

Der ITAS TRAP-Handler ist eine leistungsfähige und gleichzeitig einfach zu handhabende Software, die SNMP-Traps meldet. Da nicht alle Traps von Interesse sind oder bei einem Alarm möglicherweise mehrere Traps vom System generiert werden, lassen sich unwichtige Traps ausfiltern, die zukünftig nicht mehr gemeldet werden. SNMP-Traps aller System können mit dem Trap-Handler zentral verwaltet und analysiert werden.

### Reporting Configuration Infos & Logs ITEM

ITAS-TRAP-Handler  
Version:3.2(0)

Gruppenname	Trap Meldungen	aktuelle Traplogfile	aktuelle Emergency's	Backup Traplogfile
Netzwerk	185	<input type="checkbox"/>	<input type="checkbox"/>	
Switche	0	<input type="checkbox"/>	<input type="checkbox"/>	
firewall	3090	<input type="checkbox"/>	<input type="checkbox"/>	21Jan07_21Uhr09
windows	0	<input type="checkbox"/>	<input type="checkbox"/>	
router	1986	<input type="checkbox"/>	<input type="checkbox"/>	28Jan07_22Uhr03
undefined	15	<input type="checkbox"/>	<input type="checkbox"/>	

Systeme, die SNMP-Traps zum Trapdaemon schicken, in Gruppen aufnehmen

Systemnamen Filter:

Gruppe1	Gruppe2	Gruppe3	Gruppe4	Gruppe5
Netzwerk	Switche	firewall	windows	router
System aufnehmen	System aufnehmen	System aufnehmen	System aufnehmen	System aufnehmen
Message <input type="checkbox"/>	Message <input type="checkbox"/>	Message <input type="checkbox"/>	Message <input type="checkbox"/>	Message <input type="checkbox"/>
Mail <input type="checkbox"/>	Mail <input type="checkbox"/>	Mail <input type="checkbox"/>	Mail <input type="checkbox"/>	Mail <input type="checkbox"/>
Black Berry <input type="checkbox"/>	Black Berry <input type="checkbox"/>	Black Berry <input type="checkbox"/>	Black Berry <input type="checkbox"/>	Black Berry <input type="checkbox"/>
submit	submit	submit	submit	submit
ADSL-Router <input type="checkbox"/>	Switch <input type="checkbox"/>	Firewall <input type="checkbox"/>	POD1 <input type="checkbox"/>	ADSL-Router <input type="checkbox"/>
delete	delete	delete	delete	delete

### Monitoring Reporting Configuration Infos & Logs ITEM

SNMP Traps anzeigen  
Version:3.2(0)

100 Meldungen in Gruppe: firewall

Meldungen für System: all (100 von 3090)

2007-02-02 16:10:52 Firewall :::: EXPRESSION: MIB::sysUpTimeInstance = INTEGER: 1072442888  
SNMPv2-MIB::snmpTrapOID.0 = OID: BRIDGE-MIB::topologyChange  
Kein Kommentar zur Meldung vorhanden.

2007-02-02 16:10:23 Firewall :::: EXPRESSION: MIB::sysUpTimeInstance = INTEGER: 1072443290  
SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::Index.11 = INTEGER: 11 IF-MIB::Descr.11 = STRING: FastEthernet0/10 IF-MIB::Type.11 = INTEGER: ethernetSmac(6)  
OLD-CISCO-INTERFACES-MIB::actReason.11 = STRING: "up"  
Kein Kommentar zur Meldung vorhanden.

2007-02-02 16:10:19 Firewall :::: EXPRESSION: MIB::sysUpTimeInstance = INTEGER: 1072442948  
SNMPv2-MIB::snmpTrapOID.0 = OID: BRIDGE-MIB::topologyChange  
Kein Kommentar zur Meldung vorhanden.

2007-02-02 16:10:19 Firewall :::: EXPRESSION: MIB::sysUpTimeInstance = INTEGER: 1072442946  
SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::Index.11 = INTEGER: 11 IF-MIB::Descr.11 = STRING: FastEthernet0/10 IF-MIB::Type.11 = INTEGER: ethernetSmac(6)  
OLD-CISCO-INTERFACES-MIB::actReason.11 = STRING: "down"  
Kein Kommentar zur Meldung vorhanden.

2007-02-01 22:9:47 Firewall :::: EXPRESSION: MIB::sysUpTimeInstance = INTEGER: 1065959762  
SNMPv2-MIB::snmpTrapOID.0 = OID: BRIDGE-MIB::topologyChange  
Kein Kommentar zur Meldung vorhanden.

### Monitoring Reporting Configuration Infos & Logs ITEM

TRAP-Handler - Filter  
Version:3.2(0)

Filterlauf über aktuelle Meldungen

Filter aus Gruppe: firewall

Counter reset

Filter: exakt Treffer: 5 reset last reset: 12.05.04 09:36 Uhr

2007-02-02 16:10:52 Firewall :::: EXPRESSION: MIB::sysUpTimeInstance = INTEGER: 1072442888  
SNMPv2-MIB::snmpTrapOID.0 = OID: BRIDGE-MIB::topologyChange

2007-02-02 16:10:22 Firewall :::: EXPRESSION: MIB::sysUpTimeInstance = INTEGER: 1072443290  
SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::Index.11 = INTEGER: 11 IF-MIB::Descr.11 = STRING: FastEthernet0/10 IF-MIB::Type.11 = INTEGER: ethernetSmac(6)  
OLD-CISCO-INTERFACES-MIB::actReason.11 = STRING: "up"

2007-02-02 16:10:19 Firewall :::: EXPRESSION: MIB::sysUpTimeInstance = INTEGER: 1072442946  
SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::Index.11 = INTEGER: 11 IF-MIB::Descr.11 = STRING: FastEthernet0/10 IF-MIB::Type.11 = INTEGER: ethernetSmac(6)  
OLD-CISCO-INTERFACES-MIB::actReason.11 = STRING: "down"

### Trap-Handler Features:

- Der Trap-Handler stellt einen zentralen SNMP-Trap Server für alle Netzwerksysteme zur Verfügung.
- Eingehende Traps werden durch defnierbare Filter auf ihre Relevanz hin untersucht.
- Es stehen 3 verschiedene Filterarten zur Verfügung:
  - exakt: Trap matched - bis auf die Ziffern
  - tolerant: wie exakt - bis auf Informationen in Klammern
  - assimilieren: Schnittmenge artgleicher Traps
- Kommentieren wichtiger Traps. Diese Kommentare werden als zusätzliche Information zum Trap mit angezeigt.
- Kategorisierung der Netzwerksysteme in Gruppen
- Archivierung aller Traps in Gruppenlogfiles zur nachträglichen Bearbeitung.
- Maximales Alter der Logfiles einstellbar.
- Suchfunktionen mit Schlüsselwörtern helfen dem Administrator das aktuelle oder ältere Logfiles zu analysieren
- Traps von nicht zugeordneten Systemen werden in der Gruppe „undefined“ gespeichert.
- Benachrichtigung der zuständigen Administratoren mittels eMail bei Erkennung eines relevanten Traps.
- definieren von „Emergency Traps“, um über bestimmte Traps informiert zu werden, auch wenn die Mailbenachrichtigung allgemein ausgeschaltet ist.
- Emergency Traps können mit On/Off-Traps getriggert werden, um im „aktuellen Status“ des ITAS Monitor einen Alert zu erzeugen bzw. zu beenden.
- Emergency Traps können mit variablen Mustern arbeiten, um bestimmte Alerts als Eindeutig zu erkennen (z.B. die MAC Adresse einer WLAN Komponente)