

IBM Inter-University Programming Contest 2012 Training

Chapter 2:Tivoli Netcool/OMNibus

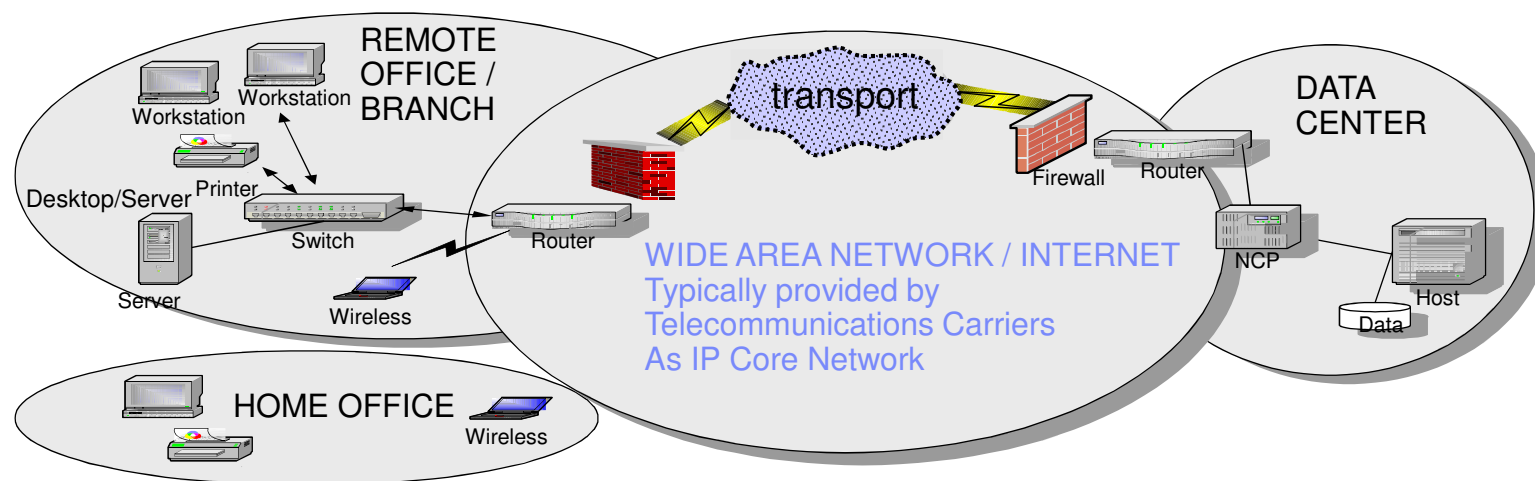


IBM Inter-University **Programming Contest** **2012**

February 11, 2012 (Saturday)
Cliftons, Hong Kong



What is Event Management? – Extended into Complex Networked Environments



- Large complex infrastructures, increasingly interconnected by variety of providers
- Ever increasing dependency on higher bandwidth / broadband for new “triple play” services (e.g., Voice, Video, and Data)
- Maintaining high Quality of Service (QoS) is key for multiple services sharing the same network
- Increased range and reach of networks leads to reliance on skilled operators when solving problems
- Determining the actual cause of certain problems requires understanding events across IT and Network disciplines

The goal of **End-to-End Event Management** is to consolidate events, to focus on “root causes” (and identify related “symptoms”), and – where possible – to automate the resolution in response to any problem in the entire environment reducing MTTR (Mean time to Repair) and maintaining QoS within the network.

Tivoli Netcool/OMNibus

Market Leading
Event Consolidation, Correlation &
Automation

Meeting the challenges of
Dynamic Infrastructure Management



More smart assets
Greater complexity
Escalating event volumes

- Maximize Service Availability. Leverage hundreds of out-of-the-box integrations, with included domain intelligent event reduction rules, to monitor end-to-end infrastructure status and health.
- Reduce Operational Costs. Consolidate NOCs, tools and management sources into a single pane-of-glass and integrated management infrastructure.
- Improve Staff Productivity. Utilize normalization, de-duplication, aggregation, correlation capabilities, as well as time, device, and service based event reductions.

Seamless UI navigation based on common Tivoli GUI architecture delivers task-based workflows that represent common operations used to perform operations and service management actions

- Minimize human intervention. Exchange information between peer systems and automate maintenance actions and procedures.
- Increase Confidence. Leverage proven availability and reliability, with huge event throughput capability, trusted system redundancy, failover and security.

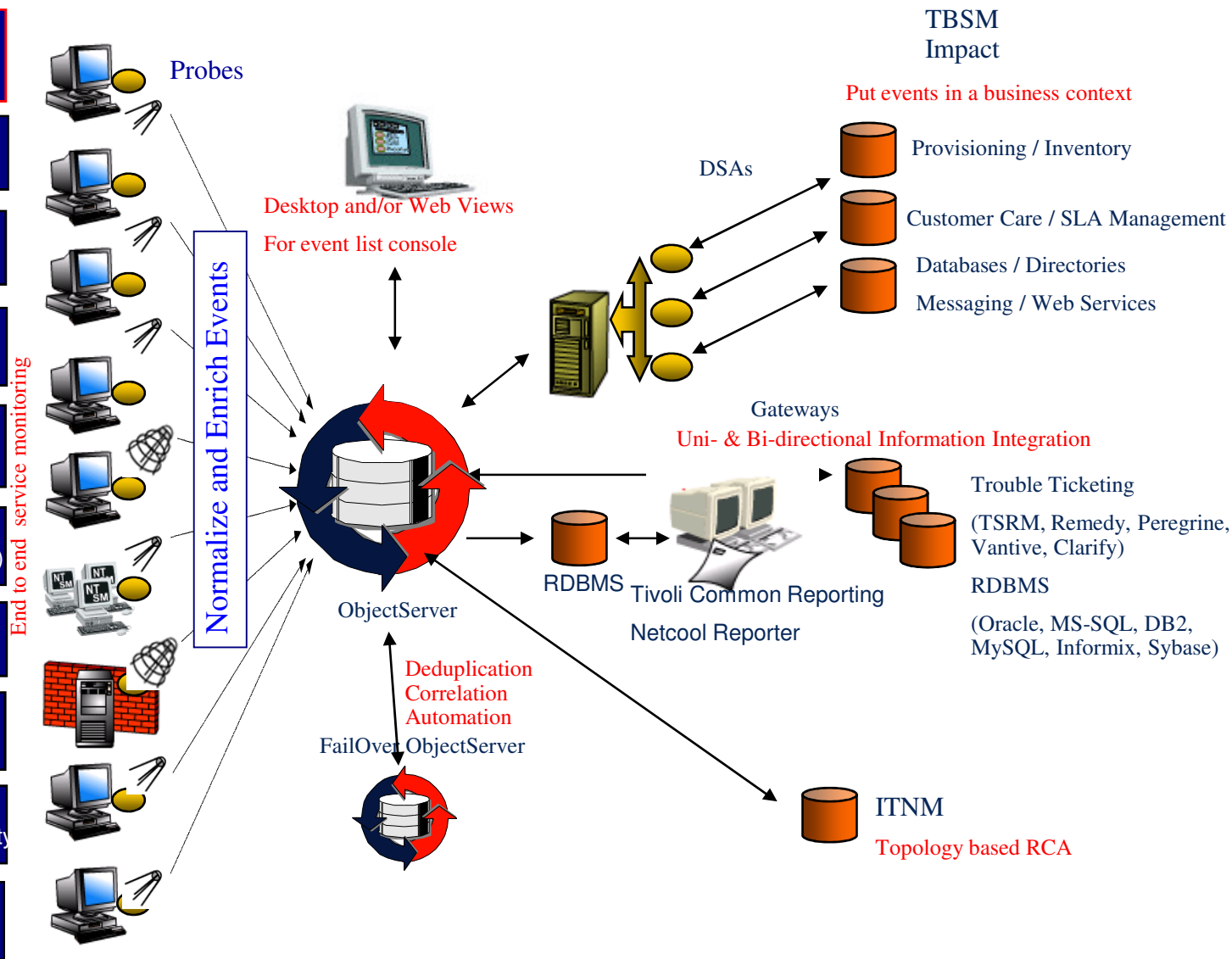


IBM Tivoli Netcool OMNIbus

Tivoli software

Tivoli Netcool/OMNibus Solution

- Tivoli Suite
ITM, TEC, OMEGAMON
- Data Network
(SNMP, Syslog)
- Systems & Applications
(Mainframe, Unix, Windows)
- Other Management Systems
(HP OpenView, BMC, Mercury...)
- Voice Network
(PBX, IVR, Class 5 switches)
- Voice Over IP
(Cisco, Nortel, Avaya, Siemens)
- End User Experience and
Transaction Monitoring
- Security/Firewalls
- Non-IT Resources
(HVAC, UPS's, Physical Security)
- Future



Netcool/OMNIbus Integrations (250+)

Netcool Knowledge Library SNMP support (>175 MIBs), including:

Bridge MIB RFC 1493	ATM Forum MIB RFC 1695 for ATM switches	31 different Cisco MIBs (including MPLS VPNs)
MIB-II RFC 1213/2096	ATM Forum PNNI (Single Pier) MIB	21 Nortel MIBs
RMON MIBs	ATM Forum ILMI MIB	6 different Extreme Networks MIBs (inc VLANs)
OSPF MIB	ATM Forum LANE Client MIB	Juniper MPLS VPN support
BGP MIB	Frame Relay MIB RFC 1315	
ifStack MIB	FDDI MIB RFC 1512	
VRRP MIB		

Alcatel OMC-R Probe
 Alcatel OMC-S Probe
 Alcatel OSOS TSM
 Alcatel S12 Probe
 Alcatel SMC 1360 S12 Q3 Probe
 AMS Probe
 Aprisma Spectrum Probe
 ARCOM Probe
 Ascom PANMAN Probe
 Ascom TimePlex TimeView Probe
 Avaya Definity G3 Probe
 BMC Patrol Probe
 CA Unicenter TNG Probe
 Castlerock SNMP Probe
 CEMF Probe
 CFS Probe
 Ciena Oncenter Probe
 CLOG Probe
 CMS400 Probe
 Converse Probe
 Dantel Pointmaster Probe
 Datawatt Probe
 Dawcom Probe
 DEC VAX OpCom Probe
 DFMS Probe
 Eagle STP Probe
 ECI LightSoft probe
 ECI eNM, EMS-XDM and EMS-Syncom probe
 EIF Probe
 Email Probe
 Ericsson ACP1000 Probe
 Ericsson AXE10 TSM
 Ericsson BNSI Probe

Gateway for MS SQL
 Gateway for MySQL (ODBC)
 Gateway for ODBC
 Gateway for Oracle
 Gateway for Peoplesoft Vantive
 Gateway for Peregrine Service Center
 Gateway for Remedy ARS
 Gateway for Reporter
 Gateway for Siebel 6 eCommunications
 Gateway for Siebel 6 Field Service Desk
 Gateway for SNMP
 Gateway for Sockets
 Gateway for Sybase
 Generic Logfile Probe
 Glenayr VMS Probe
 Heartbeat Probe
 HP IT/Operations Probe
 HP NNM Probe
 HTTP Common Log Format Probe
 HTTP Server Error Log Probe
 Huawei T2000 MML Probe
 Hughes Probe
 IBM Netview Probe
 IBM/Tivoli TEC Oracle Probe
 IBM/Tivoli TEC Sybase Probe
 IBM/Tivoli TME 10 TEC Adapter Probe
 IDNX Probe
 INET Geoprobe Probe
 Informix Probe
 IOC Probe
 Ion Networks Sentinel 2000 Probe
 KBU Probe
 Kodak EMS

Motorola OMC-R Q3 Probe
 Mototola OMC-R 3GPP Probe
 NET 5000 Probe
 NET Promina Probe
 Netlabs Probe
 NewNet SMS Probe
 Nokia Netact for Broadband Probe
 Nokia Netact for Wireless Probe
 Nokia NMS100 Probe
 Nokia NMS2000 Probe
 Nokia SBT Probe
 Nortel BSSM Probe
 Nortel DMS TSM
 Nortel DMS10 Probe
 Nortel EAI Probe
 Nortel EC1 Probe
 Nortel EVDO Probe
 Nortel FMBB Probe
 Nortel Magellan NMS Probe
 Nortel MDM Probe
 Nortel Meridian Probe
 Nortel MG9000 Probe
 Nortel OMC-R Q3 Probe
 Nortel OSSI Probe
 Nortel PTM Probe
 Nortel PWI 3GPP Probe
 Nortel STP Probe
 Nortel USP Probe
 NT Event Log Probe
 Octel Probe
 ODBC Probe
 Okeford Probe
 Open Nervecenter Probe

Vendor Alliances (~25) on OPAL:

- Alcatel
- Motorola
- Siemens
- Ericsson
- Tellabs
- Marconi
- Lucent
- Nokia
- Huawei
- Fujitsu
- Ciena
- Cisco
- Juniper
- Checkpoint
- Cramer
- Metasolv
- SAP
- Xtera
- Voyence

New and updated versions are developed and deployed on a quarterly basis.



IBM Tivoli Netcool OMNIbus Probe

Tivoli software

What are Probes?

- **Probes are software components used to collect event information and send it to the ObjectServer.**
- **Probes enable the ObjectServer to be independent of the systems or devices being monitored.**
 - Over 300 types of probe
 - Both generic and vendor-specific probes exist
- **Probes can modify and enrich event information**
 - Use additional information from lookup tables
 - Perform arithmetic functions
- **Probes are resilient**
 - Reliable TCP connection
 - Store and forward functionality (SAF)
 - Automatic fail-over to alternate ObjectServer

What are Probes? (continued)

- **The ObjectServer obtains most of its event data via the probes**
 - Event data may be also obtained via Automations, Tools, Gateways or SQL
- **Every probe comprises a binary, a rules file and a properties file:**
 - *Probe binary* retrieves and tokenises event streams, and sends the event to the ObjectServer.
 - Interpreted *rules file* used to populate the field values within alerts.status
 - *Properties files* determine the run-time settings of the probe.

Netcool Omnibus Probes

- Collection
 - Source-specific code for integrating with 3rd party systems and event synchronisation
 - Standard protocols: SNMP, Syslog, ODBC, 3GPP...
 - Custom message formats: Socket, Logfile
 - Proprietary/API: Many Vendors
- Normalisation
 - Common code for rules-based event processing:
 - Normalisation
 - Enrichment
 - Human Readability
 - Pre-classification for ObjectServer Correlation and Netcool processing

Types of Probes

- Device
- Log file
- Database
- API
- CORBA
- Miscellaneous
- Security

Netcool Omnibus Probes – Rules File Example

```

if( match( @Manager, "ProbeWatch" ) )
{
  switch(@Summary)
  {
    case "Running ...":
      @Severity = 1
      @AlertGroup = "probestat"
      @Type = 2
    case "Going Down ...":
      @Severity = 5
      @AlertGroup = "probestat"
      @Type = 1
    default:
      @Severity = 1
  }
  @AlertKey = @Agent
  @Summary = @Agent + " probe on " + @Node + ": " + @Summary
}
else
{
  @Manager      = "Simnet Probe"
  @Class        = 3300
  @Node         = $Node
  @Agent        = $Agent
  @AlertGroup   = $Group
  @Summary      = $Summary
  @Severity     = $Severity
  @Identifier   = $Node + $Agent + $Severity + $Group

  if (nmatch($Summary, "Port failure"))
  {
    @AlertKey = $PortNumber
  }
  else if (nmatch($Summary, "Diskspace"))
  {
    @AlertKey = $PercentFull + "% full"
  }

  if(regmatch($Summary, ".*Down.*")){
    @Identifier = "Down" + @Identifier
    @Type = 1
  }
  if(regmatch($Summary, ".*Up.*")){
    @Type = 2
  }
}

```

- Base Fields
 - Identifier
 - Severity
 - Node
 - AlertGroup
 - AlertKey
 - Summary
 - Agent
 - Type



IBM Tivoli Netcool/OMNIbus Web GUI

Tivoli software

AEL Features

Active Event List

Default Default

Sev	Ack5	Node [1]	Last Occurrence [2]	Alert Group	Summary
✖	No	Beijing	09/10/09 10:16:55	Stats	Diskspace alert
⚠	No	Beijing	09/10/09 10:18:28	Stats	Diskspace alert
✖	No	Berlin	09/10/09 10:48:28	Link	Port failure : port reset
⚠	No	device_0	09/10/09 10:22:46	Systems	Machine has gone offline
ℹ	No	device_0	09/10/09 10:29:33	Systems	Machine has gone online
✔	No	device_10	09/10/09 10:47:28	Link	Link Up on port
⚠	No	device_10	09/10/09 10:48:21	Link	Link Down on port
⚠	No	device_100	09/10/09 10:43:50	Systems	Machine has gone offline
ℹ	No	device_100	09/10/09 10:47:55	Systems	Machine has gone online
⚠	No	device_1000	09/10/09 09:42:50	Systems	Machine has gone offline
ℹ	No	device_1000	09/10/09 09:46:55	Systems	Machine has gone online
⚠	No	device_10000	12/08/09 15:55:30	Stats	Diskspace alert
⚠	No	device_10000	12/08/09 16:32:56	Stats	Diskspace alert
⚠	No	device_10001	12/08/09 15:09:15	Stats	Diskspace alert

Filter and view type icon

Multi-column sorting on client-side

Icons in severity column

Column locking

Multiple data sources

Next refresh time indicator

Alternative event selection. Tivoli L&F.

Large number of events

63,101 rows inserted, 63,102 rows updated, and 0 rows deleted.

Data Source(s): UK,NCOMS,GERMANY QuickFilter: None Auto refresh in: 50 sec.

4976 50 13150 12781 32124 20 All Events (63101)

Active Event List – ‘Tivoli Enterprise Console’ Style Look and Feel

The screenshot shows a window titled "Active Event List" with a menu bar (File, Edit, View, Alerts, Tools, Help) and a toolbar. The main area contains a table with the following data:

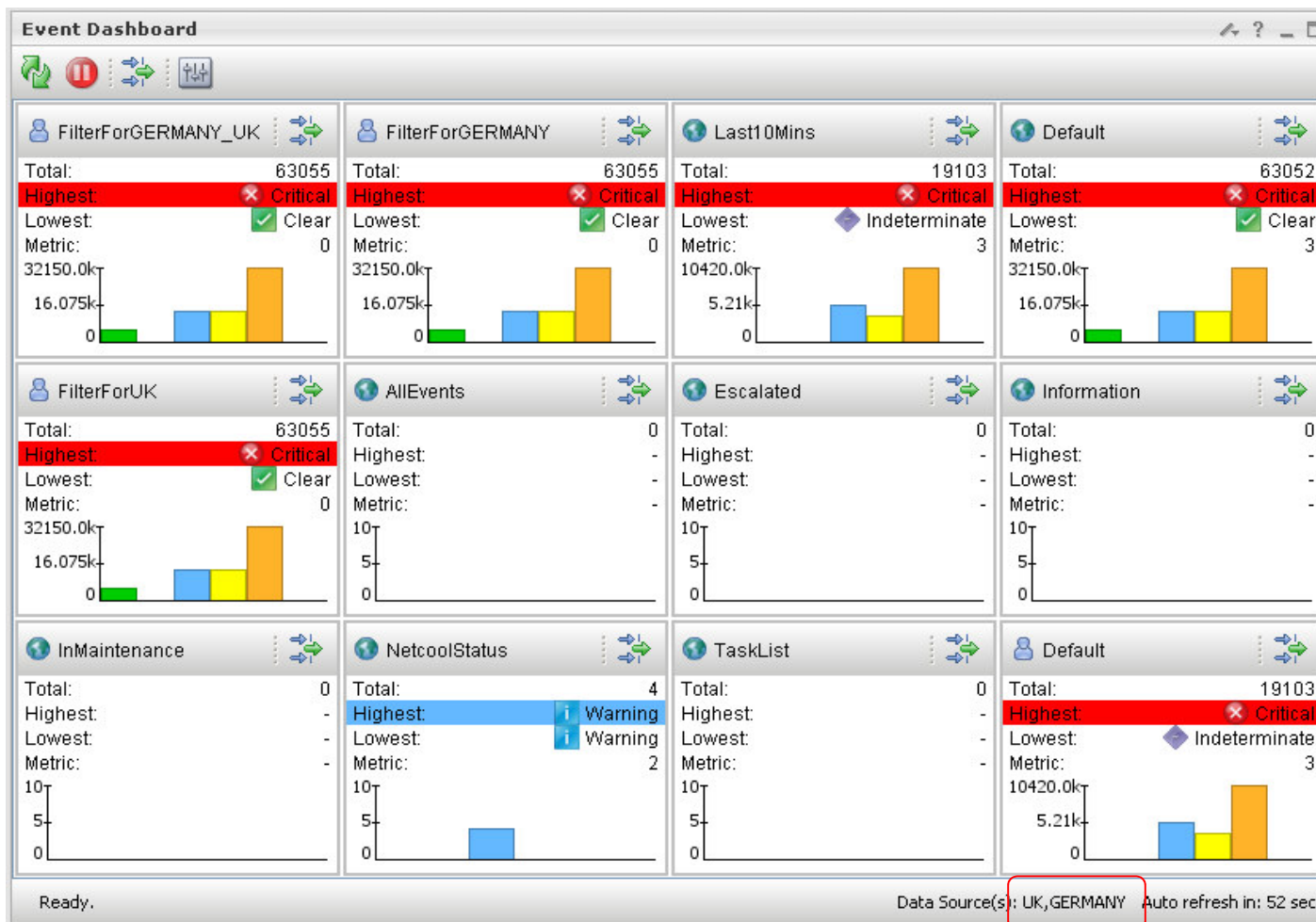
Sev	Freeze/Unfreeze updates to this window (Ctrl+Z)	Alert Group	Summary	
▼	No	WebServer3	Systems	Machine has gone offline
▼	No	WebServer2	Systems	Machine has gone offline
▼	No	LoadBalancerPrimary	Systems	Machine has gone offline
▼	No	link4	Link	Link Down on port
▼	No	FirewallBackup	Systems	Machine has gone offline
▼	No	WebServer1	Systems	Machine has gone offline
▼	No	FirewallPrimary	Systems	Machine has gone offline
▼	No	link2	Link	Link Down on port
▼	No	London	Systems	Machine has gone offline
▼	No	link3	Link	Link Down on port
▼	No	link1	Link	Link Down on port
▼	No	link5	Link	Link Down on port
▼	No	LoadBalancerBackup	Systems	Machine has gone offline
▼	No	Moscow	Systems	Machine has gone offline
▼	No	DatabasePrimary	Stats	Diskspace alert

At the bottom, there is a status bar with three colored segments: a blue segment with "16", a yellow segment with "2", and an orange segment with "17". To the right of these segments is a button labeled "All Events (35)". Below the status bar, it says "1 rows selected" and "Data Source(s): LOADED,NCOMS QuickFilter: None Auto refresh in: 10 sec."

Event Dashboard

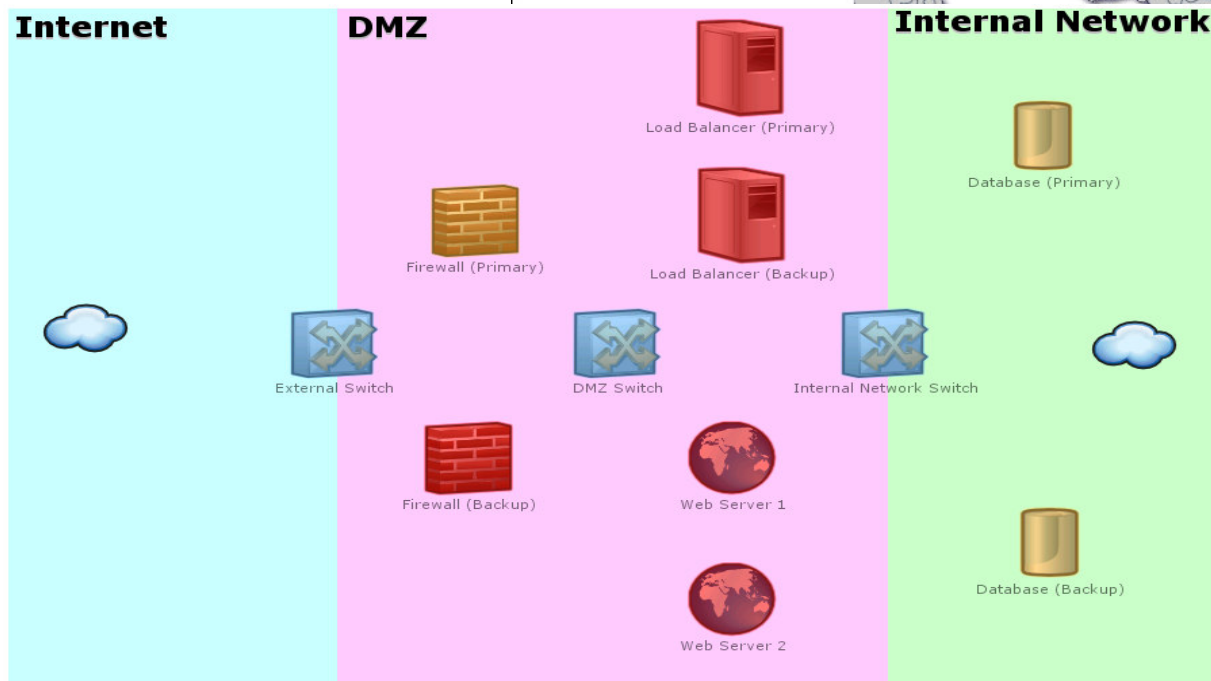
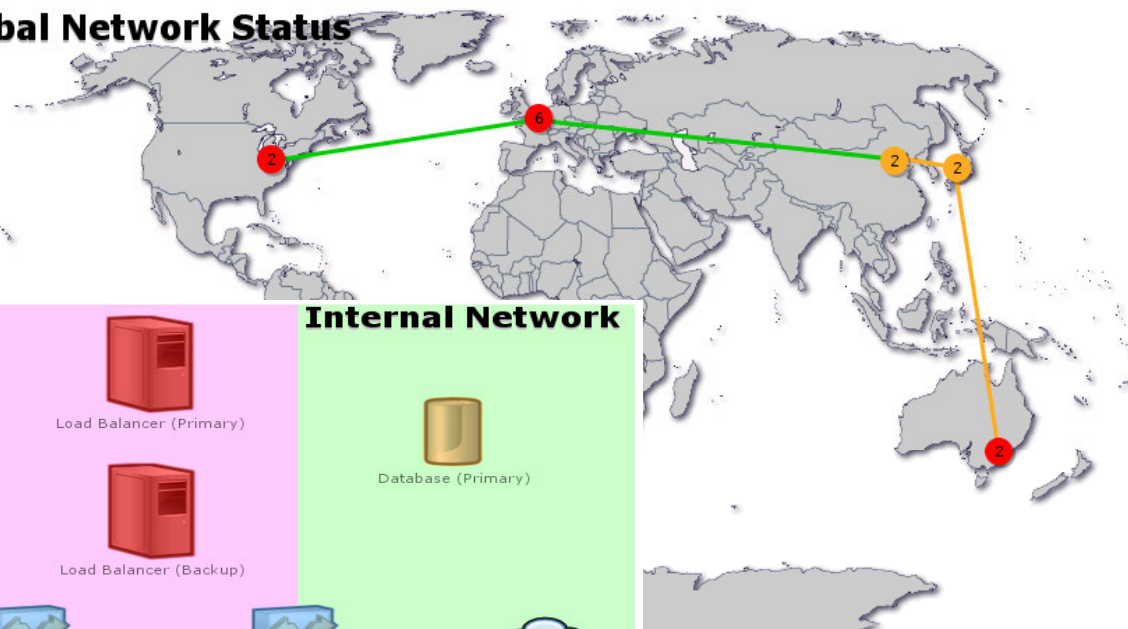
Tivoli software

Event Dashboard



Map Refresh

Global Network Status



Event Triggers for Automation

Tivoli software

Clear Event Trigger

Configuration of NCOMS on dash:4100

Name	Group	Kind	Priority	Debug	Enabled	Group E...
audit_config_alter...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_alter...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_alter...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_alter...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_alter...	audit_config	Signal	1	✗ false	✓ true	✗ false
audit_config_alter...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_alter...	audit_config	Signal	1	✗ false	✓ true	✗ false
audit_config_alter...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_crea...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_crea...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_crea...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_crea...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_crea...	audit_config	Signal	1	✗ false	✓ true	✗ false
audit_config_crea...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_crea...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_crea...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_crea...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_drop...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_drop...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_drop...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_drop...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_drop...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_drop...	audit_config	Signal	1	✗ false	✓ true	✗ false
audit_config_drop...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_drop...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_drop...	audit_config	Database	1	✗ false	✓ true	✗ false
audit_config_per...	audit_config	Signal	1	✗ false	✓ true	✗ false
automatic_backup	automatic...	Temporal	1	✗ false	✗ false	✓ true
backup_counterp...	gateway_tri...	Signal	1	✗ false	✗ false	✓ true

Rows: 85

Trigger Language

The screenshot shows a software interface with a tabbed menu at the top containing 'Settings', 'When', 'Evaluate', 'Action', and 'Comment'. The 'Action' tab is selected, displaying a PL/SQL trigger definition. The code is as follows:

```

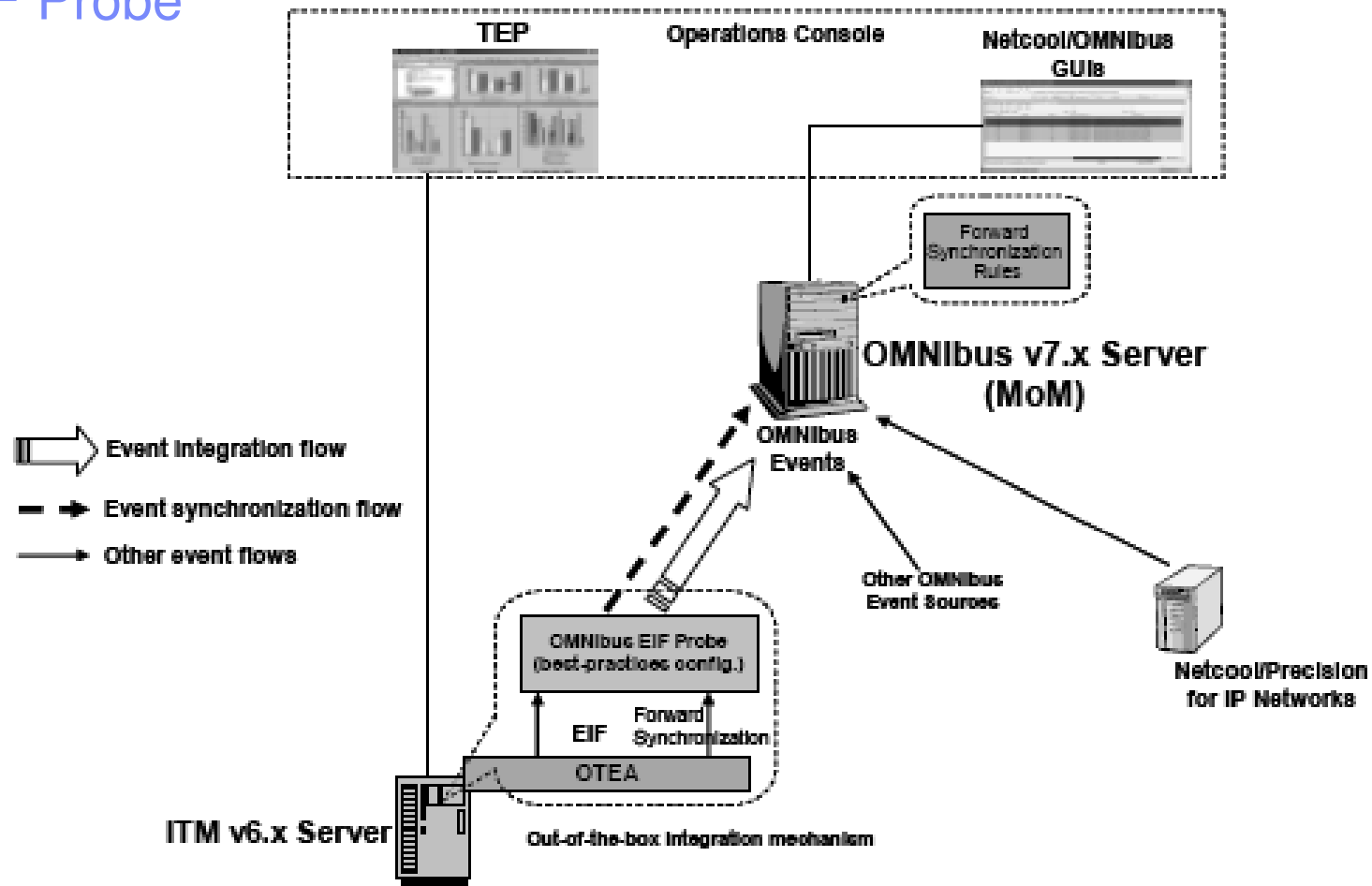
begin
  -- Populate a table with ITM Type 20 events corresponding to any
  -- uncleared Type 21 events.
  for each row problem in alerts.status where
    problem.ITMStatus = " and problem.Type = 20 and
    problem.Severity > 0 and
    (problem.Manager) in
      ( select Manager from alerts.status where Severity >
0 and Type = 21 )
  begin
    insert into alerts.itm_problem_events values (
      problem.Identifier, problem.LastOccurrence,
      problem.ITMHostname, problem.ITMStatus, problem.ITMTime,
      problem.ITMEventData, problem.TMResetFlag, problem.ITMThruNode,
      problem.ITMAppLabel,
      problem.ITMTime, problem.AlertSource, problem.AlertKey
  
```

On the right side of the code editor, there is a vertical toolbar with several icons: an 'SQL' icon, a red and blue box icon, a yellow arrow icon, a yellow percentage icon, a red and blue box icon, and a blue checkmark icon.

Event Clear Trigger and Dashboard Status Update Demonstration

Tivoli software

Tivoli EIF Probe



- Sends Event Integration Facility (EIF) events (Tivoli Enterprise Console Events) to OMNibus.
- Maps TEC event fields to OMNibus fields.

What we need for sending EIF events

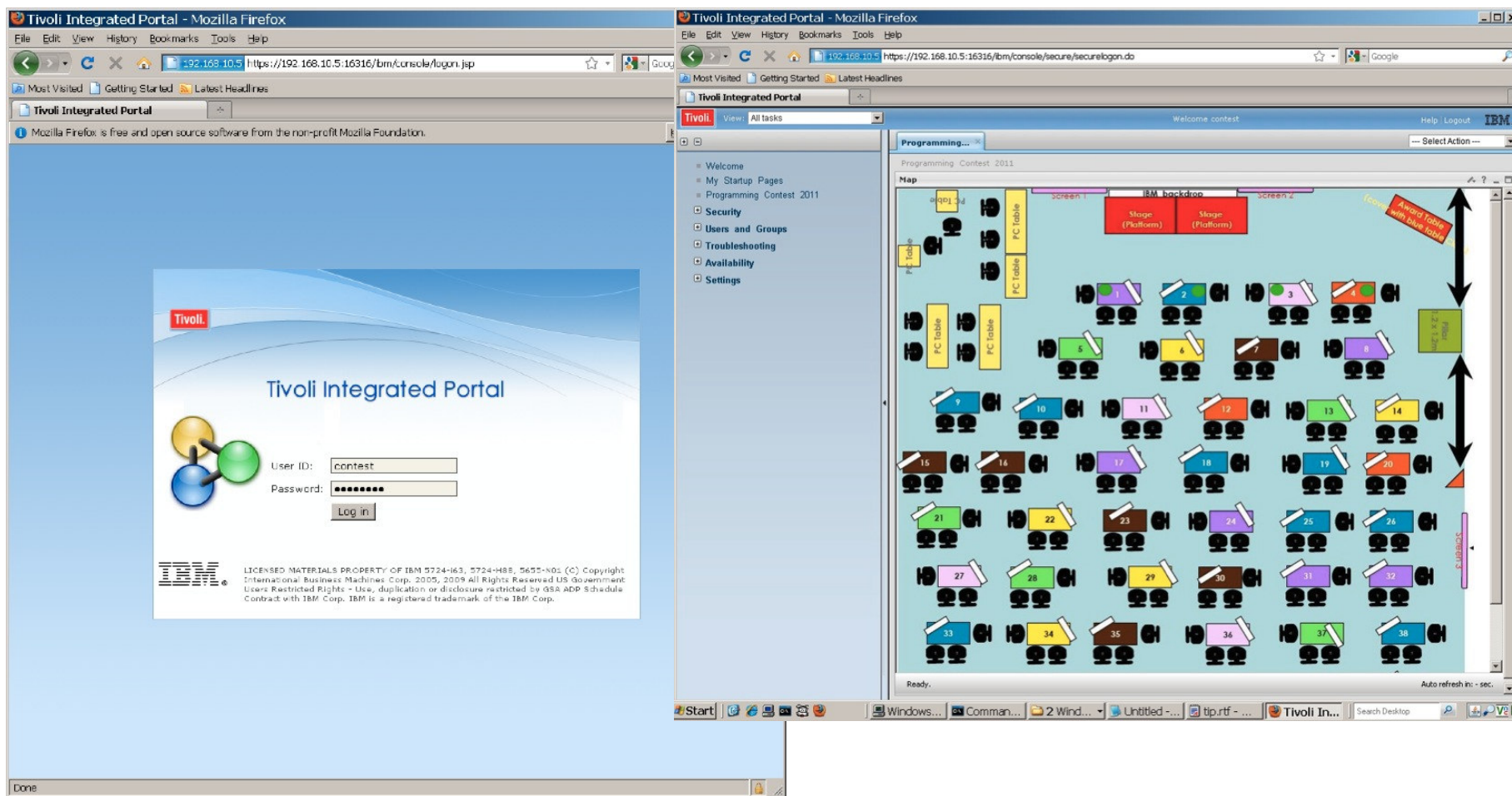
- Postzmsg
- Omnibus IP and receive ports and put it into a config file with the below contents:

```
#  
#=====  
# Licensed Materials - Property of IBM  
# "Restricted Materials of IBM"  
#  
# Sample program file showing updates for OMNIBus to allow error  
#   events to be sent to EIF probe  
#  
# (C) Copyright IBM Corp. 2007 All Rights Reserved.  
#=====  
#  
#  
ServerLocation=192.168.10.5  
ServerPort=9998  
#BufferEvents=NO  
BufEvtPath=/tmp/itm_sync_error.cache  
#BufEvtMaxSize=4096
```


Syntax for postzmsg

- Create a RED color event:
 - `postzmsg.exe -f my.conf -r CRITICAL -m contest EventID=101 situation_name="team1" satuation_status="Y" integration_type="U" situation_origin=team1 situation_displayitem='team1' team1 ITM`
- Create a GREEN color for clear event:
 - `postzmsg.exe -f my.conf -r CRITICAL -m contest EventID=101 situation_name="team1" satuation_status="N" integration_type="U" situation_origin=team1 situation_displayitem='team1' team1 ITM`

Access to Omnibus Web GUI



Lab Guide

- Click -> Start -> Command Prompt
- cd "Desktop\Poly Training\Dashboard Lab"
- sendevent team<your team no.>
 - E.g.: sendevent team1



Questions
&
Answers