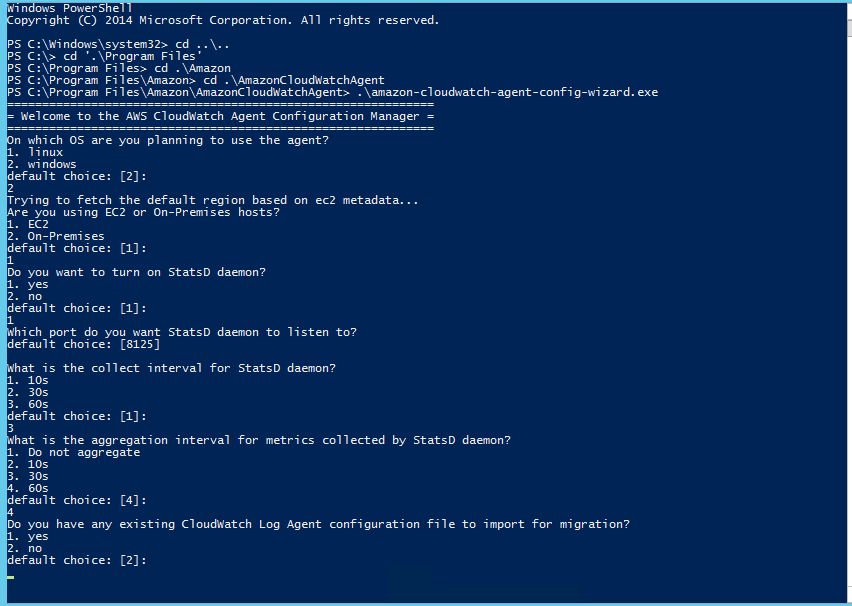
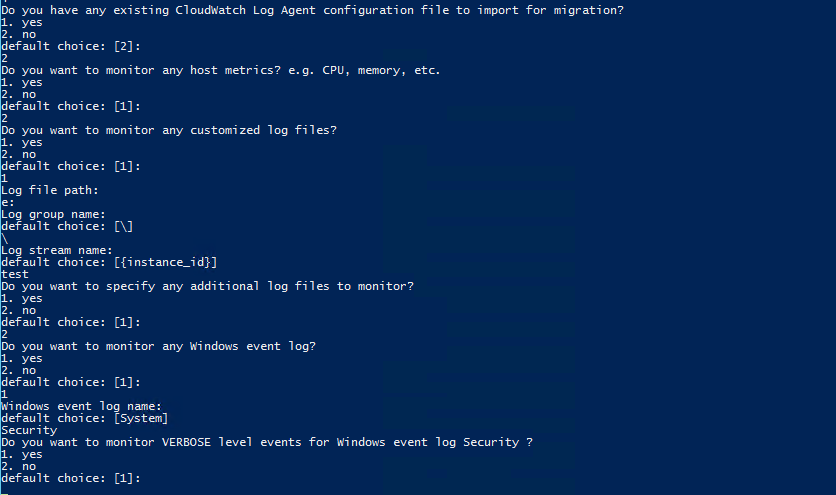
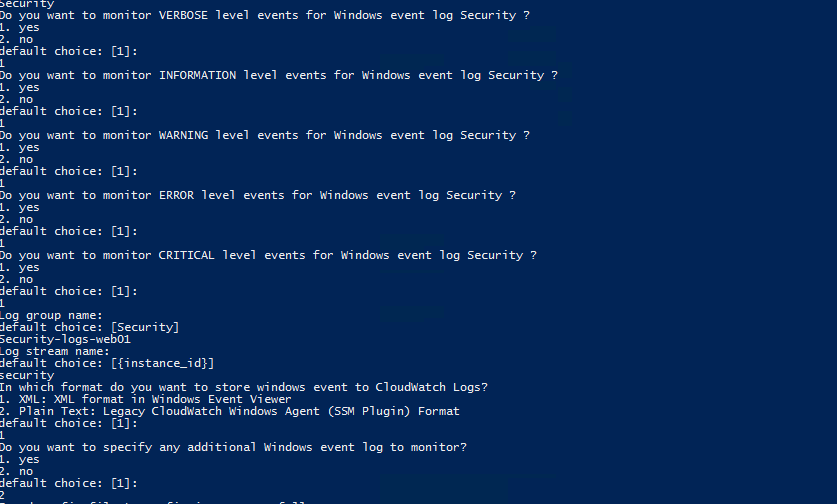
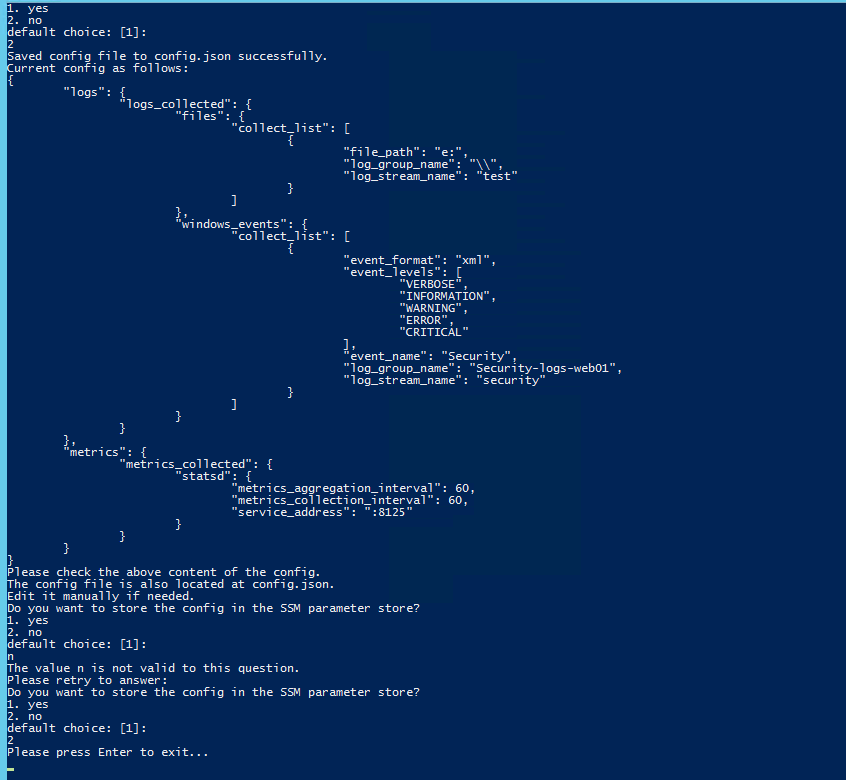
Enable – Windows Event viewer logs on AWS WEB Servers

* Security – To see who logs on (Part SOC)
* Application –

To enable - -Open POwershell (in admin)

* PS C:\Program Files\Amazon\AmazonCloudWatchAgent>
* Note commect out config.json1
* PS C:\Program Files\Amazon\AmazonCloudWatchAgent> .\amazon-cloudwatch-agent-config-wizard.exe
* Note
* 
* 





|  |
| --- |
| {  "logs": {  "logs\_collected": {  "files": {  "collect\_list": [  {  "file\_path": "D:\\inetpub\\wwwroot\\Accounting\\App\_Data\\logs\\logs.log",  "log\_group\_name": "accounting-logs-web01",  "log\_stream\_name": "accounting"  },  {  "file\_path": "D:\\inetpub\\wwwroot\\CloudCabinet\\App\_Data\\logs\\logs.log",  "log\_group\_name": "cloudcabinet-logs-web01",  "log\_stream\_name": "cloudcabinet"  },  {  "file\_path": "D:\\inetpub\\wwwroot\\AOAdmin-Prod\\App\_Data\\logs\\logs.log",  "log\_group\_name": "aoadmin-logs-web01",  "log\_stream\_name": "aoadmin"  },  {  "file\_path": "D:\\inetpub\\wwwroot\\AOCommon\\App\_Data\\logs\\log.txt",  "log\_group\_name": "aocommon-logs-web01",  "log\_stream\_name": "aocommon"  },  {  "file\_path": "D:\\inetpub\\wwwroot\\Awpurchase-Prod\\App\_Data\\logs\\log.txt",  "log\_group\_name": "awpurchase-logs-web01",  "log\_stream\_name": "awpurchase"  },  {  "file\_path": "D:\\inetpub\\wwwroot\\AWAuth\\logs\\\*.log",  "log\_group\_name": "awauth-logs-web01",  "log\_stream\_name": "awauth"  },  {  "file\_path": "D:\\inetpub\\wwwroot\\EmailAPI\\App\_Data\\logs\\log.txt",  "log\_group\_name": "emailapi-logs-web01",  "log\_stream\_name": "emailapi"  },  {  "file\_path": "D:\\inetpub\\wwwroot\\PracticeRelief\\App\_Data\\logs\\log.txt",  "log\_group\_name": "practicerelief-logs-web01",  "log\_stream\_name": "practicerelief"  },  {  "file\_path": "D:\\inetpub\\wwwroot\\Login\\App\_Data\\logs\\log.txt",  "log\_group\_name": "awlogin-logs-web01",  "log\_stream\_name": "awlogin"  }  ]  },  "windows\_events": {  "collect\_list": [  {  "event\_format": "xml",  "event\_levels": [  "VERBOSE",  "INFORMATION",  "WARNING",  "ERROR",  "CRITICAL"  ],  "event\_name": "Security",  "log\_group\_name": "security-logs-web01",  "log\_stream\_name": "security"  }  ]  }  }  },  "metrics": {  "metrics\_collected": {  "statsd": {  "metrics\_aggregation\_interval": 60,  "metrics\_collection\_interval": 60,  "service\_address": ":8125"  }  }  }  } |

|  |
| --- |
| PS C:\Program Files\Amazon\AmazonCloudWatchAgent> .\amazon-cloudwatch-agent-ctl.ps1  Invalid action:  usage: amazon-cloudwatch-agent-ctl.ps1 -a stop|start|status|fetch-config|append-config|remove-config [-m ec2|on  Premise|auto] [-c default|ssm:<parameter-store-name>|file:<file-path>] [-s]  e.g.  1. apply a SSM parameter store config on EC2 instance and restart the agent afterwards:  amazon-cloudwatch-agent-ctl.ps1 -a fetch-config -m ec2 -c ssm:AmazonCloudWatch-Config.json -s  2. append a local json config file on onPremise host and restart the agent afterwards:  amazon-cloudwatch-agent-ctl.ps1 -a append-config -m onPremise -c file:c:\config.json -s  3. query agent status:  amazon-cloudwatch-agent-ctl.ps1 -a status  -a: action  stop: stop the agent process.  start: start the agent process.  status: get the status of the agent process.  fetch-config: use this json config as the agent's only configuration.  append-config: append json config with the existing json configs if any.  remove-config: remove json config based on the location (ssm parameter store name,  file name)  -m: mode  ec2: indicate this is on ec2 host.  onPremise: indicate this is on onPremise host.  auto: use ec2 metadata to determine the environment, may not be accurate  if ec2 metadata is not available for some reason on EC2.  -c: configuration  default: default configuration for quick trial.  ssm:<parameter-store-name>: ssm parameter store name  file:<file-path>: file path on the host  -s: optionally restart after configuring the agent configuration  this parameter is used for 'fetch-config', 'append-config', 'remove-config' action only. |

|  |
| --- |
| PS C:\Program Files\Amazon\AmazonCloudWatchAgent> .\amazon-cloudwatch-agent-ctl.ps1 -a fetch-config -m ec2 -c file:confi  g.json -s |