

A Newton's cradle with five silver spheres in a row, set against a light blue background. The spheres are slightly out of focus, creating a sense of depth. The cradle's frame is visible on the left and right sides.

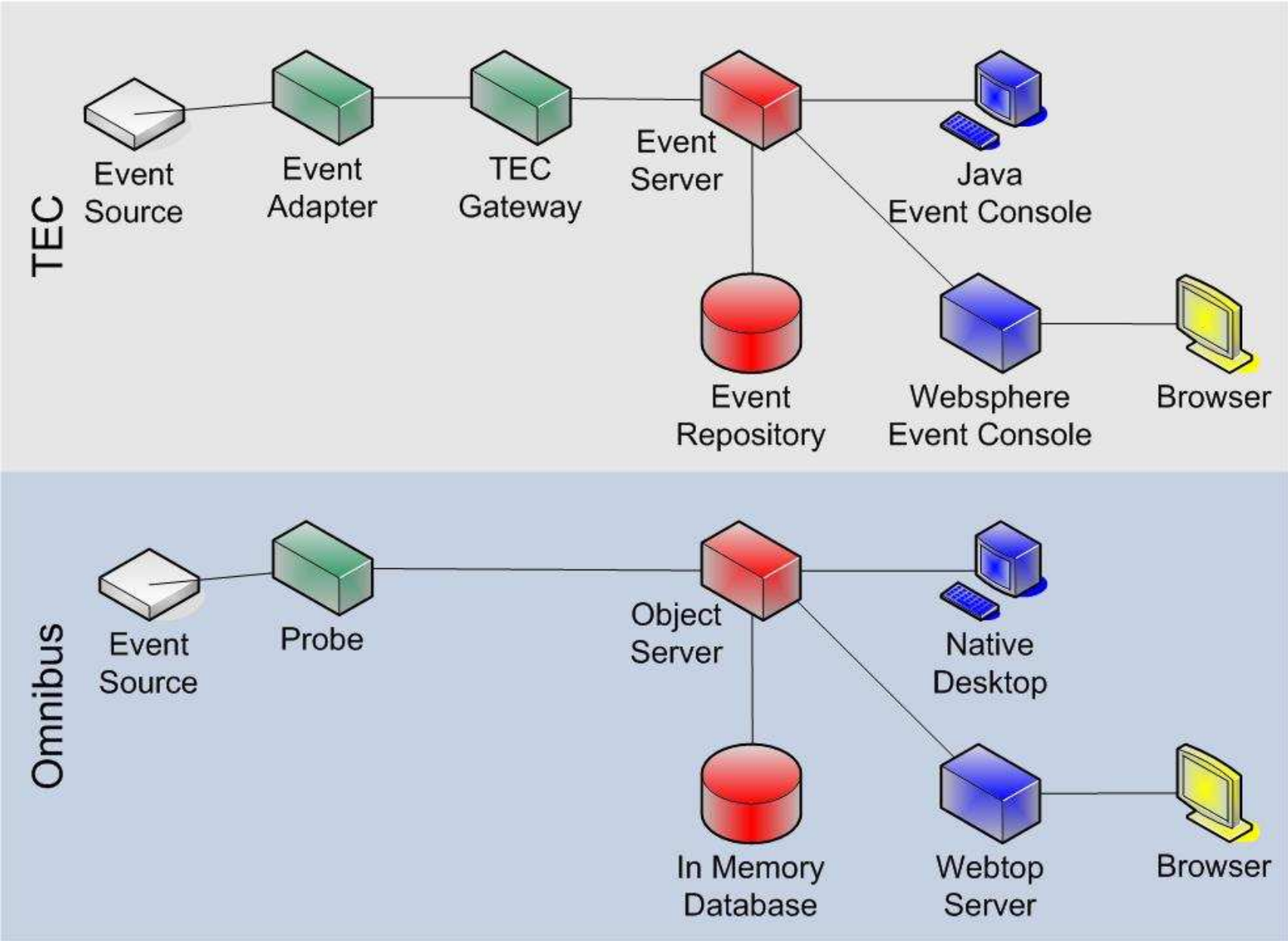
# ACT<sup>®</sup>

MORE THAN JUST IT SERVICE...

**Technical Comparison TEC – Omnibus**

Wolfgang Schumacher

- ▶ Architecture and terminology
- ▶ Event sources
- ▶ Consoles
- ▶ Event processing
- ▶ High-level comparisons
  - Functionality
  - Installation
- ▶ Netcool and TEC test environment
- ▶ Demonstration of functions
- ▶ Migration path from TEC to Omnibus
- ▶ Event flow migration process
- ▶ Demonstration of the migration process



# Event Sources – Adapter/Probe

TEC

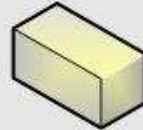
Event Source



```
2006-12-10 17:01:03 application1 Error description
2006-12-10 17:01:04 application1 Warning description
2006-12-10 17:01:05 application1 Information description
```

logfile  
/tmp/l1.txt

Event Adapter



```
ServerLocation=@EventServer
PollInterval=20
LogSources=/tmp/l1.txt
```

configuration file: tecad\_nt.conf

configuration file: tecad\_nt.fmt

```
FORMAT Logfile1
%s %s application1 Error %s*
hostname DEFAULT
origin DEFAULT
severity "CRITICAL"
msg $3
END
```

Omnibus

Event Source



```
2006-12-10 17:01:03 application1 Error description
2006-12-10 17:01:04 application1 Warning description
2006-12-10 17:01:05 application1 Information description
```

logfile  
/tmp/l1.txt

Logfile Probe



configuration file: glf.rules

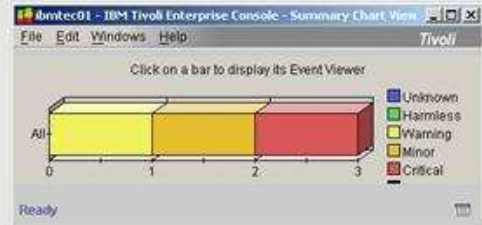
configuration file: glf.props

```
Manager      : "Generic Log File"
LogFileName  : "/tmp/l1"
RulesFile    : "$OMNIHOME/probes/linux2x86/glf.rules"
```

```
@Class      = 7955
@Agent      = "/tmp/l1"
@Identifier  = @Manager + @AlertGroup
@Manager     = "glf"
@Summary    = $Details
switch($FieldVal04)
{case "Error":      @Severity = 5
                    @Type = 1
case "Information": Severity = 3
                    @Type = 2
}
```

# Consoles – Event Contents

TEC



ibmtec01 - Event Viewer: Group All -

Time Received	Event Type	Class	Hostname	Severity	Status	Message
12.12.2006 12:46:10	Other	Logfile1	ibmtec01	Critical	Open	Beschreibung
12.12.2006 13:58:51	Other	Logfile1	ibmtec01	Minor	Open	Beschreibung
12.12.2006 13:59:51	Other	Logfile1	ibmtec01	Warning	Open	Beschreibung

Currently viewing details for event 1 of 1

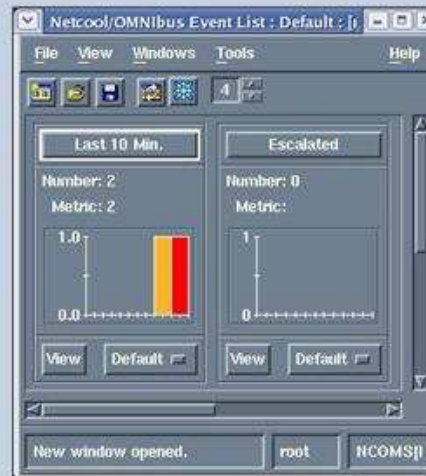
Open Critical Logfile1 event received on 12.12.2006 12:46:10.

General | Event Source | Status | Related Events | Attribute List

Attribute Name	Attribute Value
credibility	1
date_event	Dec 12 12:46:10 2006
date_reception	1165923970
duration	0
event_hndl	1
hostname	ibmtec01
last_modified_time	1165923970
msg	Beschreibung

Show Base Attributes  Show Extended Attributes  
 Display Formatted Names and...

Omnibus



Netcool/OMNibus Event List : Filter="Last 10 Min.", View="Default"

Node	Alert Group	Summary
nc2	Logfile	2006-12-10 17:04:03 Anwendung1 Error Beschreibung
nc2	Logfile	2006-12-10 17:04:04 Anwendung1 Warning Beschreibung

Event Information: Alert Status for Serial Number 3105

Alert Group: Logfile  
RAD\_TimeWindowEnd: 12/12/06 15:03:56  
Class: Generic Log File Probe  
Flash: No  
RAD\_WebtopTool1:  
RAD\_WebtopTool2:  
URL:  
Summary: 2006-12-10 17:04:03 Anwendung1 Error B

# Consoles – Filter Definition

TEC



**Edit Event Group Filter**

Name: node\_ibmtec01

Description: Alle Events von Node ibmtec01

Constraints:

Hostname	Equal to (=)	ibmtec01
----------	--------------	----------

Buttons: Add Constraint, Add SQL, Edit, Delete, Test SQL, OK, Cancel, Help

Omnibus



Netcool/OMNIBUS Filter Builder : Last 10 Min. : [none]

Name: Last 10 Min. Editable

Buttons: Condition, Negate, Leading Logical, Trailing Logical, Sub Query, Delete Element, Delete Tree, Edit SQL ...

Logical AND

Logical OR

AND

- AND
  - LastOccurrence >= getdate - 600
  - Manager not like '^.\*Watch\$'
- Severity > Clear

SQL: ( ( LastOccurrence >= getdate - 600 ) and ( Manager not like '^.\*Watch\$' ) ) and ( Severity > 0 )

# Consoles – Event Processing

TEC



Java  
Event  
Console

Time Received	Event Type	Class	Hostname	Severity	Status	Message
12.12.2006 13:58:51	Other	Logfile1	ibmttec01	Minor	Open	Beschreibung
12.12.2006 13:59:51	Other	Logfile1	ibmttec01	Warning	Open	Beschreibung

Omnibus



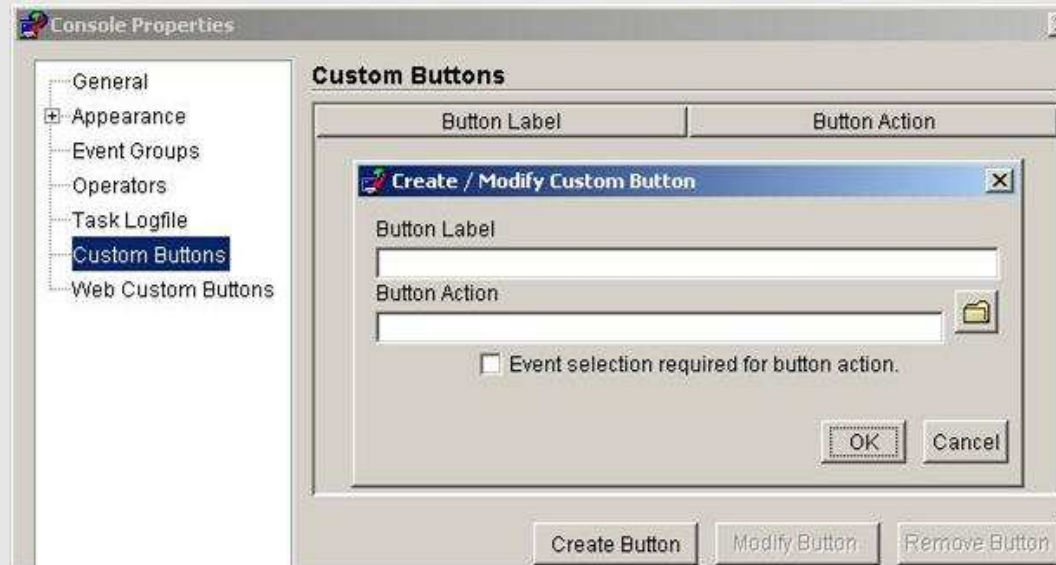
Native  
Desktop

Node	Related Events	Task List	Summary
nc2			2006-12-10 17:04:03 Anwendung1 Error Beschreibung
nc2			2006-12-10 17:04:04 Anwendung1 Warning Beschreibung

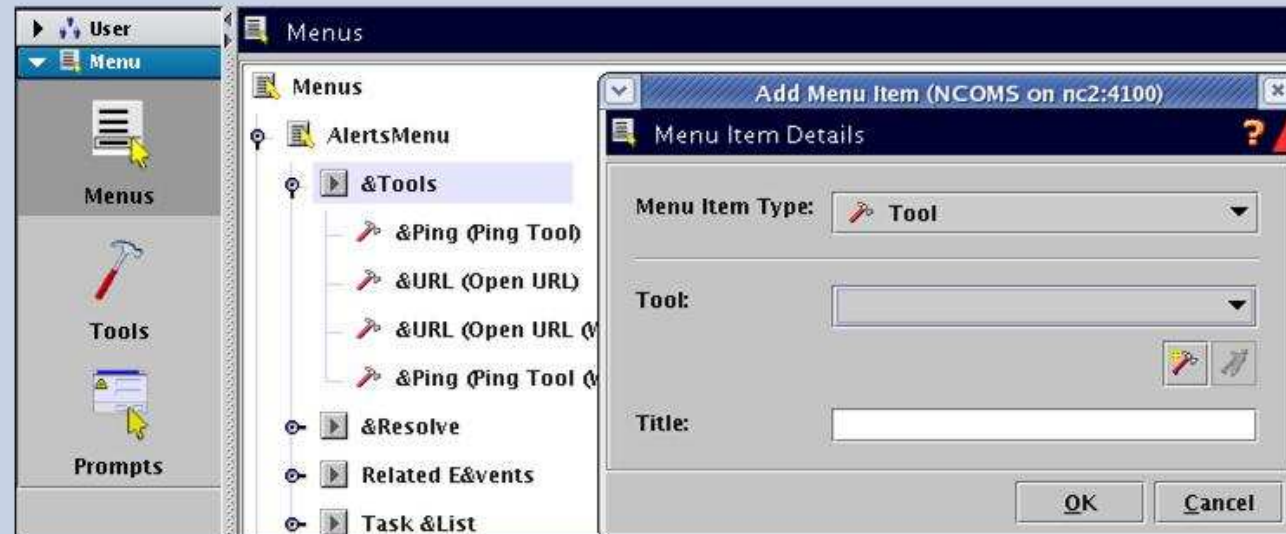
# Consoles – Customization Options

ACT®

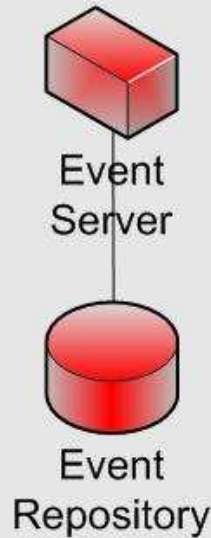
TEC



Omnibus



TEC



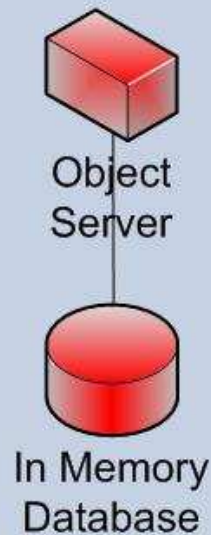
Events are defined as specialized classes

```
root.baroc
class_name (alphanumeric )
date_reception
source
severity duplicates
hostname with
msg dup_detect
...
```

Customizations  
custom class names  
inherited fields  
modified fields  
additional fields

Server has to be restarted

Omnibus

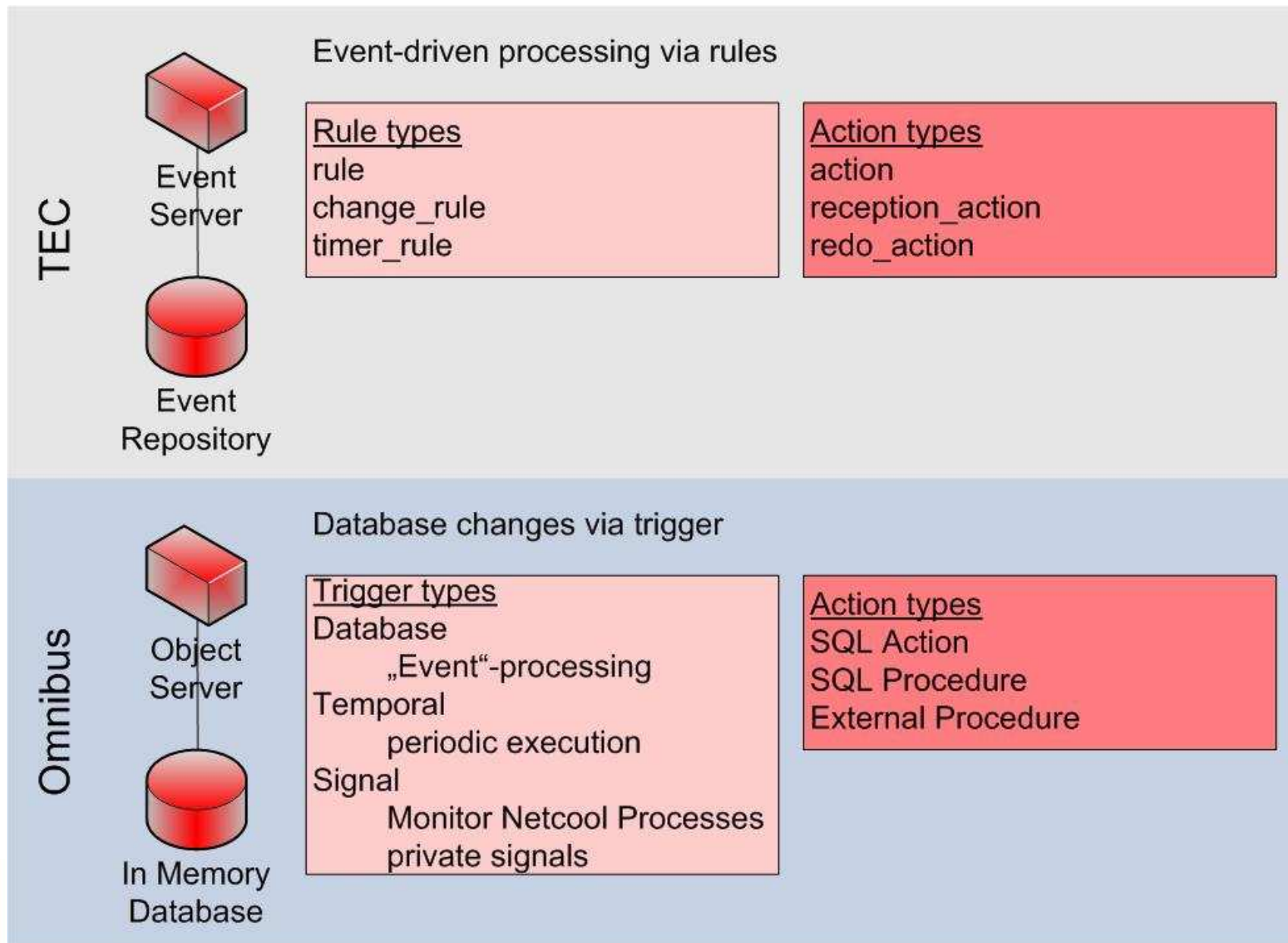


There is only one class for all event types

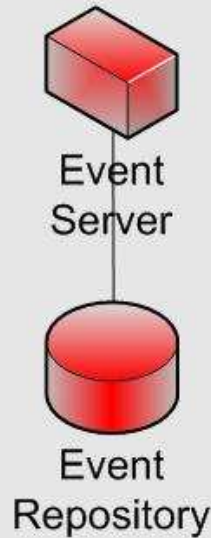
```
Default fields in the object server
Class (numeric)
Identifier
Agent duplicates via
Severity Identifier
Node
Summary
...
```

Customizations  
custom fields

no server restart necessary,  
only console resynchronization



TEC



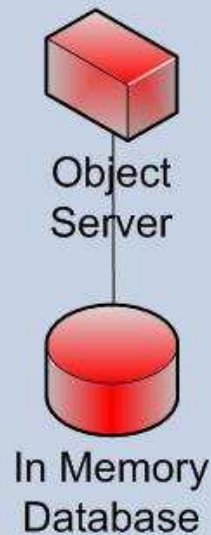
## Rule Base

Out of the box rules  
none

## Typical rules

check for duplicate events  
generic and special processing  
escalate  
forward to trouble ticket system  
correlate: cause - effect - solution

Omnibus



## Rule Base

Out of the Box Trigger  
Database  
deduplication  
Temporal  
flash\_not\_ack  
generic\_clear  
delete\_clears

## Typical triggers

X in Y escalation

## Additional functions

various gateways, for ex. uni- or bidirectional or flat file gateways

TEC	Omnibus
<pre> rule: set_timer: (   description: 'Set timer on NFS_No_Response',   event: _event of_class 'NFS_No_Response',   action: set_timer:   (     set_timer(_event, 60, 'level1'),     increment_slot(_event, timer, 1, 'NO')   ) ). timer_rule: escalate_1: (   description: 'When a NFS_No_Response stays               open for more than 1 minute we               want to increase the severity to               CRITICAL',   event: _event of_class 'NFS_No_Response',   timer_info: equals 'level1',   action: escalate:   (     set_event_severity(_event, 'CRITICAL'),     decrement_slot(_event, timer, 1, 'NO')   ) ).                     </pre>	<pre> Temporal Trigger Name: flash_not_ack Intervall: every 60 seconds comment: Will set Flashing on (Flash=1) for events that are Critical (Severity=5) and are 10 minutes old but have not been acknowledged by a user yet (Acknowledge = 0). It sets SuppressEscl to 1 as a further indication of the events' escalation status. content:  begin  update alerts.status   set Flash = 1,   SuppressEscl = 1   where Flash = 0 and         Acknowledged = 0 and         Severity = 5 and         FirstOccurrence &lt;= (getdate - 600);  End                     </pre>

```
reception_action:
( first_duplicate(_event,
  event: _duplicate_ev
  where
    ( hostname:      equals _hostname,
      source:       equals _source,
      origin:       equals _origin,
      adapter_host: equals _adapter_host,
      status:       outside ('CLOSED'),
      repeat_count: _old_repeat_count
    ),
    _event - 4000 - 300
  ),
  set_event_status( _duplicate_ev, 'CLOSED'),
  bo_set_slotval( _event, 'repeat_count', _old_repeat_count),
  add_to_repeat_count( _event, 1),
```

begin

```
set old.Tally = old.Tally + 1;
```

```
set old.LastOccurrence = new.LastOccurrence;
```

```
set old.StateChange = getdate();
```

```
set old.InternalLast = getdate();
```

```
set old.Summary = new.Summary;
```

```
set old.AlertKey = new.AlertKey;
```

```
if (( old.Severity = 0) and (new.Severity > 0))
```

```
then
```

```
    set old.Severity = new.Severity;
```

```
end if;
```

end

The screenshot shows the 'Database Trigger Details' configuration window. The 'Name' field is 'deduplication' and the 'Group' is 'default\_triggers'. The 'Settings' tab is active, showing 'On' set to 'alerts' and 'status'. The 'Run' section has 'Priority' set to '1' and 'Pre database action' selected. The 'Apply To' section has 'Row' selected. The 'State' section has 'Enabled' checked.

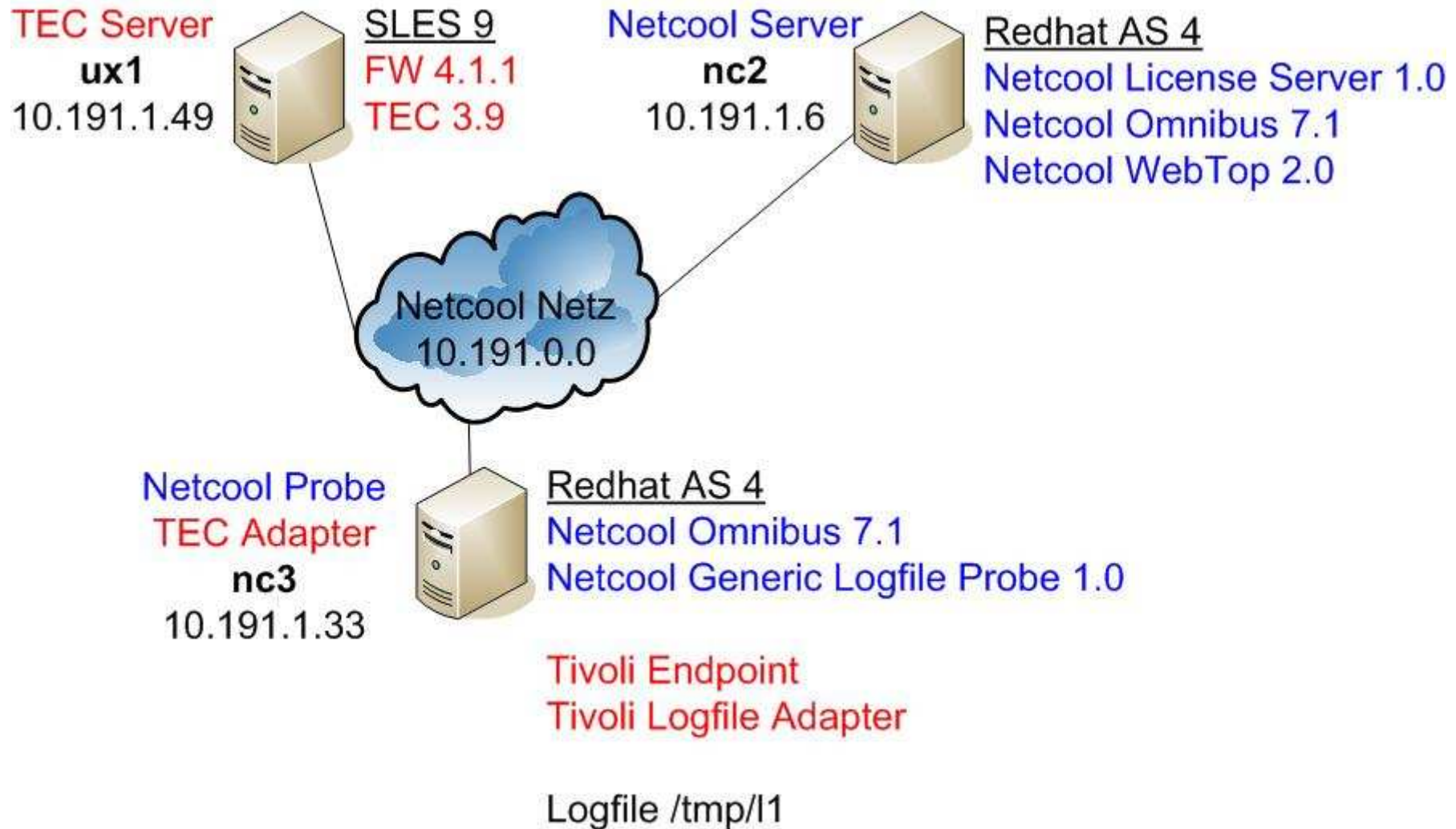
# Functions – High-level Comparison



Function	TEC	Omnibus
event sources	adapters	probes
event console	TEC console	event list
event management	TEC event server	object server
automation	prolog rules engine	database trigger
database	external (DB2, Oracle..)	internal, in memory
distributed event management	State Correlation Engine	none
event visualization	WAS TEC console	Webtop
communication	Framework + RIM	IDUC over TCP/IP
scalability	Filter at endpoints, correlation at gateways	Probe filters; Collection Object Srv.
failover	customer developed	uni- and bidirectional gateways
configuration tools	TEC console + CLI	Conductor + Config Manager GUI

<b>TEC</b>	<b>Omnibus</b>
OS – AIX, HP, Redhat, Solaris, Suse, Windows	OS – AIX, HP, Redhat, Solaris, Suse, Windows
Install Framework	Create an OS user
Install database	Install license server and enter licenses
Allocate TEC DB	Install Omnibus
Install TEC	Create internal database
Configure TEC (groups, consoles, operators)	Define connection to Object Server
Effort: approx. 1 hour Framework and TEC (30 min with quick install)	Effort: approx. 30 minutes

# Netcool and TEC Test Environment



## ▶ Event source

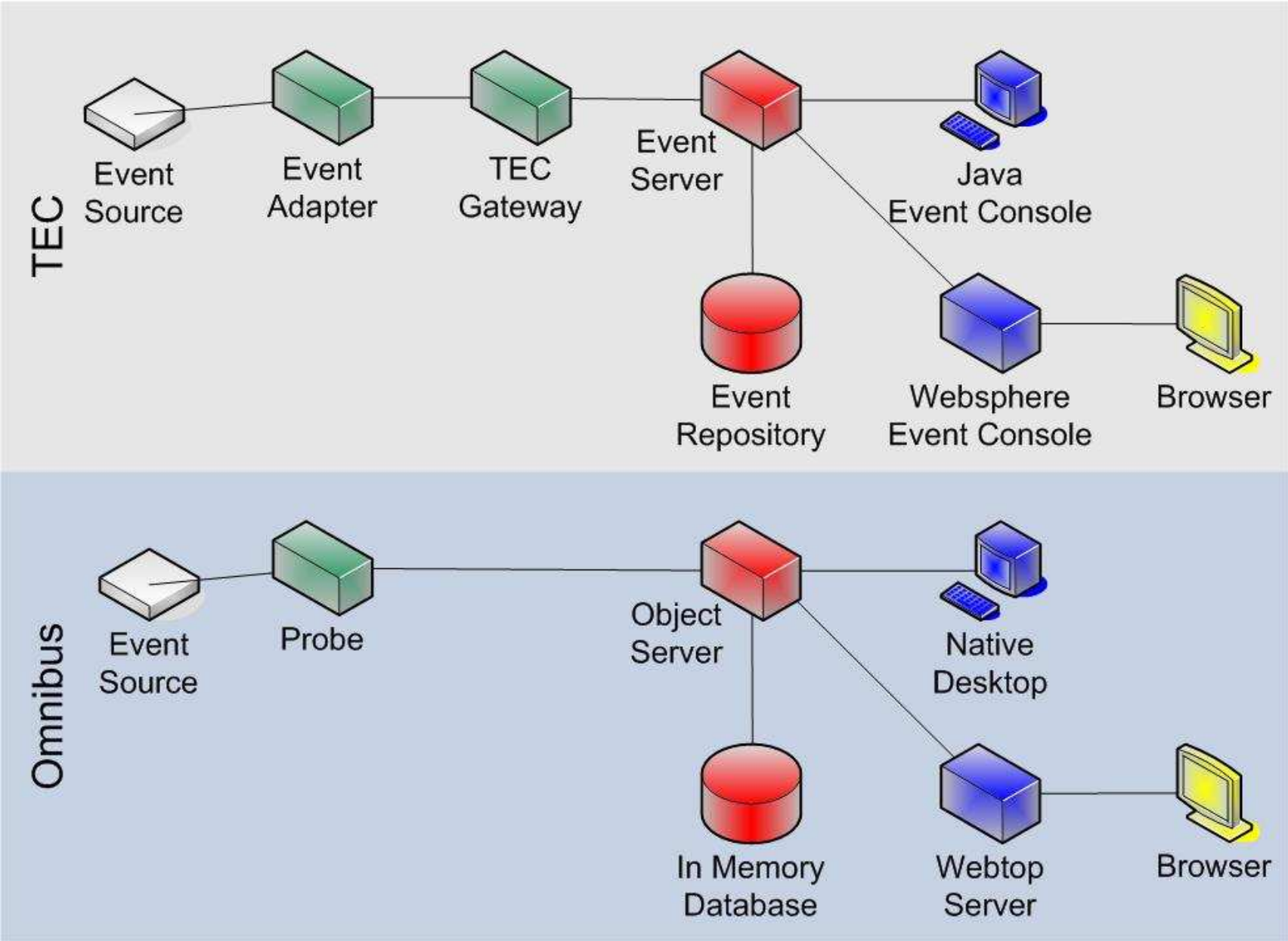
- /tmp/l1

- 2006-12-10 17:01:03 application1 Error description
- 2006-12-10 17:01:04 application1 Warning description
- 2006-12-10 17:01:05 application1 Information description

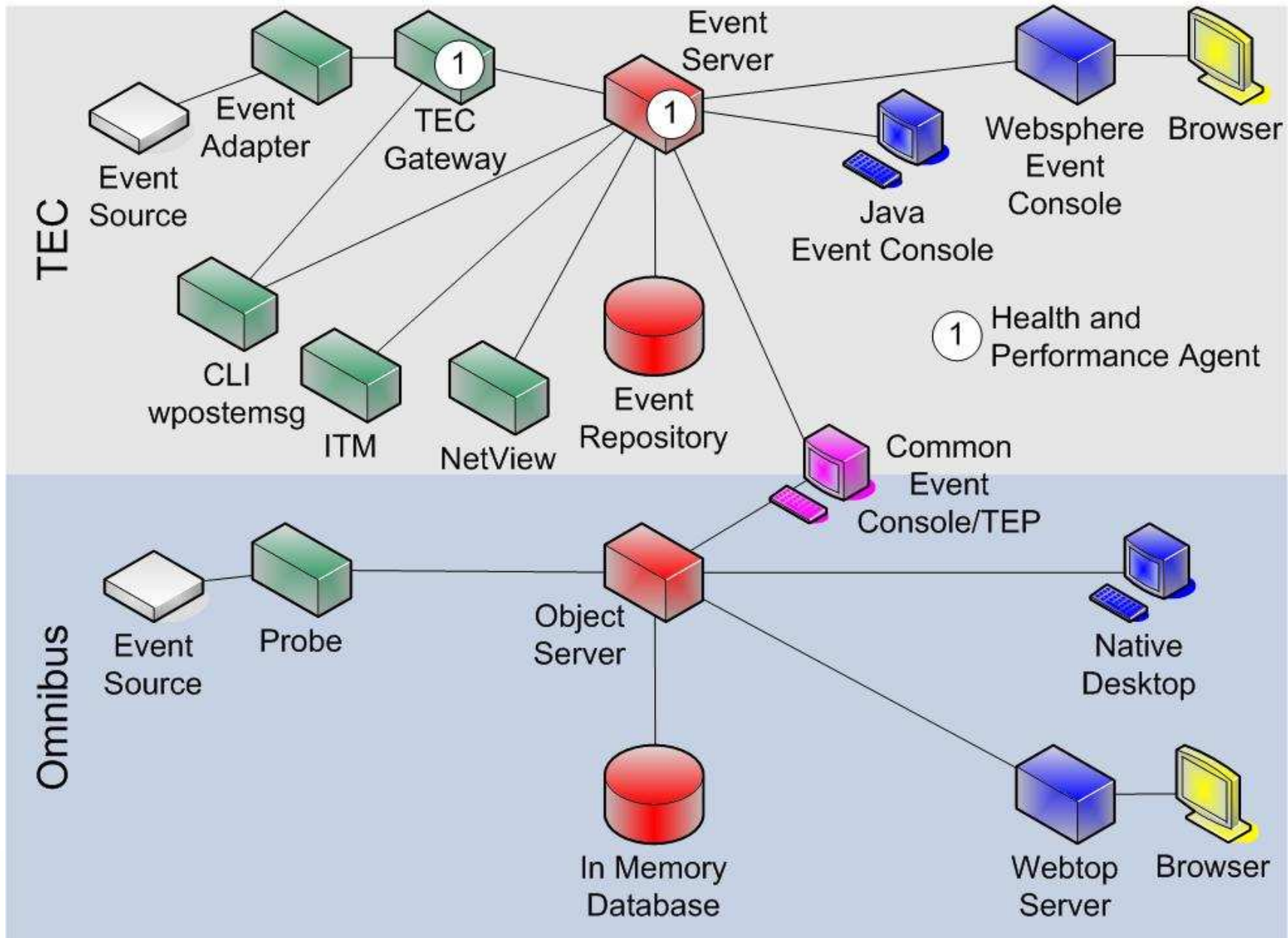
- Adding a line results in

- Netcool processing via probe
- TEC processing via TEC adapter

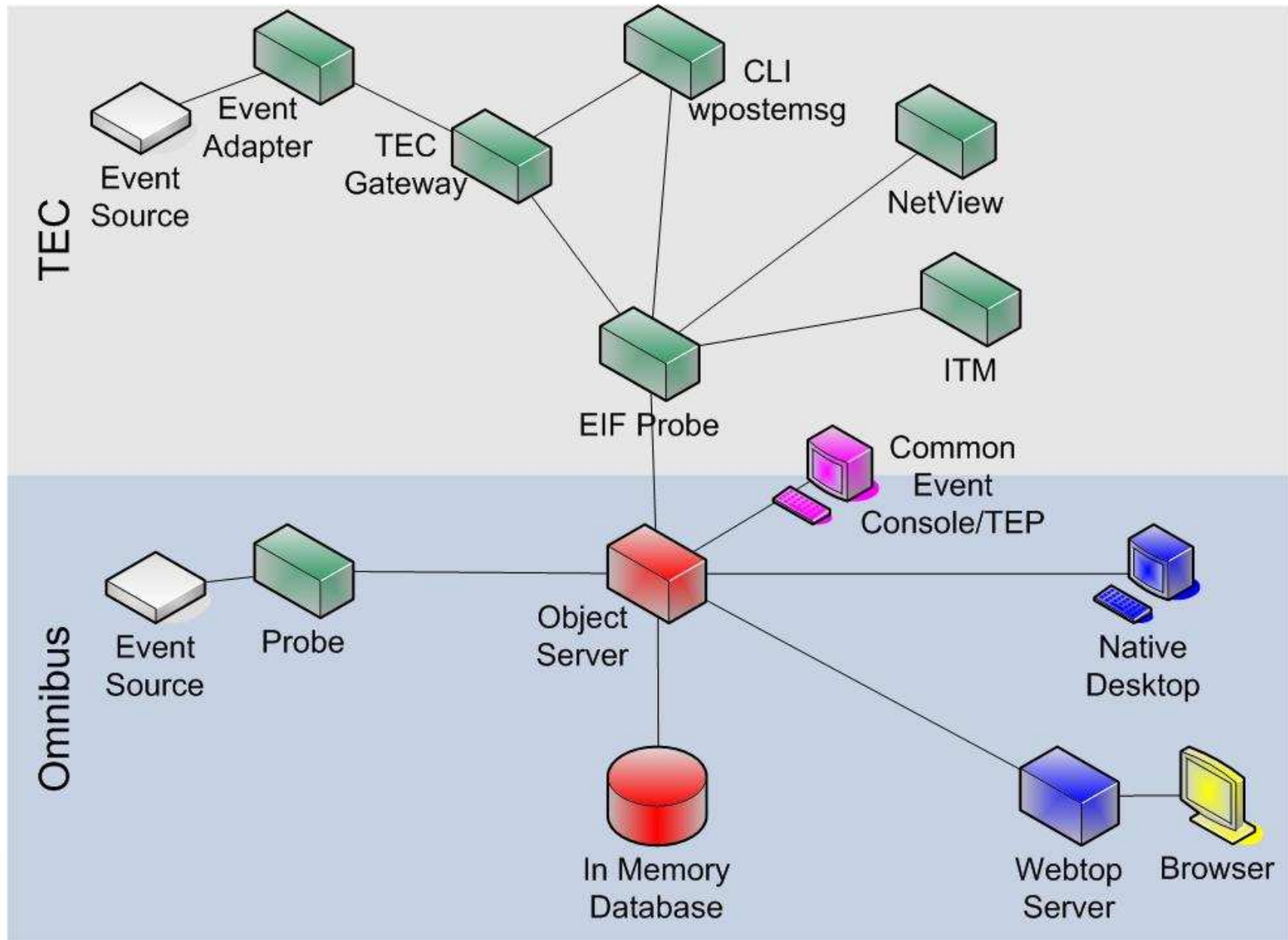
## ▶ Analysis of both configurations and processing rules



# Migration path from TEC to Omnibus - 1



# Migration path from TEC to Omnibus - 2



- ▶ Install Netcool Omnibus
- ▶ Install non-native and EIF probes
- ▶ Extend the table alerts.status
- ▶ Start EIF probe
- ▶ Create, configure and distribute a tec\_gateway\_sce profile to all endpoint gateways

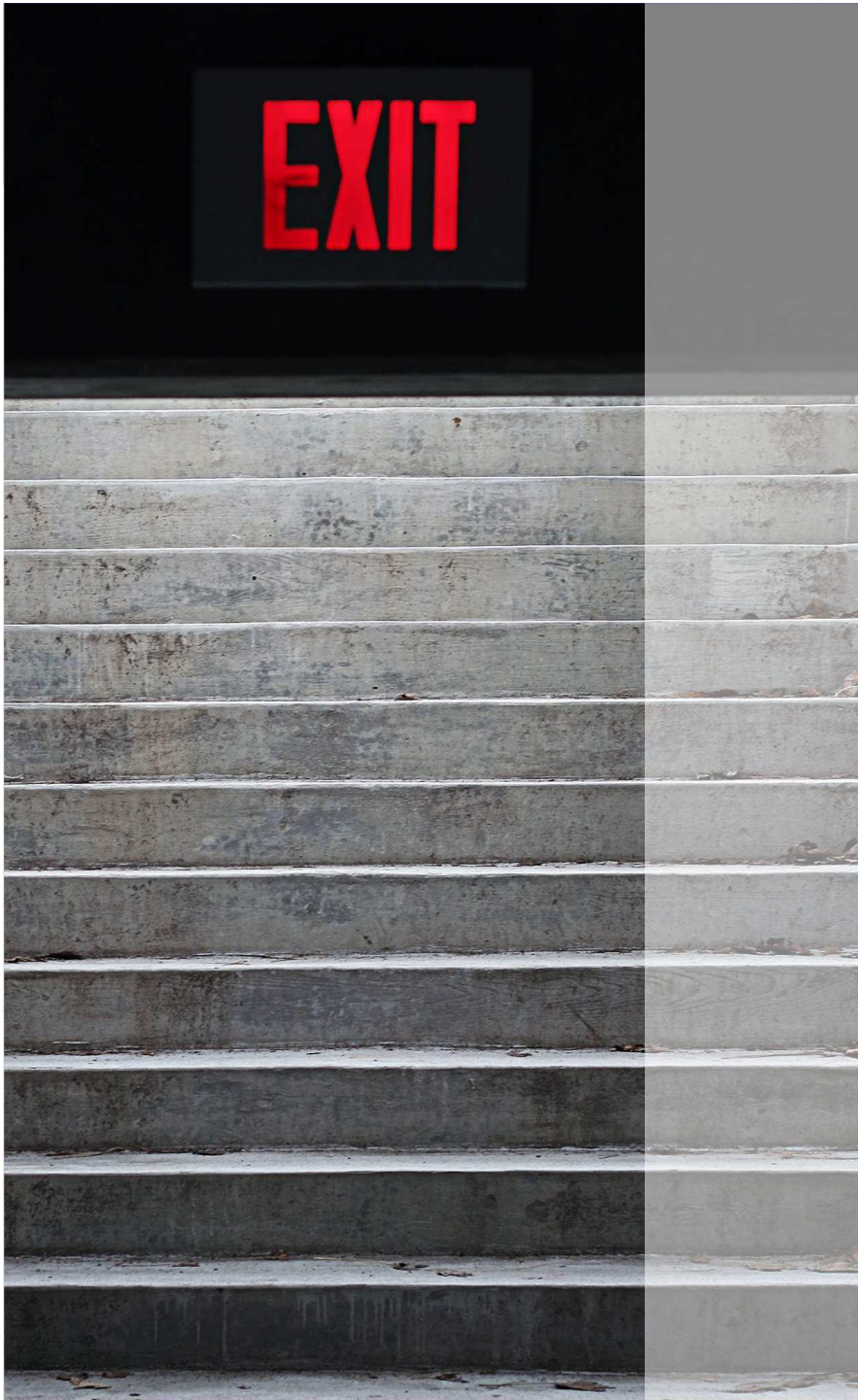
OR

Create, configure and distribute a tecad\_\* profile to all endpoints

- ▶ Finished – that`s all!

- ▶ Create and configure tecad\_\* profile
- ▶ Distribute the profile
- ▶ Event source
  - Adding a line results in
    - Netcool processing via probe
    - TEC processing at the Endpoint
    - Netcool EIF processing at the Omnibus server
    - Visualization with the Netcool Event Console

- ▶ Reasons for migration from TEC to Omnibus
  - Technical
    - **Too many events**
    - **High availability**
  - Political
    - **Using IBM's strategic event management**
- ▶ Organisation
  - Change in event processing
    - **TEC – Status and Severity**
    - **Omnibus – only Severity**



**ACT IT-Consulting & Services AG**

Rudolf-Diesel-Straße 18

D-53859 Niederkassel

**Telefon:** +49 (0)228 97125 - 0, **Fax:** +49 (0)228 97125 - 40

**E-mail:** [info@act-online.de](mailto:info@act-online.de), **Internet:** <http://www.act-online.de>