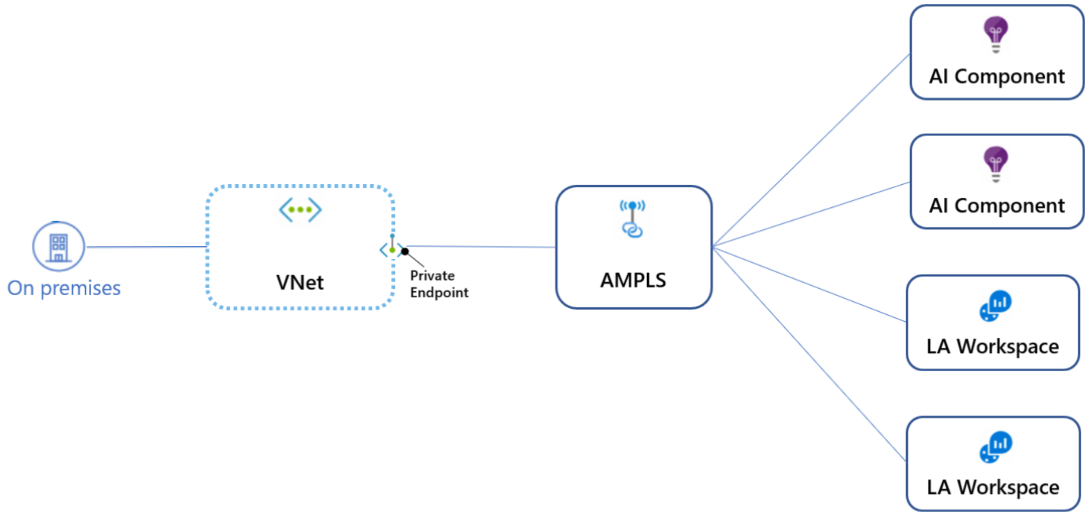
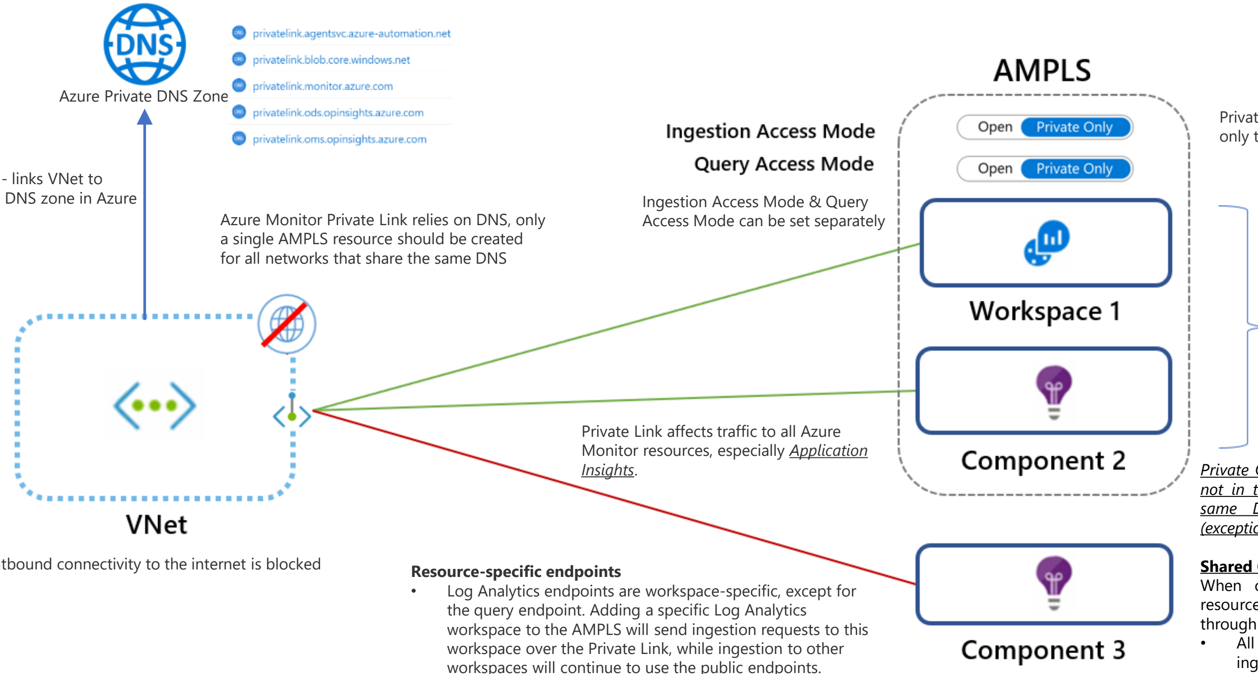
Azure Monitor Private Link Scope - AMPLS



- AMPLS connects a Private Endpoint to a set of Azure Monitor resources.
- Traffic from the Private Endpoint will go over the Microsoft Azure backbone.
- Disabling Public Access will allow only Private Link traffic.
- Azure Monitor uses a single Private Link connection, from the VNet to an AMPLS
- Doc:
  - https://docs.microsoft.com/en-us/azure/azure-monitor/logs/private-link-security
  - https://docs.microsoft.com/en-us/azure/azure-monitor/logs/private-link-design
  - https://docs.microsoft.com/en-us/azure/azure-monitor/logs/private-link-configure

AMPLS – Private only access mode


DNS
Azure Private DNS Zone
privatelink.agentsvc.azure-automation.net
privatelink.blob.core.windows.net
privatelink.monitor.azure.com
privatelink.ods.opinsights.azure.com
privatelink.oms.opinsights.azure.com
VNet
AMPLS
Ingestion Access Mode
Query Access Mode
Open
Private Only
Open
Private Only
Workspace 1
Component 2
Component 3
Added to AMPLS

V-Link - links VNet to private DNS zone in Azure

Azure Monitor Private Link relies on DNS, only a single AMPLS resource should be created for all networks that share the same DNS

Outbound connectivity to the internet is blocked

Ingestion Access Mode & Query Access Mode can be set separately

Private Link affects traffic to all Azure Monitor resources, especially *Application Insights*.

Private Only mode - allows traffic only to Private Link resources

Resources added to AMPLS will be accessible from the VNet using Private IP

Private Only access mode will block traffic to resources not in the AMPLS across all networks that share the same DNS, regardless of subscription or tenant (exception Log Analytics ingestion requests)

Resource-specific endpoints

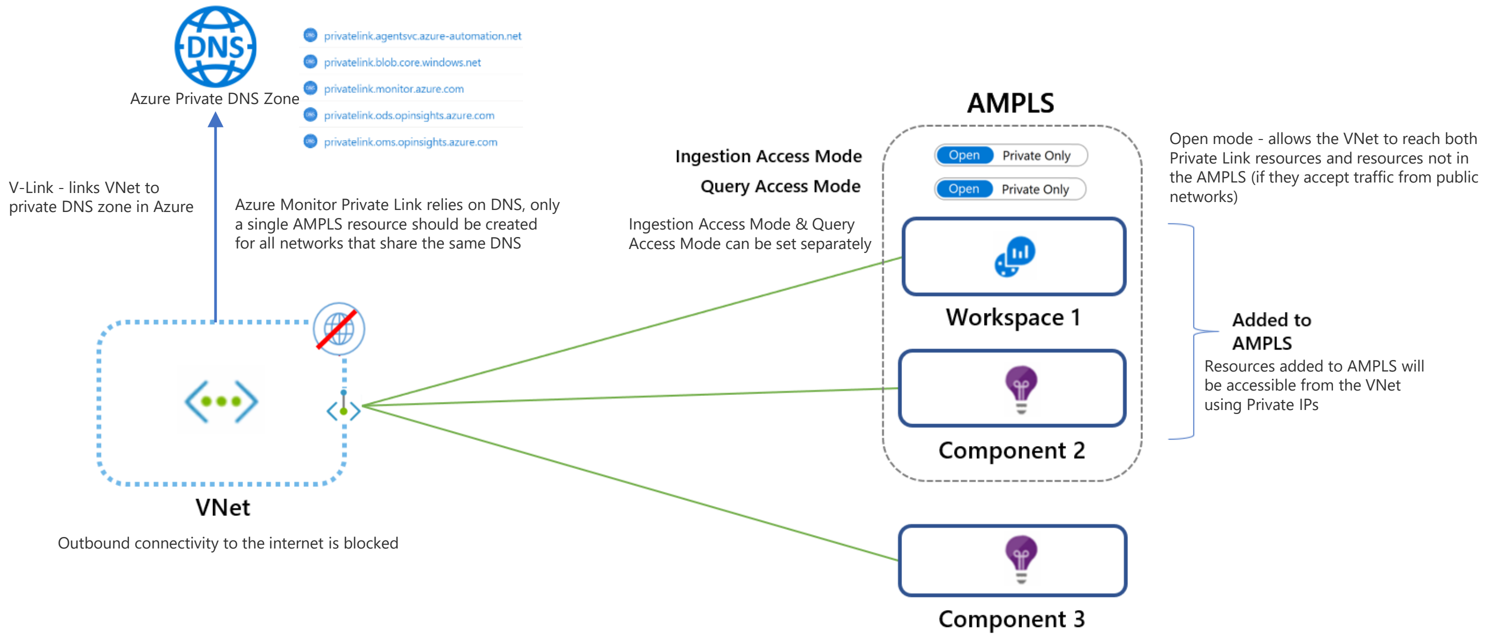
- Log Analytics endpoints are workspace-specific, except for the query endpoint. Adding a specific Log Analytics workspace to the AMPLS will send ingestion requests to this workspace over the Private Link, while ingestion to other workspaces will continue to use the public endpoints.
- Data Collection Endpoints are also resource-specific and allow you to uniquely configure ingestion settings for collecting guest OS telemetry data from your machines (or set of machines) when using the new Azure Monitor agent and Data Collection Rules. Configuring a data collection endpoint for a set of machines does not affect ingestion of guest telemetry from other machines using the new agent.

Shared Global Endpoints

When configuring Private Link even for a single resource, traffic to the below endpoints will be sent through the allocated Private IPs.

- All Application Insights endpoints handling ingestion like live metrics, profiler, debugger etc. to Application Insights endpoints are global.
- The Query endpoint handling queries to Application Insights & Log Analytics are global.

AMPLS – Open access mode



- privatelink.agentsvc.azure-automation.net
- privatelink.blob.core.windows.net
- privatelink.monitor.azure.com
- privatelink.ods.opinsights.azure.com
- privatelink.oms.opinsights.azure.com

V-Link - links VNet to private DNS zone in Azure

Azure Monitor Private Link relies on DNS, only a single AMPLS resource should be created for all networks that share the same DNS

Outbound connectivity to the internet is blocked

Ingestion Access Mode [✓ Open] Private Only

Query Access Mode [✓ Open] Private Only

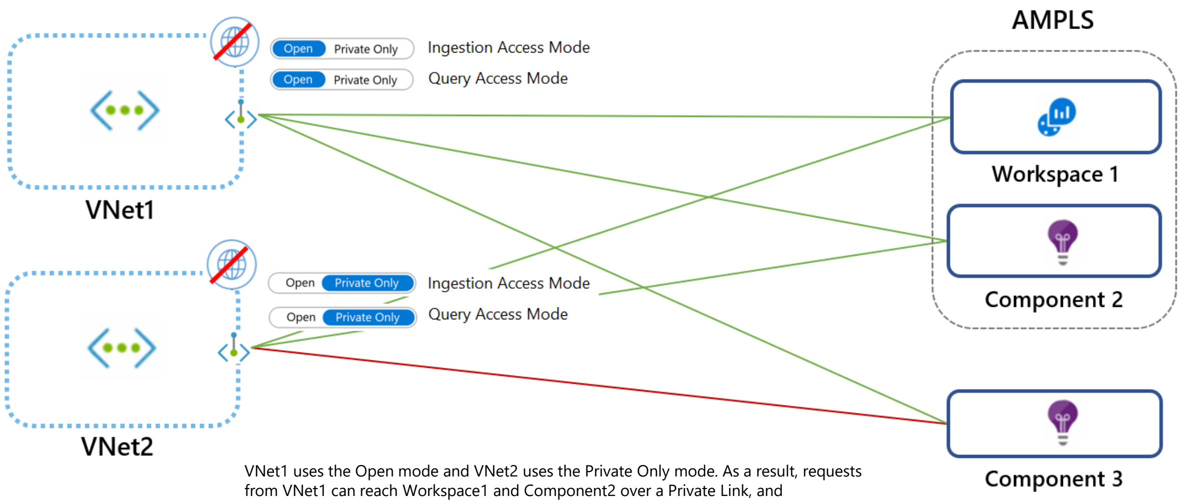
Ingestion Access Mode & Query Access Mode can be set separately

Open mode - allows the VNet to reach both Private Link resources and resources not in the AMPLS (if they accept traffic from public networks)

Resources added to AMPLS will be accessible from the VNet using Private IPs

Private Link design set up – scenario 1

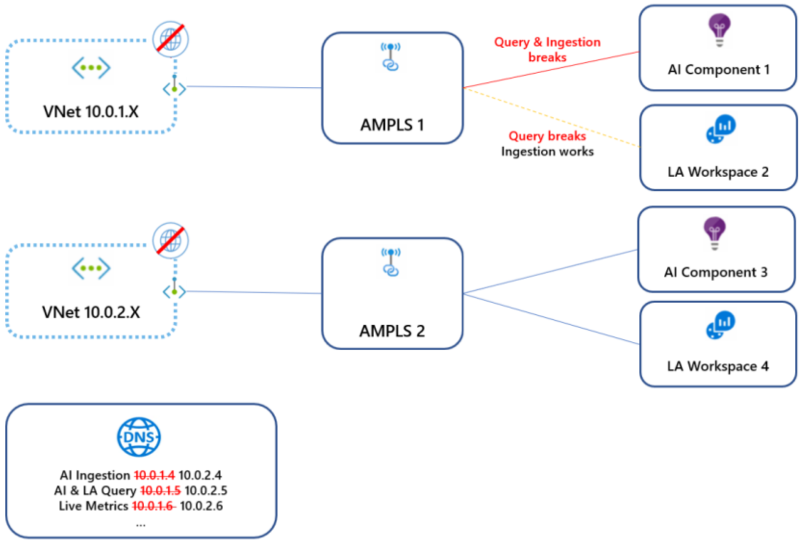
Setting access modes with different networks



VNet1 uses the Open mode and VNet2 uses the Private Only mode. As a result, requests from VNet1 can reach Workspace1 and Component2 over a Private Link, and Component3 not over a Private Link (if it accepts traffic from public networks). However, VNet2 requests won't be able to reach Component3

Private Link design set up – scenario 2

Avoid DNS overrides by using a single AMPLS

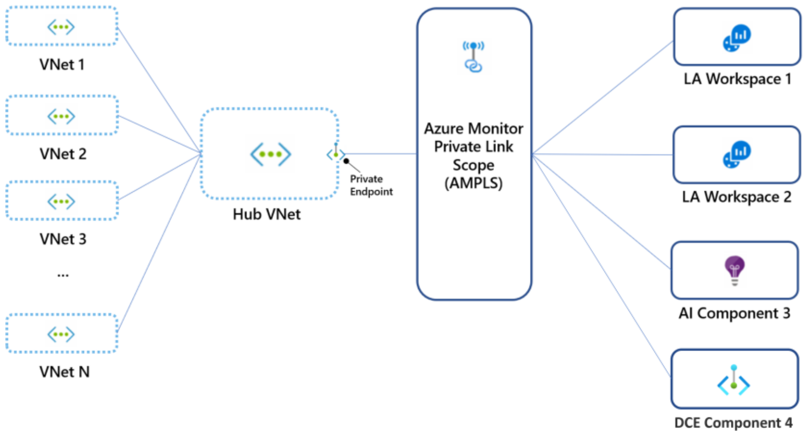


VNet 10.0.1.x connects to AMPLS1 which creates DNS entries mapping Azure Monitor endpoints to IPs from range 10.0.1.x.
Later, VNet 10.0.2.x connects to AMPLS2, which overrides the same DNS entries by mapping the same global/regional endpoints to IPs from the range 10.0.2.x. Since these VNets aren't peered, the first VNet now fails to reach these endpoints.

To avoid this conflict, create only a single AMPLS object per DNS.

Private Link design set up – scenario 3

Hub-and-spoke networks



Hub-and-spoke networks should use a single Private Link connection set on the hub (main) network, and not on each spoke VNet.