

# **Axibase Fabrica**

v199a

Date: 28 Jan 2008

# Agenda

- Event enrichment
- Historical event reporting
- **Event notifications**
- Event acknowledgements

# Event Notifications

- Real-time and deferred event notifications to email subscribers with powerful filtering
- Can be defined at agent, host, group, or application level (ITM defines notifications at situation level). Example: group notification will capture any event raised against any host/agent that is a member of the group
- Use expressions to filter out events (exclude particular situations, agents, days of the week, event properties, Tier, etc.)
- Use notification delay and expressions to discard notifications if event status or properties change by the end of the delay interval. Example: discard notification if event is acknowledged within 15 minutes
- Expressions can be used to evaluate extended properties (such as `icmp_check` or `tcp_check_port`) to discard `MS_Offline` events if the host is pingable (`icmp_check` returns `TRUE`)
- Email messages include event reports in PDF formats with embedded charts and links to additional reports and tools

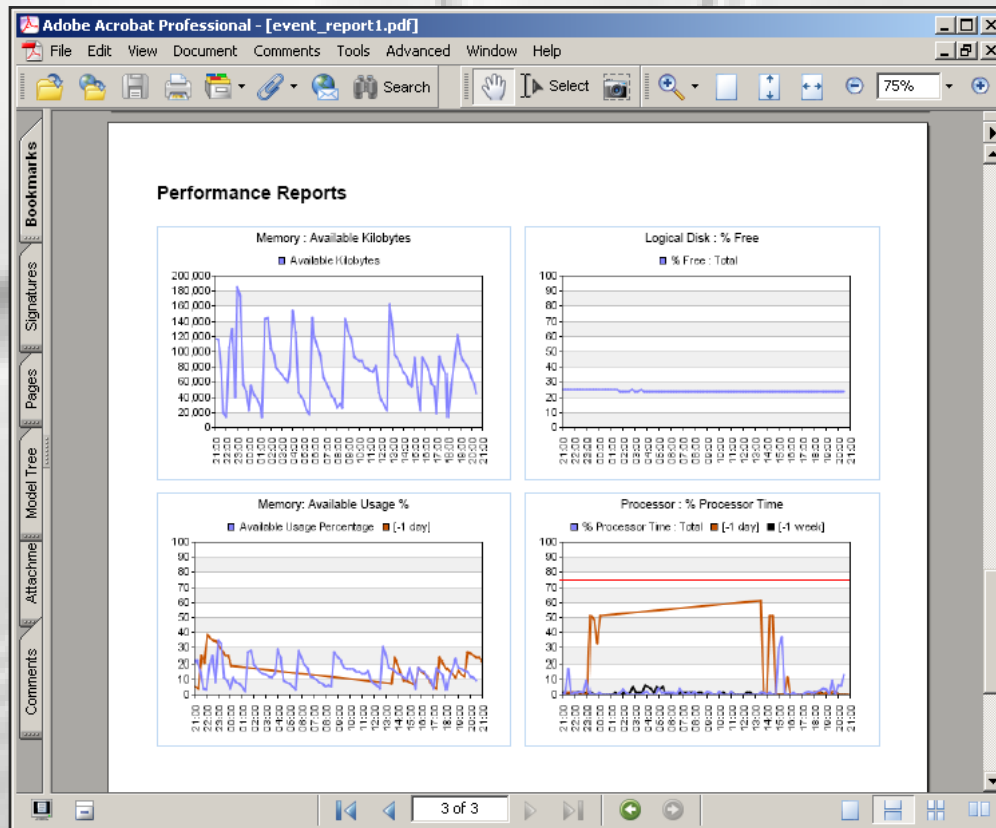


# Event Notifications - Content

- User-friendly HTML templates
- Comprehensive content:
  - Resource information (agent, host, ip, os, patch level, TEMA online status)
  - Situation information (name, formatted formula, help text, interval, severity)
  - Detailed event information (status, timestamps, display item (if any), formatted text, **impact**, and formatted event attributes based on EIF slots)
  - Historical time-series graphs for the host (as a PDF attachment)
- **Impact** is a comma-separated list of applications affected by this event source (agent).
- Links allow user to generate historical event and service level reports for the affected host in PDF format.
- Tools launch an event property window (user must have access permissions against the agent)

# Event Notifications – PDF

- PDF attachment includes historical charts based on currently running scheduled templates



# Event Notifications - Expressions

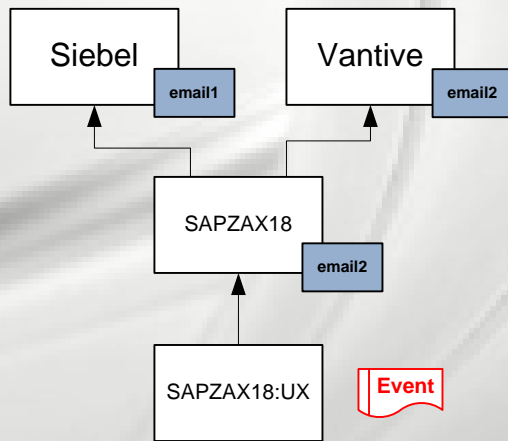
- Notification properties can be defined for each agent, host, group and application similar to Tier/Admin Status
- Multiple notifications for the same resource are supported

## Configuration

Admin Status	<input type="text" value="OK"/>						
Tier	<input type="text" value="- None -"/>						
Notification	<table><thead><tr><th>Subscribers</th><th>Delay</th><th>Expression</th></tr></thead><tbody><tr><td><input type="text" value="support@company.com"/></td><td><input type="text" value="15"/></td><td><input type="text" value="status_text = 'Open'"/></td></tr></tbody></table>	Subscribers	Delay	Expression	<input type="text" value="support@company.com"/>	<input type="text" value="15"/>	<input type="text" value="status_text = 'Open'"/>
Subscribers	Delay	Expression					
<input type="text" value="support@company.com"/>	<input type="text" value="15"/>	<input type="text" value="status_text = 'Open'"/>					
Custom Properties	<input type="text"/> <input type="text"/>						
	<input type="button" value="Save"/>						

# Event Notifications – Processing

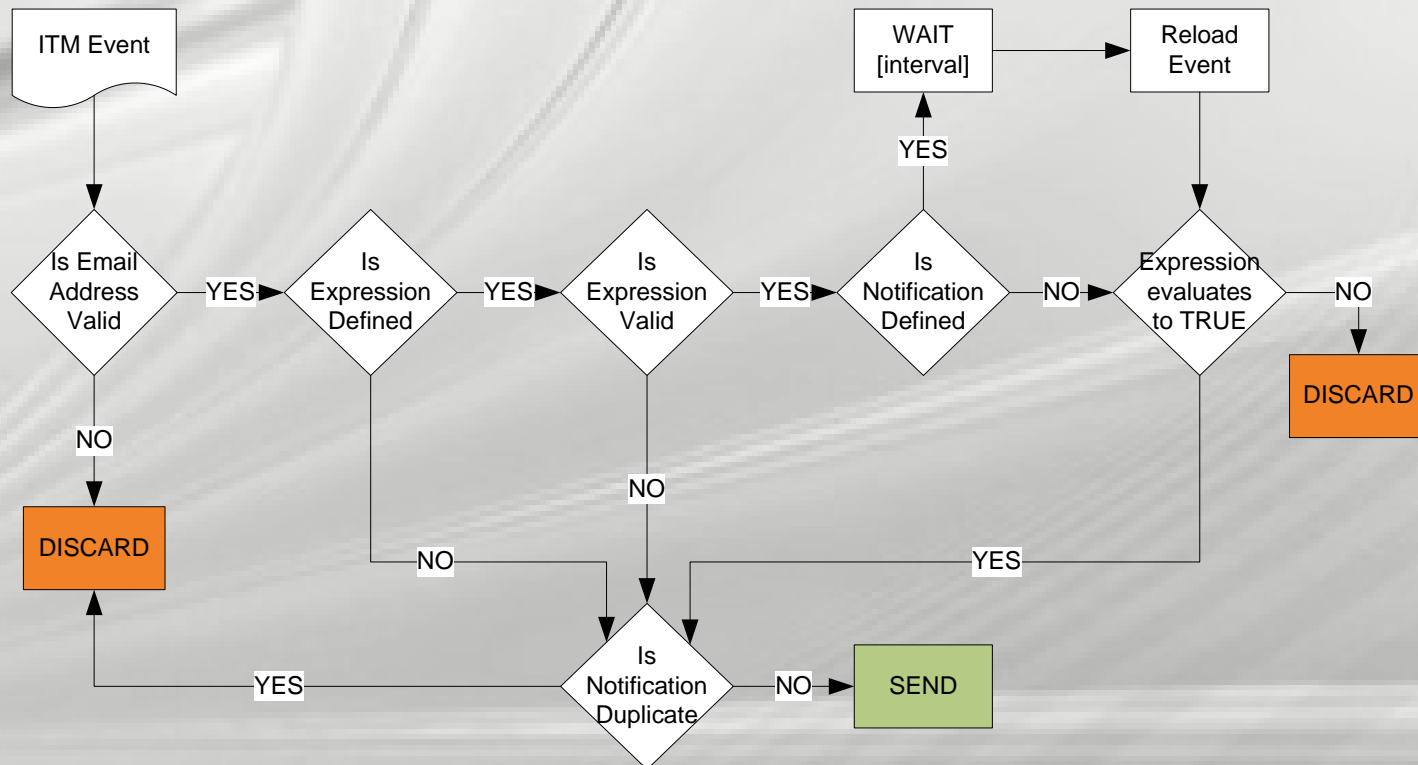
- Multiple notifications configurations for the same event are de-duplicated based on email address



Email will be sent to:  
email1, email2 (once)

# Event Notifications – Expressions

- Simple syntax (similar to SQL except wildcards are \* and ?)
- Example: `situation NOT LIKE 'MS_Offline'`
- Example: `adminStatus < 1`
- Example (notifyDelay = 15 min): `status_text != 'Open'`



# Event Notifications – Expressions

- Exclude MS\_Offline situation from notifications:  
`situation != 'MS_Offline'`
- Notify if agent is offline only if ICMP ping returns down or unreachable:  
`situation != 'MS_Offline' OR source.icmp_ping = FALSE`
- Exclude notifications from agents in maintenance mode:  
`source.adminstatus < 1`
- Only notify if the agent is Tier 1 or Tier 2:  
`source.tier > 0 AND source.tier < 3`
- Discard notification if the event is acknowledged or closed within 15 minutes (set Delay Interval to 15):  
`status_text != 'Open'`
- Discard non-critical notifications:  
`severity >= 6 or severity_text = 'Critical'`

*Note: expressions are case-insensitive except LIKE and MATCH operands. Parameters are evaluate in the order specified (place expensive parameters such as icmp\_ping at the end of the expression)*

# Event Notifications – Expressions

- Available event properties:

## Event Properties

<b>severity</b>	event severity code (0 - 6)
<b>severity_text</b>	event severity text (normal, warning, etc)
<b>status</b>	event status code (0 - 15)
<b>status_text</b>	event status text (open, ack, closed, etc.)
<b>source</b>	agent identifier (e.g. Primary:ABC:NT)
<b>host</b>	host (e.g. ABC)
<b>situation</b>	situation name
<b>rule</b>	situation name
<b>instance</b>	display item (such as C: for disk name)
<b>text</b>	event message

## Event Timestamps (received, created, modified)

<b>received_day</b>	day of the month (1-31)
<b>received_month</b>	month (1-12)
<b>received_hour</b>	hour of the day (in 24h format)
<b>received_minute</b>	minute
<b>received_dow</b>	day of the week (0-6, Sunday - Monday)
<b>received_text</b>	'dd-MMM-yy HH:mm:ss'

## Event Attributes (from EIF – replace space with \_):

<b>attribute_name</b>	returns attribute_value as string
-----------------------	-----------------------------------

## Agent/host properties are accessible by using dot notation

<b>source.ip</b>	IP address of the agent
<b>source.adminstatus</b>	agent maintenance mode (1 if TRUE)
<b>source.os_name</b>	OS name of the agent
<b>host.icmp_check</b>	TRUE if the host is pingable
<b>host.tcp_check_80</b>	TRUE if the host is listening at port 80 (TCP)

# Event Notification – Reports

- Click on ‘Resources’ tab, enter a query into the search box:
  - **select id, notify\_email, p\_notify\_email, p\_notify\_delay, p\_notify\_expression from src where notify\_email != ''**  
*list effective and defined email notifications for all resources*

id	notify_email	p_notify_email	p_notify_delay	p_notify_expression
<a href="#">CUPITMNT20</a>	support@axibase.com	support@axibase.com	2	source.severity > 2
<a href="#">CUPITMNT20:20</a>	support@axibase.com			
<a href="#">CUPITMNT20:21</a>	support@axibase.com			
<a href="#">CUPITMNT20:22</a>	support@axibase.com			
<a href="#">CUPITMNT20:SY</a>	support@axibase.com			
<a href="#">CUPITMNT20:Warehouse</a>	support@axibase.com			
<a href="#">HUB_CUPITMNT20</a>	support@axibase.com			
<a href="#">Primary:CUPITMNT20:NT</a>	support@axibase.com			