**Azure Monitor**

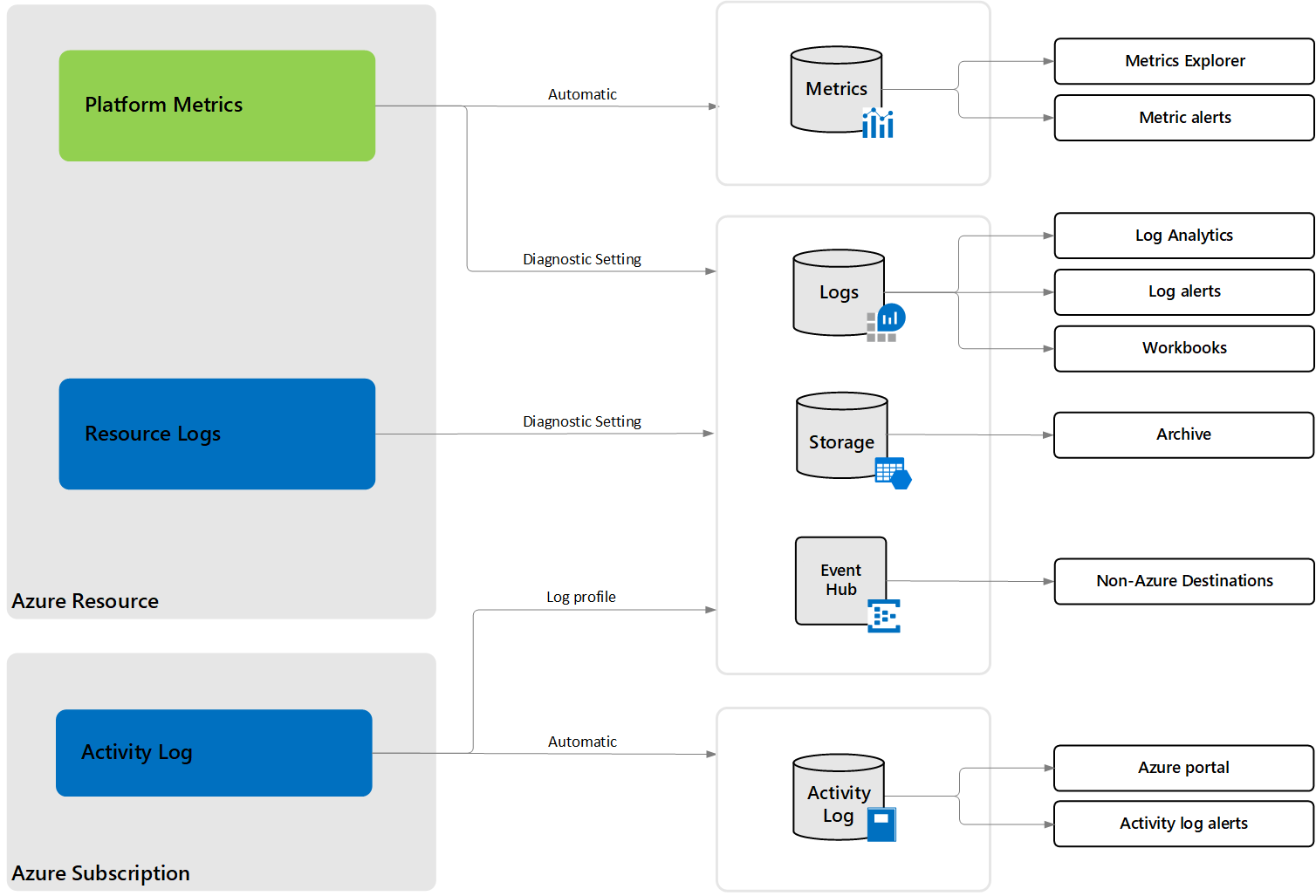
Monitor Azure + other cloud + on premise

Apply to all services but VM + app services also have guest OS that can generate logs and metrics

As soon as you create a resource, Azure Monitor is enabled and starts collecting metrics and Activity logs. No cost for monitoring on data collected / default

Time-series DB

(Table AzureActivity)



From inside.

Generated auto

Not collected

From outside.

Management Pane

**Platform logs = Activity log + Resource log + AAD logs (sign in, audit change…)**

You may need to collect more information (metrics and logs).

Use: **Diagnostic settings, Insights, Solutions**

**Insights =** “tools” beyond the standard features of Azure monitor.

**Solutions =** complementary solutions from marketplace that can integrate with Azure monitor (can be Microsoft or third party).

**Diagnostic settings:** define Where platform logs and metrics should be sent.

3 destinations possible:

1. Log Analytic Workspace (consolidate from multiple tenants / subscriptions) + keep more than default delay.
2. Azure storage (dedicated is better): audit static analysis + immutable + same region as resource.
3. Event Hub: store out of Azure, SIEM, other log analytic solution.

Each Azure resource require its own diagnostic setting.

* A single diagnostic => a single destination
* Each resource can have up to 5 diagnostic settings.

Where to configure:

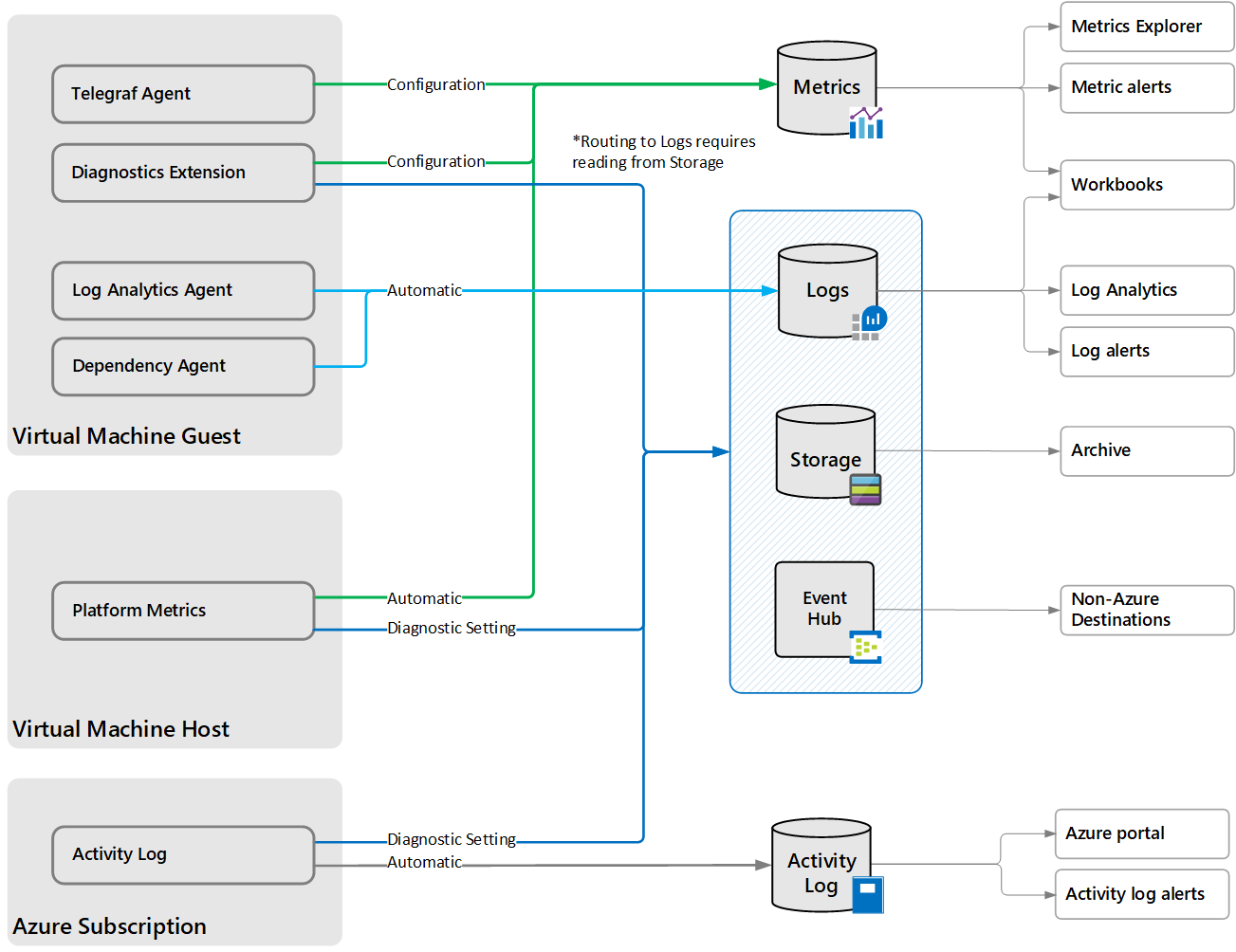
* Resource by resource : portal -> resource -> monitor -> diag settings
* Multi resources: Azure monitor -> settings -> diag settings
* Specific to Activity log: see menu bar and button “Diag settings”.

**Monitor Azure VM guest OS metrics AND logs using VM diagnostic settings**

Platform metrics collected only for VM Host => use agents to collect metrics for Guest OS.

VMs don’t generate resource logs => use agents to collect logs for Guest OS.

Diagnostic settings are changing for VM with better wizard and simultaneous integration with storage account (mandatory) + insights + log analytic workspace.



WAD / LAD

**Guest OS agents:**

[***Azure Diagnostic extension***](https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#azure-diagnostics-extension)(WAD / LAD) - used to collect guest performance data from Azure Vm (only) and send them to Azure Monitor Metrics, Storage account or event Hub for WAD and Azure monitor metrics for LAD.

Collect: (WAD) event log, ETW event performance, IIS logs, .Net app logs, Crash dumps, File based logs and (LAD) Syslog perf

***(Influx)*** [***Telegraf agent***](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/collect-custom-metrics-linux-telegraf)  - Collect performance data from {Azure, on-prem and other clouds} Linux VMs into Azure Monitor Metrics

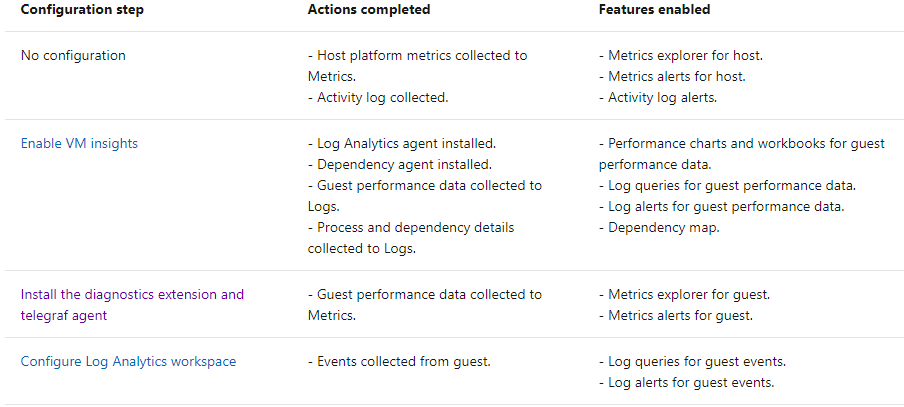
[***Log Analytics agent***](https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent) ***(MMA Microsoft Monitoring Agent) –*** Collect same data as WAD/LAD + insights + solutions from {Azure, on-prem and other clouds} L/W VMs and send them to azure monitor log. Same agent used for SCOM.

[***Dependency agent***](https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#dependency-agent) - Require MMA to transmit data into Azure.Collects data about the processes running on L/W VMs located in {Azure, on-prem, other clouds}.

***NEW! Azure monitor agent*** - used to replace WAD / LAD, MMA, Telegraf, and dependency agents.

<https://docs.microsoft.com/fr-fr/azure/azure-monitor/agents/azure-monitor-agent-overview>

The Log Analytics agent for Windows is often referred to as Microsoft Monitoring Agent (MMA). The Log Analytics agent for Linux is often referred to as OMS agent.



**To install the diagnostic extension agent (WAD):**

Portal -> VM -> monitoring -> Diagnostic settings -> enable guest-level monitoring

**To install the Telegraf agent**

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/collect-custom-metrics-linux-telegraf>

**To install the Log analytics agent**

setup a log analytic workspace and install agent from the workspace data sources to VM OR use Insights (automatic install)

**To install the dependency agent**

<https://docs.microsoft.com/fr-fr/azure/virtual-machines/extensions/agent-dependency-windows>

OR use Insights (automatic install)

**To install the new Azure Monitor Agent (AMA)**

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-install?tabs=ARMAgentPowerShell%2CPowerShellWindows%2CPowerShellWindowsArc%2CCLIWindows%2CCLIWindowsArc