# AZ300-something Notes

Export Azure diagnostic log data to:

* Azure Storage
* Event Hub: subscribe to event data funneled into the hub
* Azure Monitor logs: Kusto Query Language (KQL) to query

**Logs** are **blob** objects,  
**Metrics** (measured values, counts representing time series 🡪 they form the baseline) as **tables**.

Configure log collection for public IP address resource:  
- Monitor  
- Settings, Diagnostic settings  
- Add diagnostic setting: logs/metrics are resource specific (eg DDoS logs for IP)  
(we could have done this via Resource Manager API, Azure CLI or PowerShell)

**Alerts:**  
- Azure Monitor  
- Alerts  
 New Alert Rule (we can select from multiple Azure subscriptions)  
 - **Trigger:** can be either **Metrics** or **Activity Log** (listen to particular events)  
 Actions, Add: send email, sms, or trigger Function or, Logic App, send webhook, start Azure  
 Azure Automation runbook or integrate with our IT Service Management platform

We can even create a KQL query and use it in an Alert as a rule

**Action groups:** take action automatically when an alert is fired  
Generally, best practice is to create Action Groups first, then reuse them later on in alert definitions  
- Azure Monitor  
- Manage Actions, Add Action Group (specify subscription and resource group)