Filename: microsoft-ms101-10-2-1-plan-for-deployment-on-prem-rights-management-connector
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Azure Information Protection (AIP)
EpisodeName: Plan for Deployment On-Prem Rights Management Connector
Description: Adam and Wes discuss the steps necessary to help you successfully plan for deployment of the On-Prem Rights Management Connector.

Plan for Deployment On-Prem Rights Management Connector

Manage Microsoft 365 Governance and Compliance (35-40%)

Implement Azure Information Protection (AIP)
• Plan AIP Solution
• Plan for Deployment On-Prem Rights Management Connector
• Plan for Windows Information Protection (WIP) Implementation
• Plan for Classification Labeling
• Configure Information Rights Management (IRM) for Workloads
• Configure Super User
• Deploy AIP Clients
• Implement Azure Information Protection Policies
• Implement AIP Tenant Key

==========

Plan for Deployment On-Prem Rights Management Connector

This connector acts as a communications interface (a relay) between the on-premises servers and the Azure Rights Management service that is used by Azure Information Protection to protect Office documents and emails.

To use this connector, you must configure directory synchronization between your Active Directory forests and Azure Active Directory.

```
Exchange Server:

    • Exchange Server 2016
    • Exchange Server 2013
    • Exchange Server 2010
```

Office SharePoint Server:

```
    • Office SharePoint Server 2016
    • Office SharePoint Server 2013
    • Office SharePoint Server 2010


File servers that run Windows Server and use File Classification
```

Infrastructure (FCI):

```
    • Windows Server 2016
    • Windows Server 2012 R2
    • Windows Server 2012
```

NOTE: Because file servers that run Windows Server 2008 R2 do not have a built-in file management task action to apply Rights Management protection, you cannot use the Rights Management connector for this scenario.

However, you can use File Classification Infrastructure and Azure RMS on these operating systems if you configure a custom file management task to run an executable or script that can protect files by using Azure RMS.

If you want to protect multiple file types (not just Office documents) by using File Classification Infrastructure, do not use the RMS connector, but instead, use the AzureInformationProtection cmdlets.

What are the Prerequisites for the RMS connector?

```
    Prerequisites for the RMS connector.docx
```

What are the steps to install and configuring the Azure Rights Management connector?

https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector

NOTE: the admin account used to configure the RMS Connector MUST NOT be configured to require Multi-factor Authentication, because the tool does not support it.

In addition, if you use Azure AD Conditional Access, do not block legacy authentication for this account.

The connector also has some character restrictions for this password.

You cannot use a password that has any of the following characters:

Ampersand (&); left angle bracket ([ ); right angle bracket ( ]); straight quotation ("); and apostrophe (')