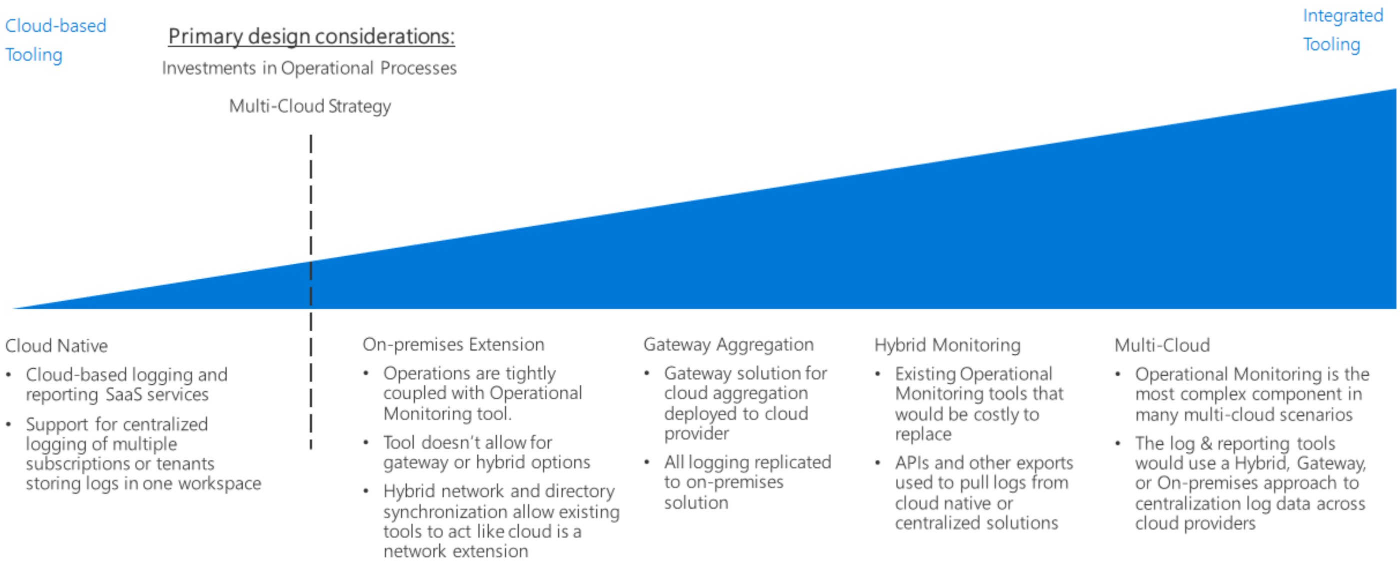
Logging and reporting decision guide

02/11/2019 • 7 minutes to read • Contributors

In this article

All organizations need mechanisms for notifying IT teams of performance, uptime, and security issues before they become serious problems. A successful monitoring strategy allows you to understand how the individual components that make up your workloads and networking infrastructure are performing. Within the context of a public cloud migration, integrating logging and reporting with any of your existing monitoring systems, while surfacing important events and metrics to the appropriate IT staff, is critical in ensuring your organization is meeting uptime, security, and policy compliance goals.



Cloud-based Tooling
Primary design considerations:
Investments in Operational Processes
Multi-Cloud Strategy
Integrated Tooling
Cloud Native
• Cloud-based logging and reporting SaaS services
• Support for centralized logging of multiple subscriptions or tenants storing logs in one workspace
On-premises Extension
• Operations are tightly coupled with Operational Monitoring tool.
• Tool doesn't allow for gateway or hybrid options
• Hybrid network and directory synchronization allow existing tools to act like cloud is a network extension
Gateway Aggregation
• Gateway solution for cloud aggregation deployed to cloud provider
• All logging replicated to on-premises solution
Hybrid Monitoring
• Existing Operational Monitoring tools that would be costly to replace
• APIs and other exports used to pull logs from cloud native or centralized solutions
Multi-Cloud
• Operational Monitoring is the most complex component in many multi-cloud scenarios
• The log & reporting tools would use a Hybrid, Gateway, or On-premises approach to centralization log data across cloud providers

Jump to: Planning your monitoring infrastructure | Cloud-native | On-premises extension | Gateway aggregation | Hybrid monitoring (on-premises) | Hybrid monitoring (cloud-based) | Multicloud | Learn more

The inflection point when determining a cloud logging and reporting strategy is based primarily on existing investments your organization has made in operational processes, and to some degree any requirements you have to support a multicloud strategy.

There are multiple ways to log and report on activities in the cloud. Cloud-native and centralized logging are two common software as a service (SaaS) options that are driven by the subscription design and the number of subscriptions.

Planning your monitoring infrastructure

When planning your deployment, you need to consider where logging data is stored and how you will integrate cloud-based reporting and monitoring services with your existing processes and tools.

Question	Cloud-native	On-premises extension	Hybrid monitoring	Gateway aggregation

Question	Cloud-native	On-premises extension	Hybrid monitoring	Gateway aggregation
Do you have an existing on-premises monitoring infrastructure?	No	Yes	Yes	No
Do you have requirements preventing storage of log data on external storage locations?	No	Yes	No	No
Do you need to integrate cloud monitoring with on-premises systems?	No	No	Yes	No
Do you need to process or filter telemetry data before submitting it to your monitoring systems?	No	No	No	Yes

Cloud-native

If your organization currently lacks established logging and reporting systems, or if your planned deployment does not need to be integrated with existing on-premises or other external monitoring systems, a cloud-native SaaS solution such as Azure Monitor, is the simplest choice.

In this scenario, all log data is recorded and stored in the cloud, while the logging and reporting tools that process and surface information to IT staff are provided by the Azure platform and Azure Monitor.

CustomAzure Monitor-based logging solutions can be implemented ad hoc for each subscription or workload in smaller or experimental deployments, and are organized in a centralized manner to monitor log data across your entire cloud estate.

Cloud-native assumptions. Using a cloud-native logging and reporting system assumes the following:

- You do not need to integrate the log data from you cloud workloads into existing on-premises systems.
- You will not be using your cloud-based reporting systems to monitor on-premises systems.

On-premises extension

It may require substantial redevelopment effort for applications and services migrating to the cloud to make use of cloud-based logging and reporting solutions such as Azure Monitor. In these cases it may make sense to allow these workloads to continue to send telemetry data to existing on-premises systems.

To support this approach, your cloud resources will need to be able to communicate directly with your on-premises systems through a combination of hybrid networking and cloud hosted domain services. With this in place, the cloud virtual network functions as a network extension of the on-premises environment. Therefore, cloud hosted workloads can communicate directly with your on-premises logging and reporting system.

This approach capitalizes on your existing investment in monitoring tooling with limited modification to any cloud-deployed applications or services. This is often the fastest approach to support monitoring during a "lift and shift" migration. However, it won’t capture log data produced by cloud-based PaaS and SaaS resources, and it will omit any VM-related logs generated by the cloud platform itself such as VM status. As a result, this pattern should be a temporary solution until a more comprehensive hybrid monitoring solution is implemented.

On-premises–only assumptions:

- You need to maintain log data only in your on-premises environment only, either in support of technical requirements or due to regulatory or policy requirements.
- Your on-premises systems do not support hybrid logging and reporting or gateway aggregation solutions.

- Your cloud-based applications can submit telemetry directly to your on-premises logging systems or monitoring agents that submit to on-premises can be deployed to workload VMs.
- Your workloads don't depend on PaaS or SaaS services that require cloud-based logging and reporting.

Gateway aggregation

For scenarios where the amount of cloud-based telemetry data is large or existing on-premises monitoring systems need log data modified before it can be processed, a log data gateway aggregation service may be required.

A gateway service is deployed to your cloud provider. Then, relevant applications and services are configured to submit telemetry data to the gateway instead of a default logging system. The gateway can then process the data: aggregating, combining, or otherwise formatting it before then submitting it to your monitoring service for ingestion and analysis.

Also, a gateway can be used to aggregate and preprocess telemetry data bound for cloud-native or hybrid systems.

Gateway aggregation assumptions:

- You expect large volumes of telemetry data from your cloud-based applications or services.
- You need to format or otherwise optimize telemetry data before submitting it to your monitoring systems.
- Your monitoring systems have APIs or other mechanisms available to ingest log data after processing by the gateway.

Hybrid monitoring (on-premises)

A hybrid monitoring solution combines log data from both your on-premises and cloud resources to provide an integrated view into your IT estate's operational status.

If you have an existing investment in on-premises monitoring systems that would be difficult or costly to replace, you may need to integrate the telemetry from your cloud workloads into preexisting on-premises monitoring solutions. In a hybrid on-premises monitoring system, on-premises telemetry data continues to use the existing on-premises monitoring system. Cloud-based telemetry data is either sent to the on-premises monitoring system directly, or the data is sent to Azure Monitor then compiled and ingested into the on-premises system at regular intervals.

On-premises hybrid monitoring assumptions. Using an on-premises logging and reporting system for hybrid monitoring assumes the following:

- You need to use existing on-premises reporting systems to monitor cloud workloads.
- You need to maintain ownership of log data on-premises.
- Your on-premises management systems have APIs or other mechanisms available to ingest log data from cloud-based systems.

> **Tip**
>
> As part of the iterative nature of cloud migration, transitioning from distinct cloud-native and on-premises monitoring to a partial hybrid approach is likely as the integration of cloud-based resources and services into your overall IT estate matures.

Hybrid monitoring (cloud-based)

If you do not have a compelling need to maintain an on-premises monitoring system, or you want to replace on-premises monitoring systems with a centralized cloud-based solution, you can also choose to integrate on-premises log data with Azure Monitor to provide centralized cloud-based monitoring system.

Mirroring the on-premises centered approach, in this scenario cloud-based workloads would submit telemetry direct to Azure Monitor, and on-premises applications and services would either submit telemetry directly to Azure monitor, or aggregate that data on-premises for ingestion into Azure Monitor at regular intervals. Azure Monitor would then serve as your primary monitoring and reporting system for your entire IT estate.

Cloud-based hybrid monitoring assumptions: Using cloud-based logging and reporting systems for hybrid monitoring assumes the following:

- You don't depend on existing on-premises monitoring systems.
- Your workloads do not have regulatory or policy requirements to store log data on-premises.
- Your cloud-based monitoring systems have APIs or other mechanisms available to ingest log data from on-premises applications and services.

Multicloud

Integrating logging and reporting capabilities across a multiple-cloud platform can be complicated. Services offered between platforms are often not directly comparable, and logging and telemetry capabilities provided by these services differ as well. Multicloud logging support often requires the use of gateway services to process log data into a common format before submitting data to a hybrid logging solution.

Learn more

Azure Monitor is the default reporting and monitoring service for Azure. It provides:

- A unified platform for collecting app telemetry, host telemetry (such as VMs), container metrics, Azure platform metrics, and event logs.
- Visualization, queries, alerts, and analytical tools. It can provide insights into virtual machines, guest operating systems, virtual networks, and workload application events.
- REST APIs for integration with external services and automation of monitoring and alerting services.
- Integration with many popular third-party vendors.

Next steps

Logging and reporting is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. Visit the decision guides overview to learn about alternative patterns or models used when making design decisions for other types of infrastructure.

Architectural decision guides