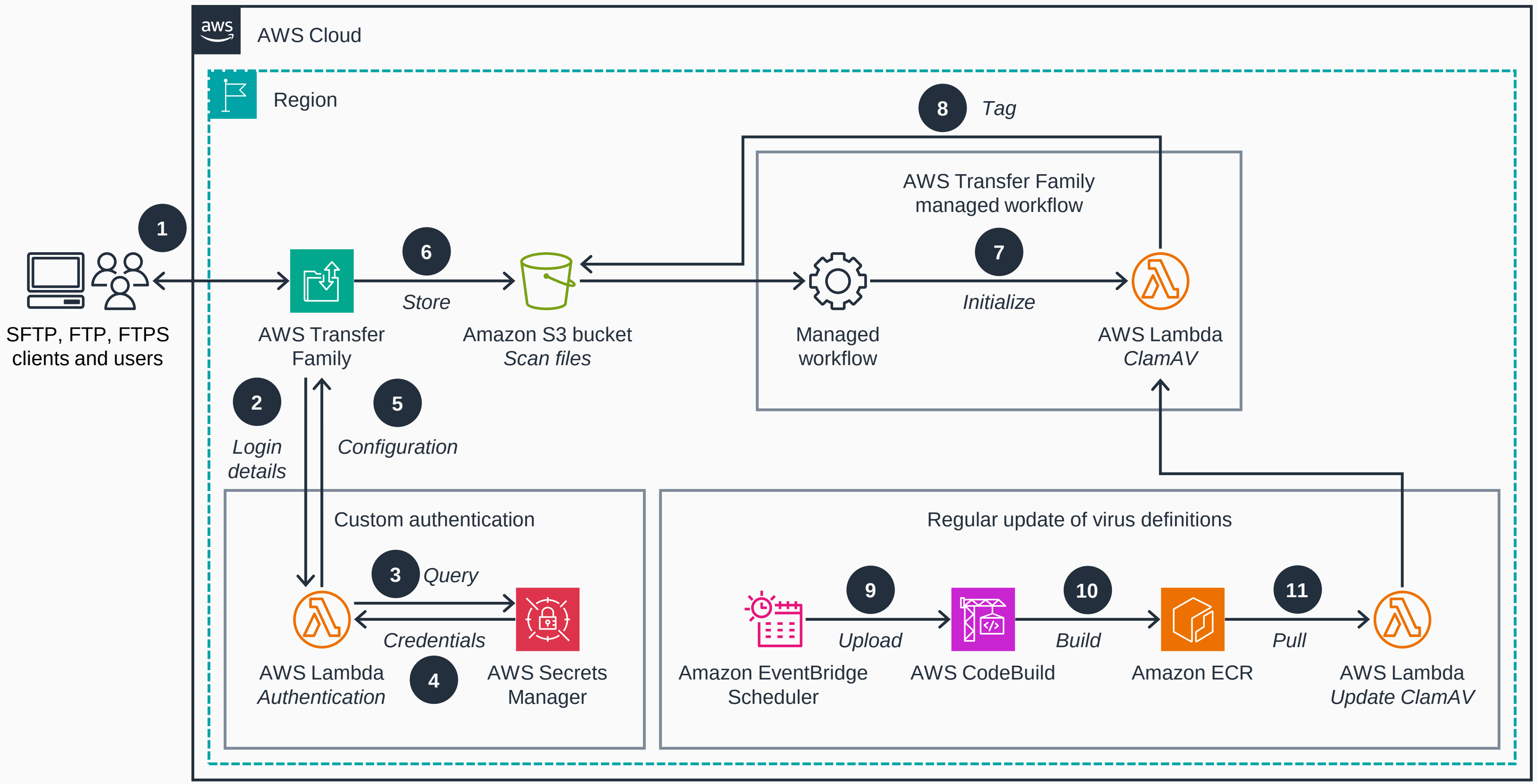
7 A **Transfer Family** managed workflow initializes a sequence of configured processing steps. In a workflow step, the ClamAV **Lambda** function scans each file using a container image with ClamAV installed.

Reviewed for technical accuracy August 21, 2024

AWS Reference Architecture

Guidance for Detecting Malware Threats Using AWS Transfer Family

Steps 8-11.



8 Based on the scan result from the ClamAV **Lambda** function, the managed workflow tags the scanned files as either “infected” or “clean” in the same **Amazon S3** bucket as in Step 6. (Infected objects cannot be downloaded.)

9 In **Amazon EventBridge**, an Amazon EventBridge Scheduler rule is configured to run based on a cron expression to update the ClamAV image and virus definition by means of an automated pipeline.

10 An **AWS CodeBuild** pipeline builds the container image with the latest ClamAV virus definitions and uploads it to **Amazon Elastic Container Registry (Amazon ECR)**.

11 A **Lambda** Update ClamAV function pulls the newly built container image from **Amazon ECR** and updates the container image in the ClamAV function, which is a part of the managed workflow.

Reviewed for technical accuracy August 21, 2024

AWS Reference Architecture