

Application Gateway

The queries below allow you to query various diagnostic and metric data for the Application Gateway, including the Web Application Firewall. These queries have been updated to be compatible with WAF v2.

Optimal rendering options are also included below each query.

List Monitored Application Gateways (individual list)

List all application gateways currently being monitored. This query can be executed against `AzureMetrics` or `AzureDiagnostics`.

AzureMetrics

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAY"
| distinct Resource, ResourceGroup
```

AzureDiagnostics

```
AzureDiagnostics
| where ResourceId contains "APPLICATIONGATEWAY"
| distinct Resource, ResourceGroup
```

#table

List Monitored Application Gateways (comparitive list - join)

List all application gateways currently being monitored. This query joins both, `AzureMetrics` and `AzureDiagnostics`, to create an all-inclusive list of gateways being monitored.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAY"
| distinct Resource, ResourceGroup
| as Metrics
| union withsource=Source
(
  AzureDiagnostics
  | where ResourceId contains "APPLICATIONGATEWAY"
  | distinct Resource, ResourceGroup
  | as Diagnostics
)
```

#table

List Unmonitored Application Gateways (XOR list)

List all application gateways currently being monitored, but only have one setting turned on - *either* `AzureMetrics` or `AzureDiagnostics` - but, not both. This creates a union of outer joins against both tables and returns results that are exclusive to either table and not found in both. Additionally, the query reports which setting is missing for the application gateway.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAY"
| distinct Type, Resource, ResourceGroup
| join kind=leftanti
(
  AzureDiagnostics
  | where ResourceId contains "APPLICATIONGATEWAY"
  | distinct Type, Resource, ResourceGroup
)
on Resource, ResourceGroup
| as Diagnostics
| union withsource=MissingSetting
(
  AzureMetrics
  | where ResourceId contains "APPLICATIONGATEWAY"
  | distinct Type, Resource, ResourceGroup
  | join kind=rightanti
  (
    AzureDiagnostics
    | where ResourceId contains "APPLICATIONGATEWAY"
    | distinct Type, Resource, ResourceGroup
  )
  on Resource, ResourceGroup
  | as Metrics
)
| project Resource, ResourceGroup, MissingSetting
```

#table

Average Throughput per second (Bytes)

Display the average throughput per second of the application gateways. The results display the average of 5-minute blocks by each application gateway resource.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAY"
| where MetricName == "Throughput"
| summarize avg(Average) by Resource, bin(TimeGenerated, 5m)
| project TimeGenerated, avg_Average, Resource
```

[#timechart](#)[#barchart](#)[#areachart](#)

Average Throughput per second (Mb)

The same as the query above, but converted to megabytes (Base 10).

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAY"
| where MetricName == "Throughput"
| summarize avg(Average) by Resource, bin(TimeGenerated, 5m)
| extend ThroughputMb = todecimal((avg_Average/1000)/1000)
| project TimeGenerated, ThroughputMb, Resource
```

[#timechart](#)[#barchart](#)[#areachart](#)

Unhealthy Hosts (Compared to Healthy)

Show when hosts connected to the application gateway become unreachable. This query will produce a comparison graph between the number of nodes that are healthy and those that are unhealthy for a *single* application gateway. The results display the average health in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAY" and Resource == "<your gateway's name>"
| where MetricName == "UnhealthyHostCount" or MetricName == "HealthyHostCount"
| summarize avg(Total) by Resource, MetricName, bin(TimeGenerated, 5m)
| project TimeGenerated, MetricName, avg_Total
```

[#timechart](#)[#areachart](#)[#piechart](#)

Unhealthy Hosts (for all gateways)

Show when hosts connected to the application gateway become unreachable. This query will produce the number of nodes that are unhealthy for *all* application gateways. The results display the average disconnected state in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAY"
| where MetricName == "UnhealthyHostCount"
| summarize avg(Total) by Resource, bin(TimeGenerated, 5m)
| project TimeGenerated, Resource, avg_Total
```

#timechart

#areachart

Healthy Hosts (for all gateways)

Show healthy, reachable hosts connected to the application gateway. This query will produce the number of nodes that are healthy for *all* application gateways. The results display the average connected state in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAY"
| where MetricName == "HealthyHostCount"
| summarize avg(Total) by Resource, bin(TimeGenerated, 5m)
| project TimeGenerated, Resource, avg_Total
```

#timechart

#areachart

All Errors (by gateway)

Display requests that resulted in some type of error (error code 400 or above).

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayAccessLog"
| extend Status = toint(httpStatus_d)
| where Status >= 400
| summarize Count=count() by tostring(Status), Resource
| project Resource, Status, Count
```

#table

All Errors (by backend)

Display requests that resulted in some type of error (error code 400 or above).

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayAccessLog"
| extend Status = toint(serverStatus_s)
| extend Server = serverRouted_s
| where Status >= 400
| summarize Count=count() by tostring(Status), Server
| project Server, Status, Count
```

#table

Bad Gateway (by gateway)

Find requests that resulted in a server error of 502 - *Bad Gateway*. The results display the total errors in increments of 5-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayAccessLog"
| where serverStatus_s == 502
| summarize count() by Resource, bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)

All Operations (for all gateways)

Report all operations on the gateways in the subscription. The results display the total number of operations in increments of 15-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and ResourceType ==
"APPLICATIONGATEWAYS"
| summarize count() by OperationName, bin(TimeGenerated, 15m)
```

[#timechart](#)[#barchart](#)[#areachart](#)

Total Connections (by gateway)

Report the number of total connections per each application gateway. The results display the total number of connections in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAYS"
| where MetricName == "CurrentConnections"
| summarize sum(Total) by Resource, bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)

Average Connection Count (by gateway)

Report the number of average connections per application gateway. The results display the average number of connections in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAYS"
| where MetricName == "CurrentConnections"
| summarize avg(Average) by Resource, bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)

Average Backend Connection Time (by gateway)

Report the average backend connection time per application gateway. The results display the average number of connections in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAYS"
| where MetricName == "BackendConnectTime"
| summarize avg(Average) by Resource, bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)

Average Total Time (by gateway)

Report the average time for a request - beginning to end - per each application gateway. The results display the average number of connections in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAYS"
| where MetricName == "ApplicationGatewayTotalTime"
| summarize avg(Average) by Resource, bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)

Average Latency (per backend server)

Report the average latency per backend servers connected to your application gateway(s). The results display the average latency in seconds of servers connected to the backend pools in increments of 5-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayAccessLog"
| summarize avg(todouble(serverResponseTime_s)) by serverRouted_s,
bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)

Total Requests (by gateway)

Report the total number of requests per application gateway. The results display the total number of requests in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAYS"
| where MetricName == "TotalRequests"
| summarize sum(Total) by Resource, bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)

Average Requests (by gateway)

Report the average number of requests per application gateway. The results display the average number of requests in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAYS"
| where MetricName == "TotalRequests"
| summarize avg(Average) by Resource, bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)

Total Failed Requests (by gateway)

Report the total number of failed requests per application gateway. The results display the total number of failed requests in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAYS"
| where MetricName == "FailedRequests"
| summarize sum(Total) by Resource, bin(TimeGenerated, 5m)
```


[#timechart](#) [#barchart](#) [#areachart](#)

Average Failed Requests (by gateway)

Report the average number of failed requests per application gateway. The results display the average number of failed requests in increments of 5-minute blocks for the past 24 hours.

```
AzureMetrics
| where ResourceId contains "APPLICATIONGATEWAYS"
| where MetricName == "FailedRequests"
| summarize avg(Average) by Resource, bin(TimeGenerated, 5m)
```

[#timechart](#) [#barchart](#) [#areachart](#)

Total Successful Requests (per backend server)

Report the total number of successful requests per backend servers connected to your application gateway(s). The results display the total number of successful requests to servers connected to the backend pools in increments of 5-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayAccessLog"
| where toint(serverStatus_s) < 400
| summarize count() by serverRouted_s, bin(TimeGenerated, 5m)
```

[#timechart](#) [#barchart](#) [#areachart](#)

Total Failed Requests (per backend server)

Report the total number of failed requests per backend servers connected to your application gateway(s). The results display the total number of failed requests to servers connected to the backend pools in increments of 5-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayAccessLog"
| where toint(serverStatus_s) >= 400
| summarize count() by serverRouted_s, bin(TimeGenerated, 5m)
```

[#timechart](#) [#barchart](#) [#areachart](#)

Total Requests (per API)

Report the total number of requests per API endpoint. The results display the total number of requests to each served endpoint in increments of 5-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayAccessLog"
| summarize Count=count() by requestUri_s, bin(TimeGenerated, 5m)
```

[#table](#)[#timechart](#)[#barchart](#)[#areachart](#)

Failed Requests (per API)

Report the failed number of requests per API endpoint. The results display the failed number of requests to each served endpoint in increments of 5-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayAccessLog"
| where httpStatus_d >= 400
| summarize Count=count() by requestUri_s, bin(TimeGenerated, 5m)
```

[#table](#)[#timechart](#)[#barchart](#)[#areachart](#)

Failed Requests, include Status (per API)

Report the failed number of requests per API endpoint. The results display the failed number of requests to each served endpoint in increments of 5-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayAccessLog"
| where httpStatus_d >= 400
| summarize Count=count() by requestUri_s, httpsStatus_d, bin(TimeGenerated,
5m)
```

[#table](#)

Triggered Firewall Rules

Report all OWASP rules that have been triggered. The results display the triggers in increments of 5-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayFirewallLog"
| summarize Count=count() by ruleId_s, bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)[#piechart](#)

Blocked Firewall Rules

Report all requests that resulted in a firewall block due to an OWASP rule.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayFirewallLog"
| where action_s == "Blocked"
```

[#timechart](#)[#barchart](#)[#areachart](#)[#piechart](#)

Count Blocked Firewall Rules

Group and count all blocked requests by rule violation. The results display the triggers in increments of 5-minute blocks for the past 24 hours.

```
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK" and Category ==
"ApplicationGatewayFirewallLog"
| where action_s == "Blocked"
| summarize Count=count() by ruleId_s, bin(TimeGenerated, 5m)
```

[#timechart](#)[#barchart](#)[#areachart](#)[#piechart](#)