Azure Automanage Machine Configuration (formerly Azure Policy Guest Configuration) integrates with Azure Policy to provide management and automation VMs.

Pros:

* Centralized configuration management: Manage VM configurations from a single location, ensuring consistency and compliance.
* Code-based configuration: Define configurations using scripts
* Granular control: Target specific groups of VMs with customized configurations based on their roles or requirements. Apply to a management group, subscription, or resource group.
* Auditing and reporting: Track configuration compliance and generate reports for improved visibility and control.

Cons:

* Limited platform support: Currently supports Windows and Linux, not other operating systems.
* Potential security risks: Improperly configured scripts could introduce security risks.
* Reliance on Guest Configuration Extension: VMs require the extension installed and running for policies to be applied.
* Cost: Pay-per-server, per-month pricing model can be expensive for large deployments.

Key Points:

* Change tracking is not available when using AAMC independently.
* Enroll in Azure Automanage to access the change tracking feature.

Configuration process:

1. Prerequisites:
   * An Azure subscription with the Microsoft.GuestConfiguration resource provider registered.
   * VMs with the Azure Policy Guest Configuration extension installed and enabled.
   * Define your desired configuration settings and security policies.
2. Create an Azure Policy definition:
   * Use the Azure portal or tools like Azure CLI or PowerShell to create a policy definition.
   * Define the policy parameters, including the configuration profile (DevTest, Production, or Custom) and any applicable settings.
3. Enable Automanage for VMs:
   * Choose the appropriate built-in policy depending on your configuration profile:
   * "Configure virtual machines to be onboarded to Azure Automanage (DevTest or Production)"
   * "Configure virtual machines to be onboarded to Azure Automanage with Custom Configuration Profile"
   * Assign the chosen policy to the desired management group, subscription, or resource group.
4. Optional: Create a custom configuration profile (if using the custom policy):
   * Define the specific configuration settings you want to apply to your VMs in a JSON file.
   * Upload the JSON file to Azure and reference it in the custom policy definition.
5. Monitor and manage:
   * Use Azure Policy and Azure Monitor to track policy compliance and VM health.
   * Manage assigned configurations and adjust policies as needed.

You cannot directly use Azure Automanage Machine Configuration (AAMC) without Azure Automanage and still have the change tracking feature.

* Change Tracking is a feature specifically integrated within Azure Automanage: It's designed to track configuration changes made to VMs that are enrolled in the Automanage service.
* AAMC, when used standalone, doesn't include this feature: It focuses primarily on applying configurations, not on monitoring changes.

To achieve change tracking, you have two options:

1. Enroll your VMs in Azure Automanage: This enables you to leverage the integrated change tracking feature, along with other benefits like automated patching and configuration management.
2. Utilize alternative change tracking solutions but this are adding complexity into the tracking process:
   * Azure Activity Log: Provides a general log of activities across your Azure resources, including configuration changes.
   * Azure Monitor: Configure alerts and log queries to track specific configuration changes.