Filebeat MRF

Backup Procedure

	Action	Team
1		

Requirements

Before started with Filebeat setup, install and configure these related products:

	Action	Team
1	ELK Stack to be installed.	

Installation Procedure

	Action	Team	Comment
	NOTE ** **Filebeat will be installed on every working server related to inspection**		
1	Install Filebeat from https://www.elastic.co/downloads/beats/filebeat		
2	Extract the contents of the zip file into C:\Program Files.		
3	Rename the filebeat-<version>-windows directory to Filebeat.		
4	Open a PowerShell prompt as an Administrator (right-click the PowerShell icon and select **Run As Administrator**).		
5	From the PowerShell prompt, run the following commands to install Filebeat as a Windows service: .\install-service-filebeat.ps1		

6	**Note : In case of Inspection Server**
	
	Go to filebeat.yml in Filebeat Folder and replace with the below configuration:
	
	`filebeat.inputs:`
	
	`- type: log`
	`  enabled: true`
	`  paths:`
	`  - <inspectionRootFolder>\*\*\*-logs-*.txt`
	`  fields:`
	`  applicationType: inspectionLog`
	`  fields_under_root: true`
	`  multiline:`
	`  pattern: '^[[0-9]{4}-[0-9]{2}-[0-9]{2}'`
	`  negate: true`
	`  match: after`
	`- type: log`
	`  enabled: true`
	`  paths:`
	`  - <inspectionAdminRootFolder>\*-logs-*.txt`
	`  fields:`
	`  applicationType: inspectionAdminLog`
	`  fields_under_root: true`
	`  multiline:`
	`  pattern: '^[[0-9]{4}-[0-9]{2}-[0-9]{2}'`
	`  negate: true`
	`  match: after`
	`#============================ Filebeat modules ===============================`
	
	`filebeat.config.modules:`
	`  path: ${path.config}/modules.d/*.yml`
	`  reload.enabled: false`
	`  reload.period: 10s`
	
	`setup.template.settings:`
	`  index.number_of_shards: 1`
	
	`#------------------------------ Logstash output -------------------------------`
	`output.logstash:`
	`  # The Logstash hosts`
	`  hosts: ["192.168.46.199:8888"]`
	
	`#================================ Processors =====================================`
	
	`processors:`
	`  - add_host_metadata: ~`
	`  - add_cloud_metadata: ~`
	`  - add_docker_metadata: ~`
	`  - add_kubernetes_metadata: ~`
	`  if:`
	`  equals:`
	`  applicationType: inspectionLog`
	`  then:`
	`  - dissect:`
	`  tokenizer: '<inspectionRootFolder>\%{authority}\%{tenant}\%{FullappService}'`
	`  field: log.file.path`
	`  target_prefix: insp`
	`  else:`
	`  - dissect:`
	`  tokenizer: '<inspectionAdminRootFolder>\%{FullappService}'`
	`  field: log.file.path`
	`  target_prefix: insp`
	`#================================ Logging =====================================`
	
	`logging.level: debug`
	
	`logging.selectors: ["*"]`		

7	**Note : In case of Tomcat Server**
	
	Go to filebeat.yml in Filebeat Folder and replace with the below configuration:
	
	`filebeat.inputs:`
	`- type: log`
	`  enabled: true`
	`  paths:`
	`  - <tomcatRootFolder>\logs\catalina.*.log`
	`  fields:`
	`  applicationType: tomcat`
	`  fields_under_root: true`
	`  multiline:`
	`  pattern: '^[[0-9]{2}-[a-z,A-Z]{3}-[0-9]{4}'`
	`  negate: true`
	`  match: after`
	
	`#============================ Filebeat modules ===============================`
	`filebeat.config.modules:`
	`  path: ${path.config}/modules.d/*.yml`
	`#---------------------------- Logstash output --------------------------------`
	`output.logstash:`
	`  hosts: ["localhost:8888"]`
	`#================================ Processors =====================================`
	`processors:`
	`  - add_host_metadata: ~`
	`  - add_cloud_metadata: ~`
	`  - add_docker_metadata: ~`
	`  - add_kubernetes_metadata: ~`
	`#================================ Logging =====================================`
	`logging:`
	`  level: debug`
	`  selectors: ["*"]`		

8	replace **`inspectionRootFolder`** token with inspection deployment root folder replace **`inspectionAdminRootFolder`** token with inspection admin deployment log folder replace **`tomcatRootFolder`** token with tomcat base folder		
9	Navigate to filebeat directory in powershell		
10	**** Optional **** If you need to log **IIS** Events , just go to *modules.d* folder and rename *iis.yml.disabled* to *iis.yml*		
11	type **Start-service filebeat**		

Rollback Procedure

	Action	Source code file	Team
1	Open a PowerShell prompt as an Administrator		
2	Navigate to filebeat directory in powershell		
3	type **Stop-service filebeat**		

Release

	Release Number	URL	Team
1			

Known Bugs