Market France

ScienceLogic-SL1 **Event & Incident automation**

Step by step to enable Event Automation & Incident remediation successfully

*For legacy ITM6 FR see https://kyndryl.ent.box.com/file/968934478102?s=cxcjopuahumgjslcx56qeo7

Enabling Incident Remediation from SL1 events

Verification steps for a full Event Automation validation - overview

If any pre-req is not ready, reschedule test session

Num	Steps to follow in an online workshop to validate Event automation / Incident remediation	Actors (task owner)
1	Check **prerequisites** for automation in M&E Portal (Auto-Ticketing + Automation / Remediation in Ansible)	MnE Event SME
2	Ensure server for working session is monitored , know what is monitored for this server **and which event / incident you want to test automation.**	System Admin
3	Ensure server is enabled and connected in CACF ansible tower (Run connectivity test) Ensure the organization is visible in NEXT (after AT40 completed) Ensure remediation role is enabled/setup in event github	TAA
4	**Trigger desired alert on monitored resource / TEST server (CPU load/Service/Process/File system..)**	System Admin
5	Look for triggered alert on monitoring console (SL1)	System Admin
6	Check the event visible in Netcool console: M&EaaS Event Viewer / Dashboard	MnE operator
7	Check Event field details : • verify INCident ticket number is present Check Netcool journal view : • Check ticket is created in ISM (Snow or ICD) and sent to automation group • Check event is sent to CACF-Ansible to trigger incident remediation • Check ticket in ISM tool - Do not take ownership of the ticket	MnE operator
8	Check the Alert Key (AK) in Netcool console Event field	MnE operator
9	Check Ticket visible in Maximo/SNOW - Do not take ownership of the ticket	System Admin
10	Verify a transaction is visible in NEXT to validate the incoming event (from Netcool)	TAA
11	Check mandatory fields in NEXT are not empty : INCIDENT number, AK Check additional / optional fields in NEXT are present, and filled depending on automation : ex InstanceID	TAA (MnE Event SME if KO)
12	Validate Netcool job template is triggered in CACF with specific remediation role	TAA
13	Check status in NEXT / Return code : • Check resolution code in Netcool Event Journal • Check resolution code in ticketing tool for for incident	TAA System Admin Mne Operator
14	Prepare new try or retry if unsuccessful: • Take ownership of the ticket and close previous ticket - To ensure new try will create a new ticket • Close the alert in Netcool/SL1 to be sure to restart with fresh alerts	System Admin

kyndryl

Enabling Incident Remediation from SL1 events

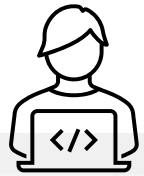
Alert/Event/Ticket/Automation flows / transactions

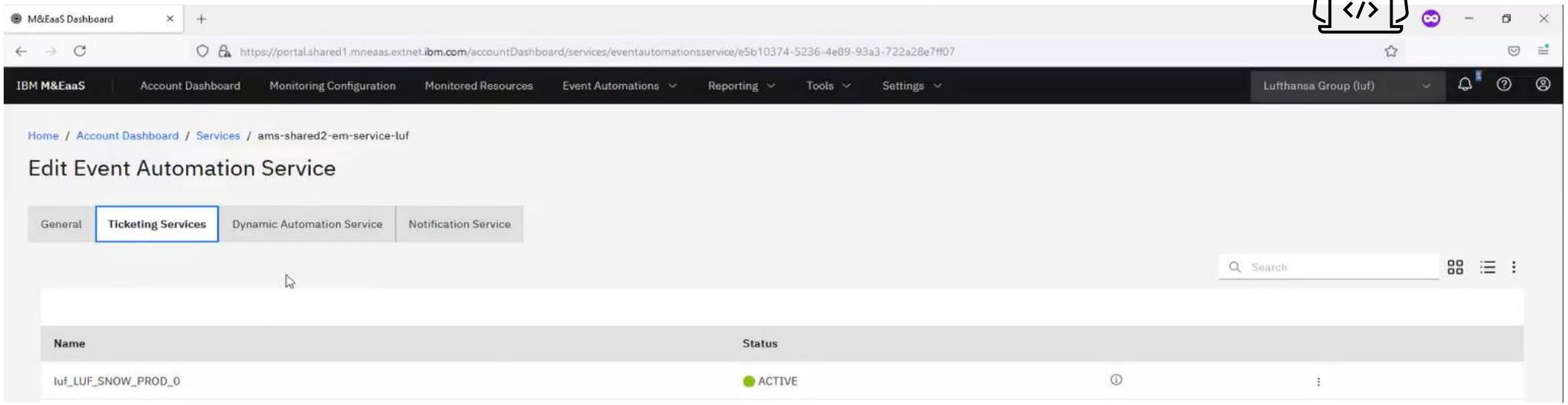
Monitoring & Event (Server / SL1 / NETCOOL) platform	Maximo / SNOW platform	CACF (ANSIBLE Tower / NEXT) platform
Generate a test alert on Server *(how-to)*		
Alert triggered by Science Logic → Alert forwarded to Netcool		
Alert in Netcool is enriched and if automation is requested (by config.)		
→ Netcool creates incident ticket in SNOW/MAXIMO in Automation queue	Ticket Created	
→ Netcool sends a request to NEXT for remediation (with inc. ticket number)		
		NEXT identifies event automation role (Smart Event Mapper) and triggers incident remediation in ANSIBLE Tower
		CACF ANSIBLE Tower connects to server and runs incident diagnosis / remediation code
		ANSIBLE Tower sends inc. remediation role return code (RC) back to NEXT
		NEXT sends back status (RC) to Netcool
Incoming Updates on alert are handled by Netcool	Ticket maybe Updated	NEXT may be updated
Netcool updates ticket on Status / Remediation code	Ticket Updated	
Case : Remediation with Corrective closure or Validation Closure (Success)	Ticket Closed in ISM	
Case : Remediation unsuccessful → Netcool escalates ticket to resolver (Failure)	Ticket Escalated to desired support group in ISM	

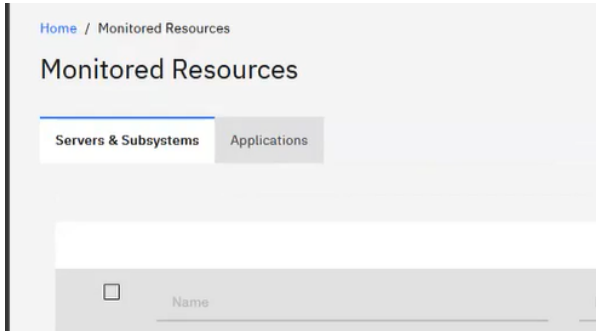
Enabling Incident Remediation from SL1 events

1. Prerequisite for automation in M&E Enablement :

Auto-Ticketing + Event Remediation is associated to the monitored server or resources in M&E Portal





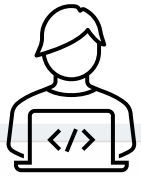


https://pages.github.kyndryl.net/mne/mneaas-userguide/account-dashboard/services/em/automation/

Enabling Incident Remediation from SL1 events

3. AT40 has **completed** - Check in Next : Account Organization settings

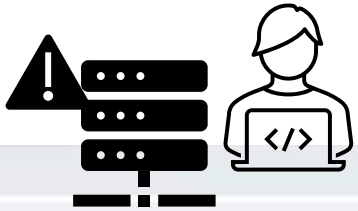
GitHub - **xxx_jobtemplate_netcool** repository exists, and automation job template is defined

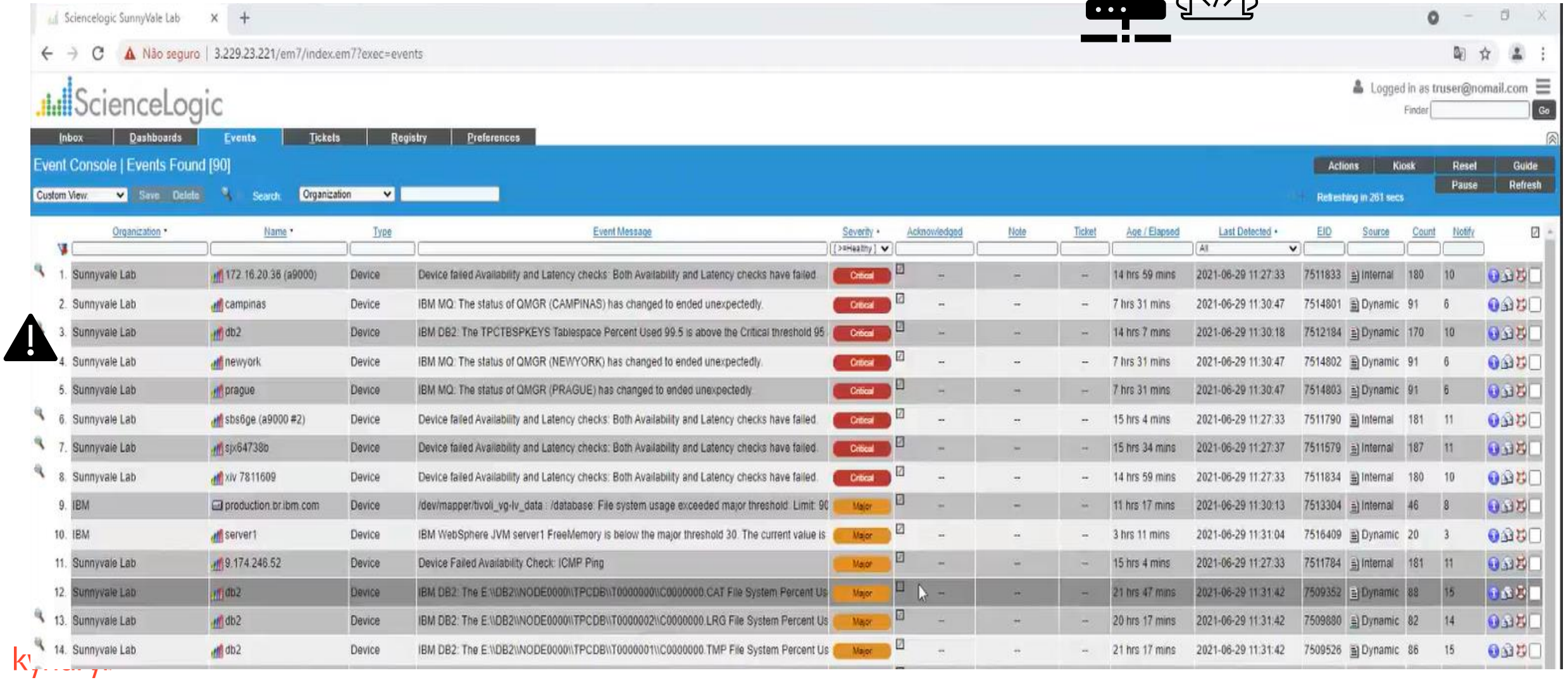


Enabling Incident Remediation from SL1 events

4. Trigger a test event on server (OS admin shall know how to do it)

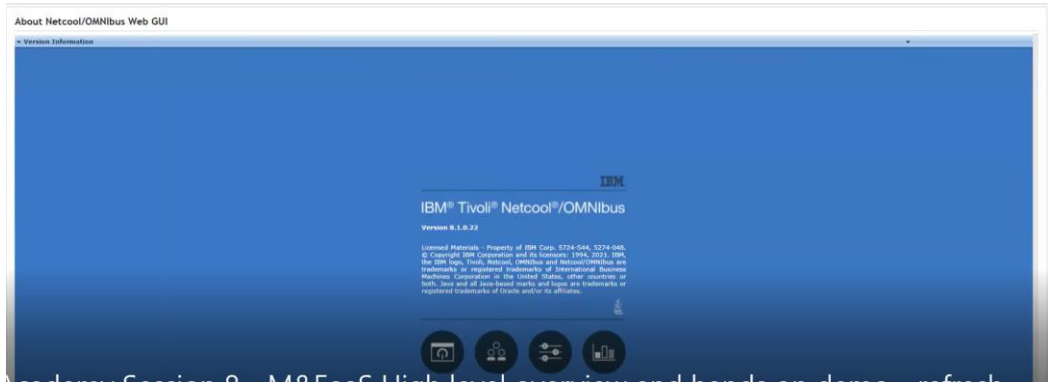
5. Check the event shows up on SL1 Events console

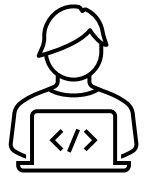


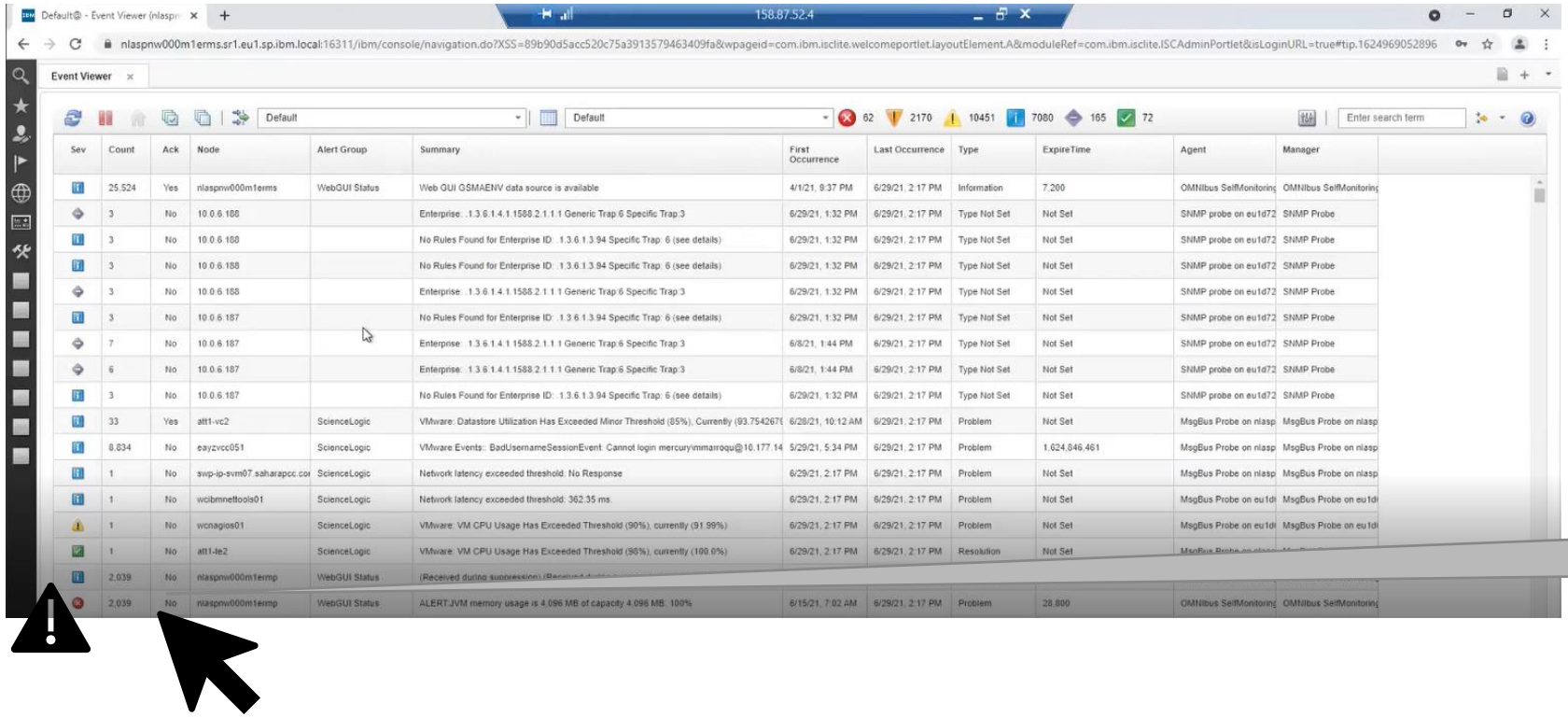


Enabling Incident Remediation

6. Check the event received on Netcool / Events Viewer dashboard







Enabling Incident Remediation

7. & 8. Check Event details & journal

Events journal

Event fields

Properties for event 3584378 on GSMAENV - Google Chrome

nlaspnw000m1erms.sr1.eu1.sp.ibm.local:16311/ibm/console/webtop/eventviewer/eventProperties.jsp?dir=ltr...

Properties for event 3584378 on GSMAENV

Fields | Details | Journal

Field	
InstanceId	overall
InstanceSituation	VMware: VM CPU Usage Has Exceeded Threshold
InstanceValue	91.99
InternalLast	6/29/21, 2:17 PM
JournalSent	0
LastOccurrenceUSec	0
LifecycleState	Unknown
LocalNodeAlias	
LocalPriObj	
LocalRootObj	
LocalSecObj	
Location	
MachineType	
ManagedSystemGroups	
Manager	MsgBus Probe on eu1d67lpppprtnp1

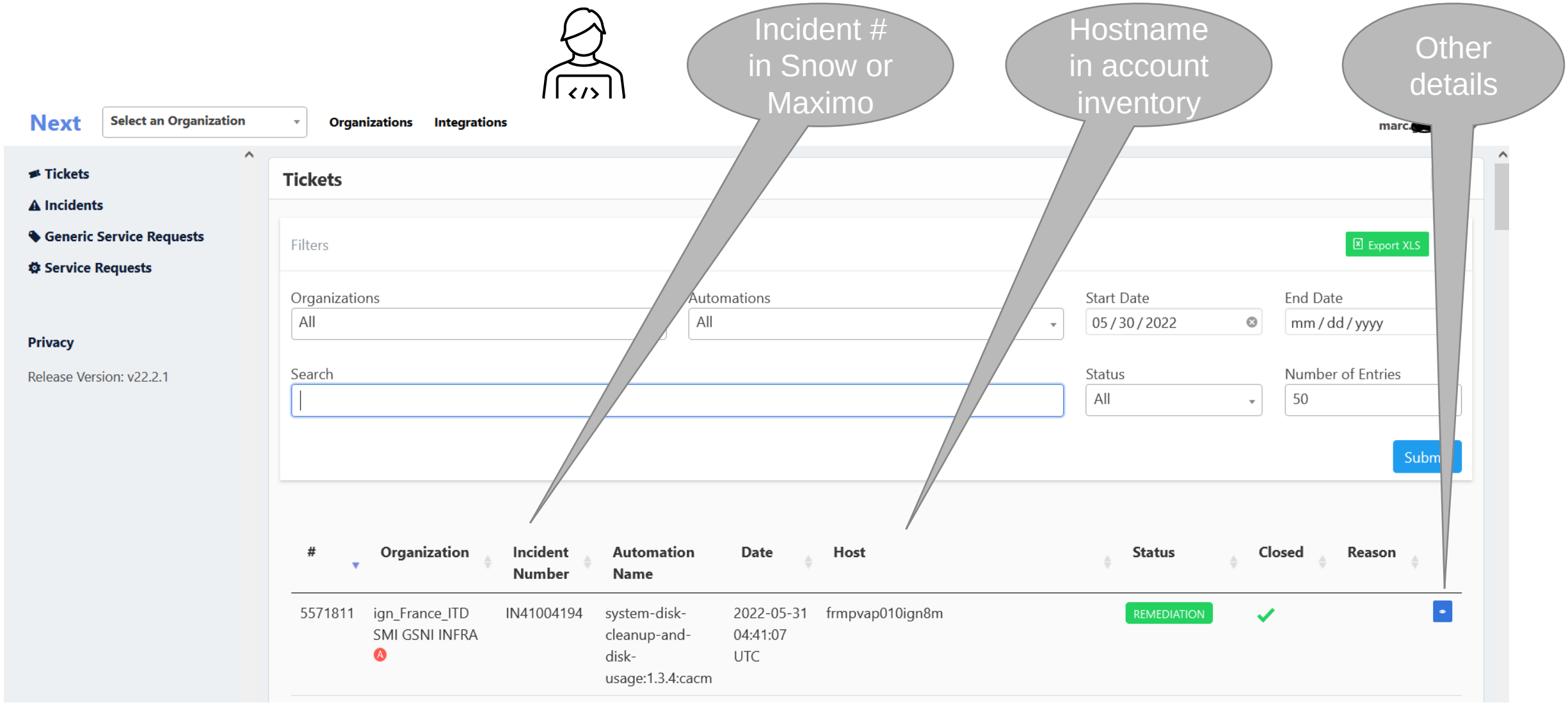
Close

Fields | Details | Journal

User ID	Date/Time	Journal Entry
root	Fri May 27 08:10:47 GMT 2022	Requesting Automation Engine Remediation with ActionId: 223 and AMID: 1223
root	Fri May 27 08:10:48 GMT 2022	Automation Engine Remediation activated using Automation Engine :Ansible_Tower_EU1_Sonepar
impact	Fri May 27 08:10:53 GMT 2022	Ticket (IN40995198) AMTicket () CREATE_SUCCESSFUL
root	Fri May 27 08:11:00 GMT 2022	Request to Automation Engine Accepted. Waiting for results.
root	Fri May 27 08:11:02 GMT 2022	Create acknowledged; IPIM received Estimated time to perform : 60 minutes.
root	Fri May 27 08:11:05 GMT 2022	Ticket sucesfully updated: IN40995198 Assigned
impact	Fri May 27 08:11:05 GMT 2022	Ticket (IN40995198) AMTicket (5541898) UPDATE_SUCCESSFUL
root	Fri May 27 08:11:11 GMT 2022	Request to update IPIM ticket with IPC ticket number has completed successfully.
root	Fri May 27 08:13:44 GMT 2022	Successfully RESOLVED by Automation Engine, for more information see IPC TICKET number :IN40995198
impact	Fri May 27 08:13:51 GMT 2022	Ticket (IN40995198) AMTicket (5541898) UPDATE_SUCCESSFUL
root	Fri May 27 08:13:51 GMT 2022	Ticket sucesfully updated: IN40995198
impact	Fri May 27 08:30:44 GMT 2022	Ticket (IN40995238) AMTicket (5541898) CREATE_SUCCESSFUL

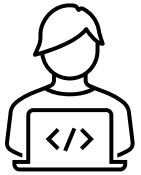
Enabling Incident Remediation

10. Verify Incident ticket corresponding to test event in Next



Enabling Incident Remediation

11. & **12.** Look into Next ticket details and verify contents



Next | Select an Organization | **Organizations** | **Integrations**

- **Tickets**
- **Incidents**
- **Generic Service Requests**
- **Service Requests**

Privacy

Release Version: v22.2.1

```
CLOSURE CODE: Remediation with Corrective Closure
RC: 0
RESULTS: resolve
Automation Result: "Free space on C: is bigger than  10 % after automation execution. It has 32.54 GB
 or 33321 MB
 or 32.68 % free
after automation execution."
```

TICKET Description :

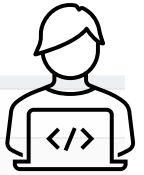
```
Summary: Windows Logical Drive:C: space problem. Percent Free:7. MB Free:7616. Thresholds: 15. 10. 5. Attention commas replaced by dots.
Date: 2022-05-31T06:41:06Z
Severity: 2
ResourceId: frmpvap010ign8m.inf.ibmfr.bluecare.ibm.com
CustomerCode: inf
InstanceId: C:
InstanceSituation: alert if disk free space is low
AlertKey: all_dskspce_g06w_win_gen
TicketGroup: I-DTE-XX-CLD-CL3-AUTOM
InstanceValue: MON_M
ComponentType: OperatingSystem
Component: Windows
SubComponent: Disk
ApplId: WIN
Node: inf_frmpvap010ign8m
NodeAlias: 129.39.133.220
AlertGroup: ITM_K06_LOGICAL_DISK
EventType: 6830
MonitoringSolution: win
EventKey: undefined
```

Enabling Incident Remediation

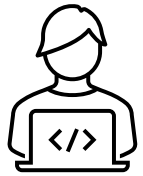
13. Validate return codes in each place :

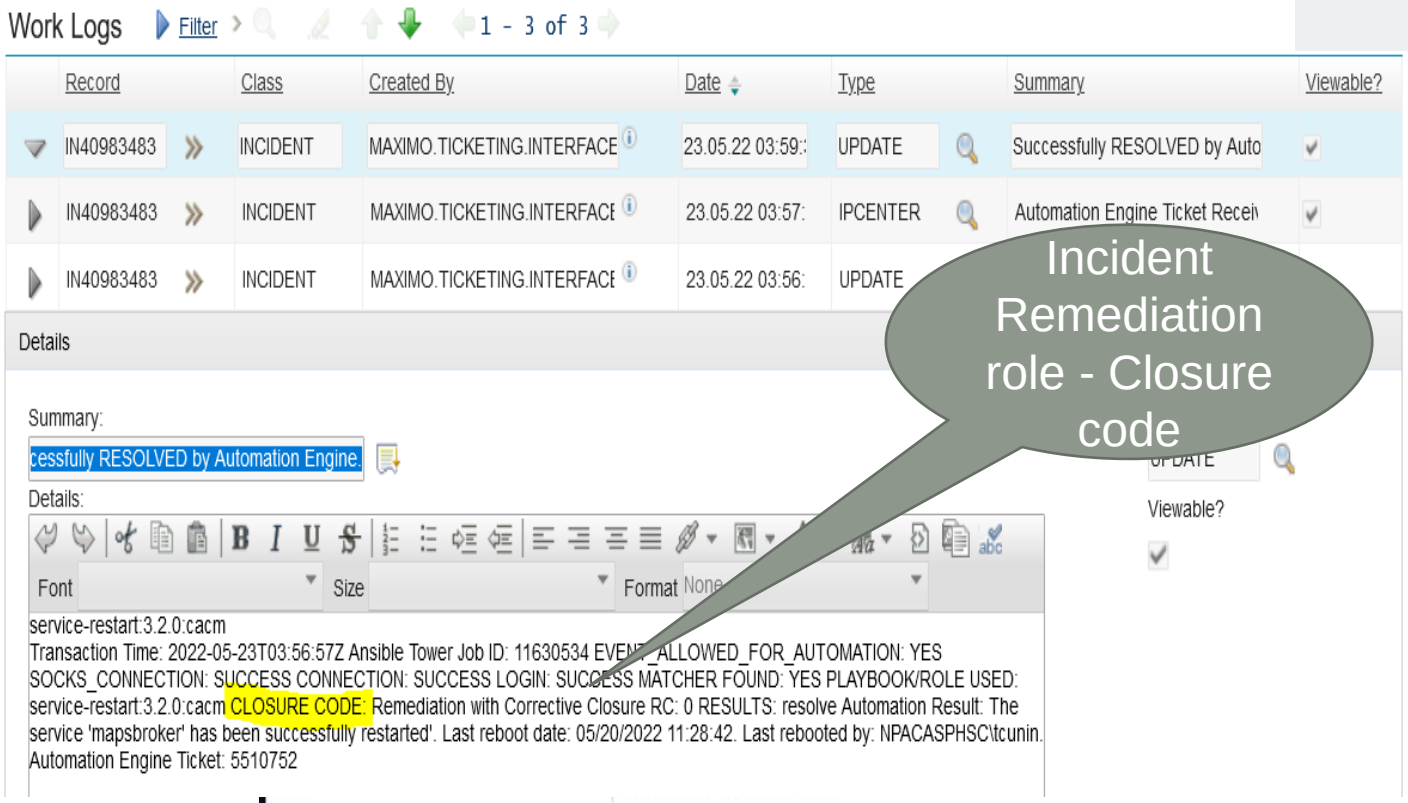
'Note: when Incident remediation completed OK, the ticket shall be closed in ticketing system (Maximo / Snow).

in NEXT : status

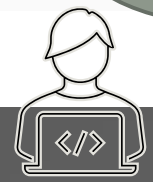


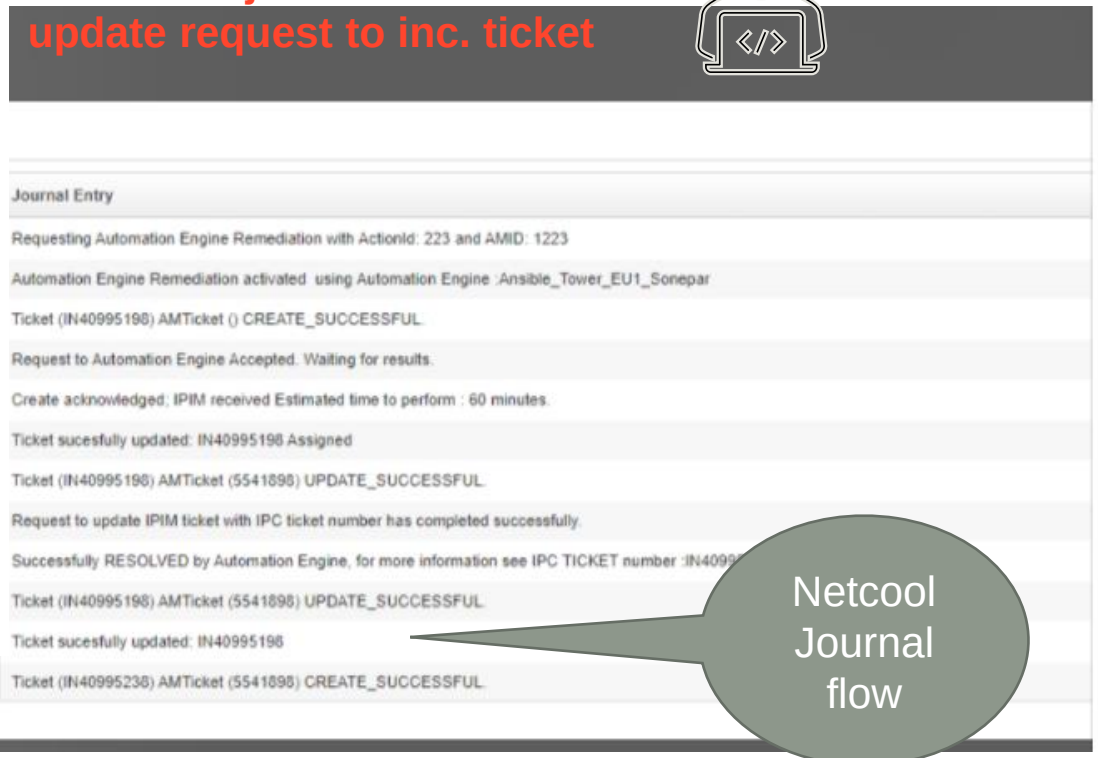
in ISM (Maximo) : Closure code shows end to end was successful (RC = 0)





in Netcool journal : check update request to inc. ticket

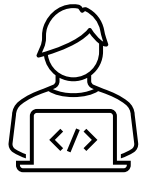




Enabling Incident Remediation

KSI Automation performance provides a summary view (with small delay)

- Based on NEXT data only, with detail on CACF return codes
- Remember: No end-to-end insight in ticketing system (Maximo or SNOW)



kyndryl Service Insights — CACF Automation Performance Dash (EMEA & Japan) — Kyndryl Delivery

mrspl00173.cc0.ibmfr.bluecare.ibm.com	107
mrs-db-00030.cc0.ibmfr.bluecare.ibm.com	52
lpb000ansx01.bcrs.fr	44
frmppdb00sri1xm.inf.ibmfr.bluecare.ibm.com	36
ledci035.edd.ibmfr.bluecare.ibm.com	33
oncgp2p1.mna.ibmfr.bluecare.ibm.com	32
sg2vm001.map.ibmfr.bluecare.ibm.com	28
parvem001.mic.ibmfr.bluecare.ibm.com	26

Export: Raw Formatted

1 2 3 4 5 ... 1000 »

cma_project_hwsw_scanning	11,021
cma_project_ilmt_aicv3	10,711
cfr_project_hwsw_scanning	9,535
scs_project_cacftools	8,901
cma_project_eu_services	8,598
scs_project_hwsw_scanning	8,227
scs_project_vulnerability-scanner_find-log4j	7,770
cma_project_at_host_connectivity	5,870

Export: Raw Formatted

1 2 3 4 5 ... 102 »

Connectivity_Check.yml	19,927
GCM-Scan-Windows-OS.yml	16,204
sdms_playbook.yml	16,066
find-log4j.yml	14,044
NoSocksTunnel_gather_facts_sss_unix.yml	13,614
generic_single_extractor.yml	12,366
checkconn_unix.yml	11,221
Hello_Windows.yaml	10,836

Export: Raw Formatted

1 2 3 4 5 ... 28 »

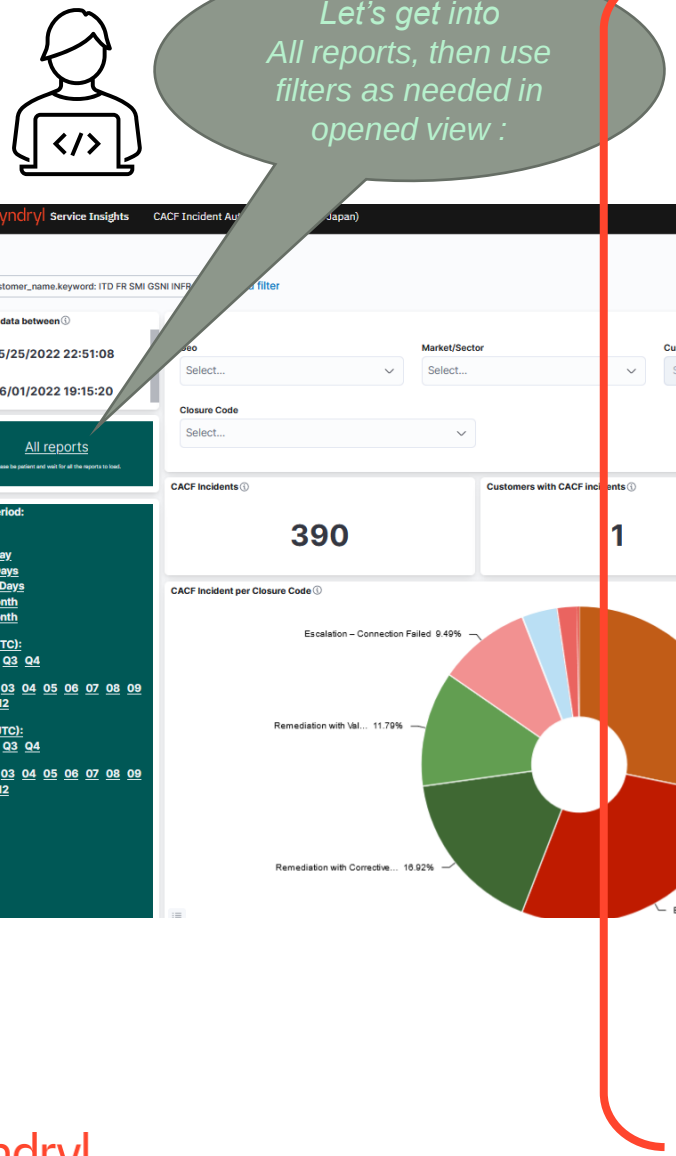
Task Level Details

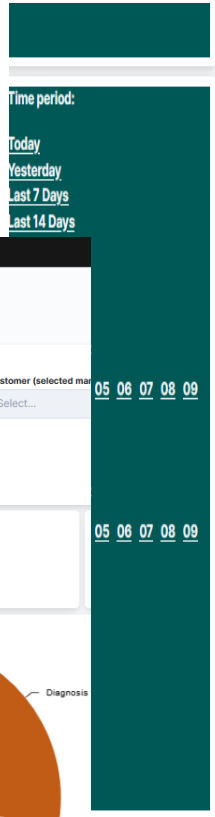
403160 documents

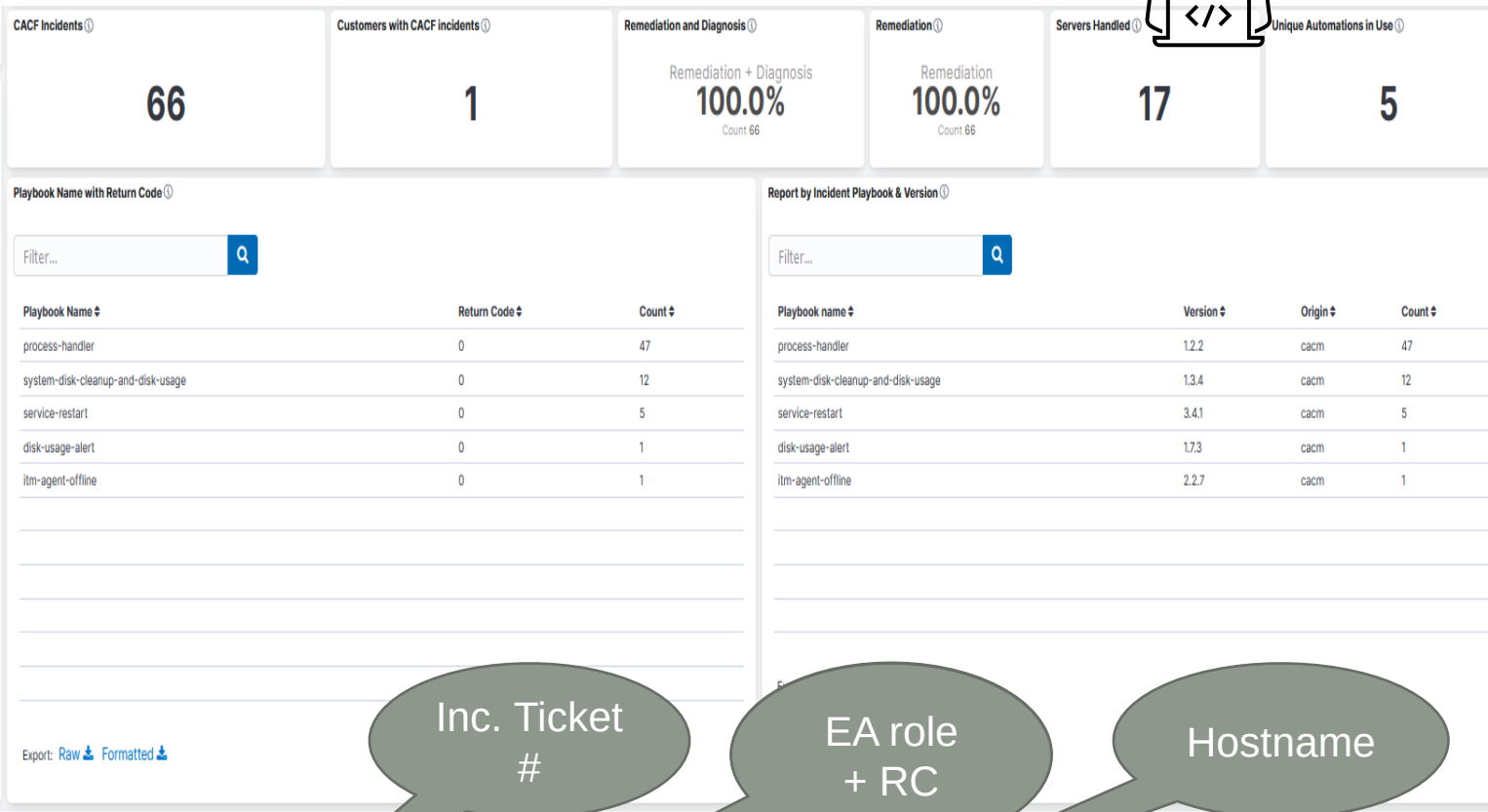
Time	Account	host_name	job_id	rc_support	rc_group	rc_number
May 31, 2022 @ 09:01:24.822	CMA-CGM GROUP	mrspl00272.cc0.ibmfr.bluecare.ibm.com	11821171	developer	Success Without Return Code	-1
May 31, 2022 @ 09:00:52.886	ITD FR SMI GSNI INFRA	SRMEUWAS02.inf.ibmfr.bluecare.ibm.com	11821149	undetermined	Connection Issue	-2
May 31, 2022 @ 09:00:41.024	Michelin	atlpswvp21.mna.ibmfr.bluecare.ibm.com	11821147	developer	Success Without Return Code	-1
May 31, 2022 @ 09:00:39.592	Michelin	vldrdiil001.mic.ibmfr.bluecare.ibm.com	11821145	account	Connection Issue	106
May 31, 2022 @ 09:00:23.239	CMA-CGM GROUP	mrspl00173.cc0.ibmfr.bluecare.ibm.com	11821122	developer	Success Without Return Code	-1
May 31, 2022 @ 09:00:21.101	Cegid	vcli01dwaaa001.cdg.lan	11821119	developer	Success Without Return Code	-1

Enabling Incident Remediation

KSI Incident Automation provides a pretty complete overview of EA roles execution end to end







Thank you for using this guide.

Any suggestion or correction is welcome.

→ contact owners: Marc Galabert / Fred Michelis