To enable File Integrity Monitoring (FIM) on on-premises Windows and Linux servers using Azure Monitor and the Azure Monitor Agent (AMA), follow these steps:

## Prerequisites

1. **Azure Subscription**: Ensure you have an active Azure subscription.
2. **Onboarding Servers to Azure Monitor**: The servers (both Windows and Linux) must be onboarded to Azure Monitor.
3. **Log Analytics Workspace**: Create a Log Analytics Workspace in Azure, if not already available.
4. **Permissions**: Ensure you have the necessary permissions to configure and manage Azure Monitor and Log Analytics.

## Step-by-Step Guide

### 1. Create and Configure Log Analytics Workspace

1. **Create Log Analytics Workspace**:
   - Go to the Azure portal.
   - Search for and select "Log Analytics workspaces".
   - Click "Add" to create a new workspace. Fill in the required details and create the workspace.
2. **Get Workspace ID and Key**:
   - Navigate to the created Log Analytics workspace.
   - Go to "Agents management".
   - Note down the "Workspace ID" and "Primary Key".

### 2. Install Azure Monitor Agent (AMA)

**For Windows Servers**:

1. **Download and Install Agent**:
   - Download the Azure Monitor Agent installer from the Azure portal.
   - Run the installer on your Windows server.
   - During installation, select "Connect the agent to Azure Monitor".
   - Provide the Workspace ID and Primary Key you noted earlier.

**For Linux Servers**:

1. **Install the Azure Monitor Agent**:
   - Run the following commands on your Linux server to download and install the AMA
   - wget https://aka.ms/InstallAzureMonitorAgentLinux

- bash InstallAzureMonitorAgentLinux.sh --workspace-id <Workspace ID> --workspace-key <Primary Key>

Replace <Workspace ID> and <Primary Key> with your specific details.

### 3. Configure Data Collection Rules for FIM

1. **Create Data Collection Rule (DCR)**:
   - In the Azure portal, navigate to "Azure Monitor".
   - Go to "Data Collection Rules" under "Settings".
   - Click "Create" to create a new DCR.
2. **Configure File Integrity Monitoring**:
   - Define the data sources. For FIM, specify the paths to monitor for file changes.
   - Add the Windows or Linux servers as targets for this rule.
   - Save and apply the DCR.

### 4. Deploy the FIM Configuration

1. **Assign the DCR to the Servers**:
   - Ensure that the DCR created for FIM is assigned to the Windows and Linux servers.

### 5. Set Up Alerts

1. **Navigate to Azure Monitor**:
   - In the Azure portal, go to "Azure Monitor".
2. **Create an Alert Rule**:
   - Go to "Alerts" and then "New alert rule".
   - Define the condition based on the logs collected from FIM.
   - Specify the action group that will handle the alert (e.g., sending an email, triggering an automation, etc.).
   - Name and create the alert rule.

## Verification

1. **Verify Agent Status**:
   - Ensure that the Azure Monitor Agent on your servers is successfully connected and sending data to Azure Monitor.
2. **Monitor FIM Alerts**:
   - Regularly check the Azure Monitor logs and alerts to ensure FIM is functioning correctly and capturing file changes.