

Der ITAS Event-Handler ist ein leistungsstarker Syslogserver, der es dem Administrator ermöglicht alle Syslog-Events zentral zu verwalten. Viele Netzwerksysteme können Logmeldungen an Syslogserver schicken. Ebenso können z.B. Windows Events an Syslogserver geschickt werden. Der Event-Handler filtert diese Meldungen und informiert den Administrator im Fehlerfall. Das zeitaufwendige, regelmäßige Durchforsten der Systemlogfiles wird dem Administrator vom Event-Handler abgenommen. Fehlerzustände werden zeitnah erkannt und gemeldet. Netzwerkausfälle verringern sich dadurch drastisch.



Gruppenname	Meldungen für System	aktuelles Eventlogfile	Backup Eventlogfile	
Network	5432			show
Windows	0			show
Linux	8		21Feb07_19uhr08	show
RM	0			show
undefined	30			show

Systeme, die Events zum Syslogdaemon schicken, in Gruppen aufnehmen

Systemnamen Filter:

Gruppe1	Gruppe2	Gruppe3	Gruppe4	Gruppe5
Network	Windows	Linux	RM	
System aufnehmen	System aufnehmen	System aufnehmen	System aufnehmen	System aufnehmen
Message	Message	Message	Message	Message
Mail	Mail	Mail	Mail	Mail
Black Berry	Black Berry	Black Berry	Black Berry	Black Berry
submit				
ADSL-Router	P001	P010	P010	
delete	delete	delete	delete	delete



Events anzeigen
Version:3.2(0)

100 Meldungen in Gruppe: Network Meldungen für System: all (100 von 5432)

2007-02-23 09:09:22 firewall 474: 2w6d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up Kommentar zur Meldung: Alles OK, Interface wieder up	select
2007-02-23 09:09:22 firewall 473: 2w6d: %LINK-3-UPDOWN: Interface FastEthernet0/10, changed state to up Kein Kommentar zur Meldung vorhanden	select
2007-02-23 09:09:20 firewall 472: 2w6d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down Kein Kommentar zur Meldung vorhanden	select
2007-02-23 09:09:20 firewall 471: 2w6d: %LINK-3-UPDOWN: Interface FastEthernet0/10, changed state to down Kein Kommentar zur Meldung vorhanden	select
2007-02-22 13:35:28 firewall 470: 2w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up Kommentar zur Meldung: Alles OK, Interface wieder up	select



Event-Handler - Filter
Version:3.2(0)

Filterlauf über aktuelle Meldungen Filter vom System: Firewall

Filter aus Gruppe: Network Counter reset reset GO

Filter: exakt Treffer: 122 reset last reset: 10.11.05 14:27 Uhr show filtered

2007-02-23 09:09:22 firewall 474: 2w6d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up	<input type="checkbox"/> exakt <input type="checkbox"/> tolerant <input type="checkbox"/> assimilieren <input type="checkbox"/> forward <input type="checkbox"/> delete
2007-02-23 09:09:22 firewall 473: 2w6d: %LINK-3-UPDOWN: Interface FastEthernet0/10, changed state to up	<input checked="" type="checkbox"/> exakt <input type="checkbox"/> tolerant <input type="checkbox"/> assimilieren <input type="checkbox"/> forward <input type="checkbox"/> delete
2007-02-23 09:09:20 firewall 472: 2w6d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down	<input type="checkbox"/> exakt <input type="checkbox"/> tolerant <input type="checkbox"/> assimilieren <input type="checkbox"/> forward <input type="checkbox"/> delete

Event-Handler Features:

- Der Event-Handler stellt einen zentralen Syslog Server für alle Netzwerksysteme zur Verfügung.
- Eingehende Syslog-Events werden durch defnierbare Filter auf ihre Relevanz hin untersucht.
- Es stehen 3 verschiedene Filterarten zur Verfügung:
 - exakt: Event matched - bis auf die Ziffern
 - tolerant: wie exakt - bis auf Informationen in Klammern
 - assimilieren: Schnittmenge artgleicher Events
- Kommentieren wichtiger Syslogmeldungen. Diese Kommentare werden als zusätzliche Information zum Event mit angezeigt.
- Kategorisierung der Netzwerksysteme in Gruppen
- Archivierung aller Meldungen in Gruppenlogfiles zur nachträglichen Bearbeitung.
- Maximales Alter der Logfiles einstellbar.
- Suchfunktionen mit Schlüsselwörtern helfen dem Administrator das aktuelle oder ältere Logfiles zu analysieren
- Syslogmeldungen von nicht zugeordneten Systemen werden in der Gruppe „undefined“ gespeichert.
- Benachrichtigung der zuständigen Administratoren mittels eMail bei Erkennung eines relevanten Events.
- Systemnamenfilter erleichtern das Bearbeiten von Meldungen bestimmter Systeme.
- Anzeige der Anzahl gefundener Events pro Gruppe
- Trotz gruppenweiser Zuordnung der Syslogmeldungen werden diese systembezogen angezeigt.
- Begrenzung der angezeigten Meldungen auf eine definierbare Anzahl.