**Question 3: Explain the differences between Active Directory, Azure Active Directory, and Azure AD Domain Services (ADDS), and recommend which one(s) would be suitable for this scenario.**

**Answer: Active Directory (AD)**

**Overview:**

* On-Premises directory service developed by Microsoft.
* Manages user identities, authentication, and authorization within a corporate network.
* Provides a centralized way to manage user accounts, groups, computers, and other resources.

**Key Features:**

* Supports Group Policy for centralized management of Windows devices.
* Offers directory services for on-premises applications and file sharing.
* Integrates with traditional Windows-based services and infrastructure.

**Use Case:**

* Suitable for organizations with an on-premises infrastructure that need a local domain controller for user management and access control.

**Azure Active Directory (Azure AD)**

**Overview:**

* Cloud-based identity and access management service provided by Microsoft.
* Designed for managing users and applications in the cloud, providing single sign-on (SSO) and access control.

**Key Features:**

* Supports cloud-based applications, including Office 365, SaaS applications, and custom apps.
* Provides authentication through protocols like OAuth, OpenID Connect, and SAML.
* Offers features such as Multi-Factor Authentication (MFA), Conditional Access, and Identity Protection.
* Integrates with on-premises AD for hybrid scenarios.

**Use Case:**

* Ideal for managing cloud-based resources, SaaS applications, and providing identity services to cloud applications. It’s commonly used for modern applications and services in the cloud.

**Azure Active Directory Domain Services (Azure AD DS)**

**Overview:**

* Provides managed domain services like domain join, group policy, and LDAP/NTLM authentication without the need for on-premises AD infrastructure.
* Runs in the cloud and integrates with Azure AD.

**Key Features:**

* Offers domain-join capability for virtual machines and applications hosted in Azure.
* Supports legacy applications that require domain services such as group policies and Kerberos/NTLM authentication.
* Ideal for applications that need traditional Active Directory features but are running in Azure.

**Use Case:**

* Suitable for scenarios where you need to lift-and-shift legacy applications to the cloud without modifying them to work with Azure AD. Useful if you need domain join or group policy management in a cloud environment without setting up and managing a traditional AD domain controller.

**Recommendation for Media Processing Application**

For the media processing application scenario described:

**Azure Active Directory (Azure AD):**

* **Recommended:** For managing user identities, access control, and authentication to cloud-based resources, applications, and services. Azure AD will handle authentication and authorization for the cloud-based application and provide SSO for users.

**Azure Active Directory Domain Services (Azure AD DS):**

* **Consider if needed:** If the media processing application has legacy components or specific requirements for domain services that can’t be accommodated by Azure AD alone. For instance, if you have legacy applications or services running in Azure VMs that require domain-join capabilities or traditional Active Directory features, Azure AD DS could be beneficial.

Basically, for a cloud-based media processing application, **Azure AD** is generally the best choice for managing users and access in the cloud. Azure AD DS might be considered if there are specific requirements for legacy domain services in a cloud environment.