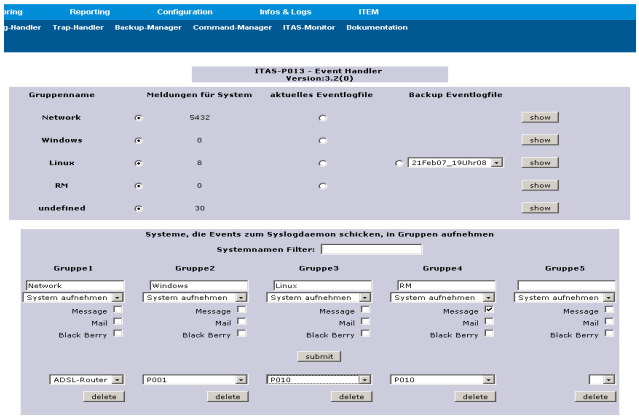
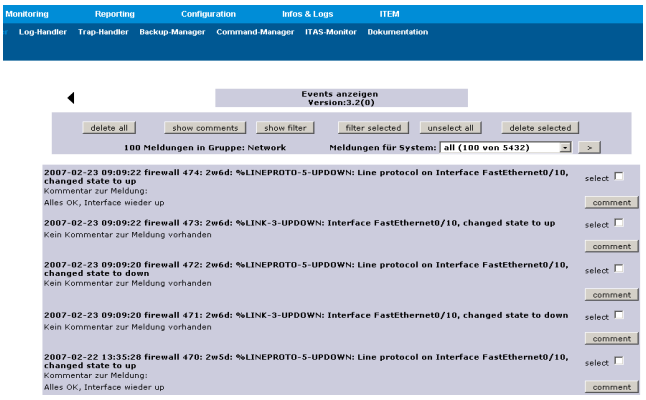
ingenieurgesellschaft thivessen

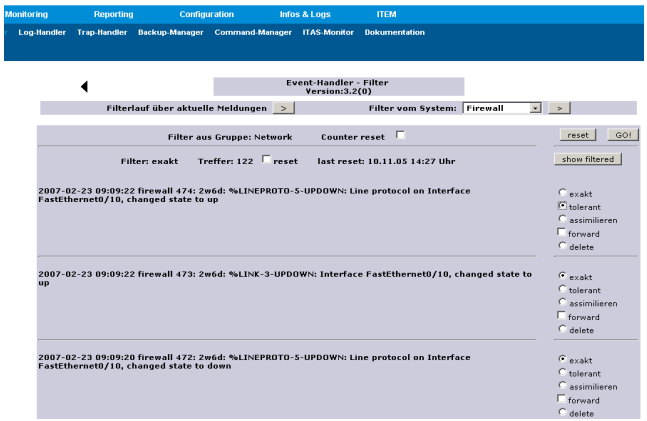
ITAS

Modul: Event-Handler - der Syslogserver

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 Duchforsten der Systemlogfiles wird dem Administrator vom Event-Handler abgenommen. Fehlerzustände werden zeitnah erkannt und gemeldet. Netzwerkausfälle verringern sich dadurch drastisch.







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.