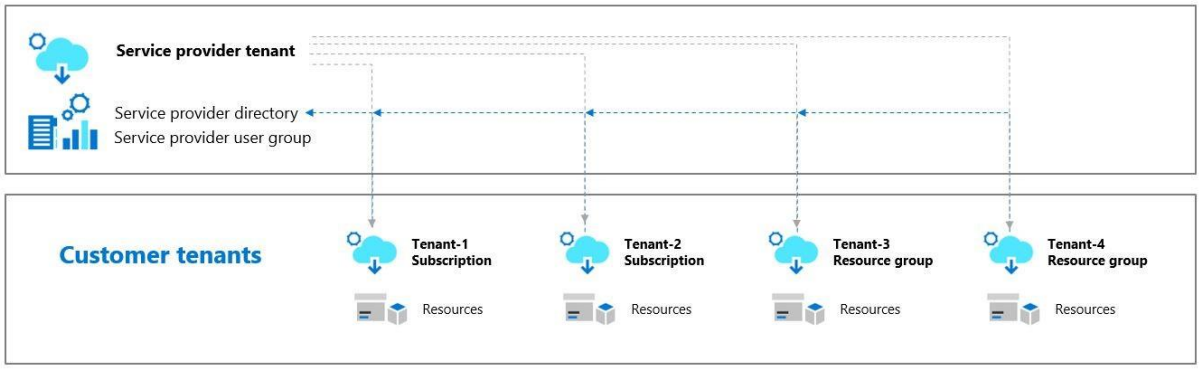
DSI Custom Monitoring Framework

DSI Managed Services implement a custom monitoring solution to provide visibility into the performance and operation of all the client solutions we build and subsequently manage. This enables the DSI Managed Services team to view both platform and application status and operational performance information and receive alerts to out-of-tolerance events in a single platform.

1. ARCHITECTURE

1. Azure Lighthouse

The DSI monitoring solution uses Azure Lighthouse to enable DSI to manage client environments at scale. Azure Lighthouse enables multi-tenant management with scalability, higher automation, and enhanced governance across resources. With Azure Lighthouse, DSI can deliver managed services using comprehensive and robust tooling built into the Azure platform. As a result, customers maintain control over who has access to their tenant, which resources they can access, and what actions can be taken.



With Azure Lighthouse, DSI can: -

- View alerts for delegated client subscriptions, with the ability to view and refresh alerts across all subscriptions.
- View activity log details for delegated client subscriptions.
- Query data from remote client Log Analytics workspaces.
- Create, view, and manage metric alerts, log alerts, and activity log alerts in client tenants.
- Create alerts in client tenants that trigger automation, such as Azure Automation runbooks or Azure Functions, in the DSI tenant.

2. Azure Monitor

The data source for the DSI monitoring solution leverages Azure Monitor, which is a comprehensive solution for collecting, analyzing, and acting on telemetry from the cloud and on-premises environments configured in your Azure environment. This information helps DSI Managed Services understand how solutions are performing and proactively identify issues affecting them and the resources they depend on. Just a few examples of what you can do with Azure Monitor include: -

- Detect and diagnose issues across applications and dependencies with Application Insights.
- Correlate infrastructure issues with VM insights and Container insights.
- Drill into monitoring data with Log Analytics for troubleshooting and deep diagnostics.
- Support operations at scale with smart alerts and automated actions.
- Create visualizations with Azure dashboards and workbooks.
- Collect data from monitored resources using Azure Monitor Metrics.

Azure Monitor provides base-level infrastructure metrics, alerts, and logs for all Azure services. Azure diagnostic logs are emitted by a resource and provide rich, frequent data about the operation of that resource. These can be augmented with custom information sent from any application.

3. Log Data Sources

Azure Monitor Logs is a feature of Azure Monitor that collects and organizes log and performance data from monitored resources. Data from multiple sources can be consolidated into a single workspace. These sources include: -

- Platform logs from Azure services.
- Log and performance data from virtual machine agents.
- Usage and performance data from applications via Application Insights.
- Custom log data, ingested via the Azure Monitor Data Collector API.

4. Application Insights

Application Insights is a feature of Azure Monitor that provides extensible application performance management (APM) and monitoring for live web apps, enabling DSI to perform the following for any application developed and hosted in Azure: -

- Automatically detect performance anomalies.
- Help diagnose issues by using powerful analytics tools.
- See what users actually do with apps.
- Help continuously improve app performance and usability.

Application Insights: -

- Supports a wide variety of platforms, including .NET, Node.js, Java, and Python.
- Works for apps hosted on-premises, hybrid, or on any public cloud.
- Integrates with DevOps processes.
- Has connection points to many development tools.
- Can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

Full integration between Application Insights and Log Analytics allows full access to all the features of Log Analytics while keeping application, infrastructure, and platform logs in a single consolidated location.

5. Data Analytics & Power BI

1. Data Engineering

Within any Azure Data Factory, or Synapse Analytics data movement pipelines, Databricks notebooks, or other aspects of an analytics solution custom log details need to be recorded to indicate the details of any success or failure of any process, the state of any data quality or validity checks, or any other information other than that available from the data ingested by Log Analytics by default, pertinent for support, tuning and maintenance.

The Azure Monitor Data Collector API enables DSI to capture custom telemetry to Log Analytics from the data integration solutions we build, allowing us to obtain the additional level of insight required into the operation and performance when in production. For Python notebooks, it is also possible to use Application Insights for detailed telemetry as for any other application. More detailed logs and metrics will assist in determining performance anomalies, issue diagnosis and continuously improve performance and usability.

2. Power BI

Power BI Premium integrates with Log Analytics to enable administrators and Premium workspace owners to configure a Log Analytics connection to their Power BI subscription to save activity logs. The Power BI integration with Log Analytics exposes events from the Analysis Services engine, and events are derived from existing diagnostic logs available for Azure Analysis Services.

6. Log Analytics

Log Analytics enables the efficient query of the data stored in Azure Monitor Logs, and DSI leverages a combination of Azure Lighthouse and Log Analytics to capture the results of Log Analytics queries against a customer's Log Analytics workspace. These can be simple queries that use features of Log Analytics to sort, filter, and analyze data, or more advanced queries to perform statistical analysis and visualize the results in a chart to identify a particular trend.

Built using the Azure Data Explorer database engine, the same technology is: -

- Used by the Azure SQL and Power BI teams to troubleshoot performance, run monitoring queries, and find service anomalies.
- Used for storing and querying the Microsoft Office Client telemetry data stream.
- Used by Azure Resource Graph, which powers Azure portal's search bar, and browses 'All resources' experience.

7. Alerts

Alongside visibility to log data, alerts can be raised based on events of differing categories & severity levels, with notifications sent to multiple groups or individuals.

- Metric alerts in Azure Monitor provide a way to get notified when a metric crosses a threshold.
- Metric Alerts for Logs enables metric alert capabilities on a predefined set of Log Analytics logs.
- Log alerts which use a Log Analytics query to evaluate resource logs at a set frequency.
- Alert recipients can be contacted via Email, SMS, Push or Voice.
- Alerts can also trigger actions, E.g., Logic Apps, Automation Runbooks etc.

2. Security & Data Governance

1. Security

Leveraging Azure Active Directory (Azure AD), Azure Lighthouse uses delegated resource management to enable the appropriate access, following the principle of least privilege to delegated resources (subscriptions and/or resource groups) in your tenant. For monitoring only, the permissions can be limited to those only required to enable read access to the data stored in Azure Monitor; however, this monitoring forms part of a more extensive managed services offering from DSI. Any permissions will be evaluated on an individual client basis.

2. Data Governance

Data collected by Azure Monitor in your Azure environment stays in your environment, and any retention and access policies are implemented to control this data and its lifecycle. However, the DSI monitoring platform retrieves aggregate data from a client's Log Analytics workspace, resulting in queries to persist the data required for longitudinal performance analysis and remove the need for clients to persist this data in their Log Analytics workspaces. DSI leverages the features available as part of all Azure data analytics solutions for the data retrieved to ensure security and compliance.

3. Costs

DSI always recommends configuring Azure Monitor for any production deployment as it forms the de facto monitoring solution for Azure solutions. Pricing for Azure Monitor is primarily based on the volume of data ingested and the retention period, with the initial 30 days of retention free (3 months for application insights) and a cost of CDN$ 3.51 per GB per month for data ingestion with a fee of CDN$ 0.15 per GB, per month for data persistence. Typical data volumes are approx—10 GB per month.

Alerts are costed based on the number of metrics monitored, and the frequency examined, but a budgeted amount of CDN$ 50 per month is typical. For notifications, 1,000 emails, 1,000 push notifications and 100,000 webhooks are included for free per month, which is often sufficient.

The DSI monitoring platform ensures the historical data required for time series analysis is retrieved and stored at no additional cost to our clients by storing this in a DSI Azure storage account, enabling our clients to leverage the default retention period. Additionally, there are no additional costs associated with using Azure Lighthouse to manage Azure resources.