

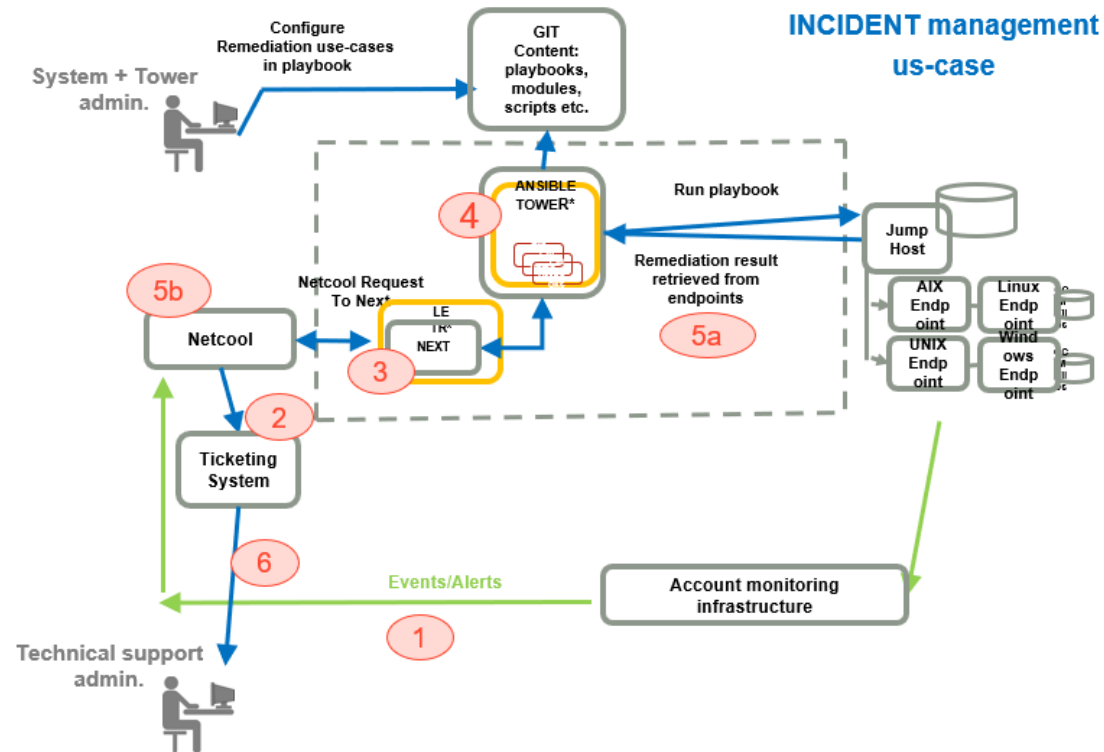
# Event Automation

# Understanding Event Automation Components and Configuring an Event Automation Role

# Event Automation Workflow

## Automation workflows

### Event / incident automation use-case



## Important Event Automation Components

- Event Automation Repo and Roles in CE's Github
- Event Automation Playbook (event\_wrapper.yml)
- Event Automation Roles

### Generic Roles, Remediation Roles

- Event Data
- Alert Key (AK)
- requirements.yml
- mapper.config.yml vs Smart Event Mapper Based on Machine Learning
- config.yml
- extract\_event\_data.yml

## Event Data (netcool)

Summary: Windows Service:KOQAGENT\_IH17NYH0 has a problem. Run status:NOT\_RUNNING  
Date: 2022-04-11T09:17:35Z  
Severity: 4  
ResourceId: win001206.mic.ibmfr.bluecare.ibm.com  
CustomerCode: mic  
InstanceId: KOQAGENT\_IH17NYH0  
InstanceSituation: problem with service status  
AlertKey: all\_svcprb\_g06c\_win\_gen  
TicketGroup: I-TEA-FR-TIA-AD2-DAU-AUTOM  
InstanceValue: NOT\_RUNNING  
ComponentType: OperatingSystem  
Component: Windows  
SubComponent: Service  
ApplId: WIN  
Node: mic\_win001206  
NodeAlias: 10.226.120.2  
AlertGroup: ITM\_K06\_SERVICES  
EventType: 6399  
MonitoringSolution: win  
EventKey: undefined

# Event Data (Ansible)

affected\_host: win001206.mic.ibmfr.bluecare.ibm.com

event\_data:

Asset:

AssetID: win001206

Asset\_Tag: win001206

AssignedTo:

AssignedGroup: I-TEA-FR-TIA-AD2-DAU-AUTOM

Incident:

Abstract: 'Windows Service:KOQAGENT\_IH17NYH0 has a problem. Run status:NOT\_RUNNING'

Description: "Summary: Windows Service:KOQAGENT\_IH17NYH0 has a problem. Run status:NOT\_RUNNING \rDate: 2022-04-11T09:17:35Z \rSeverity: 4 \rResourceId: win001206.mic.ibmfr.bluecare.ibm.com \rCustomerCode: mic \rInstan

FlexFields:

ITEM: >-

MIC:4:WIN001206.MIC.IBMFR.BLUECARE.IBM.COM:WINDOWS:SERVICE:KOQAGENT\_IH17NYH0:WIN

alertgroup: ITM\_K06\_SERVICES

alertkey: all\_svcprb\_g06c\_win\_gen

component: Windows

componenttype: OperatingSystem

event\_class: '1'

fqdn: win001206.mic.ibmfr.bluecare.ibm.com

host\_state: '1'

instanceid: KOQAGENT\_IH17NYH0

instancesituation: problem with service status

instancevalue: NOT\_RUNNING

ipaddress: 10.226.120.2

ipcenabled: 'true'

lastoccurrence: '1649660941'

location: null

monitoring: >-

source\_paramfile=;monthreshold=(MonitoringSolution=Nwin AND

STRSCAN(Status

originating\_event\_id: 'FRMPPN000SRI1XM\_P:145717868:mic'

service\_state: '2'

severity: Critical

subcomponent: Service

tec\_id: FRMPPN000SRI1XM\_P

RequesterID: 'FRMPPN000SRI1XM\_P:145717868:mic'

RequesterSeverity: '4'

TradingPartnerID: mic

Transaction:

TransactionDateTime: '2022-04-11T09:17:35Z'

TransactionName: CREATE

TransactionNumber: '16496614461457178680'

TransactionRouting: 'ASYNCR::micINC'

TransactionType: '2'

schemaLocation: 'http://b2b.ibm.com/schema/IS\_B2B\_CDM/R2\_2 IS\_B2B\_CDM\_R2\_2.xsd'

# requirements.yml

```
17   src: git+https://github.kyndryl.net/IBM-GTS-EU-EU01/ansible-role-event-final-ack.git
18   version: master
19 - name: ansible-role-event-pre-check
20   src: git+https://github.kyndryl.net/IBM-GTS-EU-EU01/ansible-role-event-pre-check.git
21   version: master
22 - name: ansible-role-event-socks-tunnel
23   src: git+https://github.kyndryl.net/IBM-GTS-EU-EU01/ansible-role-event-socks-tunnel.git
24   version: master
25 - name: ansible-role-event-blacklisting
26   src: git+https://github.kyndryl.net/IBM-GTS-EU-EU01/ansible-role-event-blacklisting.git
27   version: master
28 - name: ansible-role-event-global-eventwrapper
29   src: git+https://github.kyndryl.net/IBM-GTS-EU-EU01/ansible-role-event-global-eventwrapper.git
30   version: master
31 - name: service-restart
32   src: git+https://github.kyndryl.net/Continuous-Engineering/ansible-role-service-restart.git
33   version: 3.4.1
34 - name: high-memory-handler
35   src: git+https://github.kyndryl.net/Continuous-Engineering/ansible-role-high-memory-handler.git
36   version: 1.5.3
37 - name: windows-os-event-log-alert
38   src: git+https://github.kyndryl.net/Continuous-Engineering/ansible-role-windows-os-event-log-alert.git
39   version: 1.5.6
40 - name: cpu-aggregate-high-handler
41   src: git+https://github.kyndryl.net/Continuous-Engineering/ansible-role-cpu-aggregate-high-handler.git
42   version: 1.3.4
43 - name: process-handler
44   src: git+https://github.kyndryl.net/Continuous-Engineering/ansible-role-process-handler.git
45   version: 1.2.2
46 - name: zombie-process
47   src: git+https://github.kyndryl.net/Continuous-Engineering/ansible-role-zombie-process.git
48   version: 1.1.7
49 - name: cpu-spike-handler-unix
50   src: git+https://github.kyndryl.net/Continuous-Engineering/ansible-role-cpu-spike-handler-unix.git
51   version: 1.3.0
52 - name: check-http-status-code
53   src: git+https://github.kyndryl.net/Continuous-Engineering/ansible-role-check-http-status-code.git
54   version: 1.3.0
```

## matchers.config.yml

```
## - name: service-restart-daemon-handler
##   enabled: false
##   matcher_expressions:
##     - item: put_service-restart-daemon-handler_match_here
##     - item: ^.*put_service-restart-daemon-handler_match_here.*$

# - name: high-memory-handler
#   enabled: true
#   matcher_expressions:
#     - alertkey: all_memavl_wntc_win
#     - alertkey: all_memmon_wntc_win
#     - alertkey: ^.*memutil.*$
#     - alertkey: ^.*memreal.*$

## - name: windows-os-event-log-alert
##   enabled: true
##   matcher_expressions:
##     - alertkey: all_evtalrt_g064_win_v2_gen
##     - alertkey: ^.*all_evtalrt_g064_win_v2_gen.*$
## - name: cpu-aggregate-high-handler
##   enabled: false
##   matcher_expressions:
##     - item: put_cpu-aggregate-high-handler_match_here
##     - item: ^.*put_cpu-aggregate-high-handler_match_here.*$

## - name: process-handler
##   enabled: true
##   matcher_expressions:
##     - alertkey: put_process-handler_match_here
##     - alertkey: ^.*all_procmon.*$

## - name: zombie-process
##   enabled: true
##   matcher_expressions:
##     - alertkey: inf_zom_xuxc_aix
##     - alertkey: ^.*_zom_xuxc.*$

## - name: cpu-spike-handler-unix
##   enabled: false
##   matcher_expressions:
##     - item: put_cpu-spike-handler-unix_match_here
##     - item: ^.*put_cpu-spike-handler-unix_match_here.*$
```



## smart even mapper based on machine learning


VARIABLES ?


YAML


JSON


```
36 - alertkey: '[a-z0-9]{3}_erralrt_x074_aix_v2'
37 - alertkey: '[a-z0-9]{3}_erralrt_x073_aix'
38 - alertkey: '[a-z0-9]{3}_erralrt_x074_aix_2'
39 - alertkey: '[a-z0-9]{3}_erralrt_x074_aix'
40 - alertkey: '[a-z0-9]{3}_erralrt_x071_aix'
41 - alertkey: '[a-z0-9]{3}_erralrt_x074_aixdev_2'
42 - alertkey: '[a-z0-9]{3}_erralrt_x074_aixdev'
43 - alertkey: '[a-z0-9]{3}_erralrt_x075_aix_v2_gen'
44 - alertkey: '[a-z0-9]{3}_erralrt_x073_aix_v2_gen'
45 - name: check-http-status-code
46   enabled: true
47   matcher_expressions:
48     - alertkey: '[a-z0-9]{3}_urlmon_.*$'
49 - name: cluster-events
50   enabled: true
51   matcher_expressions:
52     - alertkey: '[a-z0-9]{3}_haproc_xuxc_hacmp'
53     - alertkey: '[a-z0-9]{3}_logalrt_.{4}_.*hacmp.*$'
54     - alertkey: '[a-z0-9]{3}_syslog_.{4}_.*hacmp.*$'
55 - name: cpu-aggregate-high-handler
56   enabled: true
57   matcher_expressions:
58     - alertkey: '(?i).*CPUhasexceededthreshold.*$
59       affected_host_ostype: '(?i).*linux|unix.*$
60     - alertkey: '(?i).*CPUutilizationabovethreshold.*$
61     - alertkey: '[a-z0-9]{3}_cpupct_goqw_std'
62     - alertkey: '[a-z0-9]{3}_cpuoff_xuxc_aix'
63     - alertkey: '[a-z0-9]{3}_cpucup_xuxc_aix'
64     - alertkey: '[a-z0-9]{3}_cpuitm_nlzc_linux_v2'
65     - alertkey: '[a-z0-9]{3}_avacpu_xuxc_aix'
66     - alertkey: '[a-z0-9]{3}_entcpu_xvac_vios'
67     - alertkey: '[a-z0-9]{3}_sysload_n08f_redhat'
```

# config.yml


 master ▾ [gmb\\_eventautomation](#) / [service-restart](#) / [config.yml](#)

 **CE Automation** Updating service-restart/config.yml

 0 contributors

 14 lines (14 sloc) | 278 Bytes

```
1  add_last_boot_info: false
2  event_counts: 5
3  event_minutes: 60
4  final_wait_time: 0
5  handle_always_list: []
6  remediation:
7    path_folder: C:\service_restart_logs
8    threshold: 0
9  resolve_status: []
10 restart_list: []
11 sr_allowlist: []
12 sr_blocklist: []
13 start_manual: true
14 uptime_threshold: 0
```

 README.md

## Variables

Please provide the service names in lowercase where you are asked to provide a list of service names (e.g. allowlist, restart list). More details and examples are available in 'Example configuration with description' paragraph further below.

Parameter	Choices/Defaults	Comments
uptime_threshold (Integer)	default is 0 (mins)	The host uptime should be equal or higher than this value to execute the full workflow.
sr_blocklist (List)	default is empty list	A list of service names that are prohibited to be restarted.
sr_allowlist (List)	default is empty list	A list of service names that are allowed to be restarted.
handle_always_list (List)	default is empty list	A list of service names to be handled even if other rules prohibit the restart (e.g. manual services disabled and given service does have manual startMode).
event_counts (Integer)	default is 5	If entries from event log is extracted, max. this number of entries are extracted.
event_minutes (Integer)	default is 60	If entries from event log is extracted, the lookup goes back in history for this number of minutes.
resolve_status (List)	default is empty list	The list of service startModes (manual, disabled) that should mark the execution as resolved without any action.

# extract\_event\_data.yml

0 contributors

5 lines (5 sloc) | 262 Bytes

```
1 instanceid: '{{ event_data['Incident']['FlexFields']['instanceid'] }}'
2 restart_reswas: '{{ summary.lower() | replace(' ', '') is search('resagentoffline')
3   }}'
4 service_info: '{{ instanceid }}'
5 summary: '{{ event_data['Incident']['Abstract'] }}'
```

```
affected_host: win001206.mic.ibmfr.bluecare.ibm.com
event_data:
  Asset:
    AssetID: win001206
    Asset_Tag: win001206
  AssignedTo:
    AssignedGroup: I-TEA-FR-TIA-AD2-DAU-AUTOM
  Incident:
    Abstract: 'Windows Service:KOQAGENT_IH17NYH0 has a problem. Run status:NOT_RUNNING'
    Description: "Summary: Windows Service:KOQAGENT_IH17NYH0 has a problem. Run status:NOT_RUNNING \rDate: 2022-04-11T09:17:35Z"
    FlexFields:
      ITEM: >-
        MIC:4:WIN001206.MIC.IBMFR.BLUECARE.IBM.COM:WINDOWS:SERVICE:KOQAGENT_IH17NYH0:WIN
        alertgroup: ITM_K06_SERVICES
        alertkey: all_svcprb_g06c_win_gen
        component: Windows
        componenttype: OperatingSystem
        event_class: '1'
        fqdn: win001206.mic.ibmfr.bluecare.ibm.com
        host_state: '1'
        instanceid: KOQAGENT_IH17NYH0
        instancesituation: problem with service status
        instancevalue: NOT_RUNNING
        ipaddress: 10.226.120.2
        ipenabled: 'true'
        lastoccurrence: '1649660941'
        location: null
        monitoring: >-
          source_paramfile=;monthreshold=(MonitoringSolution=Nwin AND
          STRSCAN(Status
        originating_event_id: 'FRMPPN000SRI1XM_P:145717868:mic'
        service_state: '2'
        severity: Critical
        subcomponent: Service
        tec_id: FRMPPN000SRI1XM_P
      RequesterID: 'FRMPPN000SRI1XM_P:145717868:mic'
      RequesterSeverity: '4'
      TradingPartnerID: mic
    Transaction:
      TransactionDateTime: '2022-04-11T09:17:35Z'
      TransactionName: CREATE
      TransactionNumber: '16496614461457178680'
      TransactionRouting: 'ASYNCR:micINC'
      TransactionType: '2'
    schemaLocation: 'http://b2b.ibm.com/schema/IS_B2B_CDM/R2_2 IS_B2B_CDM_R2_2.xsd'
```

## Configuring and Testing An Event Automation Role

- Create a dev/test branch in EA(Event Automation) repository
- Configure/check the role's remediation steps (config.yml)
- Configure/check the event data (extract\_event\_data.yml)
- Create a test project and test job template pointing to dev/test branch
- Test the role with sample event data
- Create a pull request to production(master/main) branch
- Sync. netcool\_project.

kyndryl™

Thank You