



DATA SHEET

Windows Eventlog

Monitoring

Voordelen

- ✓ Ontvang eventlog meldingen op een centrale plaats.
- ✓ Eventlog meldingen worden direct doorgestuurd.
- ✓ Stuur de meldingen naar de juiste persoon.
- ✓ Uitgebreid filtermeganisme.
- ✓ Ontvang eventlog meldingen van andere domeinen.
- ✓ Voorkom dubbele meldingen.
- ✓ Tijdelijke filters mogelijk.
- ✓ Ontvang alleen zinvolle meldingen.

Overzicht

Er worden tegenwoordig zoveel meldingen in de windows eventlog gelogd dat veel beheerders al niet eens meer de moeite nemen de eventlog te controleren. Toch is dit niet wenselijk, er kunnen nl. belangrijke meldingen in de eventlog staan die inzicht geven in het functioneren van het systeem.

Daarom is het belangrijk om de belangrijke meldingen te scheiden van de minder belangrijke meldingen. TSMS biedt daarom een uitgebreid filtermeganisme zodat u precies kunt aangeven welke meldingen u wel en welke u niet wenst te ontvangen. Dit voorkomt dat belangrijke meldingen over het hoofd worden gezien.

TSMS ontvangt de meldingen van al uw systemen op een centraal punt. Daar worden ze ook gearchiveerd zodat u later makkelijk kunt rapporteren hoe vaak een bepaalde melding de afgelopen maand is voorgekomen.

Eventlog meldingen van een bepaalde applicatie bijv. SQLServer kunnen doorgestuurd worden naar de database beheerders. Zo krijgt iedere beheerder de meldingen die belangrijk zijn voor zijn vakgebied/verantwoordelijkheid.



Features

- Cluster monitoring

Het is ook mogelijk om de meldingen van andere cluster leden te ontvangen.

- Suppress equal messages

Wanneer een applicatie binnen korte tijd heel vaak dezelfde melding logt dan bestaat de mogelijkheid om alleen de eerste te ontvangen en gedurende enige tijd de dubbele meldingen te onderdrukken.

- Meerdere domeinen.

Het is met TSMS mogelijk om eventlog meldingen van andere domeinen te ontvangen.

- Centraal verzamel punt

De meldingen worden op de TSMS server verzameld en ook gearchiveerd. Vanuit een centraal punt (Web based) kunt u alle instellingen controleren.

- Filtering

Meldingen die vaak voorkomen en die voor u niet van belang zijn kunt u op een uitsluitingslijst plaatsen, deze meldingen zullen dan niet meer doorgestuurd worden.

- Groepen

Eventlog meldingen van een bepaalde applicatie kunt u automatisch door laten sturen naar de applicatie beheergroep.

- Escalaties

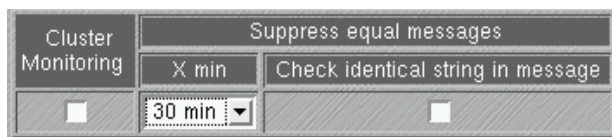
U kunt zelf instellen welke events u via mail wilt ontvangen en welke via bijv. sms.

- Tijdelijke filtering

U kunt ook tijdelijke filters maken die automatisch expireren, dit is bijv. handig als u een virus uitbraak heeft.

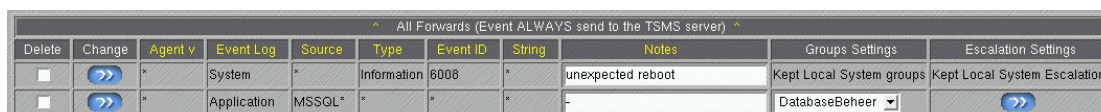
Screenshots

- Cluster monitoring/Suppress equal messages



In dit screenshot worden dubbele meldingen gedurende 30 minuten onderdrukt.

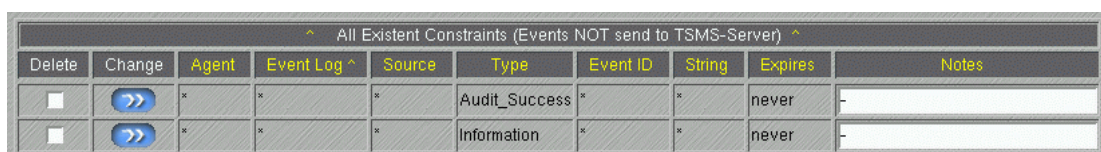
- Forwards



Delete	Change	Agent v	Event Log	Source	Type	Event ID	String	Notes	Groups Settings	Escalation Settings
<input type="checkbox"/>		*	System	*	Information	6008	*	unexpected reboot	Kept Local System groups	Kept Local System Escalation
<input type="checkbox"/>		*	Application	MSSQL*	*	*	*	-	DatabaseBeheer	

In dit screenshot worden alle information records uit de system eventlog die als event id 6008 hebben door gestuurd naar de groepen die bij de agent horen en als escalatie setting worden ook de instellingen van de agent genomen. De MSSQL meldingen gaan direct naar de Database beheer groep en daarvoor zijn er speciale escalatie settings opgegeven.

- Constraints



Delete	Change	Agent	Event Log	Source	Type	Event ID	String	Expires	Notes
<input type="checkbox"/>		*	*	*	Audit_Success	*	*	never	-
<input type="checkbox"/>		*	*	*	Information	*	*	never	-

In dit screenshot worden alle meldingen van het type Audit_Success en Information tegen gehouden.

Screen shots

➤ Escalations

Event Log Escalations (These events have different escalating settings)										
Delete	Change	Agent ^	Event Log	Source	Type	Event ID	String	Notes	Groups Settings	Escalation Settings
<input type="checkbox"/>		*	*	*	Error	*	*	-	Kept Local System groups	
<input type="checkbox"/>		*	*	*	Warning	*	*	-	Kept Local System groups	
<input type="checkbox"/>		*	*	*	Information	*	*	-	Kept Local System groups	
-		TEMPLATE	*	*	*	*	*	-	Kept Local System groups	Kept Local System Escalation

In dit screenshot zijn er verschillende settings voor Error, Warning en Information records gebruikt.

Start Time		End Time		Semafoon	Popup	E-mail	SMS		M
hour	min	hour	min						
8	0	17	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Monday
8	0	17	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Tuesday
8	0	17	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Wednesday
8	0	17	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Thursday
8	0	17	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Friday
8	0	17	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Saturday
8	0	17	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Sunday
8	0	17	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Holidays

U kunt verschillende tijden aangeven waarop u geëscaleerd wenst te worden.

Triangle Solutions b.v.
Developer of TSMS

www.tsms.nl
sales@tsms.nl



An account manager will contact you to ensure that your evaluation can be conducted successfully.