

Wrong-Escalation-Walkthrou

First of it all, we had the Escalation-step-through-problem again, but the machine was down only for a short time. The back-to-OK-SMS hasn't been sent till now:

2010.Mar.21 02:22:01	Server [REDACTED] is unreachable	OK	Average
2010.Mar.21 02:20:30	Server [REDACTED] is unreachable	PROBLEM	Average

Here the events displayed in the gui:

Event Source Details

Host: [REDACTED]

Trigger: Server [REDACTED] is unreachable

Severity: Average

Expression: [REDACTED]agent.ping.nodata(80))=1

Event generation: Normal

Disabled: No

Event details

Event: Server [REDACTED] is unreachable

Time: 2010.Mar.21 02:20:30

Status: PROBLEM

Duration: 1m 31s

Acknowledged: -

Acknowledges

Time	User	Comments
...		

Message actions

Time	Type	Status	Retries left	Recipient(s)	Message	Error
Step: 2 Time: 2010.Mar.21 02:22:33	Email	sent		[REDACTED]	Subject: Trigger Server [REDACTED] is unreachable is going PROBLEM at 2010.03.21 02:20:30 Message: Verantwortlichkeit: Team ServerNetz Beschreibung: MSSQL2005-Datenbankserver	
Step: 2 Time: 2010.Mar.21 02:22:33	Email	sent		[REDACTED]	Subject: Trigger [REDACTED] is unreachable is going PROBLEM at 2010.03.21 02:20:30 Message: Verantwortlichkeit: Team ServerNetz Beschreibung: MSSQL2005-Datenbankserver	
Step: 2 Time: 2010.Mar.21 02:22:33	Email	sent		[REDACTED]	Subject: Trigger [REDACTED] unreachable is going PROBLEM at 2010.03.21 02:20:30 Message: Verantwortlichkeit: Team ServerNetz Beschreibung: MSSQL2005-Datenbankserver	
Step: 3 Time: 2010.Mar.21 02:26:35	Email	sent		[REDACTED]	Subject: Trigger Server [REDACTED] is unreachable is going PROBLEM at 2010.03.21 02:20:30 Message: Verantwortlichkeit: Team ServerNetz Beschreibung: MSSQL2005-Datenbankserver	
Step: 4 Time: 2010.Mar.21 04:22:37	SMS	sent		[REDACTED]	Subject: Trigger [REDACTED] is unreachable is going PROBLEM at 2010.03.21 02:20:30 Message: Verantwortlichkeit: Team ServerNetz Beschreibung: MSSQL2005-Datenbankserver	

This means that beginning with step2 all steps were absolutely WRONG, because the machine was up again before...

Now I was taking a look into the db:

First: Select the associated TriggerID 13155 for the unreachable-check for the machine:

triggerid	expression	description	url	status	value	priority	lastchange	dep_level	comments	error	templateid	type
13148	{12291}=0	DNS server is running		0	2	3	0	0	0x444E...	Tri...	0	0
13154	{19070}<1	Zabbix_agentd is not running on {HOSTNAME}		0	0	2	1266416373	0	0x		13061	0
13155	{29925}=1	Server {HOSTNAME} is unreachable		0	0	3	1269134521	0	0x		13059	0

The lastchange is ok:

Timestamp:

In GMT. Example: 1010342461.

Timezone:

Timezone which the result will be given in.

1269134521 translates to **Sunday, March 21st 2010, 02:22:01 (GMT +1)**

Next this screenshot is from table "events":

eventid	source	object	objectid	clock	value	acknowledged
3176839	0	0	13155	1269134521	0	0
3176816	0	0	13155	1269134430	1	0
3176042	0	0	13155	1268941118	1	0

The top 2 are the corresponding warning and ok-events...

This screenshot is from table "escalations":

escalationid	actionid	triggerid	eventid	r_eventid	nextcheck	esc_step	status
340822	34	13155	3176816	3176839	0	5	2
54375	5	13155	207860	0	0	0	2
53964	5	13155	206617	0	0	0	2

Top2 are the corresponding. This tells me that r-eventid (=going back to OK) is inserted Also you can see the esc_step has been completely counted up.

The last screenshot is from table "alerts":

alertid	actionid	eventid	userid	dock	mediatypeid	sendto	subject	message	status	retries	error	nextcheck	esc_step	alerttype
789294	34	3176816	6	1269141757	2	[REDACTED]	Trigger Server [REDACTED]	0x566572616E74776F72746C696368686569743A0A546...	1	0		0	4	0
789245	34	3176816	28	1269134795	1	[REDACTED]	Trigger Server [REDACTED]	0x566572616E74776F72746C696368686569743A0A546...	1	0		0	3	0
789242	34	3176816	15	1269134553	1	[REDACTED]	Trigger Server [REDACTED]	0x566572616E74776F72746C696368686569743A0A546...	1	0		0	2	0
789243	34	3176816	4	1269134553	1	[REDACTED]	Trigger Server [REDACTED]	0x566572616E74776F72746C696368686569743A0A546...	1	0		0	2	0
789244	34	3176816	3	1269134553	1	[REDACTED]	Trigger Server [REDACTED]	0x566572616E74776F72746C696368686569743A0A546...	1	0		0	2	0