1 Einleitung

SNMP-Basic-Agent BS2000 V5.0 (SBA-BS2) und SNMP-Standard-Collection BS2000 V5.0 (SSC-BS2) bieten die Basis-Funktionalität für BS2000/OSD-Systeme, um in SNMP-basierte Managementumgebungen, wie z.B. Unicenter TNG der Firma COMPUTER ASSOCIATES, eingebunden werden zu können. SBA-BS2 und SSC-BS2 erlauben Netz-, System- und Anwendungsmanagement über SNMP von einer zentralen Management-Station aus. Für die Integration in Management-Plattformen wird ein Integrationspaket (SMBS2 bzw. SMAWsmbs2) ausgeliefert. Zu dem in SBA-BS2 enthaltenen Console Monitor gibt eine Management-Anwendung CMBS2 (Integrationspaket CMBS2 bzw. SMAWcmbs2) auf der Management-Seite. Der SNMP-Subagent für SM2 (SSA-SM2-BS2), der SNMP-Subagent für *open*UTM (SSA-OUTM-BS2) sowie die Subagenten für die Produkte *open*Net Server (BCAM-Subagent) und *inter*Net Services ergänzen die ständig wachsende Zahl und Funktionalität der BS2000/OSD-Subagenten. Darüber hinaus ermöglicht das SNMP-Management für BS2000/OSD den Web-Zugriff auf Management-Informationen.

1.1 Zielsetzung

Dieses Handbuch beschreibt einerseits die Einbettung von SBA-BS2, SSC-BS2 und den additiven Subagenten SSA-SM2-BS2 und SSA-OUTM-BS2 in BS2000/OSD und die zum Betrieb notwendigen Installations- und Konfigurationsschritte sowie den Betrieb selbst. Die zur Überwachung notwendigen Agenten und ihre MIBs werden detailliert vorgestellt. Andererseits wird die Installation und Konfiguration von SMBS2 / SMAWsmbs2 sowie von CMBS2 / SMAWcmbs2 und PMBS2 / SMAWpmbs2 auf der Management-Station dargestellt. Jeweils ein eigenes Kapitel ist den Themen „Web-Zugriff auf Management-Informationen“ und „Trap-Server für Solaris und Reliant UNIX“ gewidmet.

1.2 Zielgruppe

Das vorliegende Handbuch wendet sich an Netzplaner, -verwalter, -operateure und Systembetreuer, die BS2000/OSD-Systeme in ein SNMP-basiertes Netz-, System- und Anwendungsmanagement integrieren bzw. ein solches System bedienen wollen. Kenntnisse des Betriebssystems BS2000/OSD sowie der TCP/IP-Grundbegriffe werden vorausgesetzt.

1.3 Wegweiser durch das Handbuch

Das vorliegende Handbuch ist wie folgt strukturiert:

- Kapitel 2: Überblick

  Dieses Kapitel führt in die SNMP-Architektur ein, stellt Grundlagen vor und beschreibt die Einbettung in BS2000/OSD sowie die Funktionalität von SBA-BS2, SSC-BS2, SSA-SM2-BS2 und SSA-OUTM-BS2. Die Arbeitsweise des Master- und der Subagenten wird vorgestellt.

- Kapitel 3: Installation und Konfiguration

  In diesem Kapitel werden die Installationsvoraussetzungen sowie die Installation selbst beschrieben, einerseits für SBA-BS2, SSC-BS2 und die additiven Subagenten in BS2000/OSD, andererseits auf der Management-Station für SMBS2 / SMAWsmbs2, CMBS2 / SMAWcmbs2 und PMBS2 / SMAWpmbs2. Die Konfigurationsschritte werden ebenfalls aus Sicht des BS2000/OSD und aus Sicht der Management-Station dargestellt.

- Kapitel 4: Betrieb

  Im Kapitel 4 werden die BS2000/OSD-Kommandos zur In- und Außerbetriebnahme des Master- und der Subagenten beschrieben.

- Kapitel 5: Funktionen des BASIC-AGENT

  Dieses Kapitel beschreibt die System- und SNMP-Gruppe der MIB-II für das Management durch den Masteragenten und den Supervisor Subagenten sowie für die Anwendungsüberwachung durch den Application Monitor Subagenten und die Konsolüberwachung durch den Consol Monitor Subagenten. Außerdem beschreibt das Kapitel die Funktionen des HTML-Subagenten zur Erzeugung kundenspezifischer Web-Seiten.

- Kapitel 6: Funktionen der STANDARD-COLLECTION

  Die in der STANDARD-COLLECTION enthaltenen Subagenten werden in Kapitel 6 beschrieben. Neben Funktionsbeschreibungen finden Sie hier auch vollständige Auflistungen der zugehörigen MIBs.

- Kapitel 7: SNMP-Management zur erweiterten Performance-Überwachung mit SM2

  Der additive Subagent zur SM2-basierten Performance-Überwachung ist Thema von Kapitel 7. Es wird die Funktionalität beschrieben und die MIB aufgelistet.

- Kapitel 8: SNMP-Management zur Überwachung von *open*UTM und *open*UTM-Anwendungen

  Funktionalität und MIB des additiven Subagenten zur Überwachung von *open*UTM-Anwendungen sind in Kapitel 8 dargestellt.

- Kapitel 9: Betrieb der Management-Station

  Die zum Einsatz auf Management-Stationen zur Verfügung stehenden Management-Anwendungen werden in Kapitel 9 detailliert erläutert.

- Kapitel 10: Web-Zugriff auf Management-Informationen

  Kapitel 10 beschreibt den Zugriff auf Management-Informationen über das World Wide Web (WWW). Nach der Beschreibung der Web-Schnittstelle sowie des Handlings der Web-Oberfläche werden Erstellung und Konfiguration benutzer-spezifischer Web-Seiten, sog. Custom-Pages, erläutert.

- Kapitel 11: Trap-Server

  In Kapitel 11 wird der Trap-Server beschrieben, der für Solaris und Reliant UNIX angeboten wird. Neben dem Trap-Server-Prozess werden das Kommandoprogramm für die Server-Konfiguration, die Trap-Sende-Programme sowie das Trap-Empfangs-Programm erläutert.

- Kapitel 12: Konfigurationsbeispiele

  In diesem Kapitel werden Konfigurationsbeispiele zu den Themen Basisüberwachung, Meldungsüberwachung, Überwachung von Anwendungen und Performance-Überwachung vorgestellt.

- Anhang

  Im Anhang sind die DCAM-Returncodes (Application Monitor Subagent) aufgelistet.

Diese Handbuch enthält eine Reihe von Abbildungen, welche die Anzeige der von den einzelnen Subagenten gelieferten Informationen auf den verschiedenen Management-Plattformen sowie an der Web-Schnittstelle wiedergeben.

1.4 Typografische Gestaltungsmittel

In diesem Handbuch werden folgende Mittel zur Darstellung von funktional wichtigen Textteilen verwendet:

für Hinweistexte

für Warnhinweise

kursive Schrift
: für Dateinamen, Namen von Auftragsfenstern, Parameterbezeichnungen, Menütitel und Menüeinträge sowie Kommandos und Variablen im Fließtext.

<spitze Klammern>
: kennzeichnen Variable, wenn Sie dafür Werte einsetzen müssen.

`dicktengleiche Schrift`
: für die Darstellung von Eingaben für das System, Systemausgaben und für Dateinamen in Beispielen.

kommando
: In der Syntaxbeschreibung für Kommandos werden diejenigen Bestandteile (Bezeichnungen von Kommandos und Parametern) fett dargestellt, die unverändert eingegeben werden müssen.

1.5 Änderungen gegenüber der Vorgängerversion

Mit der Version V5.0 des SNMP-Managements für BS2000/OSD werden folgende neue Funktionen unterstützt:

- Verfügbarkeit des Integrationspakets SMAWsmbs2 unter Solaris (in Verbindung mit der Management-Plattform Unicenter TNG)
- Unterstützung eines Trap-Servers für Solaris und Reliant UNIX
- Remote-Fähigkeit des Masteragenten für die SINIX2000-Subagenten
- Trap-Acknowledge-Gruppe für den Supervisor Subagenten
- Erweiterung der STANDARD-COLLECTION (SSC-BS2) um den HSMS-Subagenten
- Unterstützung eines generischen Trap-Formats im Application Monitor Subagenten und im Console Monitor Subagenten. Filter bei der Dateien-Überwachung im Application Monitor Subagenten.
- Erweiterung des *open*FT-Subagenten um neue Traps sowie um neue MIB-Objekte, die zusammen mit den Traps versendet werden
- Trap-Anzeige im Web-Browser

1.6 Readme-Datei

Funktionelle Änderungen und Nachträge der aktuellen Produktversion zu diesem Handbuch entnehmen Sie bitte ggf. der produktspezifischen Readme-Datei. Sie finden die Readme-Datei auf Ihrem BS2000/OSD-Rechner unter dem Dateinamen SYSRME.*SBA-BS2.050.D*. Die Benutzerkennung, unter der sich die Readme-Datei befindet, erfragen Sie bitte bei Ihrer zuständigen Systembetreuung. Die Readme-Datei können Sie mit dem Kommando /SHOW-FILE oder mit einem Editor ansehen oder auf einem Standarddrucker mit folgendem Kommando ausdrucken:

/PRINT-DOCUMENT *dateiname*,LINE-SPACING=*BY-EBCDIC-CONTROL

2 Überblick

SNMP steht für **S**imple **N**etwork **M**anagement **P**rotocol und wurde als Protokoll für Netzmanagement-Dienste in TCP/IP-Netzen entwickelt. Die Überwachung und Administration von LAN-Komponenten, wie z.B. Bridges, Routers, Hubs usw. in heterogenen Netzen mit TCP/IP-Protokollen war ursprünglich die einzige Aufgabe von SNMP. Inzwischen hat sich der Anwendungsbereich von SNMP um System- und Anwendungsmanagement erweitert. Ähnlich wie bei TCP/IP, wo der Begriff nicht nur die Protokolle als solche, sondern das gesamte entsprechende Netzwerk bezeichnet, steht auch SNMP nicht nur für das Protokoll allein, sondern für das gesamte auf SNMP basierte Management-System.

Wie im TCP/IP-Bereich üblich, werden auch die für SNMP relevanten Dokumente vom IAB (Internet Architecture Board) in RFCs (Request for Comment) abgelegt. Die grundlegenden RFCs für SNMPv1 (Version 1) sind:

– RFC 1155: "Structure and Identification of Management Information for TCP/IP-based Internets (SMI)", Mai 1990

– RFC 1157: "A Simple Network Management Protocol (SNMP)", Mai 1990

– RFC 1212: "Concise MIB Definitions", März 1991

– RFC 1213: "Management Information Base for Network Management of TCP/IP-based Internets: MIB-II", März 1991

SNMP Stufe 5 des SNMP-Managements von BS2000/OSD unterstützt auch SNMPv3 (Version 3). Die zugehörigen RFCs sind:

– RFC 2271: "An Architecture for Describing SNMP Management Frameworks", Januar 1998

– RFC 2272: "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", Januar 1998

– RFC 2273: "SNMPv3 Applications", Januar 1998

– RFC 2274: "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", Januar 1998

– RFC 2275: "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", Januar 1998

2.1 Grundlagen der SNMP-Management-Architektur

Zentraler Bestandteil einer SNMP-Installation ist die Management-Plattform. Als Leitstand mit Grafikterminals ermöglicht die Management-Plattform eine übersichtliche Darstellung der verwalteten Komponenten und eine komfortable Bedienung. Von der Management-Plattform aus lässt sich das Netz mit all seinen Systemen und Anwendungen überwachen und steuern. SNMP ist nicht auf eine bestimmte Management-Plattform fixiert.

Auf der Management-Plattform residiert der SNMP-Manager, auch Management-Station genannt. Der SNMP-Manager ist eine Anwendung, die via SNMP über ein TCP/IP-Netz mit Partneranwendungen, den SNMP-Agenten, kommuniziert. Auf jeder verwalteten Komponente liegt ein Agent, der dem SNMP-Manager aktuelle Informationen über diese Komponente liefert. Die Initiative zur Steuerung der Aktivitäten liegt überwiegend auf Seiten des SNMP-Managers, wodurch die Belastung der verwalteten Komponenten mit Management-Aufgaben gering gehalten wird.

Grundlage für das Management der zu verwaltenden Komponenten ist die genaue Beschreibung der zu administrierenden Bestandteile (Objekte) dieser Komponenten in der MIB (Management Information Base). Die MIB ist das informationstechnische Rückgrat eines jeden Management Agents. Sie enthält Informationen zu Eigenschaften, wie z.B. Name, Syntax, Zugriffsrechte und Status jeder einzelnen Komponente. Für viele Hard- und Softwarekomponenten werden vom Hersteller eigene MIBs mitgeliefert. Die Codierung der MIB erfolgt in ASN.1 (Abstract Syntax Notation One). ASN.1 wurde auch von ISO als Standard für den Presentation Layer genormt (siehe ISO/IEC 8824 und 8825).

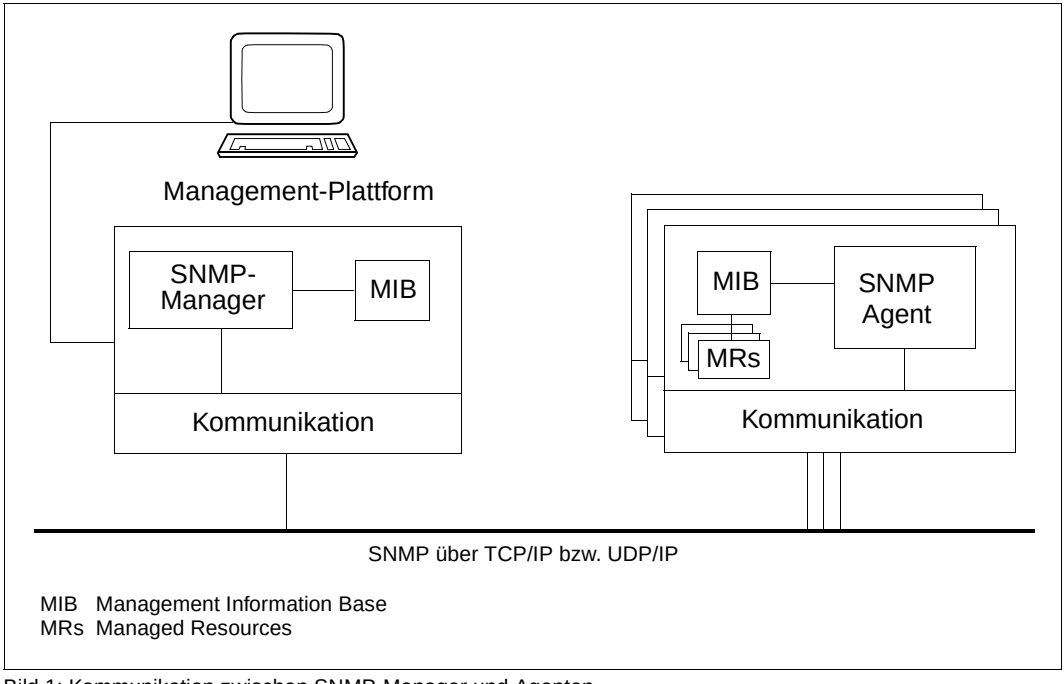


Bild 1: Kommunikation zwischen SNMP-Manager und Agenten

SNMP-Protokollelemente

Der Transport der Informationen über das Netz erfolgt mithilfe von funktionsabhängigen SNMP-Protokollelementen. SNMPv1 benötigt zum Abfragen, Setzen und Anzeigen von Werten, die relevante Management-Informationen (Objektwerte) enthalten, nur vier verschiedene Protokollelemente. Ein fünftes Protokollelement, Trap, dient dem Agenten zum asynchronen Melden wichtiger Ereignisse.

Protokollelement	Typ	Funktion
GetRequest-PDU	0	Leseanforderung des Managers für ein genau definiertes Objekt
GetNextRequest-PDU	1	Leseanforderung des Managers für das nächste (unbekannte) Objekt
GetResponse-PDU	2	Rückmeldung des Agenten mit den geforderten Werten
SetRequest-PDU	3	Schreibanforderung des Managers auf ein genau definiertes Objekt
Trap-PDU	4	Asynchrone Meldung des Agenten bei besonderen Ereignissen

SNMPv1-Protokollelemente

Die eigentliche SNMP-Nachricht ist recht einfach aufgebaut. Sie besteht aus dem SNMP-Header sowie der PDU (Protocol Data Unit). Der SNMP-Header enthält ein Versionskennzeichen und den Community-Namen.

Die PDU besteht aus dem Feld für den PDU-Typ sowie einer Liste von

– zu lesenden Variablen (bei GetRequest und GetNextRequest) oder
– zu setzenden Variablen (bei SetRequest).

Jede Variable besteht aus dem Namen eines überwachten Objekts und dem zugehörigen Wert. Die Liste der zu einer SNMP-Nachricht gehörenden Variablen wird Variable-Bindings genannt.

2.2 SNMP-Management im BS2000/OSD - Einbettung und Funktionalität

Für den Anschluss des BS2000/OSD an ein SNMP-Management bietet Siemens Lösungen mit unterschiedlicher Zielsetzung.

- Mit den Produkten SNMP-Basic-Agent BS2000 V5.0 (SBA-BS2) und SNMP-Standard-Collection BS2000 V5.0 (SSC-BS2) lassen sich BS2000/OSD-Systeme direkt in SNMP-basierte Management-Plattformen, z.B. Unicenter TNG, TransView oder OpenView, integrieren. SNMP-Basic-Agent und SNMP-Standard-Collection ermöglichen Netz-, System- und Anwendungsmanagement über eine Implementierung des SNMP-Protokolls in BS2000/OSD. Außerdem gestattet der SNMP-Basic-Agent den Zugriff auf Management-Informationen über HTTP/HTML (siehe Kapitel „Web-Zugriff auf Management-Informationen“ auf Seite 407).
  Der SNMP-Subagent für SM2 (SSA-SM2-BS2), der SNMP-Subagent für *open*UTM (SSA-OUTM-BS2) sowie die Subagenten für die Produkte *open*Net Server und *inter*Net Services ergänzen die ständig wachsende Zahl und Funktionalität der BS2000/OSD-Subagenten.
- Im Rahmen des HIPLEX-Konzepts bietet sich zusätzlich die Möglichkeit, die BS2000/OSD-Systeme in der Startup- und Shutdown-Phase zu überwachen, von der Management-Plattform aus mit POWER ON bzw. POWER OFF BS2000/OSD-Rechner zentral ein- bzw. auszuschalten und alle weiteren SKP-Aktivitäten durchzuführen. Voraussetzungen dafür sind der Einsatz einer Management-Plattform (CA Unicenter TNG oder TransView Control Center) sowie eine LAN-Vernetzung (TCP/IP) zu den entsprechenden SKP-Konsolen und zum Produkt HIPLEX OP (siehe Handbuch zu HIPLEX OP).
- Das Produkt SNMP-Proxy BS2000/PDN (UNIX) erschließt die TRANSDATA-Welt durch Umsetzen des NMCP-Protokolls in das SNMP-Protokoll. Als Gateway dient dabei ein UNIX-Rechner. Auf diese Weise kann das Netzmanagement in einem TRANSDATA-Netz für BS2000/OSD-, PDN-, SINIX- und INCA-Systeme mit proprietären TRANSDATA-Protokollen (NMCP) betrieben werden.
- Auch der HNC (**H**igh-Speed **N**et **C**onnect) ist in das zentrale SNMP-Management eines heterogenen Systemverbunds eingebunden.

Bild 2 auf der nächsten Seite gibt einen Überblick über die SNMP-Integration von BS2000/OSD.

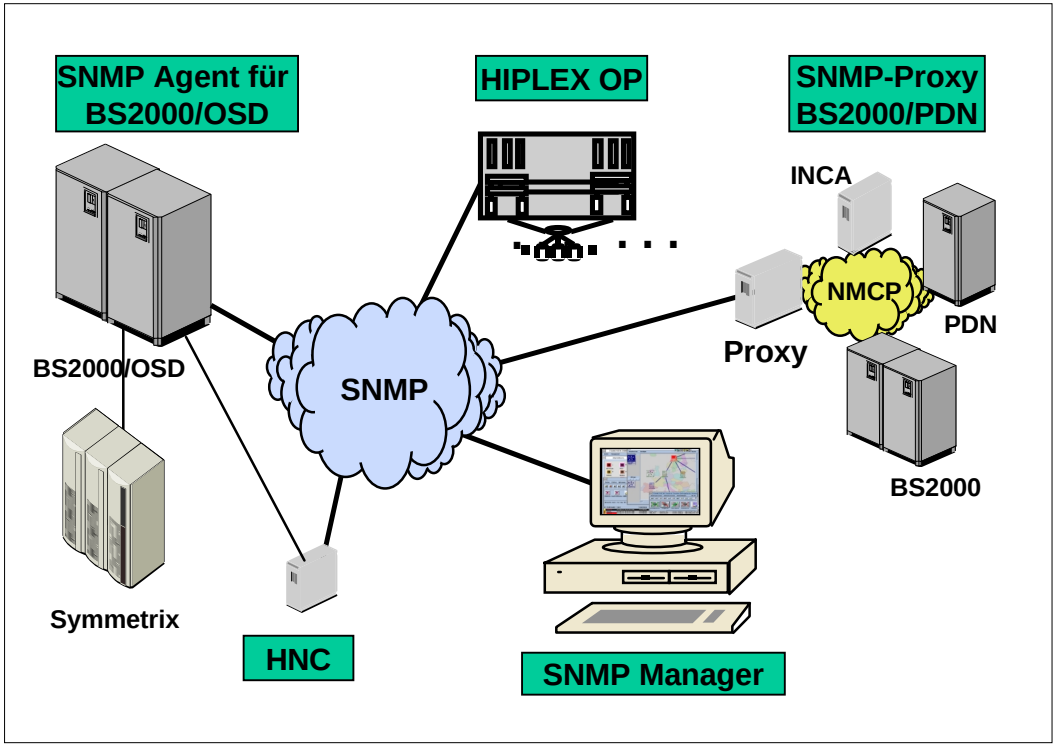


Bild 2: Überblick über die mit SNMP administrierbaren Systeme

2.2.1 Produktstruktur

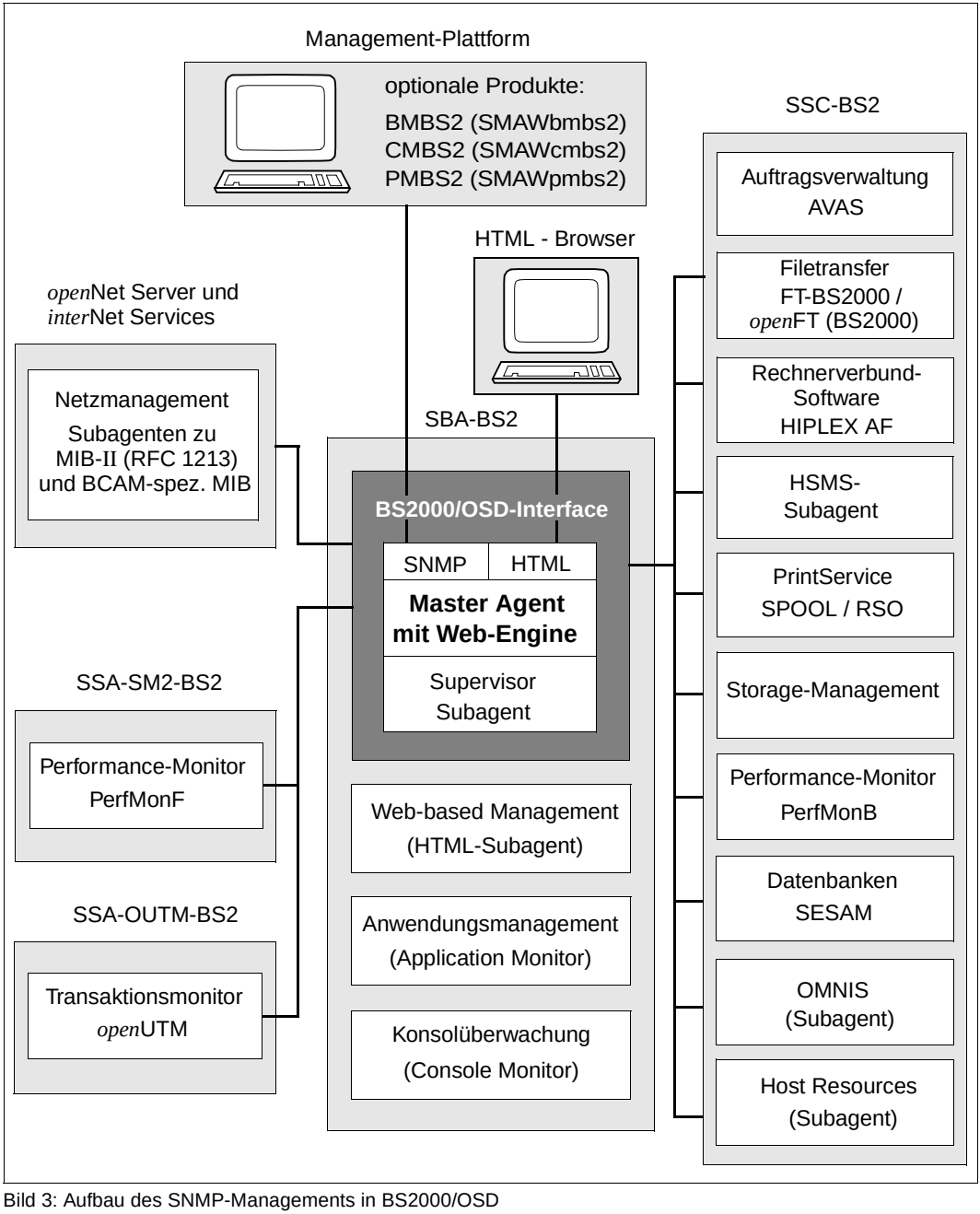


Bild 3: Aufbau des SNMP-Managements in BS2000/OSD

SBA-BS2 (SNMP-Basic-Agent BS2000)

Der Masteragent wird mit der Liefereinheit SBA-BS2 V5.0 ausgeliefert. Die Liefereinheit enthält außerdem die Subagenten „Supervisor Subagent“, „Application Monitor Subagent“, „Console Monitor Subagent“ und „HTML-Subagent“.

- Der Masteragent ist einerseits der BS2000/OSD-Kommunikationspartner der Management-Station, der das SNMP-Protokoll abwickelt. Andererseits steuert er die Kommunikation mit den Subagenten. Zusätzlich bietet er Zugriffe auf die System- und die SNMP-Gruppe der MIB-II (RFC 1213) sowie auf Objekte weiterer standardisierter SNMP-MIBs (RFC 2272 - RFC 2275) und erlaubt so die Überwachung des Systems und der SNMP-relevanten Werte. Ferner ermöglicht der Masteragent den Web-Zugriff auf Informationen aus den MIBs.
- Der Supervisor Subagent überwacht die anderen Subagenten und die von ihnen gemeldeten Ereignisse.
- Der Application Monitor Subagent überwacht Benutzeranwendungen, BCAM-Anwendungen, Tasks, Jobvariablen und BS2000/OSD-Subsysteme. Außerdem überwacht er Logging-Dateien in BS2000/OSD, POSIX und NFS. DCAM-Anwendungen können zyklisch überwacht werden. Logisch zusammengehörige Objekte aus einem Business-Prozess können mit dem Application Monitor Subagent als Gruppe zusammengefasst werden und sowohl gemeinsam als auch einzeln überwacht werden.
- Der Console Monitor Subagent dient der Konsolüberwachung. Er bietet Ihnen einerseits die Möglichkeit, Konsolmeldungen als Traps weiterzuleiten; die Menge der zu erfassenden Meldungen kann dabei gezielt definiert werden. Andererseits können Sie von der Management-Station aus BS2000/OSD-Kommandos absetzen und das Resultat dieser Kommandos abfragen.

  Die zugehörige Management-Anwendung, die auf der mitgelieferten CD-ROM enthalten ist, ermöglicht die netzweite Darstellung von Konsolmeldungen sowie die komfortable Konsolbedienung aller überwachten BS2000/OSD-Systeme.
- Der HTML-Subagent ermöglicht die Definition kundenspezifischer Web-Seiten (Custom-Pages) für den Web-Zugang zu den Management-Informationen von BS2000/OSD.

SBA-BS2 enthält außerdem zwei SDF-Kommandos zum Versenden von Traps.

SSC-BS2 (SNMP-Standard-Collection BS2000)

Mit SSC-BS2 V5.0 wird ein Set von Subagenten für BS2000/OSD-spezifische Management-Aufgaben ausgeliefert.

- Der AVAS-Subagent überwacht den Gesamtzustand von AVAS, die zentralen Prozesse und Ablaufsteuerungen sowie die Jobnetze und Strukturelemente.
- Der *open*FT (BS2000)-Subagent liefert Informationen über FT-Systemparameter und Statistikdaten des laufenden Betriebs. Weitere Funktionen sind das Starten und Stoppen des FT, die Steuerung der Diagnose, das Ändern des Public-Key zur Verschlüsselung und das Ändern des Status eines FT-Partners.
- Der Subagent für HIPLEX-AF informiert über die aktuelle Konfiguration im HIPLEX-Verbund und meldet alle relevanten Änderungen.
- Der HSMS-Subagent ermöglicht das Lesen und Ändern von globalen HSMS-Daten. Ferner liefert er detaillierte Informationen über HSMS-Aufträge. Der Umfang der Aufträge kann durch die Auswahlkriterien „Zustand“ und „Herkunftsort“ eingeschränkt werden.
- Der Subagent für Spool & Print Service überwacht die Geräte für SPOOL und RSO und liefert Informationen zu Druckaufträgen.
- Der Subagent für das Storage-Management liefert Informationen über Pubsets und Platten. Außerdem kann der Subagent ausgewählte oder alle Pubsets und Platten überwachen.
- Der Subagent Host Resources liefert Informationen über das System, über Geräte und Datei-Systeme sowie über die installierte Software und meldet Zustandswechsel.
- Der OMNIS-Subagent überwacht Datenstationen, Partner und Anwendungen und ermöglicht die Administration von OMNIS selbst.
- Der Subagent für das Management von SESAM-Datenbanken liefert Informationen über SESAM-Datenbanken und SESAM-DBHs, mit denen diese Datenbanken prozessiert werden (RDBMS-MIB gemäß RFC 1697).
- Der Subagent zur Performance-Basisüberwachung mit SM2 (PerfMonB) liefert Durchschnittswerte zur Überwachung des CPU-Verbrauchs und der I/O-Raten.

SSA-SM2-BS2 (SNMP-Subagent für den Performance-Monitor SM2)

Der SM2-basierte Performance-Subagent SSA-SM2-BS2 liefert Basisinformationen zum SM2 selbst, d.h. zum Status des Subsystems, zur Version, zur Größe des Messintervalls und zum Stichprobenzyklus. Die eigentlichen Messwerte entsprechen den SM2-bekannten Reportgruppen und informieren über

- die CPU-Auslastung,
- I/O-Aktivitäten,
- die Auslastung des Hauptspeichers und des virtuellen Adressraums,
- die Belegung des Hauptspeichers durch die vier Standardkategorien von Tasks,
- Ein- und Ausgabeoperationen auf periphere Geräte während eines Messintervalls,
- applikationsspezifische Daten von *open*UTM-Anwendungen,
- Verbrauchswerte einzelner Tasks.

Zur Darstellung und Bewertung der gelieferten Messwerte auf der Management-Station steht die auf der mitgelieferten CD-ROM enthaltene Management-Anwendung PMBS2 zur Verfügung, die auch die gleichzeitige Überwachung mehrerer BS2000/OSD-Systeme ermöglicht.

SSA-OUTM-BS2 (SNMP-Subagent für *open*UTM in BS2000/OSD)

Der ebenfalls zu den additiven Subagenten gehörende *open*UTM-Subagent SSA-OUTM-BS2 bietet folgende Leistungen:

- Überwachung und Steuerung ausgewählter *open*UTM-Anwendungen,
- Informationen über Systemparameter, physikalische und logische Terminals, Terminal-Pools, Transaktionscodes, Transaktionsklassen, Benutzerdaten, Verbindungen und Statistikdaten,
- Änderung von Anwendungseigenschaften und Systemparametern,
- Sperren bzw. Entsperren von UTM-Datenstationen,
- Beenden einer *open*UTM-Anwendung.

Für *open*UTM in Reliant UNIX gibt es den Subagenten SSA-OUTM-SX.

SNMP-Subagenten für *open*Net Server und *inter*Net Services

Es steht ein MIB-II-Subagent gemäß RFC 1213 zum Netzmanagement zur Verfügung. Zusätzlich wird auch ein Subagent angeboten, der Informationen zu BCAM-spezifischen Einstellungen und Werten liefert.

Folgende Produkte werden als Ergänzung angeboten:

Proxy-Agent

Müssen in einem heterogenen Netz bestimmte Teilnetze weiterhin mit proprietären Netzmanagement-Produkten verwaltet werden, dann bietet SNMP die Möglichkeit des Managements über einen Proxy-Agenten. Der Proxy-Agent bietet im Netzmanagement-Bereich eine Gateway-Funktionalität, die einerseits den Anschluss des gesamten Teilnetzes an das SNMP-Management ermöglicht, aber andererseits die Existenz des proprietären Netzmanagements innerhalb dieses Teilnetzes gewährleistet. Die SNMP-Protokollelemente werden vom Proxy-Agenten in die entsprechenden Elemente des proprietären Netzmanagement-Systems umgesetzt und umgekehrt. Für den Anschluss der TRANSDATA-Welt mit den PDN- und INCA-Systemen an das SNMP-Manangement steht der SNMP-Proxy-Agent BS2000/PDN zur Verfügung.

HIPLEX OP

HIPLEX Operation nutzt eine Schnittstelle zu den SINIX2000-basierten Service-Konsolprozessoren der BS2000/OSD-Server und bietet eine breit gefächerte Palette von Funktionen für die Administration, Bedienung und Überwachung. Das Funktionsspektrum von HIPLEX OP liegt zwischen POWER ON und POWER OFF. HIPLEX OP liefert der Management-Station Serviceprozessor-Meldungen sowie Meldungen der BS2000/OSD-Systemkonsole und von VM2000. Außerdem können die Ereignisse des SINIX2000-Ereignis-Bildschirms an die Management-Station geschickt werden. Die Filterung der Meldungen wird durch zahlreiche Standardfilter unterstützt.

HNC-SNMP

Das SNMP-Management für die Kanaladapter HNC 91849, HNC-II 91850 und HNC-III 91851 erlaubt eine umfassende Überwachung der Komponenten im HNC. Den verschiedenen HNC-Komponenten sind eigene MIBs zugeordnet. Ein ausgeprägtes Alarm-Management - dargestellt durch Trap-MIBs - unterstützt das Management der HNC-Komponenten.

2.2.2 Aufbau des SNMP-Agenten im BS2000/OSD

Der Anschluss des BS2000/OSD an SNMP erfolgt über einen mit TCP/IP-Protokollen betriebenen LAN-Anschluss. Im BS2000/OSD wird eine Agent-Applikation installiert, die die SNMP-Protokollelemente bedienen kann. Die Funktionalität des SNMP-Agenten ist aufgeteilt in einen Master- und mehrere Subagenten. Die Vorteile dieser Lösung liegen u.a. im Bereich der Ausfallsicherheit und Benutzerfreundlichkeit hinsichtlich Wartungs- und Änderungsaufwand.

Die Basis für diese Lösung stellt das Produkt EMANATE der Firma SNMP Research dar. EMANATE wurde ins BS2000/OSD portiert und steht außerdem auf Reliant UNIX und auf UNIX-Derivaten diverser namhafter Hersteller sowie auf DOS und DOS/Windows zur Verfügung.

2.2.2.1 Masteragent

Die heutigen Anforderungen an den SNMP-Agenten in einem Endsystem gehen über das normale Netzmanagement hinaus, sie reichen über System- und Anwendungsmanagement bis zum Management von Middleware (Transaktionssysteme und Datenbanken). Gerade bei größeren Endsystemen kommt auf Grund der vielfältigen Anforderungen der Wunsch auf, mehrere aufgabenspezifische Agenten einsetzen zu können, was durch die Strukturierung in Master- und Subagenten unterstützt wird.

Der Masteragent ist den Subagenten übergeordnet. Er beherrscht die grundlegenden Funktionen wie Abwicklung des SNMP-Protokolls, Sicherheitsfunktionen und das Management der Subagenten und ist auch ohne Subagenten ablauffähig. Daher ist der Masteragent auch für das Ausgeben und Setzen der Werte der System- und der SNMP-Gruppe der MIB-II sowie weiterer standardisierter MIBs (RFC 2272 - 2275) zuständig.

Neben der Verarbeitung von SNMP-Requests ermöglicht der Masteragent den Zugriff auf Management-Informationen via HTTP über das World Wide Web (Web-based Management, siehe Seite 407 ff). Dabei kann auch eine Web-Seite aufgerufen werden, die eingehende Traps tabellarisch anzeigt (siehe Seite 424).

Die Möglichkeit, Subagenten einzeln starten und beenden zu können, erleichtert Änderung und Einsatz einzelner Subagenten, ohne das gesamte Management-System beenden zu müssen, und erlaubt ein unterbrechungsfreies Management des restlichen Systems bei Ausfall einer Komponente sowie die parallele Bearbeitung von Aufträgen verschiedener Subagenten.

Die Management-Station kommuniziert nur mit dem Masteragenten. Die Kommunikation zwischen Master- und Subagent erfolgt über eine asynchrone Nachrichtenschnittstelle. Die asynchrone Nachrichtenschnittstelle garantiert ein performantes Verhalten des Masteragenten bei der Auftragsbearbeitung, da er bei der Bearbeitung längerer Aufträge nicht blockiert wird, sondern durch Nutzung des Multithreading-Verfahrens parallel weitere SNMP-Requests bearbeiten kann.

Der Masteragent ist remote-fähig für die Nutzung der SINIX2000-Subagenten, d.h. Masteragent und Subagenten müssen nicht im selben Betriebssystem ablaufen.

2.2.2.2 Subagenten

Die Subagenten sind nur bei gestartetem Masteragenten funktionsfähig. In der Initialisierungsphase meldet sich der Subagent beim Masteragenten an und übergibt dem Masteragenten seine MIB.

Subagenten arbeiten ereignisorientiert. Nach der Initialisierung läuft der Subagent in einer Warteschleife. Er verlässt die Schleife bei Eintreffen eines Ereignisses, das er bearbeiten muss. Als Ereignis werden u.a. Anforderungen des Masteragenten, Timer-Abläufe oder das Eintreffen eines vereinbarten Signals verstanden. Hat der Subagent alle vorliegenden Ereignisse abgearbeitet, kehrt er in seine Warteschleife zurück.

Eine Sonderstellung unter den Subagenten nimmt der Supervisor Subagent ein, der zwar wie ein eigenständiger Subagent agiert, aber nur zusammen mit dem Masteragenten gestartet werden kann und in derselben Task wie dieser läuft.

2.2.3 Bedienoberflächen für das SNMP-Management des BS2000/OSD

Über das Standard-Protokoll SNMP können BS2000/OSD-Systeme grundsätzlich an jede Management-Plattform angeschlossen werden, die SNMP beherrscht. Dies ist für alle markt-relevanten Management-Plattformen der Fall. Die Management-Plattformen der verschiedenen Hersteller bringen dabei ein unterschiedliches Leistungsspektrum ein. Die von Fujitsu Siemens Computers empfohlenen, strategischen Management-Plattformen CA Unicenter TNG, TransView und HP OpenView sind universell ausgerichtet und verfügen über ein ausgeprägtes Alarm-Management mit vielfältigen Möglichkeiten, Reaktionen an Ereignisse zu koppeln.

Integrationspakete und Management-Anwendungen

Für die genannten Management-Plattformen bietet Fujitsu Siemens Computers Integrationspakete (SMBS2 und SMAWsmbs2) an, die die automatische Integration des BS2000/OSD in diese Management-Plattformen ermöglichen. Diese Integrationspakete enthalten u.a. Ergänzungen zur Oberfläche.

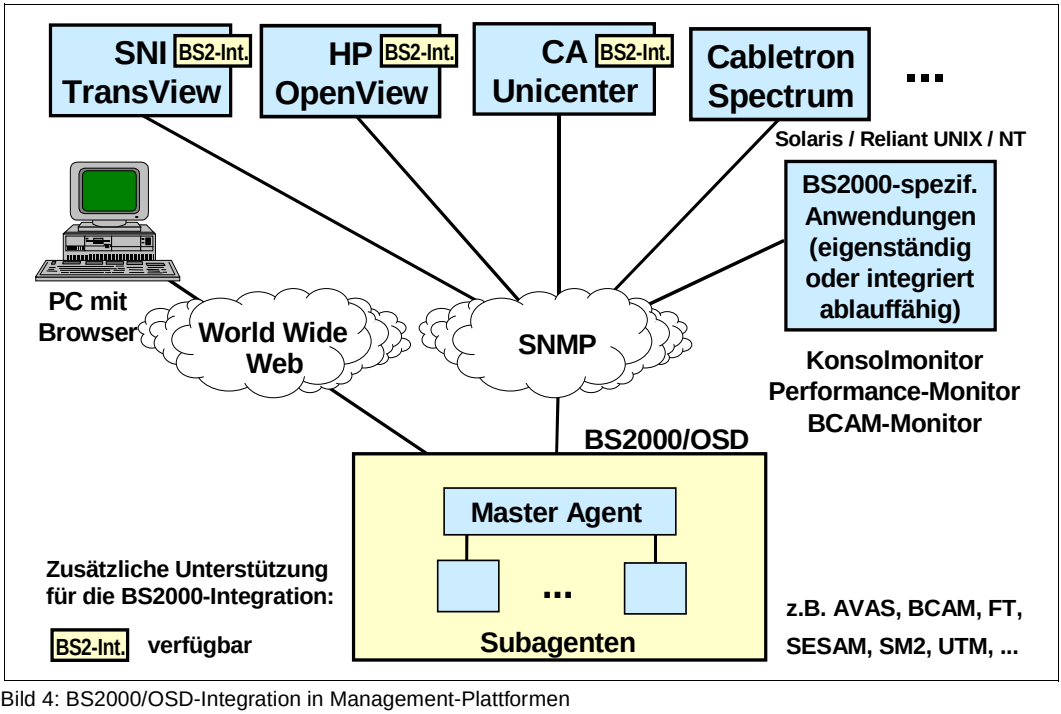


Bild 4: BS2000/OSD-Integration in Management-Plattformen

Ein Integrationspaket ist in den folgenden Produkten verfügbar:

BS2-SNMP-SO (für Solaris): SMAWsmbs2

BS2-SNMP-SX (für Reliant Unix): SMBS2

BS2-SNMP-NT (für Windows NT): SMBS2

Neben den Integrationspaketen enthalten die Produkte BS2-SNMP-SO, BS2-SNMP-SX und BS2-SNMP-NT für spezielle Subagenten eigene, auf die speziellen Eigenschaften und Aufgaben des jeweiligen Subagenten zugeschnittene Management-Anwendungen. Diese Management-Anwendungen können auf der Management-Plattform installiert werden. Sie ergänzen und verbessern die Darstellung und Handhabung der bestehenden Management-Plattform. Die Management-Anwendungen können auch eigenständig auf einem Solaris-, Reliant UNIX- oder Windows NT-System eingesetzt werden.

Übersicht über die Integrationspakete

Für die strategisch unterstützten Management-Plattformen werden folgende Integrationspakete angeboten:

Integrations-pakete	**zugehörige Agenten**	**Management-Station**	**Betriebssystem**
SMAWsmbs2 aus BS2-SNMP-SO	alle Subagenten	CA Unicenter TNG-Base	Solaris
SMBS2 aus BS2-SNMP-SX	alle Subagenten	TransView SNMP / TransView Control Center / OpenView NetWork Node Manager	Reliant UNIX
SMBS2 aus BS2-SNMP-NT	alle Subagenten	CA Unicenter TNG Framework / CA Unicenter TNG-Base	Windows NT

Übersicht über die Management-Anwendungen

Folgende speziellen Management-Anwendungen werden angeboten:

Management-Anwendungen	Paket-Namen	zugehörige Agenten	Management-Station	Betriebssystem
BCAM-Monitor BMBS2	BMBS2 bei Solaris: SMAWbmbs2	BCAM-Subagent, MIB-II-Subagent	standalone / integriert	Solaris / Reliant UNIX / Windows NT
Console Monitor CMBS2	CMBS2 bei Solaris: SMAWcmbs2	Console Monitor Subagent (SBA-BS2)	standalone / integriert	Solaris / Reliant UNIX / Windows NT
Performance Monitor PMBS2	PMBS2 bei Soaris: SMAWpmbs2	Performance-Monitor Subagent (SSA-SM2-BS2)	standalone / integriert	Solaris / Reliant UNIX / Windows NT

Web-Zugriff auf Management-Informationen

Neben dem Zugriff über traditionelle SNMP-Management-Anwendungen ermöglicht der Masteragent den Zugriff auf Management-Informationen via Web-Browser über das World Wide Web (WWW). Der Web-Zugriff ist beschrieben im Kapitel „Web-Zugriff auf Management-Informationen“ (siehe Seite 407).

3 Installation und Konfiguration

Das BS2000/OSD-SNMP-Management besteht aus folgenden Produkten für den Einsatz auf BS2000/OSD:

– SBA-BS2 V5.0

– SSC-BS2 V5.0

– SSA-SM2-BS2 V5.0

– SSA-OUTM-BS2 V5.0

Außerdem umfasst das BS2000/OSD-SNMP-Management die Pakete für die Management-Seite, die auf einer eigenen CD-ROM zusammen mit dem Produkt SBA-BS2 ausgeliefert werden bzw. im Internet zum Download verfügbar sind.

Jeweils für Reliant UNIX und Windows NT enthält die CD-ROM:

– ein Integrationspaket SMBS2 V5.0 mit Ergänzungen für die Management-Plattformen CA Unicenter TNG (auf Windows NT) bzw. TransView SNMP, TransView Control Center oder HP OpenView NNM (auf Reliant UNIX)

– die Management-Anwendungen BMBS2 V5.0 (BCAM-Monitor), CMBS2 V5.0 (Console Monitor-Anwendung) und PMBS2 V5.0 (Performance-Monitor-Anwendung bei Nutzung von SSA-SM2-BS2) in den gleichnamigen Integrationspaketen

– den zugehörigen Interpreter tclset V5.0

– den Trap-Server trpsrv (nur für Reliant UNIX)

– alle BS2000/OSD-spezifischen MIBs im ASN.1-Format

Für Solaris enthält die CD-ROM:

– ein Integrationspaket SMAWsmbs2 V5.0 mit Ergänzungen für die Management-Plattform CA Unicenter TNG auf Solaris

– die Management-Anwendungen BMBS2 (BCAM-Monitor), CMBS2 (Console Monitor-Anwendung) und PMBS2 (Performance-Monitor-Anwendung) in den Integrationspaketen SMAWbmbs2 V5.0, SMAWcmbs2 V5.0 bzw. SMAWpmbs2 V5.0

– den zugehörigen Interpreter SMAWtcl V5.0

– den Trap-Server SMAWtrpsv

– alle BS2000/OSD-spezifischen MIBs im ASN.1-Format

Die SNMP-Agenten sind hardware-unabhängig. Sie laufen auf allen Zentraleinheiten (inklusive der RISC-basierten Modelle), die von BS2000/OSD ab V2.0 bzw. OSD-SVP V2.0 unterstützt werden.

3.1 Software-Voraussetzungen

Software-Voraussetzungen für SBA-BS2

Der Einsatz des SNMP-Basic-Agent-BS2000 V5.0 setzt folgende Software voraus:

- BS2000/OSD-BC ≥ V2.0 bzw OSD-SVP V2.0
- POSIX-BC ≥ V1.0*
- SOCKETS(POSIX) ≥ 1.0*
- IMON ≥ V 2.0*
- SDF-P-BASYS V2.0B*
- JV ≥ V11.2 (optional)

Mit * gekennzeichnete Komponenten sind Bestandteil von BS2000/OSD-BC.

Software-Voraussetzungen für SSC-BS2

Der Einsatz der SNMP-Standard-Collection V5.0 setzt folgende Software voraus:

- BS2000/OSD-BC ≥ V2.0 bzw. OSD-SVP V2.0
- SBA-BS2 V5.0
- AVAS ≥ V3.0
- FT-BS2000 V5.2 bzw. *open*FT (BS2000) ≥ V6.0
- SPOOL ≥ V3.0*
- RSO ≥ V2.4
- HSMS ≥ V3.1
- OMNIS ≥ V8.1
- SDF-P-BASYS ≥ V2.0B*/**
- SESAM/SQL-Server ≥ V2.1B50***
- SM2 ≥ V11.2
- JV ≥ V11.2

Mit * gekennzeichnete Komponenten sind Bestandteil von BS2000/OSD-BC.
Mit ** gekennzeichnete Komponenten sind für den PrintService-Subagenten erforderlich.
Kennzeichnung mit *** bedeutet: Falls an einem Rechner mehrere DBHs überwacht werden sollen, ist außerdem der Einsatz von SESDCN erforderlich.

Software-Voraussetzungen für SSA-SM2-BS2

SSA-SM2-BS2 setzt SBA-BS2 V5.0 und SM2 ab V11.2 in BS2000/OSD-BC ≥ V2.0 bzw. OSD-SVP V2.0 voraus.

Software-Voraussetzungen für SSA-OUTM-BS2

SSA-OUTM-BS2 setzt *open*UTM ≥ V3.3 und die entsprechende Version von UTM-D-SP voraus. Zusätzlich werden BS2000/OSD-BC ≥ V2.0 und SBA-BS2 V5.0 vorausgesetzt.

Software-Voraussetzungen für die Subagenten für *open*Net Server und *inter*Net Services

Zum Einsatz des MIB-II-Subagenten ist SBA-BS2 V5.0 und DCAM ab V13.0 bzw. *open*Net Server V1.0 Voraussetzung. Ab DCAM V14.0 ist der BCAM-Subagent (Private MIB) ablauffähig.

Software-Voraussetzungen für die Integrationspakete SMBS2 und SMAWsmbs2

Die Nutzung von SMBS2 auf Windows NT bzw. von SMAWsmbs2 auf Solaris setzt die Installation und die Verfügbarkeit von Unicenter TNG in der Version 2.2 voraus. Wenn lediglich CA Unicenter Framework installiert ist, kann SMBS2 auf Windows NT eingeschränkt genutzt werden.

Bei Einsatz von SMBS2 auf einer TransView-Management-Plattform wird TransView SNMP ≥ V3.1 und TransView Control Center ≥ V3.1 vorausgesetzt.

Bei Einsatz von SMBS2 auf einer OpenView basierten Management-Station wird OpenView in der Version 3.3 oder 4.1 vorausgesetzt.

BMBS2, CMBS2 und PMBS2 setzen die Installation des Interpreters Tcl-Set ≥ V5.0 voraus (siehe Seite 126).

3.2 Installation in BS2000/OSD

Die Produkte SBA-BS2 und SSC-BS2 werden ebenso wie die additiven Subagenten SSA-SM2, SSA-OUTM-BS2 und die Subagenten für *open*Net Server und *inter*Net Services auf einem BS2000/OSD-Rechner installiert.

Die Installation des Integrationspakets SMBS2, der Managementanwendungen aus den Paketen BMBS2, CMBS2 und PMBS2 sowie des Interpreters tclset erfolgt auf der Management-Station in Windows NT- bzw. Reliant UNIX-Umgebung (siehe Abschnitt „Integration in die Management-Plattformen“ auf Seite 94).

Die Installation des Integrationspakets SMAWsmbs2, der Managementanwendungen aus den Paketen SMAWbmbs2, SMAWcmbs2 und SMAWpmbs2 sowie des Interpreters SMAWtcl erfolgt auf der Management-Station in Solaris-Umgebung (siehe Abschnitt „Integration in die Management-Plattformen“ auf Seite 94).

Die Installation von SBA-BS2, SSC-BS2, SSA-SM2-BS2 und SSA-OUTM-BS2 erfolgt mit dem Software-Liefer- und Informations-System SOLIS2. Die SOLIS2-Installation enthält, soweit erforderlich, BS2000/OSD-spezifische Arbeiten wie Subsystem-Katalog-Einträge etc.

Es ist darauf zu achten, dass im Subsystemkatalog ein Eintrag für das Subsystem SNMP erstellt wird.

Beachten Sie bitte, dass die interne Kommunikation zwischen Master- und Subagenten über die Portnummer 3161 abgewickelt wird. Insbesondere sollte die dynamische Portnummernvergabe von BCAM mit einem größeren Wert beginnen, der BCAM-Standardwert beträgt 4096.

Das Löschen der SINLIB nach der Installation führt zu Fehlern, da die Agenten die SINLIB auch für den Betrieb benötigen.

Die folgenden Abschnitte beschreiben die jeweiligen Installationsschritte für die Agentenseite.

3.2.1 Installation von SBA-BS2 und SSC-BS2

Das Subsystem POSIX muss gestartet sein. Die ablauffähigen Agenten von SBA-BS2 befinden sich in der SINLIB.SBA-BS2.050. Diese enthält auch alle Elemente, die ins UFS installiert werden müssen. Die Installation erfolgt unter der Kennung SYSROOT bzw. TSOS (UID=0, GID=0) mit dem POSIX-Installationstool:

```
/CALL-PROCEDURE *LIB(LIB=$TSOS.SINPRC.POSIX-BC.<version>,ELEMENT=POSINST)
```

Funktion: POSIX-Programmpakete installieren
Produktname: SBA-BS2
Produktversion: 050

Die SINLIB.SSC-BS2.050 enthält die ablauffähigen Agenten und alle Elemente von SSC-BS2, die in das UFS installiert werden müssen. Die Installation erfolgt unter der Kennung SYSROOT bzw. TSOS (UID=0, GID=0) mit dem POSIX-Installationstool:

```
/CALL-PROCEDURE *LIB(LIB=$TSOS.SINPRC.POSIX-BC.<version>,ELEMENT=POSINST)
```

Funktion: POSIX-Programmpakete installieren
Produktname: SSC-BS2
Produktversion: 050

3.2.2 Installation von SSA-SM2-BS2

Die Installation erfolgt unter der Kennung SYSROOT bzw. TSOS (UID=0, GID=0) mit dem POSIX-Installationstool:

```
/CALL-PROCEDURE *LIB(LIB=$TSOS.SINPRC.POSIX-BC.<version>,ELEMENT=POSINST)
```

Funktion: POSIX-Programmpakete installieren
Produktname: SSA-SM2-BS2
Produktversion: 050

Erfolgt die Installation von SSA-SM2-BS2 nicht mit IMON, muss nachträglich die SYSSII-Datei (IMON V2.0) aufgenommen werden.

3.2.3 Installation von SSA-OUTM-BS2

Die Installation erfolgt unter der Kennung SYSROOT bzw. TSOS (UID=0, GID=0) mit dem POSIX-Installationstool:

```
/CALL-PROCEDURE *LIB(LIB=$TSOS.SINPRC.POSIX-BC.<version>,ELEMENT=POSINST)
```

Funktion: POSIX-Programmpakete installieren
Produktname: SSA-OUTM-BS2
Produktversion: 050

3.2.4 Versionswechsel

Die folgenden Hinweise zum Versionswechsel ergänzen die in den vorangegangenen Installationsabschnitten enthaltene Information.

Umstieg von einer älteren SBA-BS2-Version auf V5.0

Auch beim Versionswechsel erfolgt die Installation über IMON oder durch Bekanntgabe der SYSSII-Datei (IMON V2.0). Bibliotheken können problemlos in die gewünschte Kennung eingespielt werden, da wegen unterschiedlicher Versionsbezeichnung Konflikte mit der Vorgängerversion ausgeschlossen sind.

Die Syntaxdatei der Vorversion muss durch die Syntaxdatei der Version 5.0 ersetzt werden. Hierzu sollten die Agenten beendet werden. Denn die Agenten der Vorgängerversion können nicht mehr mittels STOP-Kommando beendet werden, da die Version des Agenten mit der des zugehörigen Kommandoprogramms übereinstimmen muss.

Die Datei *snmpd.cnf* in */etc/snmp/agt* muss um die kundenspezifischen Einträge erweitert werden. Dazu sollte der Masteragent gestoppt werden, da dieser u.U. die Konfigurationsdatei überschreibt.

3.2.5 Deinstallation

Die Deinstallation erfolgt ebenfalls unter der Kennung SYSROOT bzw. TSOS (UID=0, GID=0) mit dem POSIX-Installationstool:

```
/CALL-PROCEDURE *LIB(LIB=$TSOS.SINPRC.POSIX-BC.<version>,ELEMENT=POSINST)
```

Funktion: POSIX-Programmpakete deinstallieren
Produktname: siehe entsprechender Name im Abschnitt "Installation"
Produktversion: <prod-version>

<prod-version> bezeichnet die Versionsnummer des zu deinstallierenden Programmpakets.

3.3 Konfiguration der Agenten in BS2000/OSD

Konfigurationsarbeiten sind sowohl auf der Management-Plattform als auch im BS2000/OSD nötig:

- Die im BS2000/OSD auszuführenden Tätigkeiten sind in den nachfolgenden Abschnitten beschrieben.
- Die auf der Management-Plattform erforderlichen Arbeiten sind ab Seite 94 beschrieben.
  - Hinweise zu Konfigurationsarbeiten auf einer Unicenter TNG-basierten Management-Plattform finden Sie auf Seite 95 ff.
  - Hinweise zu Konfigurationsarbeiten auf einer TransView SNMP-basierten Management-Plattform finden Sie auf Seite 108 ff.
  - Hinweise zu Konfigurationsarbeiten auf einer TransView Control Center basierten Management-Plattform finden Sie auf Seite 115 ff.
  - Hinweise zu Konfigurationsarbeiten auf einer OpenView basierten Management-Plattform finden Sie auf Seite 118 ff.

3.3.1 Security-Konfiguration

Die zentrale Aufgabe jedes Security-Systems besteht in der Prüfung, ob ein Benutzer die geforderte Operation ausführen darf. So schützt das Security-System der SNMP-Agenten diese Agenten vor nicht autorisierten Zugriffen auf MIB-Variable. Nur ein Benutzer, der seine Requests mit einem erlaubten, d.h. am Agenten konfigurierten, Community-String sendet, darf die gewünschte Operation ausführen.

3.3.1.1 Security-Mechanismus

Jede von einem SNMP-Manager an den Agenten gesendete Nachricht wird vom Security-System nach folgenden Kriterien überprüft:

– Wer sendet die Nachricht? (*wer?*, Authentifizierung)

– Welche Operation wird gefordert? (*was?*, Autorisierung)

– Welche Objekte in der MIB sind von der Operation betroffen? (*wo?*, Zugriffskontrolle)

– Wie wurde der Request gesendet? (*wie?*, Security Level)

Das Security-System vergleicht die Nachricht mit der Security-Konfiguration am Agenten. Je nach Ergebnis des Vergleichs erlaubt das Security-System die Ausführung der geforderten Operation oder weist sie zurück.

Bild 5 skizziert den Security-Mechanismus.

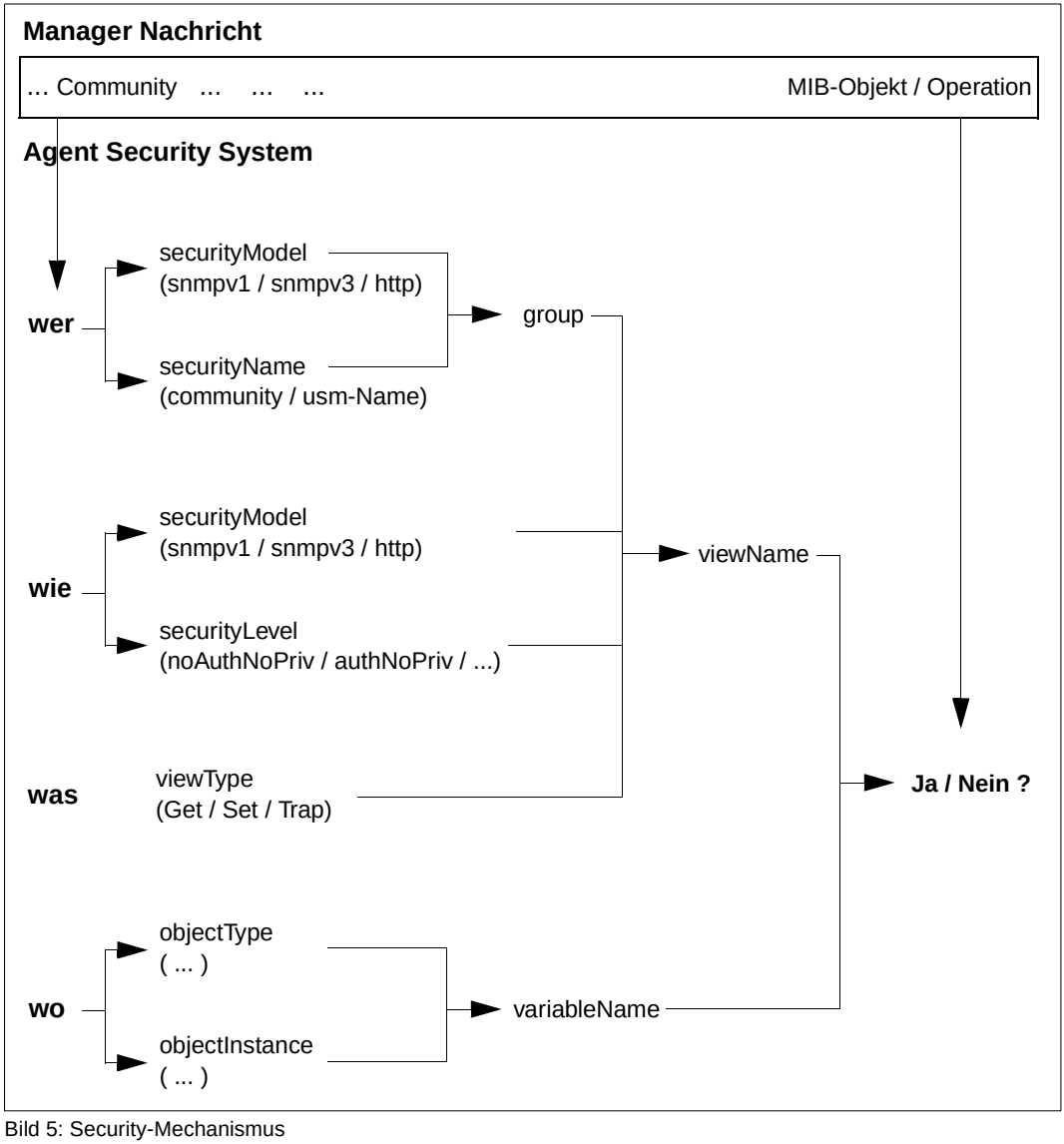


Bild 5: Security-Mechanismus

3.3.1.2 Erweiterte Security-Mechanismen in SNMPv3

In der vorliegenden Version des SNMP-Managements für BS2000/OSD werden Elemente des umfangreichen Security-Konzepts von SNMPv3 genutzt. Dabei ist es unerheblich, ob der SNMP-Manager die Nachricht als SNMPv1- oder SNMPv3-Requests sendet. Gegenüber den ursprünglichen SNMPv1-Security-Mechanismen bietet das jetzt verwendete Sicherheitskonzept folgende Erweiterungen:

– Selektive Vergabe von Zugriffsrechten auf MIB-Variablen

– Festlegung von Zugriffsrechten für eine Gruppe von Management-Stationen

– Detaillierter Trap-Empfang

– Authentifizierung von SNMP-Requests

Selektive Vergabe von Zugriffsrechten auf MIB-Variablen

In früheren Versionen des SNMP-Managements für BS2000/OSD, die auf reinen SNMPv1-Sicherheitsmechanismen basierten, konnten nur gleiche Zugriffsrechte für alle MIB-Variablen vergeben werden. So hatte ein mit Schreibberechtigung definierter Community-String schreibenden Zugriff auf *alle* MIB-Objekte, die in ihrer MIB als änderbar definiert waren. Entsprechendes galt für lesende Zugriffe: Entweder konnten *alle* MIB-Objekte gelesen werden oder keines.

In der aktuellen Version des SNMP-Managements für BS2000/OSD kann für einen Community-String die Lese- bzw. Schreibberechtigung auf einen bestimmten MIB-Zweig eingeschränkt werden. Z.B. kann man einen Community-String definieren, der zwar leseberechtigt für alle MIB-II-Objekte ist, schreibend aber nur auf die in der MIB-II als änderbar definierten Objekte der Systemgruppe mit Ausnahme von *sysName* zugreifen darf.

Die Zugriffsdefinition kann sogar auf der Ebene von Instanzen festgelegt werden. So ist es beispielsweise möglich, eine Zugriffsberechtigung auf die zweite Instanz der Interfaces-Tabelle zu beschränken.

Festlegung von Zugriffsrechten für eine Gruppe von Management-Stationen

Bereits in früheren Versionen ließ sich die Erlaubnis, Requests zu senden, auf einzelne Management-Stationen einschränken. Hierfür musste man für jeden zugelassenen Rechner den Community-String zusammen mit der IP-Adresse des Rechners in der Konfigurationsdatei eintragen. Um jedoch die Zugriffserlaubnis auf eine Menge von Management-Stationen auszuweiten, musste „0.0.0.0“ angegeben werden. Dann war aber der Zugriff von *allen* Rechnern aus möglich. Im Unterschied dazu kann in der aktuellen Version eine Familie von IP-Adressen über eine Bitmaske spezifiziert werden, von denen aus Requests mit dem definierten Community-String erlaubt sind.

Beispiel:

Es kann ein Community-String definiert werden, der den Zugriff auf die Agenten der Systeme mit den IP-Adressen 139.25.104 - 139.25.255 erlaubt.

Detaillierter Trap-Empfang

In früheren Security-Versionen wurden Traps ohne Unterschied *stets* an *alle* in der Security-Konfiguration definierten Trap-Ziele gesendet. Demgegenüber kann in der aktuellen Version je nach Enterprise und Trapnummer die IP-Adresse des Systems festgelegt werden, an das der Trap gesendet werden soll.

Beispiel

Es kann festgelegt werden, dass alle Traps mit Enterprises sni.2.34 an das System 139.22.22.22 gesendet werden.

Authentifizierung von Requests

Management-Stationen, die ihre Requests über das SNMPv3-Protokoll senden, können ihre Nachricht authentifizieren. Auf diese Weise kann der Agent sicherstellen, dass die Nachricht zwischenzeitlich weder verändert noch zurückgehalten wurde.

3.3.1.3 Konfigurationsschritte

Die Security-Konfiguration für einen Agenten umfasst folgende Schritte:

1. a) Konfiguration des Benutzers

   Die Konfiguration des Benutzers ist abhängig vom Security-Modell und erfolgt

   – für SNMPv1 durch einen *communityEntry* (ist derzeit der Regelfall),

   – für SNMPv3 durch einen *usmUserEntry*,

   – für HTTP durch einen *httpUserNameEntry*.

   b) Konfiguration der Zugriffskontrolle

   1. Mit einem *vacmViewTreeFamiliyEntry* wird ein MIB-Zweig definiert.
   2. Mit einem *vacmAccessEntry* wird eine Security-Gruppe definiert, und dieser Gruppe werden unter 1) definierte MIB-Zweige für Lese- und Schreibberechtigung sowie den Trap zugeordnet.
   3. Mit einem *vacmSecurityToGroupEntry* wird der unter a) konfigurierte Benutzer einer Security-Gruppe zugeordnet.

   c) Mit dem *snmpTargetAddressEntry* wird die Adressenkontrolle durchgeführt.

2. a) Definition der Trapziele
    1. Mit einem *snmpNotifyEntry* wird ein Notify-Eintrag definiert.
    2. Mit einem *snmpTargetAddrEntry* wird dem Notify-Eintrag eine Zieladresse und ein Target-Parameter-Eintrag zugeordnet.
    3. Mit einem *snmpTargetParamsEntry* wird ein Target-Parameter mit Community-String definiert.

    b) Konfiguration der Zugriffskontrolle
    1. Mit einem *vacmViewTreeFamiliyEntry* wird ein MIB-Zweig definiert.
    2. Mit einem *vacmAccessEntry* wird eine Security-Gruppe definiert und dieser Gruppe werden unter 1) definierte MIB-Zweige für Lese- und Schreibberechtigung sowie den Trap zugeordnet.
    3. Mit einem *vacmSecurityToGroupEntry* wird der Community-String (Punkt a3), mit dem der Trap gesendet werden soll, einer Security-Gruppe zugeordnet.

    c) Mit dem *snmpNotifySourceEntry* wird die Absenderadresse eines Traps spezifiziert.

3.3.1.4 Konfigurationsdatei *snmpd.cnf*

Alle für die Security-Konfiguration relevanten Informationen werden in Form von Security-Entries in die Konfigurationsdatei */etc/snmp/agt/snmpd.cnf* eingetragen.

Jeder Security-Entry in *snmpd.cnf* hat das folgende Format:

TAG value

Bedeutung:

– *TAG* spezifiziert den Typ des Security-Entries
– *value* spezifiziert einen für die Konfiguration gültigen Wert.

Konventionen zur Syntaxdarstellung

Für die Darstellungsmittel, die in den nachfolgenden Abschnitten zur Beschreibung der Security-Entries verwendet werden, gelten die folgenden Konventionen:

– **Fett** gedruckte Items dürfen nicht verändert werden.

– *Kursiv* gedruckte Items müssen in *snmpd.cnf* durch aktuelle Werte ersetzt werden.

– Die Zeichen [,], (,), *, | sind Metazeichen und dürfen in *snmpd.cnf* nicht angegeben werden.

– In eckige Klammern „[...]“ eingeschlossene Items müssen nicht spezifiziert werden. Stattdessen kann für diese Items in *snmpd.cnf* „-“ angegeben werden; es gilt dann der Defaultwert.

– In Runde Klammern „(...)“ eigeschlossene und durch ein „|“ getrennte Items stellen Alternativen dar; genau ein Item muss angegeben werden.

– Mit einem Stern (*) markierte Items sind Schlüsselworte, die den betreffenden Entry eindeutig bestimmen.

– Entries in *snmpd.cnf* können sich über mehrere Zeilen erstrecken, wenn am Zeilenende als Fortsetzungszeichen der „Backslash“ (\) angegeben wird.

– Leerzeichen, Zwischenräume und Carriage Returns werden ignoriert.

– Character-Strings, die Leerzeichen enthalten, müssen in doppelte Hochkommata ("...") eingeschlossen sein.

3.3.1.5 Definition des Zugriffs auf den Agenten über SNMPv1-Requests

a) Definition eines Community-String - *communityEntry*

Der *communityEntry* definiert einen Community-String und ordnet ihm eine Security-Gruppe und ein Transportlabel zu.

Tag:	**communityEntry**
Value:	**localSnmpID** *MyCommunity MyGroup* **localSnmpID -** [*MyTransTag*] **nonVolatile**

*MyCommunity**
Community-String (String 1..255), mit dem ein SNMPv1-Request erfolgen darf.

MyGroup
Zugeordnete Security-Gruppe (siehe Punkt b2). Die Security-Gruppe bestimmt den Berechtigungsumfang.

MyTransTag
Zugeordnetes Transportlabel. Das Transportlabel verweist in eine Liste von Target-Tags im *snmpTargetAddrEntry* (siehe Punkt c) und bestimmt dadurch, von welchen Systemen Requests akzeptiert werden.
Defaultwert: keine Einschränkung der Berechtigung

b) Definition der Zugriffskontrolle

b1) Definition des MIB-Zweigs - *vacmViewTreeFamilyEntry*

Die Definition des MIB-Zweigs besteht aus einem oder mehreren *vacmViewTreeFamilyEntry*-Einträgen. Jeder *vacmViewTreeFamilyEntry* ordnet dem MIB-Zweig eine OID zu oder schließt eine OID aus.

Tag:	**vacmViewTreeFamilyEntry**
Value:	*MyMIB MyOID* - (**included** | **excluded**) **nonVolatile**

*MyMIB**
Name des MIB-Zweig-Eintrags (String 1..32)

*MyOID**
OID oder symbolischer Name des MIB-Zweigs, der ein- bzw. ausgeschlossen werden soll.

included | **excluded**
der MIB-Zweig soll ein- bzw. ausgeschlossen werden. Zugreifbar sind nur die Objekte, die als Ergebnis aller *included*- bzw. *excluded*-Operationen im MIB-Zweig verbleiben.

b2) Definition der Security-Gruppe - *vacmAccessEntry*

Der *vacmAccessEntry* definiert eine Security-Gruppe und ordnet ihr MIB-Zweige für Lese- und Schreibberechtigungen zu.

Tag:	**vacmAccessEntry**
Value:	*MyGroup* **- snmpv1 noAuthNoPriv exact** [*MYRead*) [*MyWrite*] **- nonVolatile**

*MyGroup**
Name der Security-Gruppe (String 1..32). Die Security-Gruppe bestimmt den Berechtigungsumfang.

MyRead
zugeordneter MIB-Zweig für den Lesezugriff (siehe Punkt b1)

MyWrite
zugeordneter MIB-Zweig für den Schreibzugriff (siehe Punkt b1)

b3) Definition des Security-Eintrags - *vacmSecurityToGroupEntry*

Der *vacmAccessEntry* definiert eine Security-Gruppe und ordnet ihr MIB-Zweige für Lese- und Schreibberechtigungen zu

Tag:	**vacmSecurityToGroupEntry**
Value:	**snmpv1** *MyCommunity MyGroup* **nonVolatile**

*MyCommunity**
Community-String (String 1..255), mit dem ein SNMPv1-Request erfolgen darf.

MyGroup
Zugeordnete Security-Gruppe (siehe Punkt b2). Die Security-Gruppe bestimmt den Berechtigungsumfang.

c) Definition der Adressenkontrolle - *snmpTargetAddrEntry*

Der *snmpTargetAddrEntry* spezifiziert das System, von dem aus der Zugriff erfolgen darf.

Tag:	**snmpTargetAddrEntry**
Value:	*MyTarget* **snmpUDPDomain** *MyTaddr* **300 0** *MyTagList* **- nonVolatile** *MyAddrMask*

*MyTarget**
Name des Target-Eintrags (String 1..32)

MyTAddr
Internet-Adresse des Targets, d.h. des Systems, von dem aus der Zugriff erfolgen darf, in der Form **xxx.xxx.xxx.xxx:0**

MyTagList
Liste der Tags (siehe a). Die Liste muss in Hochkommata ("...") eingeschlossen werden; die einzelnen Listenelemente sind durch *ein* Leerzeichen voneinander zu trennen.

MyAddrMask
Maske in der Form **xxx.xxx.xxx.xxx:0**, analog einer Subnetz-Maske.
Eine Absenderadresse ist gültig, falls gilt:
(Absenderadresse & MyAddrMask) == (MyTAddr & MyAddrMask)

Beispiele

Beispiel 1

Von allen Systemen aus soll der Community-String „public“ lesenden Zugriff haben.

– in SNMPv1-Security (frühere Versionen): **community** public 0.0.0.0 read 1

– in SNMPv3-Security (aktuelle Version):

communityEntry localSnmpID public READ **localSnmpID -** - **nonVolatile**
vacmSecurityToGroupEntry snmpv1 public READ **nonVolatile**
vacmAccessEntry READ **- snmpv1 noAuthNoPriv exact** All - - **nonVolatile**
vacmViewTreeFamiliyEntry All dod - **included nonVolatile**

Beispiel 2

Vom System 139.22.22.22 aus soll der Community-String „master“ schreibenden Zugriff haben.

– in SNMPv1-Security (frühere Versionen): **community** master 139.22.22.22 write 1

– in SNMPv3-Security (aktuelle Version):

communityEntry localSnmpID master WRITE **localSnmpID -** TarTag1 **nonVolatile**
vacmSecurityToGroupEntry snmpv1 master WRITE **nonVolatile**
vacmAccessEntry WRITE **- snmpv1 noAuthNoPriv exact** All All **- nonVolatile**
vacmViewTreeFamiliyEntry All dod **- included nonVolatile**
snmpTargetAddrEntry Ta1 **snmpUDPDomain** 139.22.22.22:0 300 0 TarTag1 **-**
nonVolatile 255.255.255.255:0

Beispiel 3

Von den Systemen mit den IP-Adressen 139.22.104.0 bis 139.22.111.255 aus soll der Community-String „multi“ schreibenden Zugriff haben.

– in SNMPv1-Security (frühere Versionen): nicht einstellbar

– in SNMPv3-Security (aktuelle Version):

communityEntry localSnmpID multi WRITE **localSnmpID -** TarTag2 **nonVolatile**
vacmSecurityToGroupEntry snmpv1 multi WRITE **nonVolatile**
vacmAccessEntry WRITE **- snmpv1 noAuthNoPriv exact** All All **- nonVolatile**
vacmViewTreeFamiliyEntry All dod **- included nonVolatile**
snmpTargetAddrEntry Ta2 **snmpUDPDomain** 139.22.22.22:0 300 0 TarTag2 **-**
nonVolatile 255.255.248.0:0

Beispiel 4

Von allen Systemen aus soll der Community-String „sysread“ lesenden Zugriff nur auf die Systemgruppe haben.

– in SNMPv1-Security (frühere Versionen): nicht einstellbar

– in SNMPv3-Security (aktuelle Version):

communityEntry localSnmpID sysread SysAccR **localSnmpID - - nonVolatile**
vacmSecurityToGroupEntry snmpv1 sysread SysAccR **nonVolatile**
vacmAccessEntry SysAccR **- snmpv1 noAuthNoPriv exact** SysTreeR - **-** \
nonVolatile
vacmViewTreeFamiliyEntry SysTreeR system **- included nonVolatile**

Beispiel 5

Der Community-String „syswrite“ soll schreibenden Zugriff von allen Systemen der Internet-Adressen 139.22.104.0 - 139.22.111.255 haben. Der Zugriff soll jedoch nur auf die Systemgruppe außer sysName erlaubt sein.

– in SNMPv1-Security (frühere Versionen): nicht einstellbar

– in SNMPv3-Security (aktuelle Version):

communityEntry localSnmpID syswrite SysAccW **localSnmpID** - TarTag2 ****
nonVolatile
vacmSecurityToGroupEntry snmpv1 syswrite SysAccW **nonVolatile**
vacmAccessEntry SysAccW **- snmpv1 noAuthNoPriv exact** SysTreeR SysTreeW **-**\
nonVolatile
vacmViewTreeFamiliyEntry SysTreeR system **- included nonVolatile**
vacmViewTreeFamiliyEntry SysTreeW system **- included nonVolatile**
vacmViewTreeFamiliyEntry SysTreeW sysName **- excluded nonVolatile**
snmpTargetAddrEntry Ta2 **snmpUDPDomain** 139.22.104.0:0 300 0 TarTag2 **- **
nonVolatile 255.255.248.0:0

Bild 6 auf der nächsten Seite skizziert das Vorgehen beim Erstellen der Einträge für die Security-Konfiguration.

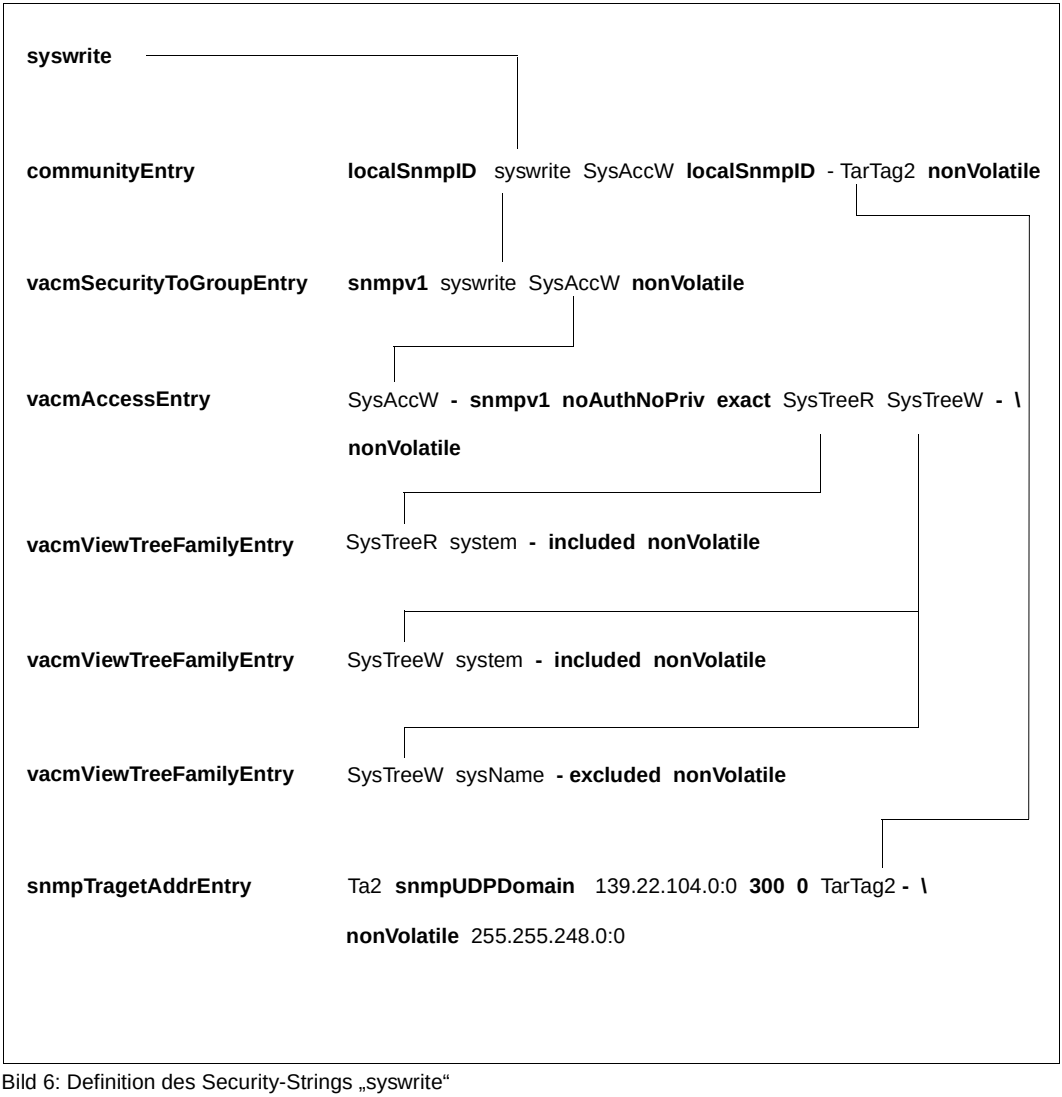


Bild 6: Definition des Security-Strings „syswrite“

3.3.1.6 Definition des Zugriffs auf den Agenten über SNMPv3-Requests

a) Definition eines SNMPv3-Benutzers - *usmUserEntry*

Der *usmUserEntry* ordnet einem SNMPv3-Benutzer eine Security-Gruppe und ein Transport-Label zu

Tag:	**usmUserEntry**
Value:	**localSnmpID** *MyUser MyAuthProt* **usmNoPrivProtocol nonVolatile** [*MyTransTag*] [*MyAuthKey*]

*MyUser**
Benutzername (String 1..32), mit dem ein SNMPv3-Request erfolgen darf.

MyMyAuthProt
Authentifizierungsprotokoll:
– usmNoAuthProtocol (keine Authentifizierung)
– usmHMACMD5AuthProtocol (Authentifizierung)

MyTransTagList
zugeordnetes Transport-Label. Das Transport-Label zeigt in eine Target-Liste (siehe Punkt e) und bestimmt dadurch, von welchen Systemen Requests akzeptiert werden. Die Angabe „-“ bedeutet: Es gibt keine Einschränkung.

MyAuthKey
Passwort für die Authentifizierung.
Die Angabe „-“ bedeutet: Es gibt kein Passwort.

b) Definition der Zugriffskontrolle

b1) Definition des MIB-Zweigs - *vacmViewTreeFamilyEntry*

Die Definition des MIB-Zweigs besteht aus einem oder mehreren *vacmViewTreeFamilyEntry*-Einträgen. Jeder *vacmViewTreeFamilyEntry* ordnet dem MIB-Zweig eine OID zu oder schließt eine OID aus.

Tag:	**vacmViewTreeFamilyEntry**
Value:	*MyMIB MyOID* **-** (**included** | **excluded**) **nonVolatile**

*MyMIB**
Name des MIB-Zweig-Eintrags (String 1..32)

*MyOID**
OID oder symbolischer Name des MIB-Zweigs, der ein- bzw. ausgeschlossen werden soll.

included | **excluded**
der MIB-Zweig soll ein- bzw. ausgeschlossen werden. Zugreifbar sind nur die Objekte, die als Ergebnis aller *included*- bzw. *excluded*-Operationen im MIB-Zweig verbleiben.

b2) Definition der Security-Gruppe - *vacmAccessEntry*

Der *vacmAccessEntry* definiert eine Security-Gruppe und ordnet ihr MIB-Zweige für Lese- und Schreibberechtigungen zu.

Tag:	**vacmAccessEntry**
Value:	*MyGroup* **- usm noAuthNoPriv exact** [*MyRead*] [*MyWrite*] **- nonVolatile**

*MyGroup**
Name der Security-Gruppe (String 1..32). Die Security-Gruppe bestimmt den Berechtigungsumfang.

MyRead
zugeordneter MIB-Zweig für den Lesezugriff (siehe Punkt b1)

MyWrite
zugeordneter MIB-Zweig für den Schreibzugriff (siehe Punkt b1)

b3) Definition des Security-Eintrags - *vacmSecurityToGroupEntry*

Der *vacmSecurityToGroupEntry* ordnet dem SNMPv3-Benutzer eine Security-Gruppe zu.

Tag:	**vacmSecurityToGroupEntry**
Value:	**usm** *MyUser MyGroup* **nonVolatile**

*MyUser**
Benutzerkennung (Character-String 1..255), unter der ein SNMPv3-Request erfolgen darf.

MyGroup
Zugeordnete Security-Gruppe (siehe Punkt b2). Die Security-Gruppe bestimmt den Berechtigungsumfang.

c) Definition der Adressenkontrolle - *snmpTargetAddrEntry*

Der *snmpTargetAddrEntry* spezifiziert das System, von dem aus der Zugriff erfolgen darf..

Tag:	**snmpTargetAddrEntry**
Value:	*MyTarget* **snmpUDPDomain** *myTaddr* **300 0** *MyTagList* **- nonVolatile** *MyAddrMask*

*MyTarget**
Name des Target-Eintrags (String 1..32)

MyTAddr
Internet-Adresse des Targets in der Form **xxx.xxx.xxx.xxx:0**

MyTagList
Liste der Tags (siehe Punkt a). Die Liste muss in Hochkommata ("...") eingeschlossen sein; die einzelnen Listenelemente sind durch *ein* Leerzeichen voneinander zu trennen.

MyAddrMask

Maske in der Form **xxx.xxx.xxx.xxx:0**, analog einer Subnetz-Maske.
Eine sourceAddr ist gültig, falls gilt:

(Absenderadresse & MyAddrMask) == (MyTAddr & MyAddrMask)

Beispiel

Der Benutzer „gast“ soll ohne Authentifizierung über ein Passwort lesenden Zugriff auf alle Objekte erhalten.

In SNMPv3-Security:

usmUserEntry localSNMPID gast usmNoAuthProtocol **usmNoPrivProtocol** \
nonVolatile - -
vacmSecurityToGroupEntry usm gast READ **nonVolatile**
vacmAccessEntry READ - **usm authNoPriv exact** All - **- nonVolatile**
vacmViewTreeFamilyEntry All dod **- included nonVolatile**

Bild 7 auf der nächsten Seite skizziert das Vorgehen beim Erstellen der Einträge für die Security-Konfiguration.

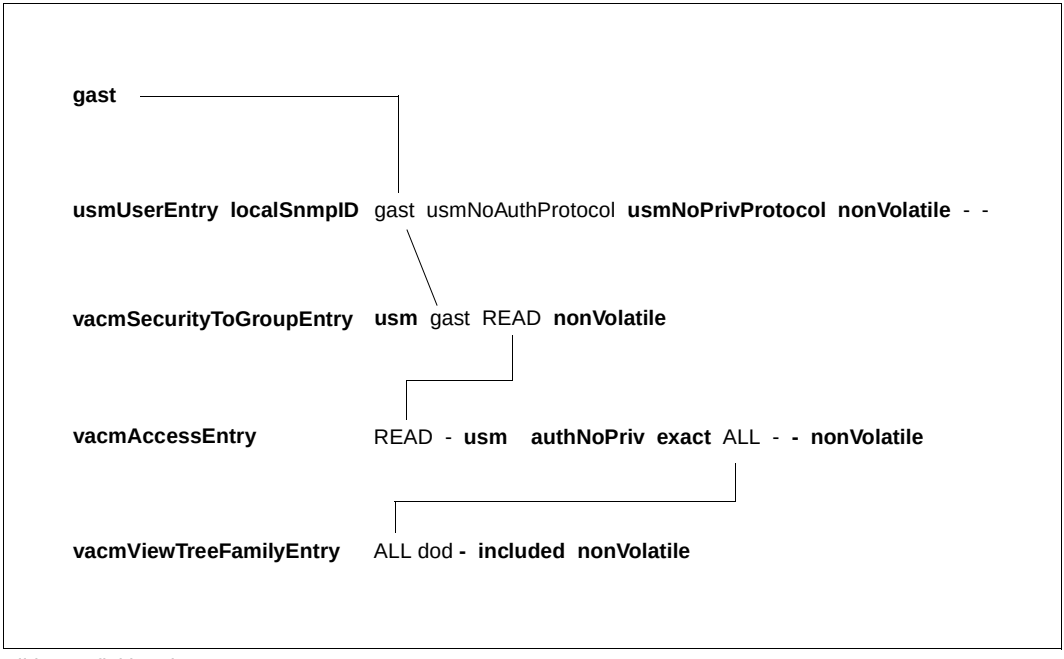


Bild 7: Definition des SNMPv3-Benutzers „gast“

3.3.1.7 Definition des Zugriffs auf den Agenten über HTTP-Requests

a) Definition einer DR-Web-Benutzerkennung- *httpUserNameEntry*

Der *httpUserNameEntry* ordnet einer Benutzerkennung eine Security-Gruppe und ein Passwort zu.

Tag:	**httpUserNameEntry**
Value:	*MyUserName MyGroup* **- nonVolatile** *MyPasswort*

*MyUserName**
Benutzerkennung (String 1..32), unter der ein HTTP-Request erfolgen darf.

MyGroup
zugeordnete Security-Gruppe (siehe Punkt b2). Die Security-Gruppe bestimmt den Berechtigungsumfang.

MyPassword
Passwort. Die Angabe „-“ bedeutet, dass für die definierte Benutzerkennung wird kein Passwort benötigt wird.

b) Definition der Zugriffskontrolle

b1) Definition des MIB-Zweigs - *vacmViewTreeFamilyEntry*

Die Definition des MIB-Zweigs besteht aus einem oder mehreren *vacmViewTreeFamilyEntry*-Einträgen. Jeder *vacmViewTreeFamilyEntry* ordnet dem MIB-Zweig ein OID zu oder schließt ein OID aus.

Tag:	**vacmViewTreeFamilyEntry**
Value:	*MyMIB MyOID* **-** (**included | excluded**) **nonVolatile**

*MyMIB**
Name des MIB-Zweig-Eintrags (String..32)

*MyOID**
OID oder symbolischer Name des MIB-Zweigs

included | **excluded**
Der MIB-Zweig soll ein- bzw. ausgeschlossen werden. Zugreifbar sind nur die Objekte, die als Ergebnis aller *included*- bzw. *excluded*-Operationen im MIB-Zweig verbleiben.

b2) Definition der Security-Gruppe - *vacmAccessEntry*

Der *vacmAccessEntry* definiert eine Security-Gruppe und ordnet ihr MIB-Zweige für Lese- und Schreibberechtigungen zu.

Tag:	**vacmAccessEntry**
Value:	*MyGroup* **- http authNoPriv exact** [*MYRead*] [*MyWrite*] **- nonVolatile**

*MyGroup**
: Name der Security-Gruppe (String 1..32). Die Security-Gruppe bestimmt den Berechtigungsumfang.

MyRead
: zugeordneter MIB-Zweig für den Lesezugriff (siehe Punkt b1)

MyWrite
: zugeordneter MIB-Zweig für den Schreibzugriff (siehe Punkt b1)

b3) Definition des Security-Eintrags - *vacmSecurityToGroupEntry*

Der *vacmSecurityToGroupEntry* ordnet der Benutzerkennung eine Security-Gruppe zu.

Tag:	**vacmSecurityToGroupEntry**
Value:	**http** *MyUserName MyGroup* **nonVolatile**

*MyUserName**
: Benutzerkennung (String 1..32), unter der ein http-Rquest erfolgen darf.

MyGroup
: zugeordnete Security-Gruppe (siehe Punkt b2). Die Security-Gruppe bestimmt den Berechtigungsumfang.

Beispiel

Ohne Authentifizierung über ein Passwort soll dem Benutzer „gast“ lesender Zugriff auf alle MIB-Objekte gewährt werden.

In DR-Web:

httpUserNameEntry gast READ **- nonVolatile** -
vacmSecurityToGroupEntry http gast READ **nonVolatile**
vacmAccessEntry READ **- http authNoPriv exact** All - **- nonVolatile**
vacmViewTreeFamilyEntry All dod **- included nonVolatile**

Das folgende Bild skizziert das Vorgehen beim Erstellen der Einträge für die Security-Konfiguration.

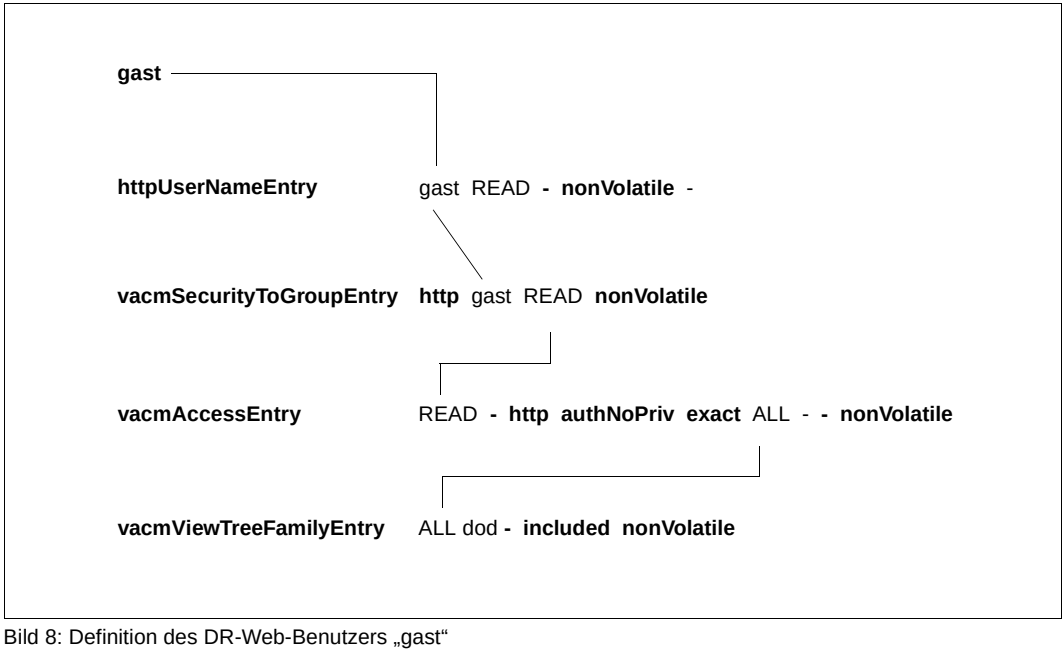


Bild 8: Definition des DR-Web-Benutzers „gast“

3.3.1.8 Definition der Trap-Ziele

a) Definition von Notify-Eintrag und Zieladresse

a1) Definition des Notify-Eintrags - *snmpNotifyEntry*

Tag:	snmpNotifyEntry
Value:	*MyNotify MyTransTag* **trap nonVolatile**

*MyNotify**
Name des Notify-Eintrags (String 1..32)

MyTransTag
zugeordnetes Transport-Label. Das Transport-Label zeigt in eine Target-Liste (siehe Punkt a2) und bestimmt, an welche Systeme die Traps gesendet werden sollen.

a2) Definition der Zieladresse - *snmpTargetAddrEntry*

Der *snmpTargetAddrEntry* ordnet dem Notify-Eintrag (siehe Punkt a1) eine Zieladresse und einen Target-Parameter-Eintrag zu

Tag:	snmpTargetAddrEntry
Value:	*MyTarget* **snmpUDPDomain** *MyTAddr* **300 0** *MyTagList MyTargetParam* **nonVolatile** *MyAddrMask*

*MyTarget**
Name desTarget-Eintrags (String 1..32)

MyTAddr
Internet-Adresse des Targets in der Form **xxx.xxx.xxx.xxx:p**;
xxx.xxx.xxx.xxx bezeichnet die IP-Adresse;
p bezeichnet den Port (p=0: Defaultwert 162 bei Traps)

MyTagList
Liste der Tags (siehe Punkt a). Die Liste muss in Hochkommata eingeschlossen ("...") sein; die einzelnen Listenelmente sind voneineander durch *ein* Leerzeichen zu trennen.

MyTargetParam
zugeordneter Parametereintrag (siehe Punkt a3)

MyAddrMask
Maske in der Form **xxx.xxx.xxx.xxx:0** (analog einer Subnetz-Maske).

Eine Zieladresse ist gültig, falls gilt:
(Zieladresse & MyAddrMask) == (MyTAddr & MyAddrMask)

a3) Definition der Target-Parameter - *snmpTargetParamsEntry*

Pro *snmpTargetParamsEntry* wird ein Target-Parameter definiert.

Tag:	snmpTargetParamsEntry
Value:	*MyTargetParam* **0 snmpv1** *MyCommunity* **noAuthNoPriv nonVolatile**

*MyTargetParam**
Name des Target-Parameter-Eintrags (String 1..32)

MyCommunity
Community-String, mit dem der Trap gesendet werden soll. Der Community-String bestimmt auch den Security-Eintrag (siehe Punkt b3).

b) Definition der Zugriffskontrolle

b1) Definition des MIB-Zweigs: *vacmViewTreeFamilyEntry*

Die Definition des MIB-Zweigs besteht aus einem oder mehreren *vacmViewTreeFamilyEntry*-Einträgen. Jeder *vacmViewTreeFamilyEntry* ordnet dem MIB-Zweig ein OID zu oder schließt ein OID aus.

Tag:	**vacmViewTreeFamilyEntry**
Value:	*MyTrap MyOID* **-** (**included** | **excluded**) **nonVolatile**

*MyTrap**
Name des MIB-Zweig-Eintrags (String 1..32)

*MyOID**
OID oder symbolischer Name des MIB-Zweigs (OID)

included | **excluded**
Der MIB-Zweig soll eigeschlossen / ausgeschlossen werden. Nur die Objekte, die als Ergebnis aller included /excluded-Operationen im MIB-Zweig verbleiben, werden mit dem Enterprise und den Variablenbindungen (variable bindings) des Traps verglichen. Sind Enterprise und Variablenbindung im MIB-Zweig enthalten, dann wird der Trap gesendet.

b2) Definition der Security-Gruppe - *vacmAccessEntry*

Der *vacmAccessEntry* definiert eine Security-Gruppe und ordnet ihr MIB-Zweige für Lese- und Schreibberechtigungen zu**.**

Tag:	vacmAccessEntry
Value:	*MyGroup* **- snmpv1 noAuthNoPriv exact - -** MyTrap **nonVolatile**

*MyGroup**
Name der Security-Gruppe (String 1..32)

MyTrap
zugeordneter MIB-Zweig für den Trap (siehe Punkt b1)

b3) Definition des Security-Eintrags: *vacmSecurityToGroupEntry*

Der *vacmSecurityToGroupEntry* ordnet dem Community-String eine Security-Gruppe zu

Tag:	vacmSecurityToGroupEntry
Value:	**snmpv1** *MyCommunity MyGroup* **nonVolatile**

*MyCommunity**
Community-String (String 1-32), mit dem der Trap gesendet werden soll.

MyGroup
zugeordnete Security-Gruppe (siehe Punkt b2). Die Security-Gruppe bestimmt, ob der Zugriff erfolgen darf oder nicht.

c) Definition der Absenderadresse eines Traps - *snmpNotifySourceEntry*

Der *snmpNotifySourceEntry* bestimmt, welche Absenderadressen für welche Trapziele verwendet werden sollen. Die Definition der Absenderadresse eines Traps ist optional.

Tag:	snmpNotifySourceEntry
Value:	*MyNotifySource MyTagList MySourceAddr* **nonVolatile**

*MyNotifySource**
: Name des NotifySource-Eintrags (String 1..32)

MyTagList
: Liste der Tags (siehe Punkt a) auf Seite 48). Die Liste muss in Hochkommata ("...") eingeschlossen sein; die einzelnen Listenelemente sind durch *ein* Leerzeichen voneinander zu trennen.

MySourceAddr
: gewünschte Absenderadresse für den Trap in der Form **xxx.xxx.xxx.xxx**

Beispiele

Beispiel 1

Traps sollen mit dem Community-String „tcom“ an den Rechner 139.22.22.22 gesendet werden.

– in SNMPv1-Security: **trap** tcom 139.22.22.22

– in SNMPv3-Security:

snmpNotifyEntry Nf1 TarTag1 **trap nonVolatile**
snmpTargetAddrEntry Ta1 **snmpUDPDomain** 139.22.22.22:0 **300 0**
TarTag1 Tp1 **nonVolatile** 255.255.255.255.0
snmpTargetParamsEntry Tp1 **0 snmpv1** tcom **noAuthNoPriv nonVolatile**
vacmSecurityToGroupEntry snmpv1 tcom TRAP **nonVolatile**
vacmAccessEntry TRAP **- snmpv1 noAuthNoPriv exact - -** All **nonVolatile**
vacmViewTreeFamiliyEntry All dod **- included nonVolatile**

Beispiel 2

Traps sollen mit dem Community-String „tcom“ an die Systeme mit den IP-Adressen 139.22.104.0 bis 139.22.111.255 gesendet werden.

– in SNMPv1-Security (frühere Versionen): nicht einstellbar

– in SNMPv3-Security (aktuelle Version):

snmpNotifyEntry Nf2 TarTag2 **trap nonVolatile**
snmpTargetAddrEntry Ta2 **snmpUDPDomain** 139.22.104.0:0 **300 0**
TarTag2 Tp1 **nonVolatile** 255.255.248.0:0
snmpTargetParamsEntry Tp1 **0 snmpv1** tcom **noAuthNoPriv nonVolatile**
vacmSecurityToGroupEntry snmpv1 tcom TRAP **nonVolatile**
vacmAccessEntry TRAP **- snmpv1 noAuthNoPriv exact - -** All **nonVolatile**
vacmViewTreeFamiliyEntry All dod **- included nonVolatile**

Beispiel 3

Traps mit Enterprises sni.2.34 sollen mit dem Community-String „tent“ an das System mit der IP-Adresse 139.22.22.22 gesendet werden. Dabei sollen Traps mit der spezifischen Trapnummer 33 nicht berücksichtigt werden.

– in SNMPv1-Security (frühere Versionen): nicht einstellbar

– in SNMPv3-Security (aktuelle Version):

snmpNotifyEntry Nf3 TarTag3 **trap nonVolatile**
snmpTargetAddrEntry Ta3 **snmpUDPDomain** 139.22.22.22:0 **300 0**
TarTag3 Tp3 **nonVolatile** 255.255.255.255:0
snmpTargetParamsEntry Tp3 **0 snmpv1** tent **noAuthNoPriv nonVolatile**
vacmSecurityToGroupEntry snmpv1 tent EpAcc **nonVolatile**
vacmAccessEntry EpAcc **- snmpv1 noAuthNoPriv exact - -** EpTreeT **nonVolatile**
vacmViewTreeFamiliyEntry EpTreeT sni.2.34 **- included nonVolatile**
vacmViewTreeFamiliyEntry EpTreeT sni.2.34.0.33 **- excluded nonVolatile**

Bild 9 auf der nächsten Seite skizziert das Vorgehen beim Erstellen der Einträge für die Security-Konfiguration.

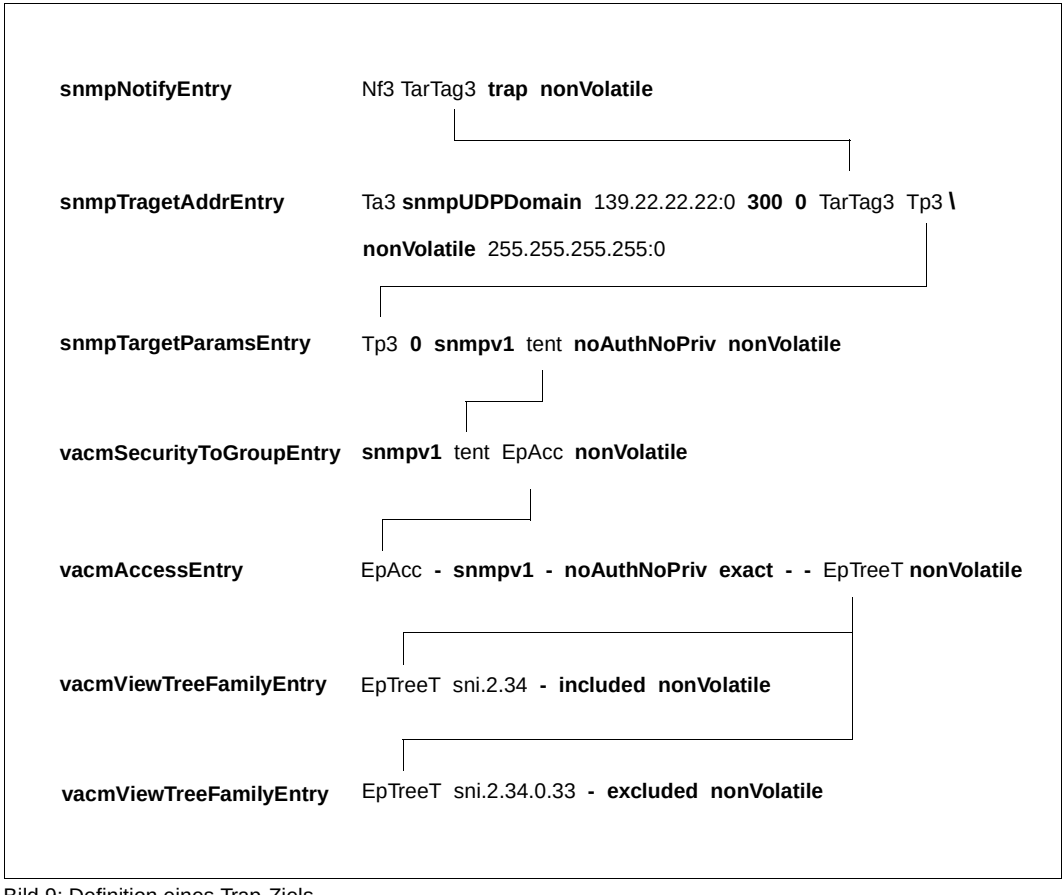


Bild 9: Definition eines Trap-Ziels

Beispiel 4

Traps an den Rechner 139.22.22.22 sollen mit der Absenderadresse 112.1.1.1 gesendet werden.

– in SNMPv1-Security (frühere Versionen): trap public 139.22.22.22 112.1.1.1

– in SNMPv3-Security (aktuelle Version):

snmpNotifyEntry Nf1 TarTag1 **trap nonVolatile**
snmpTargetAddrEntry Ta1 **snmpUDPDomain** 139.22.22.22:0 **300 0**
TarTag1 Tp1 **nonVolatile** 255.255.255.255.0
snmpTargetParamsEntry Tp1 **0 snmpv1** tcom**noAuthNoPriv nonVolatile**
snmpNotifySourceEntry NfS1 TarTag1 112.1.1.1 **nonVolatile**
vacmSecurityToGroupEntry snmpv1 tcom TRAP **nonVolatile**
vacmAccessEntry TRAP **- snmpv1 noAuthNoPriv exact - -** All **nonVolatile**
vacmViewTreeFamiliyEntry All dod **- included nonVolatile**

3.3.1.9 Beispiel

```
# Benutzerkonfiguration
communityEntry  localSnmpID public   READ    localSnmpID - -       nonVolatile
communityEntry  localSnmpID master   WRITE   localSnmpID - TarTag1 nonVolatile
communityEntry  localSnmpID multi    WRITE   localSnmpID - TarTag2 nonVolatile
communityEntry  localSnmpID sysread  SysAccR localSnmpID - -       nonVolatile
communityEntry  localSnmpID syswrite SysAccW localSnmpID - -       nonVolatile
usmUserEntry localSnmpID gast usmNoAuthProtocol usmNoPrivProtocol nonVolatile - -
httpUserNameEntry  gast READ - nonVolatile -


snmpNotifyEntry  Nf1 TarTag1 trap nonVolatile
snmpNotifyEntry  Nf2 TarTag2 trap nonVolatile
snmpNotifyEntry  Nf3 TarTag3 trap nonVolatile


# Konfiguration der Zugriffskontrolle
vacmViewTreeFamilyEntry  All      dod           - included nonVolatile
vacmViewTreeFamilyEntry  SysTreeR system        - included nonVolatile
vacmViewTreeFamilyEntry  SysTreeW system        - included nonVolatile
vacmViewTreeFamilyEntry  SysTreeW sysName       - excluded nonVolatile
vacmViewTreeFamilyEntry  EpTreeT  sni.2.34      - included nonVolatile
vacmViewTreeFamilyEntry  EpTreeT  sni.2.34.0.33 - excluded nonVolatile

vacmAccessEntry  READ    - snmpv1 noAuthNoPriv exact All      -        -
nonVolatile
vacmAccessEntry  WRITE   - snmpv1 noAuthNoPriv exact All      All      -
nonVolatile
vacmAccessEntry  SysAccR - snmpv1 noAuthNoPriv exact SysTreeR -        -
nonVolatile
vacmAccessEntry  SysAccW - snmpv1 noAuthNoPriv exact SysTreeR SysTreeW -
nonVolatile
vacmAccessEntry  TRAP    - snmpv1 noAuthNoPriv exact -        -        All
nonVolatile
vacmAccessEntry  EpAcc   - snmpv1 noAuthNoPriv exact -        -        EpTreeT
nonVolatile
vacmAccessEntry  READ    - usm    noAuthNoPriv exact All      -        -
nonVolatile
vacmAccessEntry  READ    - http AuthNoPriv exact All      -        - nonVolatile

vacmSecurityToGroupEntry  snmpv1 public   READ    nonVolatile
vacmSecurityToGroupEntry  snmpv1 master   WRITE   nonVolatile
vacmSecurityToGroupEntry  snmpv1 multi    WRITE   nonVolatile
vacmSecurityToGroupEntry  snmpv1 sysread  SysAccR nonVolatile
vacmSecurityToGroupEntry  snmpv1 syswrite SysAccW nonVolatile
vacmSecurityToGroupEntry  snmpv1 tcom     TRAP    nonVolatile
vacmSecurityToGroupEntry  snmpv1 tent     EpAcc   nonVolatile
vacmSecurityToGroupEntry  usm    gast     READ    nonVolatile
vacmSecurityToGroupEntry  http   gast     READ    nonVolatile
```

```
# Konfiguration der Adressenkontrolle
snmpTargetAddrEntry  Ta1 snmpUDPDomain 139.22.22.22:0 300 0 TarTag1 Tp1
nonVolatile 255.255.255.255:0
snmpTargetAddrEntry  Ta2 snmpUDPDomain 139.22.104.0:0 300 0 TarTag2 Tp1
nonVolatile 255.255.248.0:0
snmpTargetAddrEntry  Ta3 snmpUDPDomain 139.22.22.22:0 300 0 TarTag3 Tp3
nonVolatile 255.255.255.255:0

snmpTargetParamsEntry  Tp1 0 snmpv1 tcom noAuthNoPriv nonVolatile
snmpTargetParamsEntry  Tp3 0 snmpv1 tent noAuthNoPriv


# Absenderadresse
snmpNotifySourceEntry  NfS1 TarTag1 112.1.1.1 nonVolatile
```

3.3.2 Konfiguration des Masteragenten und des Supervisor Subagenten

Die im vorangegangenen Abschnitt beschriebene Security-Konfiguration ist der zentrale Sicherheitsmechanismus, der unberechtigte Zugriffe und Eingriffe in das Management-System und die angeschlossenen Rechner verhindert.

Neben den Parametern für die Security-Konfiguration enthält die Konfigurationsdatei */etc/snmp/agt/snmpd.cnf* u.a.die Initial System Group und optional die Startanweisung für den Supervisor Subagenten

Die Datei *snmpd.cnf* sollte nur bei gestopptem Masteragenten editiert werden, da der Masteragent die Konfigurationsdatei u.U. zwischenzeitlich überschreibt.

Initial System Group

sysDescr	
sysLocation	Siemens Mch-P *
sysContact	Help Desk *
sysObjectID	1.3.6.1.4.1.231.1.6
MAX_PDU_TIME	Wartezeit des Masteragenten auf eine Antwort des Subagenten, bevor er den Request verwirft.
MAX_THREADS	gibt die maximale Anzahl der Threads an, die gleichzeitig bearbeitet werden können. Es wird empfohlen, die Anzahl etwa doppelt so groß wie die Anzahl der Subagenten zu wählen, da die Subagenten nur jeweils einen Request bearbeiten können.
MAX_OUTPUT_WAITING	gibt die maximale Anzahl Byte an, die als Nachrichten vom Master gespeichert werden können, bevor ein "Overflow" auftritt.
MAX_SUBAGENTS	definiert die maximale Anzahl der Subagenten, die sich an den Masteragenten anschließen dürfen.
RETRY_INTERVAL	RETRY_INTERVAL wird derzeit nicht genutzt.
snmpEnableAuthenTraps	2 : es werden keine Authentisierungsfehlertraps geschickt 1 : es werden Authentisierungsfehlertraps geschickt
subagent	Wenn der Supervisor Subagent gestartet werden soll, muss hier der Name der Bibliothek angegeben werden: [:<catid>:] [$<userid>.]SYSLNK.SBA-BS2.050 oder für RISC-Maschinen: [:<catid>:] [$<userid>.]SRMLNK.SBA-BS2.050

Voreinstellung der Initial System Group
* Passen Sie bitte nur die Werte sysLocation und sysContact ihren Begebenheiten an, der Wert sysObjectID sollte unverändert bleiben.

3.3.3 Konfiguration des Application Monitor Subagenten

Der Application Monitor Subagent gestattet die Überwachung von

– Benutzer-Anwendungen,
– DCAM-Anwendungen,
– BCAM-Anwendungen,
– Subsystemen,
– Jobvariablen und
– Protokolldateien.

Außerdem können Gruppen zusammengehöriger Anweisungen als Einheit (Objekt) verwaltet werden.
Art und Umfang der Anwendungsüberwachung werden über eine Konfigurationsdatei individuell gesteuert. Der Name der Konfigurationsdatei wird dem Application Monitor Subagenten im Startkommando bekannt gegeben. Bei Syntaxfehlern in der Konfigurationsdatei wird der Startvorgang abgebrochen. Wenn keine Konfigurationsdatei angegeben wird, ist die Überwachung auf Subsysteme beschränkt.

3.3.3.1 Anweisungen für die Konfigurationsdatei

Die Konfigurationsdatei enthält Informationen darüber, welche Anwendungen, Tasks, Subsysteme, Jobvariablen und Protokolldateien überwacht werden sollen. Es können jeweils bis zu 256 Benutzer-, BCAM-Anwendungen, Jobvariablen und Protokolldateien sowie 128 DCAM-Anwendungen überwacht werden. Benutzer- und BCAM-Anwendungen sowie Tasks, die überwacht werden sollen, müssen mit Jobvariablen angestartet werden. Die Anzahl der zu überwachenden Subsysteme ist unbegrenzt.

Die Einträge in der Konfigurationsdatei werden über SDF-Anweisungen erzeugt. Mit der Anweisung //REMARK können Kommentare in der Konfigurationsdatei hinterlegt werden. Die letzte Anweisung der Datei muss immer die Anweisung //END sein. Anweisungen, die hinter der END-Anweisung stehen, werden ignoriert.

Überwachung	**Anweisung**	**Seite**
Anwendung	//ADD-APPLICATION-RECORD	61
DCAM-Anwendung	//ADD-DCAM-APPLICATION-RECORD	61
Subsystem	//ADD-SUBSYSTEM-RECORD	64
Protokolldatei	//ADD-LOG-FILE-RECORD	65
Jobvariable	//ADD-JV-RECORD	67
Gruppe von zusammengehörigen Anwendungen	//DEFINE-OBJECT	69
Trap-Format	//DEFINE-TRAP-FORMAT	71

Beispiel:

Das folgende Beispiel finden Sie auch in der Bibliothek SINLIB.SBA-BS2.050

```
//REMARK Application Monitor, SDF-Configuration File
//REMARK
//REMARK Trap Format
//DEFINE-TRAP-FORMAT TYPE = (*GENERIC, *TVCC)
//REMARK
//REMARK Application Monitoring, Type BCAM
//ADD-APPLICATION-RECORD  -
//        APPLICATION-NAME = ANW1  -
//       ,VERSION = V1.0  -
//       ,TYPE = *BCAM  -
//       ,JV-NAME = MONJV  -
//       ,TRAP-CONDITION = (A, R)  -
//       ,WEIGHT=10  -
//
//REMARK Application Monitoring, Type USER
//ADD-APPLICATION-RECORD  -
//        APPLICATION-NAME = Applikation1  -
//       ,VERSION = V01.0A00  -
//       ,TYPE = *USER  -
//       ,JV-NAME = MJV1  -
//       ,TRAP-CONDITION = A  -
//       ,WEIGHT=5   -
//       ,ACKNOWLEDGE = *YES -
//
//ADD-APPLICATION-RECORD  -
//        APPLICATION-NAME = Applikation2  -
//       ,TYPE = *USER  -
//       ,JV-NAME = MJV2  -
//       ,TRAP-CONDITION = (T, A)  -
//
//REMARK Subsystem Monitoring
//ADD-SUBSYSTEM-RECORD  -
//        NAME = EDT  -
//
//ADD-SUBSYSTEM-RECORD  -
//        NAME = MAREN  -
//       ,VERSION = 08.1  -
//       ,TRAP-CONDITION = *NONE  -
//
```

```
//REMARK File Monitoring
//ADD-LOG-FILE-RECORD  -
//        NAME = /tmp/logfile1  -
//       ,APPLICATION-NAME = Datei1  -
//       ,MONITORING = *NO  -
//       ,FORMAT = *EBCDIC  -
//
//ADD-LOG-FILE-RECORD  -
//        NAME = $HUGO.LOGFILE2  -
//       ,MONITORING = *NO  -
//       ,FORMAT = *EBCDIC  -
//       ,PATTERN = '*important*' -
//
//REMARK Jobvariables
//ADD-JV-RECORD  -
//        JV-NAME = JOBVAR  -
//       ,PATTERN = ('*terminated*', '[1-5]00*')  -
//
//REMARK DCAM Application
//ADD-DCAM-APP A-NAME=d3str10$,HOST=camilla2,KEEP-CONNECTION=*NO -
//
//ADD-DCAM-APP A-NAME=$CONSOLE,HOST=D017ZE00, -
//        MSG='@CONSOLE,TSOS,''@@@@@@@@'',V01' -
//       ,WEIGHT=99  -
//
//REMARK Object
//DEFINE-OBJECT OBJECT-NAME=OB1,BCAM-APPLICATION=ANW1,          -
//        LOG-FILE=(/tmp/logfile1),  -
//        MONITORING-TIME=*INTERVAL(START=3:00,STOP=18:11,EX=SUN)
//END
```

3.3.3.2 Wechsel der Konfigurationsdatei im laufenden Betrieb

Änderungen der aktuellen Konfigurationsdatei im laufenden Betrieb können dem Application Monitor entweder durch Setzen des Objekts *appMonConfFile* oder per Kommando vorgenommen werden.

```
/START-APPMONCMD

       x "readConfig <filename>"
```

POSIX:

```
appmoncmd x "readConfig <filename>"
```

Bei Syntaxfehlern in *appMonConfFile* wird mit der ursprünglichen Konfiguration weitergearbeitet.

ADD-APPLICATION-RECORD

Die Anweisung ADD-APPLICATION-RECORD benennt die BCAM- und Benutzeranwendungen, die überwacht werden sollen. Unter Anwendungen sind Programme oder Tasks zu verstehen.

//ADD-APPLICATION-RECORD
APPLICATION-NAME = <composed-name_1 .. 54_with-underscore>
, **VERSION** = ***NONE** / <product-version>
, **TYPE** = ***BCAM** / ***USER**
, **JV-NAME** = <filename_1 .. 54>
, **TRAP-CONDITION** = **A** / list-poss (6) : <name_1 .. 1>
, **WEIGHT= 0 /** <integer 0 .. 999>
, **ACKNOWLEDGE** = ***NO** / ***YES**

APPLICATION-NAME=<composed-name_1..54_with-underscore>
bestimmt die Anwendung, die der Subagent überwachen soll.

VERSION=*NONE / <product-version>
Versionsnummer der Anwendung
Standardwert: *NONE

TYPE=*BCAM / *USER
Typ der Anwendung.

JV-NAME = <filename_1 .. 54>
Jobvariable (MONJV), mit der die Anwendung bzw. die Task überwacht wird.

TRAP-CONDITION=A / list-poss (6) : <name_1 .. 1>
Zustände, bei denen ein Trap erzeugt werden soll.

WEIGHT= 0 / <integer 0 .. 999>
Gewichtung der für den Application Monitor Subagenten spezifischen Traps. Beim Senden eines Traps versorgt der Application Monitor Subagent beim generischen Trap das Trap-Objekt *appMonWeight* und die Trap-Nummer mit dem angegebenen Wert (siehe Abschnitt „Trap-Struktur“ auf Seite 184 im Kapitel „Funktionen des BASIC-AGENT“). Sollen in einer Anwendung für verschiedene Ereignisse verschiedene Gewichte verwendet werden, dann muss die zugehörige ADD-APPLICATION-RECORD-Anweisung mehrmals in der Konfigurationsdatei angegeben werden.
Standardwert: 0

ACKNOWLEDGE=*NO / *YES
Angabe, ob der Trap bestätigt werden muss. Es können nur Application Monitor-spezifische Traps bestätigt werden.
Standardwert: *NO

ADD-DCAM-APPLICATION-RECORD

Die Anweisung ADD-DCAM-APPLICATION-RECORD benennt die DCAM-Anwendungen, die zyklisch überwacht werden sollen. Das Überwachungsintervall für DCAM-Anwendungen liegt beim 60-fachen Wert der Timer-Einstellung, beträgt also standardmäßig 5 Minuten.

Maximal können 128 DCAM-Anwendungen überwacht werden.

//ADD-DCAM-APPLICATION-RECORD
APPLICATION-NAME = <name_1 .. 8> , **HOST**= ***OWN** / <name1 .. 8>> , **KEEP-CONNECTION** = ***YES** / ***NO** , **MSG**= ***NONE** / <c-string> / <x-string> , **WEIGHT= 0 / <integer 0 .. 999>** , **ACKNOWLEDGE**= ***NO** / ***YES**

APPLICATION-NAME=<name_1..8>
bestimmt die DCAM-Anwendung, die der Subagent überwachen soll.

HOST=*OWN / <name1..8>
Rechner auf dem die DCAM- Anwendung läuft
Standardwert: *OWN

KEEP-CONNECTION=*YES / *NO
Angabe, ob die Verbindung wieder abgebaut werden soll
Standardwert: *YES

MSG= *NONE / <c-string> / <x-string>
Verbindungsnachricht
Standardwert: *NONE

WEIGHT= 0 / <integer 0 .. 999>
Gewichtung der für den Application Monitor Subagenten spezifischen Traps. Beim Senden eines Traps versorgt der Application Monitor Subagent beim generischen Trap das Trap-Objekt *appMonWeight* und die Trap-Nummer mit dem angegebenen Wert (siehe Abschnitt „Trap-Struktur“ auf Seite 184 im Kapitel „Funktionen des BASIC-AGENT“).
Standardwert: 0

ACKNOWLEDGE= *NO / *YES
Angabe, ob der Trap bestätigt werden muss. Es können nur Application Monitor-spezifische Traps bestätigt werden.
Standardwert: *NO

ADD-SUBSYSTEM-RECORD

Die Anweisung ADD-SUBSYSTEM-RECORD definiert die zu überwachenden Subsysteme. Das Überwachungsintervall liegt bei dem fünffachen Wert der Timer-Einstellung, beträgt standardmäßig also 25 Sekunden.

//ADD-SUBSYSTEM-RECORD
NAME = <structured-name 1 .. 8> / ***ALL**
, **VERSION** = ***NONE** / <product-version>
, **TRAP-CONDITION** = ***NONE** / list-poss (8) : ***CREATED** / ***NOT-CREATED** / ***IN-DELETE** / ***IN-CREATE** / ***IN-RESUME** / ***IN-HOLD** / ***NOT-RESUMED** / ***LOCKED**
, **WEIGHT= 0 / <integer 0 .. 999>**
, **ACKNOWLEDGE** = ***NO** / ***YES**

NAME=<structured-name 1..8> / *ALL
bestimmt das Subsystem, das der Subagent überwachen soll.

VERSION=*NONE / <product-version>
Versionsnummer des Subsystems
Standardwert: *NONE

TRAP-CONDITION=*NONE / list-poss (8) : *CREATED / *NOT-CREATED / *IN-DELETE / *IN-CREATE / *IN-RESUME / *IN-HOLD / *NOT-RESUMED / *LOCKED
Zustände, bei denen ein Trap erzeugt werden soll.
Standardwert: *NONE

Hinweis:
Bei der Angabe NAME=*ALL sollten Sie TRAP-CONDITION=*NONE verwenden, da andernfalls Performance-Probleme auftreten können.

WEIGHT= 0 / <integer 0 .. 999>
Gewichtung der für den Application Monitor Subagenten spezifischen Traps. Beim Senden eines Traps versorgt der Application Monitor Subagent beim generischen Trap das Trap-Objekt *appMonWeight* und die Trap-Nummer mit dem angegebenen Wert (siehe Abschnitt „Trap-Struktur“ auf Seite 184 im Kapitel „Funktionen des BASIC-AGENT“). Sollen in einem Subsystem für verschiedene Ereignisse verschiedene Gewichte verwendet werden, dann muss die zugehörige ADD-SUBSYSTEM-RECORD-Anweisung mehrmals in der Konfigurationsdatei angegeben werden.
Standardwert: 0

ACKNOWLEDGE=*NO / *YES
Angabe, ob der Trap bestätigt werden muss. Es können nur Application Monitor-spezifische Traps bestätigt werden.
Standardwert: *NO

ADD-LOG-FILE-RECORD

Die Anweisung ADD-LOG-FILE-RECORD definiert die zu überwachenden Protokolldateien. Standardmäßig sendet der Application Monitor Subagent bei jeder Änderung einer Jobvariablen einen Trap. Es ist jedoch möglich, die Traps bzw. Einträge zu filtern.

//ADD-LOG-FILE-RECORD
NAME = <filename_1 .. 54> / <posix-pathname>
, APPLICATION-NAME = ***NONE** / <composed-name_1 .. 54_with-underscore>
, **MONITORING** = ***YES** / ***NO**
, **FORMAT** = ***EBCDIC** / ***ASCII**
, **PATTERN** = ***NONE** / list-poss (8) : <c-string_1 .. 256_with-lower-case>
, **WEIGHT= 0 / <integer 0 .. 999>**
, **ACKNOWLEDGE** = ***NO** / ***YES**

NAME=<filename_1 .. 54> / <posix-pathname>
bestimmt die Protokolldatei, die der Subagent überwachen soll.

APPLICATION-NAME=*NONE / <composed-name_1 .. 54_with-underscore>
Name der Anwendung.
Standardwert: *NONE

MONITORING=*YES / *NO
Angabe, ob die Protokolldatei überwacht werden soll.

FORMAT=*EBCDIC / *ASCII
Format der Protokolldatei.
Standardwert: *EBCDIC

PATTERN = *NONE / list-poss (8) : <c-string_1 .. 256_with-lower-case>
Angabe eines oder mehrerer Suchmuster. Fehlt die Angabe PATTERN werden alle Einträge in eine Protokolldatei per Trap gemeldet.
Es sind folgende Wildcard-Angaben zulässig:

? : ersetzt ein beliebiges Zeichen
* : ersetzt eine beliebig lange Folge von Zeichen
[s] : ersetzt genau ein Zeichen aus der Zeichenkette s
[c1 - c2]: ersetzt ein beliebiges Zeichen aus dem Bereich von c1 bis c2
Das Zeichen "\" (Backslash) muss zur Entwertung der Sonderzeichen angegeben werden.
Es wird zwischen Groß- und Kleinschreibung unterschieden.
Standardwert: *NONE

WEIGHT= 0 / <integer 0 .. 999>
Gewichtung der für den Application Monitor Subagenten spezifischen Traps. Beim Senden eines Traps versorgt der Application Monitor Subagent beim generischen Trap das Trap-Objekt *appMonWeight* und die Trap-Nummer mit dem angegebenen Wert (siehe Abschnitt „Trap-Struktur“ auf Seite 184 im Kapitel „Funktionen des BASIC-AGENT“).
Standardwert: 0

ACKNOWLEDGE=*NO / *YES
Angabe, ob der Trap bestätigt werden muss. Es können nur Application Monitor-spezifische Traps bestätigt werden.
Standardwert: *NO

ADD-JV-RECORD

Die Anweisung ADD-JV-RECORD definiert die zu überwachenden Jobvariablen. Standardmäßig sendet der Application Monitor Subagent jede Änderung einer Jobvariablen als Trap. Es ist jedoch möglich, die Traps zu filtern.

//ADD-JV-RECORD
JV-NAME = <filename_1 .. 54>
, **APPLICATION-NAME** = ***NONE** / <composed-name_1 .. 54_with-underscore>
, **PASSWORD** = ***NONE** / <c-string_1 .. 4 > / < x-string_1 .. 8>
, **PATTERN** = ***NONE** / list-poss (8) : <c-string_1 .. 256_with-lower-case>
, **WEIGHT= 0 / <integer 0 .. 999>**
, **ACKNOWLEDGE** = ***NO** / ***YES**

JV-NAME = <filename_1 .. 54>
bestimmt die Jobvariable, die der Subagent überwachen soll.

APPLICATION-NAME = *NONE / <composed-name_1 .. 54_with-underscore>
Name der Anwendung.
Standardwert: *NONE

PASSWORD = *NONE / <c-string_1 .. 4 > / <x-string_1 .. 8>
Lesepasswort der Jobvariablen.
Standardwert: *NONE

PATTERN = *NONE / list-poss (8) : <c-string_1 .. 256_with-lower-case>
Angabe eines oder mehrerer Suchmuster. Fehlt die Angabe PATTERN werden alle JV-Änderungen per Trap gemeldet.
Es sind folgende Wildcard-Angaben zulässig:

? : ersetzt ein beliebiges Zeichen
* : ersetzt eine beliebig lange Folge von Zeichen
[s] : ersetzt genau ein Zeichen aus der Zeichenkette s
[c1 - c2]: ersetzt ein beliebiges Zeichen aus dem Bereich von c1 bis c2
Das Zeichen "\" (Backslash) muss zur Entwertung der Sonderzeichen angegeben werden.
Es wird zwischen Groß- und Kleinschreibung unterschieden.
Standardwert: *NONE

WEIGHT= 0 / <integer 0 .. 999>
Gewichtung der für den Application Monitor Subagenten spezifischen Traps. Beim Senden eines Traps versorgt der Application Monitor Subagent beim gerischen Trap das Trap-Objekt *appMonWeight* und die Trap-Nummer mit dem angegebenen Wert (siehe Abschnitt „Trap-Struktur“ auf Seite 184 im Kapitel „Funktionen des BASIC-AGENT“).
Standardwert: 0

ACKNOWLEDGE = *NO / *YES
Angabe, ob der Trap bestätigt werden muss. Es können nur Application Monitor-spezifische Traps bestätigt werden.
Standardwert: *NO

DEFINE-OBJECT

Logisch zusammengehörige Bestandteile eines Prozesses (Anwendungen, Protokolldateien, Subsysteme und Jobvariablen) können mit der Anweisung DEFINE-OBJECT in einer Gruppe (Objekt) zusammengefasst werden. Alle in der DEFINE-OBJECT-Anweisung genannten Elemente müssen mit den entsprechenden ADD...-Anweisungen ebenfalls in der Konfigurationsdatei definiert werden.

```
//DEFINE-OBJECT

OBJECT-NAME = <composed-name_1 .. 8_with-underscore>
, BCAM-APPLICATION = *NONE / list-poss(5): <composed_name_1 .. 54_with-underscore>
, USER-APPLICATION = *NONE / list-poss(5): <composed_name_1 .. 54_with-underscore>
, DCAM-APPLICATION = *NONE / list-poss(5): <name_1 .. 8>
, LOG-FILE = *NONE / list-poss(5): <filename_1 .. 54>
, SUBSYSTEM = *NONE / list-poss(5): <structured-name_1 .. 8>
, JV = *NONE / list-poss(10): <filename_1 .. 54>
, MONITORING-TIME = *ALWAYS / *INTERVAL (...)
    *INTERVAL ( ...)
        , START-TIME = hh:mm
        , STOP-TIME = hh:mm
        , EXCEPT-DAYS = *NONE / list-poss(6): MON / TUE / WED / THU / FRI / SAT / SUN
, ACKNOWLEDGE= *NO / *YES
```

OBJECT-NAME = <composed-name_1 .. 8_with-underscore>
Name des Objekts.

BCAM-APPLICATION = *NONE / list-poss(5): <composed_name_1 .. 54_with-underscore>
BCAM-Anwendungen, die zu diesem Objekt gehören.
Standardwert: *NONE

USER-APPLICATION = *NONE / list-poss(5): <composed_name_1 .. 54_with-underscore>
Benutzeranwendungen, die zu diesem Objekt gehören.
Standardwert: *NONE

DCAM-APPLICATION = *NONE / list-poss(5): <name_1 .. 8>
DCAM-Anwendungen, die zu diesem Objekt gehören.
Standardwert: *NONE

LOG-FILE = *NONE / list-poss(5): <filename_1 .. 54>
Protokolldateien, die zu diesem Objekt gehören.
Standardwert: NONE

SUBSYSTEM = *NONE / list-poss(5): <structured-name_1 .. 8>
Subsysteme, die zu diesem Objekt gehören.
Standardwert: *NONE

JV = *NONE / list-poss(10): <filename_1 .. 54>
Job-Variablen, die zu diesem Objekt gehören.

MONITORING-TIME = *ALWAYS / *INTERVAL (...)
spezifiziert den Zeitraum der Überwachung.
Standardwert: *ALWAYS

***INTERVAL (...)**
spezifiziert das Überwachungsintervall. Wenn STOP-TIME größer als START-TIME ist, zählen bei der Überprüfung der EXCEPT-DAYS die Stunden nach Mitternacht zum vorherigen Tag.

Beispiel:

Die Überwachungszeit erstreckt sich von 20:00 bis 3.00 außer Samstag und Sonntag. Die Überwachung endet daher am Samstag um 3:00 morgens und beginnt wieder am Montag um 20:00 abends.

START-TIME = HH:MM
Zeitpunkt, ab dem das Objekt überwacht werden soll.

STOP-TIME = HH:MM
Zeitpunkt, bis zu dem das Objekt überwacht werden soll.

EXCEPT-DAYS = *NONE / list-poss(6): MON / TUE / WED / THU / FRI / SAT / SUN
Wochentage, an denen das Objekt nicht überwacht werden soll.
Standardwert: *NONE

ACKNOWLEDGE= *NO / *YES
Angabe, ob der Trap bestätigt werden muss.
Standardwert: *NO

Beispiel: Überwachung eines MAREN-Systems

Ein MAREN-System besteht u.a. aus folgenden Komponenten:

– Subsystem MAREN
– Steuerprogramm MARENCP
– automatische Freibandzuweisung MARENUCP

Darüber hinaus wird jede von der automatischen Freibandzuweisung reservierte VSN in der Jobvariablen TAPE.FILE.MAREN hinterlegt.

Folgende Definition eines Objekts „MAREN“ fasst diese Komponenten zusammen:

```
//DEFINE-OBJECT OBJECT-NAME = MAREN
//, USER-APPLICATION = (MARENCP, MARENUCP)
//, SUBSYSTEM = MAREN
//, JV = TAPE.FILE.YES
```

DEFINE-TRAP-FORMAT

Die Anweisung DEFINE-TRAP-FORMAT legt das Trap-Format für den Application Monitor Subagenten fest.

//DEFINE-TRAP-FORMAT
TYPE = list-poss(2) **<u>*GENERIC</u>** / **<u>*TVCC</u>**

TYPE = list-poss(2) <u>*GENERIC</u> / *TVCC
legt das Trap-Format fest.
GENERIC:

Es wird das Application Monitor-spezifische Trap-Format verwendet.
TVCC: Es wird das TV-CC-spezifische Trap-Format verwendet.
Standardwert: *GENERIC

3.3.4 Konfiguration des Console Monitor Subagenten

Der Console Monitor zur Überwachung der Konsolschnittstelle erlaubt den Empfang von BS2000-Konsolmeldungen auf der Management-Station sowie die Eingabe von BS2000/OSD-Konsolkommandos. Über UCON erhält der Console Monitor den Zugriff auf die Konsolkommandos von $CONSOLE. Folgende Vorbereitungen sind notwendig, um dem Console Monitor den Zugriff auf die BS2000/OSD-Konsole zu ermöglichen:

Einrichten der Operator-Kennung <operator-id>.

```
/ADD-USER USER-ID=<operator-id>,                              -
          PROTECTION-ATTRIBUTE=*PAR(LOGON-PASSWORD=<pass>),   -
          ACCOUNT-ATTRIBUTES=*PAR(ACCOUNT=<account-nr>)
```

Die hier festgelegten LOGON-Attribute müssen in der Start-Anweisung des Console Monitor Subagenten (siehe START-SNMP-CONSMON auf Seite 136) angegeben werden.

Für den Betrieb mit SECOS muss zusätzlich noch die Zugangsberechtigung für die Operator-Kennung zu $CONSOLE freigeschaltet werden:

```
/MOD-LOGON-PROTECTION USER-IDENTIFICATION=<operator-id>,     -
                      OPERATOR-ACCESS-PROG=*YES(PASSWORD-CHECK=*YES)
```

Der Klasse-2-Systemparameter NBBAPRIV muss auf den Standardwert N eingestellt sein.

3.3.4.1 Definition von Meldungsfiltern

Bei der Auswahl von Meldungen verwendet der Console Monitor Subagent zwei Filtervarianten:

– positiver Meldungsfilter
  wählt Meldungen aus, die an die Management-Station geschickt werden sollen.

– negativer Meldungsfilter
  wählt Meldungen aus, die nicht an die Management-Station geschickt werden dürfen.

Positiver Meldungsfilter

Für die Auswahl der Meldungen, die an die Management-Station geschickt werden, stehen zwei Filtermöglichkeiten zur Verfügung:

– Routingcode (ist jeder Konsolmeldung zugeordnet)
– Meldungsschlüssel (identifiziert jede Meldung eindeutig)

Auswahlkriterium Trap-Format

Das Trap-Format wird in der Meldungsfilter-Datei festgelegt:

```
TRAP-FORMAT=GENERIC / TVCC / ALL
```

GENERIC
: Es wird nur der für den Application Monitor-spezifische Trap verwendet. GENERIC ist Standardwert

TVCC
: Es wird nur TVCC-Trap-Format verwendet.

ALL
: Es werden beide Trap-Formate verwendet.

Auswahlkriterium Routingcode

Jede Meldung ist einem bestimmten Routingcode zugeordnet. Operator-Rollen enthalten die Routingcodes derjenigen Meldungen, die an die Management-Station geschickt werden sollen. Die Operator-Rollen werden in der Start-Anweisung des Console Monitor (siehe START-SNMP-CONSMON auf Seite 136) angegeben. Die folgenden Anweisungen zeigen, wie Operator-Rollen erzeugt und der Operator-Kennung zugeordnet werden. Voraussetzung für das Absetzen der folgenden Anweisungen ist das Privileg SECURITY-ADMINISTRATION, das standardmäßig die Benutzerkennung SYSPRIV hat.

Erzeugen der Operator-Rolle:

```
/CREATE-OPERATOR-ROLE OP-ROLE=<op-role-name>,              -
                      ROUTING-CODES=.......
```

Zuordnung der Operator-Rollen zur Operator-Kennung:

```
/MODIFY-OPERATOR-ATTR USER-ID=<operator-id>,               -
                      ADD-OPERATOR-ROLE=(<op-role-name1>,...,<op-role-namex>)
```

Bei Einsatz von SECOS muss außerdem der Operator-Kennung das Privileg OPERATING zugewiesen werden:

```
/SET-PRIVILEGE PRIV=OPERATING,USER-ID=<operator-id>
```

Auswahlkriterium Meldungsschlüssel

Die Meldungsschlüssel derjenigen Meldungen, die der Management-Station zugestellt werden sollen, werden in der positiven Meldungsfilter-Datei hinterlegt. Drei Filtermöglichkeiten stehen mit den folgenden Anweisungen zur Verfügung:

– *msgid*,
– *QUESTION*
– *TYPIO*

Der Name der Meldungsfilter-Datei wird dem Console Monitor bei dessen Start durch die Angabe MSG-FILTER mitgeteilt. Im laufenden Betrieb kann der Dateiname in dem MIB-Objekt *consMonMsgFilter* eingetragen werden.

Fehlt die Angabe einer Meldungsfilter-Datei beim Start des Console Monitor, werden alle Meldungen ausgegeben, deren Routingcode in der Operator-Rolle angegeben ist.

Enthält die Meldungsfilter-Datei keine bzw. keine gültigen Meldungsschlüssel, dann werden der Management-Station keine Traps zugestellt. Eine leere Meldungsfilter-Datei einzurichten ist nur dann sinnvoll, wenn Sie gleichzeitig den HIPLEX OP Agenten zur Überwachung der BS2000/OSD-Konsolmeldungen im Einsatz haben, aber auf die Eingabe von Konsolkommandos mithilfe des Console Monitor nicht verzichten wollen.

Für die Meldungsfilter-Datei gelten folgende Namenskonventionen:

/BS2/<datei>	BS2000/OSD-Datei
[:<catid>:]$<userid>.<datei>	BS2000/OSD-Datei
*POSIX(<datei>)	POSIX-Datei
/<pfad>/<datei>	POSIX-Datei
<datei>	in diesem Fall ist ausschlaggebend, in welcher Umgebung der Subagent gestartet wurde.

Aufbau des positiven Meldungsfilters

msgid

```
<msgid [wgt] [SOURCE=src] [DEVICE=dev] [ACKNOWLEDGE=YES]>
```

msgid Angabe eines Meldungsschlüssels.

Bei der Angabe von Meldungsschlüsseln sind folgende Wildcard-Angaben zulässig:

? :	ersetzt ein beliebiges Zeichen
* :	ersetzt eine beliebig lange Folge von Zeichen
[s] :	ersetzt genau ein Zeichen aus der Zeichenkette s
[c1 - c2]:	ersetzt ein beliebiges Zeichen aus dem Bereich von c1 bis c2

Das Zeichen "\" (Backslash) muss zur Entwertung der Sonderzeichen angegeben werden. Es wird zwischen Groß- und Kleinschreibung unterschieden.

wgt Angabe eines Meldungsgewichts (weight). Den Meldungsschlüsseln kann ein Gewicht zugeordnet werden. Dieses Gewicht wird im Trap-String der eigentlichen Meldung vorangestellt. Damit hat der Anwender die Möglichkeit, die Wichtigkeit der Meldungen selbst einzustellen und entsprechend an der Management-Station darzustellen. Fehlt die Gewichtsangabe, erhält der Meldungsschlüssel standardmäßig den Wert 0.

Die Angabe wird als Integer mit dem Wertebereich 0 - 999 erwartet.

src Angabe eines Quellennamens (source). Im Trap-String wird Quelle mit BS2-<source> versorgt. Fehlt diese Angabe, wird der Standardwert *BS2Console* eingesetzt. Mit dieser Angabe können Sie einen Alarm gezielt auf ein Objekt im Netzbild lenken. Die Angabe erfolgt alphanumerisch in der Länge 1 - 12 (siehe Seite 198).

dev Ist ein DEVICE angegeben, sendet der Console Monitor Subagent diesen Trap mit der DEVICE-Angabe als Community (siehe Seite 198).

ACKNOWLEDGE=YES

Durch die Angabe ACKNOWLEDGE=YES wird dem Subagenten angezeigt, dass dieser Trap bestätigt werden muss.

QUESTION

Question filtert alle Meldungen heraus, die eine Frage beinhalten, d.h. die eine Antwort erwarten.Tritt eine Frage auf, überprüft der Console Monitor zuerst, ob ein Muster der QUESTION-Einträge passt. Ist das nicht der Fall, werden dem Meldungstyp entsprechend die MSGID-Einträge oder die TYPIO-Einträge durchsucht.

```
<QUESTION [wgt] [SOURCE=src] [DEVICE=dev] [PATTERN=/pat1[/..patx]]
[ACKNOWLEDGE=YES]>
```

QUESTION Meldungsschlüssel einer Konsolanfrage

wgt siehe oben

src siehe oben

dev siehe oben

pat Angabe eines oder mehrerer Suchmuster (pattern).

? :	ersetzt ein beliebiges Zeichen
* :	ersetzt eine beliebig lange Folge von Zeichen
[s] :	ersetzt genau ein Zeichen aus der Zeichenkette s
[c1 - c2]:	ersetzt ein beliebiges Zeichen aus dem Bereich von c1 bis c2

Das Zeichen "\" (Backslash) muss zur Entwertung der Sonderzeichen angegeben werden. Es wird zwischen Groß- und Kleinschreibung unterschieden.

ACKNOWLEDGE=YES siehe oben

Beispiel:

`<QUESTION PATTERN=[0-9]*>` Auswahl aller Fragen, die mit einer Ziffer beginnen.

TYPIO

Eine Sonderstellung nehmen so genannte TYPE I/O-Meldungen ein. Zu den TYPE I/O-Meldungen zählen beispielsweise Nachrichten, die mit /SEND-MSG der BS2000/OSD-Konsole zugestellt werden. Die Weiterleitung der TYPE I/O-Meldungen als SNMP-Trap wird ebenfalls über die Meldungsfilter-Datei gesteuert. Der Eintrag für eine TYPE I/O-Meldung ist folgendermaßen aufgebaut:

```
<TYPIO [wgt] [SOURCE=src] [DEVICE=dev] [PATTERN=/pat1[/..patx]] [ACKNOWLEDGE=YES]>
```

wgt siehe oben

src siehe oben

dev siehe oben

pat siehe oben

ACKNOWLEDGE=YES siehe oben

Beispiel:

```
<TYPIO PATTERN=/*abc*/xyz>
<TYPIO PATTERN=/Hallo*>
<TYPIO PATTERN=/?\?*>
```

Alle TYPE I/O-Meldungen, die den String "abc" enthalten, nur aus "xyz" bestehen, mit "Hallo" beginnen oder an zweiter Stelle ein Fragezeichen haben, werden als Trap der Management-Station zugestellt.

Ein Beispiel für einen Meldungsfilter finden Sie in der Bibliothek SINLIB.SBA-BS2.050.

Negativer Meldungsfilter

Für den Console Monitor Subagenten wird auch ein negativer Meldungsfilter angeboten. Die Meldungsschlüssel derjenigen Konsolmeldungen, die nicht an die Management-Station durchgereicht werden sollen, werden in der negativen Meldungsfilter-Datei hinterlegt. Fragen können nicht unterdrückt werden. Das MIB-Objekt *consMonNegMsgFilter* verweist auf den Namen der negativen Meldungsfilter-Datei. Der Name der negativen Meldungsfilter-Datei wird beim Start des Console Monitor mit dem Operanden SUPPRESS-MSG-FILE definiert. Diese Definition kann nur beim Start des Console Monitor, aber nicht im laufenden Betrieb geändert werden.

Die Länge des Eintrags darf maximal 179 Zeichen betragen.

```
<msgid> [<msgid> ... <msgid>]
```

3.3.4.2 Ändern der Meldungsfilter-Datei im laufenden Betrieb

Änderungen der aktuellen Meldungsfilter-Datei im laufenden Betrieb können mit der Console Monitor-Anwendung entweder durch Setzen des Objekts *consMonMsgFilter* oder per Kommando vorgenommen werden.

```
/START-CONSMONCMD
       x "readConfig <filename>"
```

POSIX:

```
consmoncmd x "readConfig <filename>"
```

Bei Syntaxfehlern in der Meldungsfilter-Datei *consMonMsgFilter* wird mit der ursprünglichen Meldungsfilter-Datei weitergearbeitet.

3.3.5 Konfiguration des AVAS-Subagenten

Der AVAS-Subagent erhält über die beim Start anzugebende GENPAR-Datei die Information, welches AVAS-System zu überwachen ist. Der Subagent nutzt drei Wege zur Kommunikation mit dem AVAS-System:

– Zur Überwachung der zentralen Prozesse werden die von AVAS belegten Jobvariablen ausgewertet. Da dies keine Monitor-Jobvariablen sind, sollten Sie zumindest einige der wichtigen Prozesse mit MONJVs starten und diese vom Application Monitor überwachen lassen.

– Die Informationen zu Netzen und Strukturelementen erhält der Subagent über eine Programmschnittstelle, die ihrerseits über Inter-Task-Kommunikation mit den AVAS-Verarbeitungsprozessen in Verbindung steht.

– Zur Vermeidung inperformanter Zugriffe kann der Subagent über einen AVAS-RZ-Exit angesprochen und so über Fehlerzustände informiert werden.

Beim ersten Aufruf der Programmschnittstelle werden vom AVAS-Schnittstellenmodul weitere Module nachgeladen. Die Nachlade-Bibliothek wird automatisch über IMON ermittelt.

Wenn AVAS nicht über IMON installiert wurde, muss in der Startprozedur `START.AVAS` in der Bibliothek `SYSSPR.SSC-BS2.050` der Defaultpath `$TSOS.SYSLNK.AVAS.030` angepasst werden.

Folgende Angaben bezieht der Subagent aus der Generierungsdatei GENPAR:

AVAS-System-ID	Identifikation des AVAS-Systems.
JVPLAMZD	Jobvariable zur Überwachung der PLAM-ZD.
JVUPAMZD	Jobvariable zur Überwachung der UPAM-ZD.
JVCENTRAL	Jobvariable zur Überwachung des Zentralprozesses.
AVAK	Namen der Ablaufsteuerungen und der Jobvariablen zur Überwachung der Ablaufsteuerungen.
USER	Name und Passwort des Benutzers, als der sich der Subagent an der Programmschnittstelle anmelden soll.

AVAS-System-ID und USER

AVAS-System-ID und USER werden für das LOGON über die Programmschnittstelle ausgewertet. Die AVAS-System-ID identifiziert das zu überwachende AVAS-System. Dem Eintrag USER werden die Kennung und das Passwort entnommen. Diese LOGON-Daten bestimmen u.a. den Berechtigungsumfang. Die vom Subagenten genutzte Kennung wird entweder durch USER-Eintrag SNMPUSER in der Datei GENPAR bestimmt, oder es wird der erste eingetragene USER ausgewählt.

Kontrollierende Jobvariablen

Die Jobvariablen JVPLAMZD, JVUPAMZD, JVCENTRAL und die der Ablaufsteuerungen AVAK dienen der Überwachung der AVAS-Verarbeitungsprozesse. Es muss sichergestellt werden, dass die USERID, die den Agenten aufruft, Leseberechtigung für die Jobvariablen hat. Eventuell müssen dazu in die Datei GENPAR die kontrollierenden Jobvariablen mit der Angabe :<catid>:$<userid> eingetragen werden:

```
:<catid>:$<userid>.<jv-name>
```

Die vom AVAS-System verwendete Systemparameterdatei SYSPAR muss aus der vom Subagenten genutzten Datei GENPAR erzeugt werden.

Die für das LOGON genutzte Kennung sollte den vollen Berechtigungsumfang besitzen. Die Berechtigung zum Zugang über die Programmschnittstelle READ-AVAS-LIBRARY muss gegeben sein.

AVAS-RZ-Exit

Wenn Sie schnell über Fehlerzustände informiert werden wollen, können Sie einen speziellen AVAS-SNMP-Exit an den AVAS-Exit AVEX0001 anschließen. Dazu ist es notwendig, den in der Bibliothek SYSLNK.SSC.BS2-050 vorbereiteten Modul SNMPAV in die Exits einzubinden. In der Bibliothek SINLIB.SSC.BS2-050 steht zum Binden die Prozedur P.LNK.AVEX bereit, die Prozedur muss ggf. noch angepasst werden. Der Modul SNMPAV muss sowohl mit dem Modul AV03EXIT als auch mit AV04EXIT gebunden werden. Sollten am Exit AVEX0001 bereits eigene RZ-Routinen aufgerufen werden, empfiehlt es sich SNMPAV immer als Erstes anzuspringen, da SNMPAV den Returncode des Exits auf X’00’ (Ok, Satz wird protokolliert) setzt. Der Exit sollte nur in diejenigen AVAS-Systeme eingebunden werden, die überwacht werden sollen.

3.3.6 Konfiguration des OMNIS-Subagenten

Für den OMNIS-Subagenten muss eine Konfigurationsdatei vorbereitet werden, die die Namen mit dem/den zu startenden OMNIS/en enthält. OMNIS-Namen müssen mit Leerzeichen auf acht Stellen aufgefüllt werden. Die Konfigurationsdatei wird mit <*filename*> beim Startkommando zugewiesen (siehe Seite 150).

Im OMNIS-Handbuch "Administration und Programmierung" finden Sie in den Abschnitten "Deklaration des SNMP-Managements in OMNIS" und "SNMP-Überwachung in OMNIS" eine Beschreibung der in OMNIS notwendigen Konfigurationsarbeiten.

3.3.7 Konfiguration des SESAM-Subagenten

Der Anwender muss dem SESAM-Subagenten eine Konfigurationsdatei zur Verfügung stellen. Diese Konfigurationsdatei enthält Informationen über die an diesem Rechner hängenden SESAM-Datenbanken und die SESAM-DBHs, mit denen diese Datenbanken prozessiert werden. Darüberhinaus werden in der Konfigurationsdatei Optionen für den Subagenten und den Start des SESAM-Monitor-Pools (SESMON) hinterlegt.

Die Konfigurationsdatei muss im BS2000/OSD katalogisiert sein. Die Anweisungen werden im SDF-Format eingegeben. Dem Subagenten wird der Name der Datei beim Start mitgegeben. Syntaxfehler in der Datei führen zum Abbruch des Subagenten.

Im laufenden Betrieb kann die Konfigurationsdatei einerseits per BS2000/OSD-Kommando geändert werden:

```
/START-SESAMCMD
    x  "readConfig <filename>"
```

andererseits ab BS2000/OSD V2.0 per POSIX-Kommando:

```
sesamcmd x "readConfig <filename>"
```

Tritt hierbei ein Fehler auf, wird die alte Datei beibehalten.

Ein Beispiel für eine Konfigurationsdatei finden Sie in der Bibliothek SINLIB.SSC-BS2.50.

3.3.7.1 Kommunikation zwischen dem SESAM-Subagenten und dem SESAM/SQL-Server

Zur Erlangung einiger der vom SESAM-Subagenten bereitgestellten Informationen (Teile der *rdbmsSrvParamTable*, *rdbmsRelTable*, Traps) kommuniziert dieser über die SESAM-Programmschnittstelle mit dem bzw. den entsprechenden SESAM/SQL-Servern.

Über die SNMP-Optionen CONFIGURATION-NAME und DBH-NAME wird hierzu die Verbindung zwischen dem SESAM-Subagenten und dem bzw. den entsprechenden SESAM/SQL-Servern hergestellt.

Dabei sind folgende zwei Fälle zu unterscheiden:

1. Die durch die SNMP-Option CONFIGURATION-NAME bezeichnete SESAM-Konfiguration ist eine nicht verteilte Konfiguration, also ohne SESAM-DCN.

   In diesem Fall kann der SESAM-Subagent nur mit einem einzigen SESAM/SQL-DBH über die Programmschnittstelle kommunizieren. Dieser SESAM/SQL-DBH wird dann über die beiden SNMP-Optionen CONFIGURATION-NAME und DBH-NAME identifiziert.

   Die über die Programmschnittstelle gewonnenen Informationen können dann vom SESAM-Subagenten nur für diesen SESAM/SQL-DBH bereitgestellt werden. Alle anderen Informationen kann der SESAM-Subagent auch für alle übrigen durch das Kommando ADD-SERVER-RECORD angegebenen SESAM/SQL-DBHs bereitstellen.

2. Die durch die SNMP-Option CONFIGURATION-NAME bezeichnete SESAM-Konfiguration ist eine verteilte Konfiguration, also mit SESAM-DCN

   In diesem Fall kann der SESAM-Subagent über die Programmschnittstelle mit dem über die beiden SNMP-Optionen identifizierten SESAM/SQL-DBH kommunizieren und mit allen SESAM/SQL-DBHs, zu denen ein Zugriffspfad in der Verteiltabelle dieser SESAM-Konfiguration beschrieben ist.

   Sinnvollerweise sollten in dieser Verteilregel alle Datenbanken mit ihren Zugriffspfaden ausgewiesen sein, die durch das Kommando ADD-SERVER-RECORD in dieser SESAM-SNMP-Konfigurationsdatei angegeben sind und nicht am DBH-NAME hängen.

   Analog zum obigen Fall gilt: Die über die Programmschnittstelle gewonnenen Informationen können vom SESAM-Subagenten nur für DBH-NAME und diejenigen SESAM/SQL-DBHs bereitgestellt werden, zu denen ein Zugriffspfad in der Verteiltabelle dieser SESAM-Konfiguration beschrieben ist. Alle anderen Informationen kann der SESAM-Subagent auch für alle übrigen durch ADD-SERVER-RECORD-Kommandos angegebenen SESAM/SQL-DBHs bereitstellen.

3.3.7.2 Anweisungen für die Konfigurationsdatei

Die folgenden Anweisungen müssen in die Konfigurationsdatei eingetragen werden.

SET-SNMP-OPTIONS

Mit der Anweisung SET-SNMP-OPTIONS werden Optionen für den SESAM-Subagenten festgelegt.

//SET-SNMP-OPTIONS
CACHE-TIME = 120 / <integer 1..9999> , **CHECK-TIME** = 120 / <integer 1..9999> , **CONFIGURATION-NAME** = ***BLANK** / <alphanum-name1..1> , **DBH-NAME** = ***BLANK** / <alphanum-name1..1>

CACHE-TIME=120 / <integer 1..9999>
Festlegung, wie lange die Daten im Cache des Subagenten gültig sind. Die Angabe erfolgt in Sekunden, der Standardwert beträgt 120 Sekunden.

CHECK-TIME=120 / <integer 1..9999>
Das Zeitintervall, in dem die Datenbanken vom Subagenten überprüft werden. Der Standardwert beträgt 120 Sekunden.

CONFIGURATION-NAME=*BLANK / <alphanum-name1..1>
Name der SESAM-Konfiguration, in der der SESAM-Subagent abläuft.

DBH-NAME=*BLANK / <alphanum-name1..1>
Default-DBH für den SESAM-Subagenten.

SET-SESMON-PARAMETERS

Mit der Anweisung SET-SESMON-PARAMETERS legen Sie die Start-Parameter für den SESMON fest.

//SET-SESMON-PARAMETERS
CRTE-LIBRARY = <filename_1..54>
, **MODULE-LIBRARY** = <filename_1..54>
, **SYSOUT** = ***PRIMARY** / <filename_1..54>
, **SYSLST** = ***PRIMARY** / <filename_1..54>
, **REFRESH-TIME** = 120 / <integer 1..999>

CRTE-LIBRARY=<filename_1..54>
Name der CRTE-Bibliothek, die verwendet werden soll.

MODULE-LIBRARY=<filename_1..54>
Name der Modulbibliothek, die SESMON enthält.

SYSOUT=*PRIMARY / <filename_1..54>
Zuordnung von SYSOUT. *PRIMARY ist die Default-Einstellung.

SYSLST=*PRIMARY / <filename_1..54>
Zuordnung von SYSLST. *PRIMARY ist die Default-Einstellung.

REFRESH-TIME=120 / <integer 1..999>
Zeitintervall in Sekunden, nach dem die von SESMON bereitgestellten Daten aktualisiert werden. Standardwert: 120 Sekunden

ADD-DATA-BASE-RECORD

Mit ADD-DATA-BASE-RECORD wird die Datenbank benannt, die vom SESAM-Subagenten überwacht werden soll.

```
//ADD-DATA-BASE-RECORD

LOGICAL-NAME = <filename_1..18-without-all>
, PHYSICAL-NAME = <filename_1..18-without-all>
, USER-ID = <name_1..8>
, CONTACT = <c-string 1..64-with-low>
, SERVER_ID = *NONE / *PARAMETERS(...)
    *PARAMETERS(...)
        CONFIGURATION-NAME = *BLANK / <alphanum-name 1..1>
        , DBH-NAME = *BLANK / <alphanum-name 1..1>
        , VERSION = <product-version>
```

LOGICAL-NAME=<filename_1..18-without-all>
Logischer Name der Datenbank

PHYSICAL-NAME=<filename_1..18-without-all>
Physischer Name der Datenbank.

USER-ID=<name_1..8>
Kennung, unter der die Datenbank katalogisiert ist.

CONTACT=<c-string 1..64-with-low>
Identifikation der Kontaktperson, die für diese Datenbank zuständig ist.

SERVER_ID=*NONE / *PARAMETERS(...)
Identifikation des zugehörigen Servers

***PARAMETERS(...)**

CONFIGURATION-NAME=*BLANK / <alphanum-name 1..1>
Name der SESAM-Konfiguration, in der der SESAM-Subagent abläuft.

DBH-NAME=*BLANK / <alphanum-name 1..1>
Default-DBH für den SESAM-Subagenten.

VERSION=<product-version>
Produktversion des zugehörigen Servers

ADD-SERVER-RECORD

ADD-SERVER-RECORD definiert den Datenbankserver, den der Subagent überwachen soll. Pro Konfiguration können maximal 10 Server überwacht werden.

```
//ADD-SERVER-RECORD

IDENTIFICATION = *PARAMETERS(...)
    *PARAMETERS(...)
        | CONFIGURATION-NAME = *BLANK / <alphanum-name1..1>
        | , DBH-NAME = *BLANK / <alphanum-name1..1>
        | , VERSION = <product-version>
, PRODUCT-NAME = <c-string 1..64-with-low>
, USER-ID = <name 1..8>
, CONTACT = <c-string 1..64-with-low>
, PASSWORD = <c-string 0..3>
```

IDENTIFICATION = *PARAMETERS(...)
Identifikation des Servers

***PARAMETERS(...)**

CONFIGURATION-NAME=*BLANK / <alphanum-name1..1>
Name der SESAM-Konfiguration, in der der SESAM-Subagent abläuft.

DBH-NAME=*BLANK / <alphanum-name1..1>
Default-DBH für den SESAM-Subagenten.

VERSION = <product-version>
Produktversion des Servers

PRODUCT-NAME = <c-string 1..64-with-low>
Produktname des Servers

USER-ID = <name 1..8>
Kennung, unter der der Server abläuft.

CONTACT = <c-string 1..64-with-low>
Identifikation der Kontaktperson, die für diesen Datenbankserver zuständig ist.

PASSWORD = <c-string 0..3>
Kennwort für Administrationsanweisungen.

ADD-SERVER-PARAMETER

Mit ADD-SERVER-PARAMETER werden die Parameter für einen Datenbankserver festlegt. Die genaue Beschreibung der Parameter entnehmen Sie bitte dem Handbuch SESAM/SQL-Server Datenbankbetrieb ("DBH-Startanweisungen und -optionen").

```
//ADD-SERVER-PARAMETER

NAME= *ACCOUNTING / *ADMINISTRATOR / *COLUMNS / *CURSOR-BUFFER / *DBH-IDENTIFICATION /
        *LOG-FILE-OPEN / *MSG-OUTPUT / *OLD-TABLE-CATALOG / *REQUEST-CONTROL /
        *RESIDENT-BUFFERS  / *RETRIEVAL-CONTROL /  *SECURITY /  *SERVICE-TASKS /
        *SESSION-LOGGING-ID / *SPACES / *SQL-DATABASE-CATALOG / *SQL-SUPPORT /
        *STACK-POOL / *SUBORDERS / *SYSTEM-DATA-BUFFER / *THREADS /
        *TRANSACTION-SECURITY / *TRANSFER-CONTAINER / *USER-DATA-BUFFER / *USERS /
        *WORK-CONTAINER / *TALOG-SUPPORT / *WALOG-SUPPORT / *SESWORK-SUPPORT /
        *CURSOR-MEDIA-SUPPORT-1 / *CURSOR-MEDIA-SUPPORT-2 /
        *CURSOR-MEDIA-SUPPORT-3 / *CURSOR-MEDIA-SUPPORT-4 / *CURSOR-MEDIA-SUPPORT-5
, COMMENT = <c-string 1..128-with-low>
```

NAME = *ACCOUNTING / *ADMINISTRATOR / *COLUMNS / *CURSOR-BUFFER /
***DBH-IDENTIFICATION / *LOG-FILE-OPEN / *MSG-OUTPUT /**
***OLD-TABLE-CATALOG / *REQUEST-CONTROL /**
***RESIDENT-BUFFERS / *RETRIEVAL-CONTROL / *SECURITY /**
***SERVICE-TASKS / *SESSION-LOGGING-ID / *SPACES /**
***SQL-DATABASE-CATALOG / *SQL-SUPPORT / *STACK-POOL /**
***SUBORDERS / *SYSTEM-DATA-BUFFER / *THREADS /**
***TRANSACTION-SECURITY / *TRANSFER-CONTAINER /**
***USER-DATA-BUFFER / *USERS / *WORK-CONTAINER /**
***TALOG-SUPPORT / *WALOG-SUPPORT / *SESWORK-SUPPORT /**
***CURSOR-MEDIA-SUPPORT-1 / *CURSOR-MEDIA-SUPPORT-2 /**
***CURSOR-MEDIA-SUPPORT-3 / *CURSOR-MEDIA-SUPPORT-4 /**
***CURSOR-MEDIA-SUPPORT-5**

Bezeichnung des Parameters.

COMMENT = <c-string 1..128-with-low>
Beschreibung des Parameters.

3.3.8 Konfiguration des Subagenten für das Storage-Management

Mit dem Storage Management Subagenten können Platten und Pubsets überwacht werden.

Die Konfiguration erfolgt über eine Input-Datei:

– Für die Überwachung des Saturation-Levels einzelner Public Volumes Sets (Pubsets) müssen die betreffenden PVS in der Input-Datei des Subagenten spezifiziert werden. Dies erfolgt mit der ADD-PUBSET-RECORD-Anweisung.

– Für die Überwachung des Reconfiguration State einzelner Platten müssen die betreffenden Platten in der Input-Datei des Subagenten spezifiziert werden. Dies erfolgt mit der ADD-DISK-RECORD-Anweisung.

– Mit der Anweisung //REMARK können Kommentare in der Konfigurationsdatei hinterlegt werden.

– Die letzte Anweisung in der Konfigurationsdatei sollte die Anweisung //END sein. Alle Anweisungen, die auf die //END-Anweisung folgen, werden ignoriert.

– Maximal können 10 Pubsets oder Platten überwacht werden.

ADD-PUBSET-RECORD - Hinzufügen eines zu überwachenden Pubsets

//ADD-PUBSET-RECORD
PUBSET= <cat_id 1..4> **, CHECK**=**SATURATION-LEVEL** **, TRAP-COMMUNITY**= ***STORAGE** / ***PUBSET-NAME** / <c-string 1..64>

PUBSET=<cat_id 1..4>
CAT-ID des Pubsets, das überwacht werden soll.

CHECK=SATURATION-LEVEL
Objekt, das überwacht werden soll; derzeit ist nur die Angabe SATURATION-LEVEL möglich (Standardwert).

TRAP-COMMUNITY=*STORAGE / *PUBSET-NAME / <c-string 1..64>
Community-String, mit dem der Trap verschickt wird.
Bei Angabe von *PUBSET wird die <cat-id> als Community-Name verwendet.
Bei Angabe von <c-string 1..64> wir dieser String als Community-Name verschickt.
Standardwert: *STORAGE

ADD-DISK-RECORD - Hinzufügen einer zu überwachenden Platte

//ADD-DISK-RECORD
DISK-MN =<alphanum-name 1..4> **, CHECK=RECONFIGURATION-STATE** **, TRAP-COMMUNITY**= ***STORAGE** / ***DISK-MN** / <c-string 1..64>

DISK-MN=<alphanum-name 1 ..4>
mnemotechnischer Name des Geräts, das überwacht werden soll

CHECK=RECONFIGURATION-STATE
Objekt, das überwacht werden soll; derzeit ist nur die Angabe RECONFIGURATION-STATE möglich (Standardwert).

TRAP-COMMUNITY=*STORAGE / *DISK-MN / <c-string 1..64>
Community-String, mit dem der Trap verschickt wird.
Bei Angabe von *DISK-MN wird der bei DISK-MN angegebene Name als Community-Name verwendet.
Bei Angabe von <c-string 1..64> wird dieser String als Community-Name verschickt.
Standardwert: *STORAGE

3.3.9 Konfiguration des *open*UTM-Subagenten (SSA-OUTM-BS2)

Der folgende Abschnitt beschreibt die Tätigkeiten, die zur Inbetriebnahme des *open*UTM-Subagenten notwendig sind.

3.3.9.1 Einsatzvorbereitung

Die Kommunikation zwischen dem Subagenten und einer UTM-Anwendung erfolgt über UTM-D-SP bzw. UPIC(BS2000) V1.1. UPIC benötigt für die Kopplung zwischen dem Subagenten und der UTM-Anwendung eine Side-Information-Datei (*upicfile*). Diese Datei muss gemäß UPIC V1.1 *upicfile* heißen und im BS2000/OSD katalogisiert sein. Der Eintrag in der *upicfile* besteht aus vier Teilen:

– einem Kennzeichen, in diesem Fall HD als Kennzeichen für eine Kopplung zwischen UPIC(BS2000) und UTM(BS2000),

– dem Symbolic Destination Name, der für die aktuell ausgewählte UTM-Anwendung mit SNMP4UTM vorbelegt ist,

– dem Partnernamen, definiert durch das MIB-Objekt *utmMainBCAMAppl* und

– dem Transaktionscode; diese Angabe ist nicht erforderlich, da der Subagent den Transaktionscode mit dem *Set_TP_Name* Aufruf angibt.

Die Datei *upicfile* ist unter BS2000/OSD eine editierbare Datei. Da es im BS2000/OSD kein <newline>-Zeichen gibt, wird das Zeilenende-Zeichen durch das Semikolon (";") dargestellt, siehe Beispiel. D.h. falls in einer editierten Zeile ein Semikolon steht, reagiert UPIC so, als ob die Zeile dort abgeschlossen wäre und interpretiert den Rest der Zeile als neue Zeile (bis zum nächsten ";"-Zeichen), das gilt auch für Kommentarzeilen.

Beispiel

Side Information Datei

```
*;
*remote partner applications;
*;
*symbolic destination names for (BS2000/OSD) application ZENTRBS2;
;
HDSNMP4UTM ZENTRBS2;
```

Der UTM-Subagent meldet sich mit dem lokalen Namen SNMPUPIC beim UPIC-Kommunikationssystem an. Der Name SNMPUPIC wird mit den KDCDEF-Anweisungen PTERM bzw. TPOOL als Kommunikationspartner der Anwendung definiert.

Jeder zu überwachenden Anwendung muss mit der Anweisung BCAMAPPL ein BCAM-Anwendungsname zugeordnet werden:

```
BCAMAPPL ZENTRBS2,T-PROT=ISO
```

Für jede Partneranwendung in der *upicfile* muss ein BCMAP-Eintrag gemacht werden:

```
/BCMAP FUNCT=DEFINE,SUBFUNCT=GLOBAL,NAME=(OSI,ZENTRBS2),ES=<BS2000/OSD-M.>
       ,PTSEL-I=(8,'ZENTRBS2 '),PTSEL-N=ZENTRBS2  *)
```

Der lokale Name des UPIC-Programms wird ebenfalls per BCMAP definiert:

```
/BCMAP FUNCT=DEFINE,SUBFUNCT=LOCAL,APPL=(OSI,SNMPUPIC)
       ,TSEL-I=(8,C'SNMPUPIC‘),TSEL-N=SNMPUPIC *)
```

*) PTSEL-N und TSEL-N sind nur dann notwendig, wenn sich UPIC(BS2000) und UTM(BS2000) auf einem Rechner befinden.

Da der *open*UTM-Subagent zum Absetzen von UTM-Administrationskommandos die entsprechende Berechtigung benötigt, muss in der LTERM-Anweisung eine UTM-Benutzerkennung angegeben werden, die mit STATUS=ADMIN oder PERMIT=ADMIN definiert ist.

Zur Überwachung von Anwendungen der *open*UTM Version ≥ 4.0 nutzt der UTM-Subagent das von UTM ausgelieferte Teilprogramm KDCWADMI. Dem Teilprogramm ist der TAC KDCWADMI zugeordnet. Die KDCDEF-Generierung muss in diesem Fall um zwei Anweisungen erweitert werden:

```
PROGRAM KDCWADMI,COMP=ILCS
TAC KDCWADMI,ADMIN=Y,PROGRAM=KDCWADMI
```

3.3.9.2 Ablaufumgebung

Im BS2000/OSD wird das UPIC-Programm über Jobvariablen gesteuert.
Dazu wertet UPIC folgende Jobvariablen aus:

Jobvariable	Linkname	Bedeutung
UPICPATH	*UPICPAT	Die Jobvariable UPICPATH bestimmt das Dateiverzeichnis, unter dem die Side Information Datei abgespeichert ist. Wenn die Jobvariable nicht gesetzt ist, wir die Datei unter dem aktuellen Dateiverzeichnis gesucht. Beim Start des Subagenten unter POSIX muss die Jobvariable UPICPATH mit dem Wert „BS2/$<userid>“ versorgt werden, da UPIC andernfalls versucht, die *upicfile* im POSIX-Dateisystem zu öffnen.
UPICTRACE	*UPICTRA	Die Jobvariable UPITRACE steuert die Trace-Erzeugung (siehe nächste Seite „Diagnoseunterlagen).
UPICLOG	*UPICLOG	Die Jobvariable UPICLOG legt den Namen der Logging-Datei fest. Fehlt diese Angabe, so lautet der Name „##.USR.TMP.UPICL<tsn>“.

Beachten Sie, dass die Zuweisung nach LOGOFF verloren geht.

3.3.9.3 Diagnoseunterlagen

Neben der Trace-Datei des *open*UTM-Subagenten gibt es weitere Dateien, die im Fehlerfall hilfreich sein können:

– UPIC-Trace-Datei
– UPIC-Logging-Datei
– SYSLOG-Datei

UPIC-Trace-Datei

Beim Trägersystem UPIC ist es möglich, Trace-Information für sämtliche Schnittstellenaufrufe zu generieren. Diesen Vorgang steuern Sie durch das Setzen der Jobvariable *UPICTRACE*. Beim Aufruf *Enable_UTM_UPIC* wird der Inhalt der Jobvariable ausgewertet. Falls die Jobvariable gesetzt ist, werden beim Aufruf jeder Funktion die Parameter und die Benutzerdaten bis zu einer Länge von 128 byte prozessspezifisch in einer Datei protokolliert.

Einschalten des UPIC-Trace

Der UPIC-Trace wird wie folgt eingeschaltet:

```
/SET-JV-LINK LINK-NAME=*UPICTRA,JV-NAME=UPICTRACE
/MODIFY-JV UPICTRACE,VALUE='-S[X] [-R wrap] [-Dprefix]'
```

Bedeutung:

-S Ausführliche Protokollierung der Aufrufe, der zugehörigen Argumente und der Benutzerdaten in der maximalen Länge von 128 Bytes (Pflichtangabe)

-SX Es werden zusätzlich interne Informationen an der Schnittstelle zum Transportsystem protokolliert.

-R *wrap* Mithilfe der durch *wrap* spezifizierten Dezimalzahl wird die maximale Größe der temporären Trace-Datei bestimmt.
Defaultwert: 128.

-D*prefix* Die Trace-Dateien werden unter folgenden Namen angelegt:
– *prefix*.UPICT<tsn>
– *prefix*.UPICU<tsn>
Wenn *prefix* nicht angegeben ist, wird „##.USR.TMP“ als Präfix verwendet.

Ausschalten des UPIC-Trace

Der UPIC-Trace wird mit einem der beiden folgenden Kommandos ausgeschaltet:

```
/DELETE-JV UPICTRACE
```

```
/MODIFY-JV UPICTRACE,VALUE=''
```

UPIC-Logging-Datei

Falls die *open*UTM-Anwendung eine Conversation abnormal beendet, wird in die UPIC-Logging-Datei eine *open*UTM-Fehlermeldung geschrieben. Die UPIC-Logging-Datei wird nur zum Schreiben der Fehlermeldung geöffnet (Modus *append*) und anschließend wieder geschlossen.

SYSLOG-Datei

Beim Start einer Anwendung legt *open*UTM eine anwendungsspezifische Protokolldatei SYSLOG an. In dieser Datei werden Ereignisse, die während des Ablaufs der Anwendung eintreten, in Form von *open*UTM-Meldungen protokolliert.

3.4 Integration in die Management-Plattformen

Zu den folgenden Management-Plattformen bietet Fujitsu-Siemens Computers für Solaris ein Integrationspaket SMAWsmbs2 sowie für Reliant UNIX und Windows NT jeweils ein Integrationspaket SMBS2 an, das die automatische Integration des BS2000/OSD in die folgenden Management-Plattformen ermöglicht:

– Unicenter TNG der Firma Computer Associates (Windows NT, Solaris)
– TransView SNMP (Reliant UNIX)
– TransView Control Center (Symmetrix-Überwachung) (Reliant UNIX)
– OpenView NetWork Node Manager von HP (Reliant UNIX)

Das Integrationspaket SMBS2 bzw. SMAWsmbs2 ist keine Voraussetzung für den Einsatz des Masteragenten und seiner Subagenten.

Neben den Integrationspaketen werden für einzelne Subagenten eigene, auf diese Subagenten zugeschnittene Management-Anwendungen angeboten.

Integrationspaket und Management-Anwendungen sind Bestandteil der Produkte BS2-SNMP-SO, BS2-SNMP-SX und BS2-SNMP-NT, die Sie auf der mitgelieferten CD finden.

Im Einzelnen sind auf der CD enthalten:

Paket	**Erläuterung**
SMBS2 / SMAWsmbs2 aus BS2-SNMP-SX bzw. BS2-SNMP-NT bzw. BS2-SNMP-SO	SNMP-Management für BS2000/OSD; Paket zur automatischen Integration in System Management Plattformen
HNC-SNMP-NT	HNC-Device-Management für Windows NT (siehe Handbuch „SNMP für HNC“)

Der vorliegende Abschnitt beschreibt die Installation und Konfiguration des Integrationspakets SMBS2 bzw. SMAWsmbs2 auf den genannten Management-Plattformen.

Installation und Konfiguration der Management-Anwendungen CMBS2 bzw. SMAWcmbs2 und PMBS2 bzw. SMAWpmbs2 sind beschrieben im Abschnitt „Installation der Management-Anwendungen“ (siehe Seite 124).

3.4.1 Integration in CA Unicenter TNG unter Windows NT

Installation und Verfügbarkeit von Unicenter TNG in der Version 2.2 sind Voraussetzung für die Nutzung von SMBS2 auf Windows NT. Wenn keine Installation von Unicenter TNG gefunden werden kann, wird die Installation abgebrochen. Wenn lediglich das Framework von Unicenter TNG installiert ist, kann SMBS2 nur in eingeschränktem Umfang genutzt werden.

Das Paket SMBS2 enthält neben den anwendungsspezifischen MIBs folgende Elemente zur Ergänzung der Komponenten „World View“, „Enterprise Management“ und „Agent Technology“ von Unicenter TNG:

- World View

  Es werden die Hostklasse „SiemensBS2000“ und zusätzliche Objektinstanzen der Klassen „Method“, „Popup-Menu“, „Icon_2d“ und „Icon3d“ erzeugt, um BS2000/OSD-Systeme entweder manuell oder mithilfe der automatischen Discovery-Funktion im Netzbild platzieren zu können. Für den „Object View“ werden die BS2000/OSD-MIBs bereitgestellt.

- Enterprise Management

  Um die Überwachung von BS2000/OSD-Systemen an der Event-Konsole zu verbessern, enthält SMBS2 Meldungsformate zu allen Traps des BS2000/OSD-SNMP-Master-Agenten und seiner Subagenten. An die Meldungsformate sind Aktionen mit Meldungsausgaben gekoppelt. Dies führt zu einer verständlicheren Darstellung der Traps, wichtige Ereignisse sind hervorgehoben.

- Agent Technology

  Es wird die Hostklasse „SiemensBS2000“ definiert. Dieser Hostklasse werden folgende Agentenklassen mit DSM-Policies zugeordnet:

  – Aus dem Lieferumfang von Unicenter TNG die Agentenklassen „Ping“ und „MIB2“.

  – Neue Agentenklassen für die Überwachung der verschiedenen Subagenten in BS2000/OSD: „sieAppMonitor“, „sieAVAS“, sieHSMS“, „sieOmnis“, „sieRDBMS“, „sieStorage“, „sieSupervisor“.

3.4.1.1 Installation auf Unicenter TNG unter Windows NT

Da SMBS2 die Installation von Unicenter TNG voraussetzt, prüft die Installationsprozedur, ob Unicenter TNG installiert ist. Eine evtl. ausgegebene Warnung bedeutet nicht in jedem Fall, dass die Installationsbedingungen nicht erfüllt sind.

Stufen der Installation

Es gibt drei Stufen der Installation von SMBS2:

– „Basic Support“ lässt sich mit einer Installation des Frameworks von Unicenter TNG nutzen. Dieser Framework-Support umfasst alle Elemente von SMBS2, die den „World View“ und das „Enterprise-Management“ ergänzen.

– „Full Support“ kann mit einer Vollversion von Unicenter TNG genutzt werden. Er enthält zusätzlich die Elemente zur Nutzung der „Agent Technology“.

– „Remote Administration Client“ lässt sich mit einer Installation des Remote Administration Client von Unicenter TNG nutzen. „RemoteAdministrationClient“ enthält alle Dateien für die Ergänzung der Benutzeroberfläche.

Dateien für die Installation

SMBS2 erzeugt Dateien in den folgenden Unterverzeichnissen des Installationsverzeichnisses von Unicenter TNG:

– *Config\Abrowser*
– *Icons*
– *Images*
– *Models*
– *Schema\Included*
– *Services\Config\AWS_nsm\Dm*
– *Services\Config\AWS_WVGATE*
– *Services\Config\Mibs*

SMBS2 erzeugt Dateien mit Skripten zur Anpassung der Konfiguration von Unicenter TNG. Diese Skript-Dateien werden in einem eigenen, von Ihnen im Verlauf der Installation zu spezifizierenden, Verzeichnis abgelegt. Standardmäßig wird das Verzeichnis C:\SMBS2 gewählt.

Es handelt sich dabei um die folgenden Dateien:

- Datei *BS2000.tng*

  Inhalt:

  – Definition der Objektklasse „SiemensBS2000“ als Unterklasse von „Host“

  – eine Reihe von zusätzlich im Common Object Repository benötigten Instanzen anderer Objektklassen, wie z.B. die BS2000/OSD-Ikone

  Diese Definitionen können mit dem folgenden Kommando in das Repository importiert werden:

  ```
  TRIX -Q -R=<repository> -U=<SQL-Admin> -W=<password> -G -X <pathname>\BS2000.tng
  ```

- Datei *BS2dbscript.txt*

  Die Datei *Bs2dbscript.txt* enthält die Definitionen der neuen Meldungsformate sowie die Definitionen der an diese Meldungen gekoppelten Aktionen für die Event-Konsole des „Enterprise Management“.

  Die Meldungsformate und die an sie gekoppelten Aktionen können mit dem folgenden Kommando geladen werden:

  ```
  cautil -F <pathname>\Bs2dbscript.txt
  ```

- zwei Readme-Dateien mit den im vorliegenen Abschnitt dargelegten Informationen sowie einem Lizensierungstext

Zusätzliche Unterverzeichnisse „INST“ und „BACKUP“ im Installationsverzeichnis

Im Installationsverzeichnis von Unicenter TNG werden im Rahmen der Installation zwei zusätzliche Unterverzeichnisse „INST“ und „BACKUP“ erzeugt:

- Das Verzeichnis „INST“ enthält das Installationsprotokoll sowie die Deinstallationsprogramme *uninstall.exe* und *remove.exe*. Letzteres sollte nicht direkt ausgeführt werden, da die Funktionen von SMBS2 erst nach einer Neu-Installation wieder genutzt werden können.
- Im Verzeichnis „BACKUP“ sind Kopien aller Dateien abgelegt, die inhaltlich durch die Installation verändert wurden.

Weitere Installationsschritte

Nach dem Einrichten der Dateien bestimmen Sie den Umfang der weiteren Installationsschritte. Durch Löschen der entsprechenden Markierung(en) im Fenster des Installationsdialogs können Sie einen oder mehrere der folgenden Installationsschritte überspringen:

1. Importieren der Objektklassen in das Repository
2. Aktivierung der Meldungstexte und der an die Meldungen gekoppelten Aktionen
3. Modifizierung der DSM-Konfiguration (nur bei Full-Support)
4. ResetDSM (nur bei Full-Support)

Welche dieser Schritte Sie ausführen lassen, hängt von der gewünschten Installationsstufe ab:

– Für die „Basic Support“-Installation sind die Schritte 1) und 2) auszuführen.

– Für die „Full Support“-Installation sind die Schritte 1) bis 4) auszuführen.

– Bei der „Remote Administration Client“-Installation gibt es keine Nachbearbeitung.

Die Durchführung jedes einzelnen Schritts ist unabhängig von der Durchführung der anderen Schritte.

Das Ausschalten einzelner Installationsschritte ist nur dann sinnvoll, wenn Sie SMBS2 nachträglich noch einmal installieren, z.B. um evtl. verlorengegangene Dateien wiederherzustellen.

Bei der Erst-Installation sollten Sie unbedingt alle Installationsschritte (außer evtl. ResetDSM) durchführen. Wenn einzelne Schritte ausgelassen werden, ist SMBS2 nicht voll funktionsfähig. Die ausgelassenen Schritte müssen Sie entweder manuell oder durch eine erneute Installation des Gesamtpakets nachgeholen. Die nachträgliche manuelle Ausführung der Installationsschritte ist schwierig und zu kann zu Inkonsistenzen führen.

3.4.1.2 Konfiguration von Unicenter TNG

Nach der Installation von SMBS2 können BS2000/OSD-Systeme in das Netzbild des „World View“ eingefügt werden. Wie die Ikone in das Netzbild eingebracht werden kann, ist in der Dokumentation zu Unicenter TNG beschrieben.

Integration von BS2000/OSD-Systemen

Mit den folgenden Kommandos können Sie einzelne BS2000/OSD-Systeme durch automatische Discovery integrieren:

`dscvrone -n <Name des BS2000-Systems>` oder

`dscvrone -i <IP-Adresse der BS2000-Systems>` oder

`dscvrbe -r <Name des Repository> -7 <IP-Adresse oder Name des BS2000-Systems>`

Anzeige der Meldungstexte an der Event-Konsole

Für die bessere Zuordnung der Meldungen auf der Event-Konsole empfiehlt es sich, die Spalte „Facility“ in die Anzeige aufzunehmen.

Konfigurieren und Starten der Agent-Technologie

Nach der Installation sind die DSM-Policies nicht in jedem Fall für alle Teilnetze aktiv. Eventuell muss der DSM-Wizard aufgerufen werden, um die Teilnetze in die Überwachung zu integrieren.

Das Popup-Menü der Ikone zur Objektklasse „SiemensBS2000“ enthält in der unteren Hälfte drei Einträge zum Aufruf der Management-Anwendungen für die Subagenten „Console Monitor“, „Performance Monitor“ und „BCAM-Monitor“. Die Funktionen dieser Menü-Einträge setzen voraus, dass die Produkte CMBS2, PMBS2 bzw. BMBS2 installiert sind. Bei einer nachträglichen Installation der genannten Produkte empfiehlt sich eine Neuinstallation von SMBS2, da sich die Menü-Einträge nur so nutzen lassen.

Folgende Punkte sind bei der Installation zu beachten:

– Falls während der Installationsphase die Unicenter TNG-Services gestoppt waren, muss - auch nach Ausführung aller Installationsschritte - zur Aktivierung der Meldungsformate und der an sie gekoppelten Aktionen die Event-Konsole noch einmal mit dem Kommando *opreload* konfiguriert werden.

– Die DSM-Policies werden nur aktiviert, wenn das Kommando *resetdsm* ausgeführt wurde. Das Kommando *resetdsm* wird als letzter Installationsschritt ausgeführt, sofern es vom Benutzer nicht deaktiviert wurde. Nach Ausführung des Kommandos *resetdsm* muss die „Agent Technology“ mit dem Kommando *awservices start* neu gestartet werden.

– Falls die BS2000/OSD-MIBs im MIB-Browser der „Agent-Technology“ nicht verfügbar sind, können sie mit dem Batch-Verarbeitungsprogramm *install_siemibs.bat* nachgeladen werden.

Darstellung der Agentenobjekte zusammen mit den Unterobjekten im Netzbild

Im Unispace der BS2000/OSD-Systeme können Ikonen zu zehn verschiedenen Agentenklassen angezeigt werden, die der Klasse „SiemensBS2000“ zugeordnet sind. Zu welchen Klassen Objekte erzeugt werden, hängt davon ab, welche Subagenten im BS2000/OSD aktiv sind.

Die beiden folgenden Agenten-Ikonen enthalten Bereiche mit weiteren Ikonen:

– Die Supervisor-Ikone („sieSupervisor“) enthält einen Bereich mit Objekten der Klasse „sieBS2000Subagent“. Für jeden überwachten Subagenten, der in der Supervisor-Tabelle enthalten ist, wird ein Objekt erzeugt.

– Die Ikone für den Appliation Monitor („sieAppMonitor“) enthält einen Bereich mit Objekten aus den Klassen „sieBCAMApplication“, „sieDCAMApplication“ und „sieUserApplication“. Diese Objekte enthalten Bereiche in denen die Objekte zu den überwachten BCAM, DCAM- und Benutzeranwendungen platziert werden.

Pollset-Einstellungen

Die wichtigsten Parameter für die Kommunikation zwischen der Management-Station und dem Agenten werden in Unicenter TNG durch Pollsets definiert. Im Pollset sind unter anderem Communities für das Lesen und Setzen von Objektwerten festgelegt. Diese Definitionen müssen unbedingt mit den Einstellungen am Agenten übereinstimmen.

SMBS2 enthält einen Pollset mit dem Namen „SiemensBS2000“. Dieser ist für alle Objekte der Klasse „SiemensBS2000“ gültig, solange der Benutzer nichts ändert oder neue Pollsets hinzufügt, die auf die BS2000/OSD-Systeme im Netz anwendbar sind.

Pollsets können mit dem Pollset-Browser geändert oder neu definiert werden. Voraussetzung für den Einsatz des Pollset-Browsers ist der Service *aws_orb*. Dieser Service wird mit dem Pollset-Browser gestartet, falls er nicht aktiv ist. Er wird aber mit der Beendigung des Pollset-Browsers nicht beendet.

Die Online-Hilfe liefert genauere Informationen über die Verwendung des Pollset-Browsers. Weitere Informationen zu Pollsets und dem Pollset-Browser finden Sie in der Dokumentation zu Unicenter TNG.

Für die Änderung oder Neudefinition eines Pollsets führen Sie folgende Schritte aus:

1. Pollset-Browser aufrufen:

   Der Pollset-Browser wird mit dem folgenden Menü-Eintrag aufgerufen:

   `Start –> Programme –> Unicenter TNG –> Agent Technology–> Pollset Browser`

2. Pollset auswählen:

   Der Pollset-Browser listet alle im Repository definierten Pollsets auf.
   Neben der Liste der Pollsets werden zwei Buttons angezeigt:

   – Durch Anklicken des „D“-Buttons löschen Sie Pollset.

   – Nach Anklicken des „C“-Buttons können Sie den Pollset ändern. Der Inhalt der Pollset-Definition wird in die oberste Zeile übertragen, und links werden zwei Buttons mit den Aufschriften „yes“ und „no“ angezeigt.

3. Pollset definieren

   Den Inhalt eines neuen oder eines zu ändernden Pollsets können Sie in die oberste Zeile eingetragen:

   – Bei einem neuen Pollset tragen Sie einen Namen in das erste Feld (Namensfeld) ein.

   – Bei der Änderung eines bereits vorhandenen Pollsets ist in das Namensfeld bereits mit dem Namen dieses Pollsets belegt und nicht überschreibbar.

   In den Spalten „Agent“ und „Host“ machen Sie Angaben zum Anwendungsbereich des Pollsets:

   – In der Spalte „Host“ spezifizieren Sie wahlweise einen der folgenden Werte:

     `<Hostname>` oder `<IP–Adresse>` oder `<Subnetzmaske>` oder *

   – In der Spalte „Agent“ spezifizieren Sie wahlweise einen der folgenden Werte:

     `<Name einer Agenten–Objektinstanz>` oder
     `<Name einer Agenten–Objektklasse>` oder *

4. Pollset-Definition bestätigen

   Nach Klicken auf den „yes“-Button wird der geänderte Pollset in das Repository übernommen. Für einen neuen Pollset klicken Sie auf den „+“-Button.

5. Pollset testen

   Die Testfunktion des Pollset-Browsers rufen Sie durch Anklicken des Buttons mit dem Lupensymbol in der Toolbar-Leiste oder über das „View“-Menue auf. Geöffnet wird dann ein Formular, in dem Sie Angaben zu einem Objekt im Netzbild eintragen können. Nach Anklicken von „Go“ wird die Liste der Pollsets angezeigt, die auf das Objekt angewendet werden können. Gültig ist der an oberster Stelle stehende Pollset.

3.4.1.3 Deinstallation

Bei der Deinstallation werden die Paketdateien gelöscht und es wird versucht, die Änderungen in der Konfiguration von Unicenter TNG so weit wie möglich rückgängig zu machen. Die in das Repository eingefügte Objektklasse „SiemensBS2000“ lässt sich nicht automatisch entfernen, wenn noch Objekte zu dieser Klasse existieren. Die übrigen durch die Installation erzeugten WorldView-Klassen und Objekte werden durch die Deinstallation gelöscht.

Nach der Deinstallation kann der Benutzer die fehlenden Schritte manuell nachholen:

1. Alle Objekte der Klasse „SiemensBS2000“ im Netzbild sind einschließlich Unterobjekte zu löschen. Es wird empfohlen, sich mit dem Object Browser eine Übersicht über alle Objekte der Klasse „SiemensBS2000“ zu verschaffen und die Objekte zusammen mit ihren Unterobjekten zu löschen.
2. Die Objektklasse „SiemensBS2000“ muss mit dem Class-Wizard gelöscht werden.

3.4.2 Integration in CA Unicenter TNG unter Solaris

Installation und Verfügbarkeit von Unicenter TNG in der Version 2.2 sind Voraussetzung für die Nutzung von SMAWsmbs2 auf Solaris. Die Installationsprozedur von SMAWsmbs2 prüft, ob und in welchem Umfang Unicenter TNG installiert ist. Sind nur Teilkomponenten von Unicenter TNG installiert, so kann SMAWsmbs2 nur in eingeschränktem Umfang installiert werden. Im Installationsdialog wird angezeigt, welche für SMAWsmbs2 relevanten Komponenten von Unicenter TNG auf dem System installiert sind. Zu den angezeigten Komponenten kann dann installiert werden. Durch eine Auswahl der Komponenten können Sie den Installationsumfang von SMAWsmbs2 weiter einschränken.

- TNG Base Managers - WorldView Components and EM Java GUIs

  Es werden die Hostklasse „SiemensBS2000“ und zusätzliche Objektinstanzen der Klassen „Method“, „Popup-Menu“, „Icon_2d“ und „Icon_3d“ erzeugt, um BS2000/OSD-Systeme entweder manuell oder mithilfe der automatischen Discovery-Funktion im Netzbild platzieren zu können. Für den „Object View“ werden die BS2000/OSD-MIBs bereitgestellt.

- TNG Base Managers - Enterprise Management

  Um die Überwachung von BS2000/OSD-Systemen an der Event-Konsole zu verbessern, enthält SMAWsmbs2 Meldungsformate zu allen Traps des BS2000/OSD-SNMP-Masteragenten und seiner Subagenten. An die Meldungsformate sind Aktionen gekoppelt, die die Bedeutung der Traps verständlicher darstellen und wichtige Ereignisse hervorheben.

- TNG Agent Technology Managers and Agents

  Es wird die Hostklasse „SiemensBS2000“ definiert. Dieser Hostklasse werden folgende Agentenklassen mit DSM-Policies zugeordnet:

  – Aus dem Lieferumfang von Unicenter TNG die Agentenklassen „Ping“ und „MIB2“.

  – Neue, durch SNMP eingerichtete Agentenklassen für die Überwachung der verschiedenenSubagenten in BS2000/OSD: „sieAppMonitor“, „sieAVAS“, „sieHSMS“, „sieOmnis“, „sieRDBMS“, „sieStorage“, „sieSupervisor“.

3.4.2.1 Installation auf Unicenter TNG unter Solaris

Während der Installation müssen die Services von Unicenter TNG aktiv sein, damit Einträge in die Datenbank vorgenommen werden können. Die Services werden durch die Installationsprozeduren gestartet, werden aber nach Abschluss der Installation nicht gestoppt. Mit dem Kommando *unicntrl stop all* können Sie die Services „von Hand“ stoppen.

Dateien für die Installation

SMAWsmbs2 erzeugt Dateien in den folgenden Unterverzeichnissen des Installationsverzeichnisses von Unicenter TNG:

– *browser/images/wvicons*
– *schema/included*
– *atech/services/config/aws_nsm/dm*
– *atech/services/config/aws_wvgate*
– *atech/services/config/mibs*

Standardmäßig wird ein Unterverzeichnis *SMAWsmbs2* im Verzeichnis *opt/SMAW* erzeugt. *SMAWsmbs2* enthält die Unterverzeichnisse *scripts*, *docs, bin, include*.

Das Verzeichnis *skripts* enthält die folgenden Dateien:

- Dateien *Bs2000.tng*, *Bs2000del.tng* und *Bs2000Agtdel.tng*

  Inhalt der Datei *BS2000.tng*:

  – Definition der neuen Objektklasse *SiemensBS2000* als Unterklasse von *Host*

  – Definitionen von Objekten für das „World View“-Repository: BS2000-Ikone und Popup-Menü für die BS2000-Ikone.

  Die genannten Definitionen werden mit dem folgenden Kommando in das Repository importiert:

  ```
  trix –f <pathname>/Bs2000.tng
  ```

  Die Dateien *BS2000del.tng* und *Bs2000Agtdel.tng* werden für die Deinstallation benötigt.

- Dateien *BS2dbscript.txt* und *BS2dbscriptdel.txt*

  Inhalt:

  Definitionen der neuen Meldungsformate (Message-Records) sowie die Definitionen der an diese Meldungen gekoppelten Aktionen (Message-Aktions) für die Event-Konsole des „Enterprise Management“.

Die Meldungsformate und die an sie gekoppelten Aktionen können mit dem folgenden Kommando geladen werden:

```
cautil -f <pathname>/Bs2dbscript.txt
```

Die Datei *DB2dbscriptdel.txt* wird für die Deinstallation benötigt.

- Datei *Bs2TrapAnalyse.c*

  Inhalt:

  Quellcode der Objektdatei *Bs2TrapAnalyse* (siehe unten)

  Inhalt:

  Übersetzungsprozedur für *BS2TrapAnalyse.c*

- Unterverzeichnis *include*

  Inhalt:

  Header-Dateien *Bs2Msg.h* und *Bs2VarBindOid.h*, die für die Übersetzung von *BS2TrapAnalyse* benötigt werden.

Das Verzeichnis *bin* enthält folgende Datei:

- Datei *Bs2TrapAnalyse*

  Das Programm *Bs2TrapAnalyse* wird von den neu definierten Message-Actions aufgerufen, um Meldungstexte zu erzeugen und auszugeben.

Das Verzeichnis *docs* enthält vier Readme-Dateien mit den im vorliegenden Abschnitt dargelegten Informationen sowie einem Lizensierungstext.

Weitere Installationsschritte

Nach dem Einrichten der Dateien erhalten Sie im Verlauf des Installationsdialogs angezeigt, welche weiteren Installationsschritte erforderlich sind.

Die maximale Installation von SMAWsmbs2 umfasst die folgenden Schritte:

1. Importieren der Objektklassen in das Repository (World View)
2. Aktivierung der Meldungstexte und der an die Meldungen gekoppelten Aktionen (Enterprise-Management)
3. Modifizierung der DSM-Konfiguration (Agent Technology)
4. ResetDSM und Import der Agentenklassen (Agent Technology)

Die Durchführung jedes einzelnen Schritts ist unabhängig von der Durchführung der anderen Schritte. Das Auslassen einzelner Installationsschritte ist nur dann sinnvoll, wenn Sie SMAWsmbs2 nachträglich noch einmal installieren, z.B. um evtl. verlorengegangene Dateien wiederherzustellen.

Bei der Erst-Installation sollten Sie unbedingt alle zur Auswahl gestellten Installationsschritte durchführen. Wenn einzelne Schritte ausgelassen werden, ist SMAWsmbs2 nicht voll funktionsfähig. Die ausgelassenen Schritte müssen Sie entweder manuell oder durch eine erneute Installation des Gesamtpakets nachholen. Eine nachträgliche manuelle Ausführung der Installationsschritte ist schwierig und zu kann zu Inkonsistenzen führen.

3.4.2.2 Konfiguration von Unicenter TNG

Es stehen zwei verschiedene Benutzeroberfächen zur Verfügung, über die Sie mit Unicenter TNG auf Solaris arbeiten können:

– eine durch Java-Applets realisierte Web-Oberfläche, auf die Sie mit einem Web-Browser zugreifen können

– eine über einen „Remote Administration Client“ auf einem Windows NT-System angebotene Oberfäche

  In diesem Fall ist es erforderlich, SMBS2 auf dem „Remote Administration Client“ zu installieren (Installationsmodus „Administration Client“). Eine detaillierte Beschreibung zu Installation und Einsatz von SMBS2 in Verbindung mit Unicenter TNG auf Windows NT finden Sie im Abschnitt „Integration in CA Unicenter TNG unter Windows NT“ auf Seite 95 ff.

3.4.2.3 Konfiguration des Trap-Verteilers

Wenn Sie neben Unicenter TNG noch weitere Anwendungen starten, die Traps empfangen sollen, können Sie den Trapverteiler *catrapmux* so konfigurieren, dass er Traps auch noch an andere Ports verteilt. Hierfür fügen an das Ende der Datei *$CAIGLBL0000/snmp/config/catrapmux.conf* eine Zeile der folgenden Form an:

```
<Anwendungsname>:<Portnummer>
```

Anschließend muss der Trapverteiler *catrapmux* mit dem Kommando *unicntrl snmp stop* gestoppt und mit dem Kommando *unicntrl snmp start* neu gestartet werden.

3.4.2.4 Deinstallation

Bei der Deinstallation werden die Paketdateien gelöscht und es wird versucht, die Änderungen in der Konfiguration von Unicenter TNG so weit wie möglich rückgängig zu machen. Die in das Repository eingefügte Objektklasse „SiemensBS2000“ lässt sich nicht entfernen, wenn noch Objekte zu dieser Klasse existieren.

Nach der Deinstallation können Sie die fehlenden Schritte manuell nachholen:

1. Alle Objekte der Klasse „SiemensBS2000“ im Netzbild sind einschließlich der Unterobjekte zu löschen. Es wird empfohlen, sich mit dem Object Browser eine Übersicht über alle Objekte der Klasse „SiemensBS2000“ zu verschaffen und die Objekte zusammen mit ihren Unterobjekten zu löschen.
2. Die Objektklasse SiemensBS2000 muss mit dem Class-Wizard gelöscht werden.

3.4.3 Integration in TransView SNMP

Das Paket SMBS2 enthält auf Reliant UNIX neben den anwendungsspezifischen MIBs folgende Komponenten zum Einsatz mit TransView SNMP:

– Objektdarstellungen, diese Dateien beschreiben die ergänzenden Menüs und Tabellen, die zur Anzeige der Werte der MIB-Objekte notwendig sind. In den Tabellen werden ausschließlich Objekte dargestellt, die über mehrere Instanzen verfügen können.

– die Bilddateien zur Darstellung skalarer Objekte liefern eine einfache Möglichkeit zur Auflistung der Objekte und ihrer Werte in Formularform.

– die Netzbilddatei *.map_SMBS2*, mit der Netzbilder mit den zu überwachenden Anwendungen in eine bestehende Netzkonfiguration integriert werden können.

– Bitmapdateien mit Ikonen zur Darstellung der SNMP-Anwendungen im BS2000/OSD

– zwei Dateien mit Hilfetexten:

  Es handelt sich um eine Textdatei, die im Wesentlichen aus den Description-Texten der unterstützten MIBs besteht, und eine Datei mit den Schlüsselworten, die dem Hilfe-Index hinzugefügt werden sollen. Zu jedem Fenster wird als Hilfetext eine Aufstellung und Erläuterung zu allen Objekten des MIB-Zweiges angeboten, zu dem die im Fenster gezeigten Objekte gehören.

– Prozeduren zur Unterstützung der Installation und Deinstallation, die in TransView SNMP nicht enthalten sind.

Voraussetzungen

SMBS2 ist keine Voraussetzung für den Einsatz des Masteragenten und seiner Subagenten in BS2000/OSD. Wenn Sie SMBS2 einsetzen wollen, wird TransView SNMP ≥ V 4.0 und optional TransView Control Center ≥ V4.0 vorausgesetzt. TV SNMP kann während des Installationsvorgangs gestartet sein, wirksam wird die SMBS2-Installation allerdings erst nach einem Neustart von TV SNMP. Wenn eine Vorgängerversion von SMBS2 installiert ist, sollte diese vor der Installation der Version 4.0 von SMBS2 deinstalliert werden.

Bei der Installation vorgefundene Dateien gleichen Namens werden, sofern sie bei der Installation überschrieben werden müssen, unter den Namen *<file-name>.usr* gesichert.

Die Verfügbarkeit von *perl* ist Voraussetzung für die Installierbarkeit von SMBS2, bei Nichtverfügbarkeit von *perl* wird die Installation abgebrochen. Wesentliche Funktionen zur Nachbearbeitung der Konfigurationsdateien von TransView SNMP werden mit *perl*-Skripten durchgeführt. Da TransView SNMP für seine Installation ebenfalls *perl* benötigt, sollte diese Voraussetzung in der Regel erfüllt sein.

3.4.3.1 Installation auf TransView SNMP

Zu Beginn der Installation von SMBS2 wird angezeigt, auf welchen Plattformen SMBS2 schon installiert ist. Dabei werden nur Installationen ab der Version 3.0A berücksichtigt, die älteren Versionen werden nicht erfasst. Anschließend sucht die Installationsprozedur die installierten und für SMBS2 geeigneten Plattformen und zeigt sie in einer Liste mit ihren Versionen und Basispfadnamen an. Aus dieser Liste können Sie nun eine Plattform für die Installation auswählen.

Es ist möglich, SMBS2 für alle der angezeigten Plattformen nacheinander zu installieren. Während bei jeder Installation SMBS2 nur auf einer Plattform eingerichtet wird, wird bei einer Deinstallation SMBS2 von allen Plattformen gleichzeitig entfernt. Die Plattformen, auf denen SMBS2 installiert ist, werden zu Beginn der Deinstallation angezeigt. Hier gilt dieselbe Einschränkung wie für die Anzeige bei der Installation: Versionen älter als 3.0A werden nicht erfasst. Für alle aufgelisteten Plattformen wird eine Deinitialisierung durchgeführt. Auf den Plattformen mit älteren Versionen werden nur die mit dem Paket SMBS2 installierten Dateien gelöscht. Das kann zu funktionellen Beeinträchtigungen der Management-Plattformen führen, die sich nur durch die Reinstallation von SMBS2 auf den betroffenen Plattformen beheben lassen. (siehe hierzu Freigabemitteilungen der entsprechenden Vorgängerversionen von SMBS2).

Die Installation von SMBS2 erfolgt im *home*-Verzeichnis von TV SNMP:

– die MIBs im Unterverzeichnis *asn1*

– die Dateien für die Objektdarstellungen im Unterverzeichnis *views*

– die Bilddateien zur Darstellung skalarer Objekte, die Ikonen und die Hilfetextdateien im Unterverzeichnis *lib*

– die Netzbilddatei *.map_SMBS2* im Unterverzeichnis *maps*

TransView-SNMP-MIB

Die zentrale TransView-SNMP-MIB enthält die Definitionen aller Geräte, die verwaltet werden können. Sie wird mit der *parse*-Funktion aus den herstellerspezifischen MIBs der Geräte und Anwendungen gebildet, die von TransView SNMP überwacht werden sollen.

Während des Installationsverfahrens kann festgelegt werden, ob die neu installierten ASN.1-Dateien zum Systemmanagement im BS2000/OSD in die zentrale MIB aufgenommen werden sollen, vorausgesetzt, es wurde im *home*-Verzeichnis von TransView SNMP installiert. Eine bereits vorhandene Datei wird als *mib.org* gesichert. Die Integration einer neuen MIB kann jederzeit auch unabhängig von der Installation von SMBS2 vorgenommen werden.

Objektdarstellung in *object.views*

Die Angaben in der Datei *object.views* bilden die von den Agenten erhaltenen Werte der Objektattribute auf Anzeigen für den Benutzer ab. Sie umfassen die Menübeschreibung zum Aufruf der Fenster für die Darstellung der MIB-Objektgruppen sowie die Beschreibungen der Tabellen und Diagramme. Es kann festgelegt werden, ob die mit SMBS2 neu installierten Objektdarstellungen einer bestehenden Datei *object.views* hinzugefügt werden sollen, vorausgesetzt, es wurde im home-Verzeichnis von TransView SNMP installiert. Für die Host-Resources-MIB wird dabei die Datei *rfc1514-host. obj* verwendet, die zum Lieferumfang von TransView SNMP gehört. Die Originaldatei wird als *object.views.org* gesichert.

Hilfetextdateien

Mit Ausnahme der Host-Resources-MIB sind in SMBS2 für alle MIBs Hilfetextdateien enthalten, die aus den Description-Texten zu den MIB-Objekten gebildet wurden. Die Hilfetexte zur Host-Resources-MIB fehlen, da die in TransView SNMP enthaltene Objektdarstellungsdatei verwendet wird.

Zusätzliche Hinweise zur Installation auf TransView SNMP V3.1

Ab der Version 4.0A des TransView Control Centers sind die Domänenverzeichnisse entfallen. Den Domänen können stattdessen Dateien aus den Unterverzeichnissen des Installationsverzeichnisses von TransView SNMP zugewiesen werden. Die domänenspezifische Installation ist deshalb nicht mehr notwendig, um die Erweiterungen von SMBS2 auch in den Domänen verfügbar zu machen. Wenn im Rahmen der TransView-Version 3.1 installiert wird, kann beim Einsatz des TransView Control Centers zusätzlich in den Domänenverzeichnissen installiert werden. Zur Bestimmung der Domänennamen wird nach allen existierenden Pfadnamen der Form *<home-Verzeichnis>/tcc/*/<Domänenname> /maps* gesucht. Zu beachten ist hierbei, dass bei der Installation unter einem anderen Verzeichnis als dem Home-Verzeichnis der Kennung *tvsnmp*, in diesem Verzeichnis auch die Domänennamen gesucht werden. Wenn Domänenverzeichnisse gefunden wurden, werden dem Benutzer drei Optionen zur Auswahl gestellt:

– Installation in keiner Domäne (Standardoption)
– Installation in allen gefundenen Domänen oder
– Installation in einer Auswahl von Domänen.

Bei der dritten Option wird eine nummerierte Liste der gefundenen Domänennamen ausgegeben. Durch eine Zahlenfolge wird die Menge der Domänen bestimmt, in denen installiert wird.

In einem Domänenverzeichnis werden die MIB-Datei und die Datei *object.views* nur dann modifiziert, wenn das Unterverzeichnis *lib*, das diese Dateien enthält, tatsächlich existiert und nicht nur symbolische Verweise sind. Bei der Verwendung von symbolischen Verweisen muss deshalb darauf geachtet werden, dass die Dateien, auf die verwiesen wird, ebenfalls angepasst werden.

3.4.3.2 Konfiguration von TransView SNMP

Mit der Netzbilddatei *.map_SMBS2*, die in das Verzeichnis *<home-tvsnmp>/maps* geschrieben wird, kann eine bestehende Netzkonfiguration um die zu überwachenden BS2000/OSD-Systeme und -Anwendungen erweitert werden. Die Netzbilddatei umfasst:

– eine Ikone für den BS2000/OSD-Rechner sowie

– je eine Ikone für die zu überwachenden Subagenten für AVAS, File Transfer, Spool&Print-Services, Storage Management, SM2 (Performance-Messung), *open*UTM, SESAM, BCAM, OMNIS und HIPLEX-AF. Die anderen Subagenten werden durch die BS2000/OSD-Ikone dargestellt.

– je eine Verbindung zwischen der Ikone des BS2000/OSD Rechners und den Subagenten-Ikonen. Diese Verbindungen sind aufseiten des BS2000/OSD-Rechners einer Objektinstanz zugeordnet. Es handelt sich um die Zeile des Subagenten aus der Subagententabelle.

– die Definition der Eigenschaftsgruppen zu den Ikonen und Verbindungen. Die Eigenschaftsgruppen sind für die Management-Station neben den MIBs die Informationsbasis darüber, welche Objekte der Agent eines durch eine Ikone dargestellten Gerätes bzw. einer Anwendung unterstützt. Gleichzeitig wird durch die Eigenschaften der Gültigkeitsbereich von Alarmen und Polls definiert. Zu diesem Zweck sind den Verbindungen Eigenschaftsgruppen zugeordnet.

Die neue Netzbilddatei nehmen Sie in Ihre Netzkonfiguration folgendermaßen auf:

1. Sie starten TransView SNMP.
2. Sie wechseln in das gewünschte Netzbild.
3. Sie wählen *Aufnehmen* im Menü *Datei* aus. Tragen Sie den Dateinamen *.map_SMBS2* und den Pfad, unter dem die Datei abgelegt ist, ein (im Standardfall : *<tvsnmp-home>/maps*). Sie bestätigen den Dialog mit *Aufnehmen*.

   In Ihrem Netzbild wird die Ikone eines BS2000/OSD-Systems dargestellt, die durch Verschieben genauer platziert werden kann. Sie können diesen Vorgang wiederholen und dadurch mehrere BS2000/OSD-Systeme in das Netzbild aufnehmen. Ein Doppelklick auf die Ikone öffnet eine neue Darstellung mit einem BS2000/OSD-Rechner und den

Ikonen der zu überwachenden Anwendungen. Ist das TransView Control Center gestartet, kann in einigen Versionen der Menüeintrag *Aufnehmen* gesperrt sein. Rufen Sie in diesem Fall bitte TransView SNMP direkt auf.

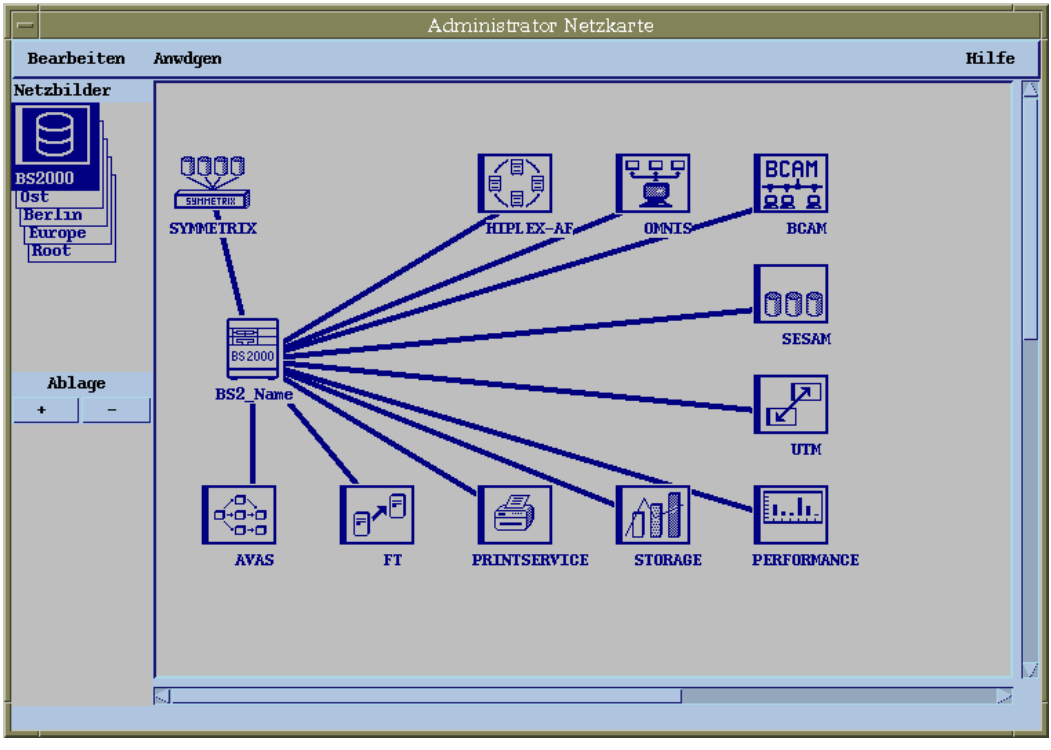


Bild 10: Administratornetzkarte

4. Sie öffnen die *Objektübersicht* zum BS2000/OSD durch Doppelklick auf die Ikone des BS2000/OSD-Rechners. Das Netzbild enthält die Ikonen für das BS2000/OSD-System und die Anwendungen.
5. Öffnen Sie die *Objektübersicht* zum BS2000/OSD durch Doppelklick auf die Ikone des BS2000/OSD-Rechners.
6. Sie tragen den Namen und die Internet-Adresse des Rechners entsprechend Ihrer Hardware-Konfiguration in die dafür vorgesehenen Felder ein.
7. Sie korrigieren den Community-String entsprechend der Konfiguration des Agentensystems.

   Wiederholen Sie die Vorgänge 5-7 für alle BS2000/OSD-Anwendungen (Subagenten).

Als Internet-Adresse der Anwendung ist die Adresse des Systems anzugeben, auf dem die Anwendung läuft. Zur Nutzung des vollen Funktionsumfangs benötigen die Agenten von BS2000/OSD-Anwendungen, deren MIBs Objekte mit Schreibzugriff haben, auch einen Community-String mit schreibendem Zugriff. Es wird empfohlen, für den BS2000/OSD-Rechner einerseits und die Anwendungen andererseits unterschiedliche Community-Strings zu verwenden, wobei die Community-Strings der Anwendungen keine Trap-Empfänger sein sollten (vgl. Seite 57).

Die Community-Strings der Anwendungen müssen gleich dem Namen des Knotens in der Netzkarte sein.

8. Zur Aktivierung der Alarme ist es notwendig, alle Ikonen und Verbindungen in den Zustand *verwaltet* zu setzen. Dieser Wert kann in den Objektübersichtsfenstern verändert werden.
9. Sie sichern die Änderungen durch *Ablegen* im Menü *Datei*.

Zur Vereinfachung dieses Verfahrens steht ab der Version 3.0A von SMBS2 das Skript *chn_map_SMBS2.pl* im Unterverzeichnis: *bin/SMBS2* zur Verfügung. Das Skript hat folgendes Aufrufformat:

```
chn_map_SMBS2.pl <dir> <ip-Adresse> <Suffix>
```

<dir> bezeichnet den absoluten oder relativen Pfadnamen, unter dem die Subnetzdatei *.map_SMBS2* im Originalzustand liegt.

<ip-Adr.> definiert die IP-Adresse, die für alle Knoten im Subnetzbild eingetragen werden soll.

<Suffix> wird als Suffix an den Namen des Subnetzbildes, die Namen der Netzknoten und in die Leitungsnamen angefügt. Weil bei allen Knoten außer *BS2_Name* Community und Name übereinstimmen müssen, werden dort auch die Community-Namen angepasst. Die ersten beiden Parameter müssen zwingend angegeben werden. *<Suffix>* darf weggelassen werden, es wird dann die IP-Adresse als Suffix verwendet. Die erzeugte Kopie bekommt den Dateinamen: *.map_SMBS2<Suffix>* bzw. *.map_SMBS2.<ip-Adr.>*.

Darstellungen der Objekte

Soll einer der Subagenten nicht betrieben werden, kann die Ikone seiner Anwendung aus dem Netzbild entfernt werden. Wählen Sie dazu die entsprechende Ikone aus. Betätigen Sie die Maustaste "Menü" (rechte Maustaste) und wählen im Popup-Menü die Funktion *Löschen*. In gleicher Weise löschen Sie die Verbindungslinie zu der entfernten Ikone.

3.4.3.3 Deinstallation

Bei der Deinstallation soll der Zustand von TransView SNMP und / oder TransView Control Center vor der Installation von SMBS2 so weit wie möglich wiederhergestellt werden. Zu Beginn der Deinstallation werden alle Plattformen aufgelistet, auf denen das Paket SMBS2 installiert ist. Ältere Versionen als die Version 3.0A von SMBS2 können dabei nicht erfasst werden. Eine Deinitialisierung wird nur auf den angezeigten Plattformen ausgeführt. Weil durch die Deinstallation auch die Dateien von Installationen der älteren Versionen gelöscht werden, ohne die betroffenen Plattformen neu zu konfigurieren, ist für den reibungslosen Betrieb dort die unverzügliche Wiederinstallation erforderlich. Sofern es sich um Versionen von TransView SNMP handelt, ist die Installation von SMBS2 sogar dringend notwendig, um gelöschte, aber benötigte Dateien wiederherzustellen.

Während der Deinstallation von SMBS2 kann entschieden werden, ob die *mib* und die *object.views* wieder in ihren Originalzustand - d.h. TransView SNMP ohne SMBS2 - zurückversetzt werden sollen. Soll dies nicht geschehen, müssen die Änderungen der TransView-SNMP-MIB und der *object.views* manuell wieder zurückgenommen werden. Während des Deinstallationsprozesses werden alle Dämonenverzeichnisse nach Dateien durchsucht, die bearbeitet werden müssen. Voraussetzung für die Bearbeitung der Dateien ist die Verfügbarkeit von *perl* während des Deinstallationsprozesses.

Die Deinstallationsprozeduren überprüfen nicht, ob zum Zeitpunkt der Deinstallation von SMBS2 Subnetzbilder für ein BS2000/OSD-System im Netzbild definiert sind. Durch das Entfernen der Ikonendateien werden die Bestandteile im Subnetzbild unsichtbar und somit der Verwaltung durch den Nutzer entzogen. Deshalb können sie nicht mehr gelöscht werden, solange SMBS2 nicht wieder installiert ist.

3.4.4 Integration in TransView Control Center

Folgende Komponenten werden zum Einsatz auf dem TransView Control Center angeboten:

– die Konfigurationsdatei *bs2symm.def* enthält Definitionen:

  a) der Applikation *BS2-Symmetrix*,

  b) von Ereignissen zu allen Referenzcodes der Symmetrix-Meldungen,

  c) des Knotens *Symmetrix* und

  d) von Relationen zwischen der Applikation *BS2- Symmetrix*, den definierten Ereignissen und dem Knoten *Symmetrix*.

  Die Ereignisdefinitionen beziehen sich auf TV-SNMP-Alarme. Sie können deshalb nur in einem Netzbild von TransView SNMP angezeigt werden.

– die Datei *bs2symmcnf*, die ein Muster für vier Zeilen enthält, die der Konfigurationsdatei des Console Monitor auf dem BS2000/OSD hinzugefügt werden sollen

– eine Prozedur, mit der die Daten aus der Konfigurationsdatei *bs2symm.def* in die Domänen des TransView Control Centers übernommen werden können.

3.4.4.1 Installation auf TransView Control Center

Im Installationsverzeichnis des TransView Control Centers (in der Regel: */opt/tcc*) wird ein Unterverzeichnis *SMBS2* eingerichtet, in dem drei Dateien abgelegt werden:

bs2symm.def

Die Konfigurationsdaten aus dieser Datei können entweder mit dem Kommando *tccadd* oder der Oberflächenfunktion *Update Domain ...* in eine TCC-Domäne aufgenommen werden.

bs2symm.cnf

Diese Datei ist nicht für die Management-Plattform, sondern für die Agentenseite bestimmt. Sie enthält die folgenden vier Zeilen:

```
<NJD0010 SOURCE=SYMMETRIX DEVICE=SYMMETRIX>
<NJD0011 SOURCE=SYMMETRIX DEVICE=SYMMETRIX>
<NJD0012 SOURCE=SYMMETRIX DEVICE=SYMMETRIX>
<NJD0013 SOURCE=SYMMETRIX DEVICE=SYMMETRIX>
```

Diese Zeilen müssen der Konfigurationsdatei des Console Monitor-Subagenten hinzugefügt werden, damit er die Symmetrix-Meldungen als Trap weitersendet (vgl. Seite 75). Der Wert des DEVICE-Parameters muss gegebenenfalls angepasst werden. Dieser Parame-

terwert bestimmt indirekt auch den Namen des Knotens im Netzbild der Management-Station. Die Community-Namen und der Knotenname im Netzbild müssen für das TransView Control Center übereinstimmen. Als Wert für den DEVICE-Parameter kann deshalb nur ein für das gesamte dargestellte Netzbild eindeutiger Knotenname verwendet werden.

upd-domain

Es handelt sich um eine Prozedurdatei, die in einem Unterverzeichnis *bin* zum Verzeichnis *SMBS2* abgelegt wird. Sie erleichtert die Aufnahme der Definitionen aus der Datei *bs2symm.def* in die TCC-Domänen. Dafür werden zuerst alle Domänennamen aufgelistet, damit der Benutzer eine Auswahl der Domänen treffen kann, für die das *tccadd*-Kommando ausgeführt werden soll. Diese Prozedur wird auch bei der Installation im Nachinstallationsverfahren von SMBS2 aufgerufen.

Deinstallation

Das Deinstallationsverfahren für TransView CC entspricht weitgehend dem für TransView SNMP beschriebenen (vgl. Seite 114), beachten Sie bitte noch folgende Zusätze. Das Unterverzeichnis *SMBS2* im Installationsverzeichnis von CC wird mit allen Dateien gelöscht. Ebenso wird die Applikation *BS2-Symmetrix* mit den verbundenen Ereignisdefinitionen aus der Konfiguration des TransView Control Centers entfernt. Der durch die Installation erzeugte Knoten *Symmetrix* bleibt bestehen.

3.4.4.2 Konfiguration von TransView Control Center

Durch die Installation von SMBS2 wird im Installationsverzeichnis von CC - in der Regel im Pfad */opt/tcc* - ein Unterverzeichnis *SMBS2* angelegt, welches die Dateien *bs2symm.def* und *bs2symm.cnf*, sowie das Unterverzeichnis *bin* mit der Prozedur *upd-domain* enthält.

Wenn an einem BS2000/OSD-System die an der Konsole gemeldeten Symmetrix-Ereignisse überwacht werden sollen, müssen folgende Schritte ausgeführt werden.

1. Die Konfigurationsdatei des Console Monitors muss um die vier Zeilen aus der Datei *bs2symm.cnf* erweitert werden. Dabei ist die DEVICE-Bezeichnung so anzupassen, dass auf der Seite der Management-Station die Eindeutigkeit dieser Bezeichnung als Knotenname im Netzbild gewährleistet ist. Der SOURCE-Parameter soll unverändert bleiben, da er Bestandteil des Applikationsnamens im TransView Control Center ist.
2. Im Netzbild der Management-Station wird ein Subnetzbild für das BS2000/OSD-System mit einer Symmetrix-Ikone eingerichtet. Das Vorgehen bei der Einrichtung dieser Ikone entspricht der Beschreibung auf Seite 111.
3. Im Subnetzbild muss bei der Symmetrix-Ikone der Knotenname mit der Community übereinstimmen. Die Community ist durch den DEVICE-Parameter der Anwendung in der Konfigurationsdatei des Console Monitor festgelegt (vgl. Punkt 1).

4. Mit der Funktion *Update Control Center* muss der neue Symmetrix-Knoten und der Knoten für das BS2000/OSD-System, der sich in der Mitte des Subnetzbildes befindet, in die Verwaltung durch die TCC-Domäne aufgenommen werden. Der BS2000/OSD-Knoten soll als reales Gerät dienen, dem im Eventmanager die Ereignisse zugeordnet werden, und der Symmetrix-Knoten als virtuelles Gerät, an dessen Ikone die Ereignisse angezeigt werden.
5. Sofern die Konfigurationsdaten aus der Datei *bs2symm.def* noch nicht in der vorgesehenen TCC-Domäne aufgenommen wurden, muss das nachgeholt werden. Dafür kann das *tccadd*-Kommando oder das Skript *upd-domain* verwendet werden. Das Letztere bietet die Möglichkeit, die Definitionen aus der Datei *bs2symm.def* in mehrere Domänen gleichzeitig aufzunehmen. Die Daten können ebenso mit der Funktion *Update-Domain* im Fenster *Integrated Applications* an der Dialogoberfläche aufgenommen werden.
6. Der neu eingerichtete Symmetrix-Knoten muss, sofern er nicht den Namen *Symmetrix* bekommen hat, mit der Applikation und den mit ihr verknüpften Ereignissen im Fenster *Activate Events and Reactions* verknüpft werden. Dazu wählt man zunächst *Applications* als Basiszuordnungsliste aus und markiert dort die Applikation *BS2-Symmetrix*. Die Knoten und Ereignisse, mit denen diese Anwendung verknüpft ist, werden nun ebenfalls markiert. Nachdem in der Knotenliste der neue Symmetrix-Knoten markiert wurde, wird durch Drücken des Knopfes *create* die erforderliche Verknüpfung hergestellt.

3.4.5 Integration in OpenView Network Node Manager

SMBS2 enthält auch eine OpenView-Anwendung für das BS2000/OSD, die in die Oberfläche des Network Node Managers integriert wird. Voraussetzung für eine erfolgreiche Installation und den fehler- und problemlosen Betrieb ist OpenView, bestehend aus den Softwarepaketen OV-IC, OV-NNMGR und OV-SNMPRN in einer der Versionen 3.3 oder 4.1. SMBS2 ist keine notwendige Bedingung für den Einsatz des SNMP Masteragenten und seiner Subagenten im BS2000/OSD-System. Das Paket wird lediglich an der OpenView Management-Station integriert.

SMBS2 enthält neben den anwendungsspezifischen MIBs folgende Dateien zur Ergänzung der OpenView NNMGR-Oberfläche:

– Die Anwendungsdatei, die neben den MIB-Dateien das Kernstück dieses Paketes darstellt. Sie enthält die Definitionen für die Menüs und Fenster, die der OpenView-Oberfläche hinzugefügt werden. In der im Paket enthaltenen Anwendung werden nur die Standardfenster für Applikationen verwendet, die auch im Application-Builder verfügbar sind. Es handelt sich um Formulare für Objektlisten, Tabellen und Grafiken.

– Drei Dateien mit Hilfetexten, die Informationen zu den drei verwendeten Fenstertypen enthalten,

– Bitmap-Dateien für die Darstellung eines BS2000/OSD-Rechners im Netzbild (in sechs verschiedenen Ikonen-Größen). Zu den Bitmap-Dateien gehören jeweils sechs Maskendateien.

– Die Konfigurationsdateien bestehend aus einer Symbol-Datei, einer Field-Datei, sowie zwei Dateien mit den Zeilen, die den Konfigurationsdateien *oid_sym* und *oid_to_type* hinzugefügt werden müssen.

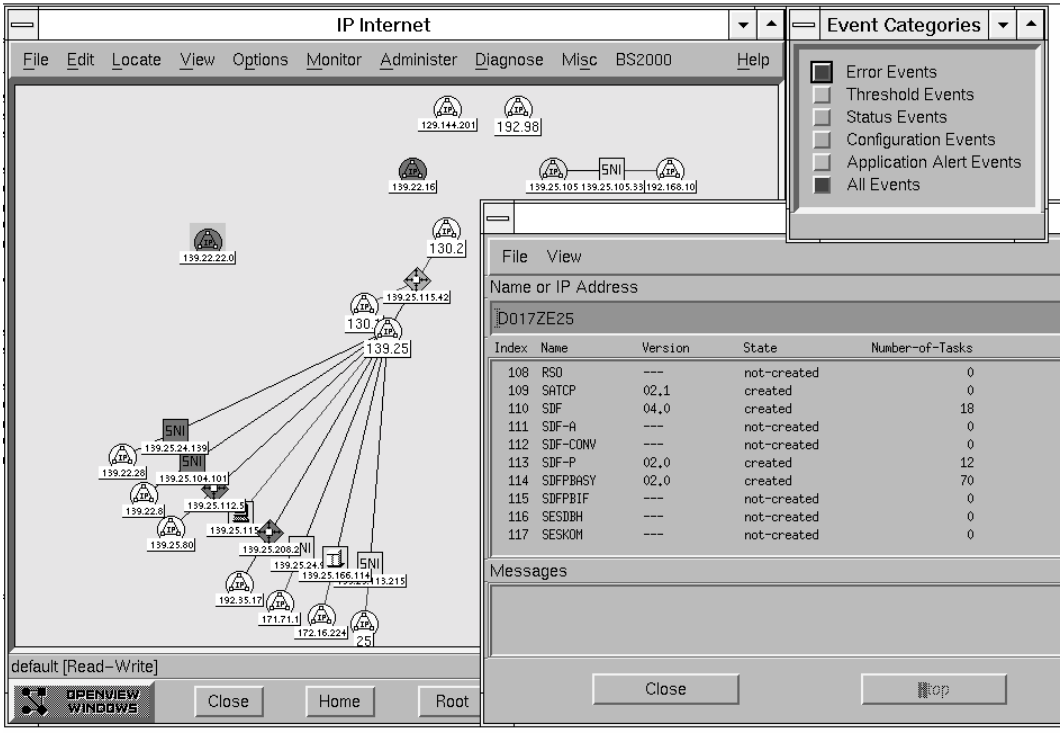


Bild 11: OpenView-Netzbild

3.4.5.1 Installation auf OpenView

Im Unterschied zu TransView SNMP, wo es möglich ist, unterschiedliche Versionen parallel zu installieren, kann SMBS2 bei OpenView NNMGR nur für die zuletzt installierte und tatsächlich verwendete Version installiert werden. Werden mehrere Versionen von OpenView NNMGR unter verschiedenen Pfadnamen gefunden, so werden diese zwar angezeigt, es wird nach der Auswahl einer dieser Versionen aber versucht, für die zuletzt installierte Version zu installieren. Der Anwender muss aus diesem Grund alle bei der Installation von SMBS2 verwendeten Pfadnamen bestätigen.

Die Installationsweise von SMBS2 hängt von der OpenView-Version ab, weil verschiedene Dateiverzeichnisse verwendet werden. Im grundsätzlichen Verfahren gibt es aber keinen Unterschied. Die Installation von SMBS2 besteht hauptsächlich in der Verteilung von Dateien auf die verschiedenen Verzeichnisse. Beim Laden von OpenView werden diese Verzeichnisse durchsucht und die gefundenen Dateien interpretiert. Weil für OpenView die Funktion einer Datei durch das Verzeichnis bestimmt ist, in dem sie eingetragen ist, ist es zwingend, dass die Dateien in denselben Verzeichnissen auch dieselbe Syntax haben. Beispielsweise werden alle Dateien im Verzeichnis */usr/OV/registration/C/ovmib* von OpenView

in der Version 3.3 als Applikations-Dateien interpretiert. Sollten andere Dateien in diesem Verzeichnis gefunden werden, führt das zu Fehlermeldungen beim Laden von OpenView. Ähnliches gilt für die Field-, Symbol- oder Bitmap-Dateien.

Im Einzelnen werden in den beiden unterstützten Versionen von OpenView die folgenden Dateiverzeichnisse verwendet:

Datei	**Version 3.3**	**Version 4.1**
MIB-Dateien	/usr/OV/snmp_mibs	/var/opt/OV/share/snmp_mibs
Anwendungsdatei	/usr/OV/registration/C/ovmib	/etc/opt/OV/share/registration
Hilfedateien	/usr/OV/help/C/ovmib/OVW/Functions	/var/opt/OV/share/help/C/ ovmib/OVW/Functions
Bitmap-Dateien	/usr/OV/bitmaps/C	/etc/opt/OV/share/bitmaps/C
Symbol-Datei	/usr/OV/symbols/C	/etc/opt/OV/share/symbols/C
Field-Datei	/usr/OV/fields/C	/etc/opt/OV/share/fields/C
Konfigurationsdatei	/usr/OV/conf/C	/etc/opt/OV/share/conf/C

Eventuell vorhandene Dateien mit gleichem Namen werden überschrieben. SMBS2 kann in der OpenView NNMGR-Umgebung nicht unter anderen Pfadnamen installiert werden. Die Pfadnamen werden in der NNMGR-Version 4.1 durch das Skript *ov.envvars.sh* geladen.

postinstall-Prozedur

In der folgenden *postinstall*-Prozedur müssen drei Verarbeitungsschritte ausgeführt werden.

1. Der Inhalt der MIB-Dateien muss in die Datenbasis übernommen werden, dies geschieht durch das Kommando *xnmloadmib*, das für jede MIB aufzurufen ist. Sind die MIBs durch eine frühere Installation schon geladen, ist eine Aktualisierung nicht unbedingt notwendig. Es gibt deshalb während der Installation eine Abfrage, ob das Neuladen der MIBs gewünscht ist. Der Defaultwert für die Antwort ist *JA*. Ein schon geladener älterer Stand der MIBs wird in diesem Fall überschrieben. Werden die MIBs nicht neu geladen, können als Folge von Inkompatibilitäten zwischen MIBs und Fensterdefinitionen im späteren Betrieb Fehler bei der Anzeige von Objekten auftreten.
2. In den Zuordnungsdateien *oid_to_sym* und *oid_to_type* muss jeweils eine Zeile für das BS2000/OSD-Symbol ergänzt werden.
3. Die Einträge in der Field-Datei müssen mit dem Kommando *own-fields* in die Datenbasis von OpenView eingebracht werden. Dieser letzte Schritt ist irreversibel. Die Field-Einträge können aus der Datenbasis nur noch durch den Austausch der kompletten Datenbasis entfernt werden.

Im vollen Umfang wird die Installation von SMBS2 erst wirksam, wenn OpenView das erste Mal nach dem Abschluss der Installation gestartet wird. Nur das Laden der MIBs hat schon Auswirkungen auch auf laufende OpenView-Aufrufe. Die MIB-Struktur ist sofort nach dem Laden der MIBs im MIB-Browser bekannt, sodass mit seiner Hilfe die Objektwerte gelesen und gesetzt werden können.

3.4.5.2 Konfiguration von OpenView NNM

Nach der erfolgreichen Installation von SMBS2 verfügt die Menüleiste über einen Eintrag für die BS2000/OSD-Oberfläche. Die Funktionen der installierten Applikation können jedoch erst genutzt werden, wenn ein BS2000/OSD-System in die Verwaltung aufgenommen ist. Dafür muss eine BS2000/OSD-Ikone im Netzbild platziert werden. Das kann automatisch geschehen, wenn der *netmon* beim Ausforschen des Netzes ein BS2000/OSD-System mit einem aktiven SNMP-Agenten entdeckt. Andernfalls wird die Ikone manuell mit folgenden Schritten eingefügt:

- Starten Sie den OpenView Network Node Manager.
- Wechseln Sie in das gewünschte Netzbild.
  Es kann notwendig sein, für das Teilnetz, in dem sich das BS2000/OSD-System befindet, ein neues Netzbild zu erzeugen. Wie dabei vorzugehen ist, kann im OpenView Handbuch nachgelesen werden.
- Wählen Sie die Funktion *Add-Object* im Menü *Edit* aus.
- Es erscheint ein Fenster mit dem Titel *Add Object: Palette*. In der oberen Hälfte des Fensters sind unter dem Titel *Symbol-Classes* verschiedene Ikonen dargestellt. Von diesen Ikonen müssen Sie mit der linken Maustaste die Ikone *Computer* anklicken. Nachdem Sie das getan haben, wird auch das darunter liegende Feld mit Ikonen gefüllt. Es handelt sich um die *Symbol Subclasses for Class Computer*. Unter ihnen befindet sich auch die BS2000/OSD-Ikone.
- Greifen Sie die BS2000/OSD-Ikone mit der Maus, indem Sie die mittlere Maustaste drücken. Mit gedrückt gehaltener mittlerer Taste wird die Ikone in das Netzbild gezogen.
- Nachdem die Maustaste losgelassen ist, wird die BS2000/OSD-Ikone an der markierten Stelle plaziert, und gleichzeitig wird das Fenster mit dem Titel *Add Object* geöffnet. In diesem Fenster können die Attribute für das neue Symbol im Netzbild eingetragen werden.
  Neben dem *Label* und dem *Selection-Name* sind die Objektattribute wichtig, die die Beziehung zum realen Objekt definieren. Diese Objektattribute sind in drei Gruppen eingeteilt, die in verschiedenen Dialogboxen bearbeitet werden. Das Fenster für eine Attributgruppe lässt sich durch die Betätigung des Druckknopfes *Set Object Attributes...* öffnen. Dieser Knopf wird jedoch nur dann freigegeben, wenn in der nebenstehenden Liste eine Attributgruppe markiert ist.

Die drei Gruppen von Objektattributen haben folgende Bedeutung:

– Capabilities

  In diesem Fenster kann nichts eingetragen werden. Alle Schalter im Fenster erscheinen schraffiert, das heißt, sie sind gesperrt. Alle dargestellten Attributwerte sind fest mit dem BS2000/OSD-Symbol verbunden und werden deshalb nur angezeigt ohne die Möglichkeit, sie zu setzen. Wichtig ist, dass die BS2000/OSD-Ikone die Eigenschaften *isSNI* und *isBS2000* erfüllt, weil dies in der Ausführungsbedingung der einzelnen Aktionen der BS2000-Anwendung vom selektierten Symbol verlangt wird.

– General Attributes

  Zu dieser Gruppe gehören vier Attribute, die im Gegensatz zu den Attributen der ersten Gruppe auch gesetzt werden können. Es handelt sich um die Attribute *isSNMPSupported*, welches gesetzt ist, *isSNMPProxied*, welches nicht gesetzt ist, und die zwei Attribute *Vendor* und *SNMPAgent* mit den Werten *SNI* und *SNI BS2000-SNMP-Agent*. Die Werte dieser Attribute sollen nicht verändert werden. Die ersten beiden Attributwerte gehören ebenfalls zur Ausführungsbedingung der Aktionen in der BS2000/OSD-Anwendung.

– IP Map

  Diese Gruppe von Attributen ist die wichtigste der drei, weil hier die Daten für die Netzverbindung zum dargestellten Gerät eingetragen werden. Es sind dies der Hostname, die IP-Adresse und die Subnet-Maske. Bevor die Daten übernommen werden können, müssen sie verifiziert sein. Diese Prüfung geschieht entweder automatisch oder muss explizit durch die Betätigung des *Verify*-Knopfes gestartet werden. Nach der erfolgreichen Prüfung wird der *OK*-Knopf entsperrt. Mit ihm kann das Fenster geschlossen werden, dabei werden die im Fenster eingetragenen Daten in die Datenbasis übernommen.

Nach dem Eintragen aller Attribute wird das Fenster mit dem *OK*-Knopf geschlossen.

- Standardmäßig wird eine bestimmte SNMP-Konfiguration für die Kommunikation mit einem Agenten verwendet. Wenn eine besondere Portnummer oder eine andere Community benutzt werden sollen, muss eine andere SNMP-Konfiguration definiert werden. Die Dialogbox dafür kann mit dem Eintrag *SNMP Configuration...* im Menü *Options* geöffnet werden. In der unteren Hälfte der Dialogbox können besondere OpenView-SNMP-Parameter für ein einzelnes Zielgerät oder eine Gruppe von ihnen eingetragen werden.

3.4.5.3 Deinstallation

Bei der Deinstallation soll der Zustand von OpenView NNM vor der Installation von SMBS2 so weit wie möglich wiederhergestellt werden. Zu Beginn der Deinstallation werden alle Plattformen aufgelistet, auf denen das Paket SMBS2 installiert ist. Ältere Versionen als die Version 3.0A von SMBS2 können dabei nicht erfasst werden. Eine Deinitialisierung wird nur auf den angezeigten Plattformen ausgeführt.

Es werden alle Paketdateien gelöscht, und aus den Zuordnungsdateien *oid_to_sym* und *oid_to_type* werden die Einträge für das BS2000/OSD-Symbol entfernt. Die neuen Field-Einträge können aus der Datenbasis nicht mehr entfernt werden, weil eine Änderung der Datenbasis grundsätzlich ausgeschlossen ist. Die BS2000/OSD-MIBs werden auf Wunsch des Benutzers nicht entladen. Sie bleiben dann im MIB-Browser verfügbar.

3.5 Installation der Management-Anwendungen

Die Installation des Software-Pakets tclset ist Voraussetzung für den Einsatz der Management-Anwendungen aus den Paketen BMBS2, CMBS2 und PMBS2 auf Reliant UNIX und Windows NT.

Die Installation des Software-Pakets SMAWtcl ist Voraussetzung für den Einsatz der Management-Anwendungen aus den Paketen SMAWbmbs2, SMAWcmbs2 und SMAWpmbs2 auf Solaris.

Die nächsten Abschnitte beschreiben die Installation des Interpreters und der Anwendungen auf Solaris und Reliant UNIX sowie auf Windows NT.

Bei den Betriebssystemen Solaris und Reliant UNIX kann zusätzlich der Trap-Server installiert werden.

Auf der mitgelieferten CD sind enthalten:

tclset / SMAWtcl	Interpreter für Tcl/Tk (Voraussetzung für die Anwendungen BMBS2, CMBS2 und PMBS2 bzw. SMAWbmbs2, SMAWcmbs2, SMAWpmbs2)
BMBS2 / SMAWbmbs2	BCAM-Monitor für BS2000/OSD
CMBS2 / SMAWcmbs2	Console Monitor für BS2000/OSD
PMBS2 / SMAWpmbs2	Performance-Monitor für BS2000/OSD
trpsrv / SMAWtrpsv	Trap-Server für Reliant UNIX bzw. Solaris

Eine ausführliche Beschreibung der Konfiguration und des Betriebs von CMBS2 und PMBS2 entnehmen Sie bitte dem Kapitel „Betrieb der Management-Station“ (siehe Seite 339).

3.5.1 Installation auf Solaris und Reliant UNIX

Installation des Interpreters Tcl-Set für Tcl/Tk-Anwendungen

Je nach eingesetztem Betriebssystem installieren Sie:

– Interpreter Tcl-Set für Solaris: SMAWtcl
– Interpreter Tcl-Set für Reliant UNIX: tclset

Installation des Interpreters Tcl-Set für Tcl/Tk-Anwendungen auf Solaris

Das Paket SMAWtcl umfasst

– Verzeichnis *bin* mit dem Hauptprogramm
– Verzeichnis *lib* mit den Tcl-Scripten und den dynamischen Bibliotheken

Während des Installationsverfahrens wird festgelegt, in welchem Verzeichnis *SMAWtclset* installiert werden soll. Standardmäßig wird das Verzeichnis *opt/SMAW* genutzt; dieses Verzeichnis muss existieren. Angelegt wird ein Verzeichnis *SMAWtcl* mit den oben genannten Unterverzeichnissen.

Die Installation im Root-Verzeichnis bzw. unter */var* ist nicht zulässig.

Installation des Interpreters Tcl-Set für Tcl/Tk-Anwendungen auf Reliant UNIX

Das Paket tclset umfasst

– Verzeichnis *bin* mit dem Hauptprogramm
– Verzeichnis *lib* mit den Tcl-Scripten und den dynamischen Bibliotheken

Während des Installationsverfahrens wird festgelegt, in welchem Verzeichnis *tclset* installiert werden soll. Standardmäßig wird das Verzeichnis */usr/local* genutzt; dieses Verzeichnis muss existieren. Angelegt wird ein Verzeichnis *tcl* mit den oben genannten Unterverzeichnissen.

Die Installation im Root-Verzeichnis bzw. unter */var* ist nicht zulässig.

Installation des Trap-Servers

Den Trap-Server für Solaris (Package *SMAWtrpsv*) und Reliant UNIX (Package *trpvsrv*) installieren Sie gemäß dem Package-Verfahren mit *pkgadd*. Nähere Informationen zum Trap-Server für Solaris und Reliant UNIX finden Sie im Kapitel „Trap-Server für Solaris und Reliant UNIX“ auf Seite 439.

Installation der Anwendungen

Im Verlauf des Installationsverfahrens legen Sie fest, in welchem Verzeichnis die Management-Anwendungen installiert werden sollen. Vorgeschlagen wird die Installation im Basisverzeichnis des Interpreters Tcl-Set. Ist dieses Verzeichnis nicht vorhanden, dann wird es angelegt. Anders lautende Verzeichnisse müssen existieren.

Angelegt werden im Verzeichnis *Bmon* (BMBS2), *Cmon* (CMBS2) bzw. *Pmon* (PMBS2) die Unterverzeichnisse *bin*, *lib*, *help*, *asn1*, *config* und *bitmaps*.

In der das Hauptprogramm einschalenden Prozedur werden die notwendigen Umgebungsvariablen gesetzt.

Konfiguration von CMBS2 (Solaris und Reliant UNIX)

Das Paket *SMAWtcl* (Solaris) bzw. *tclset* (Reliant UNIX) enthält einen Trap-Dämon *nmtrapd*. Im Paket *SMAWtrpsv* (Solaris) bzw. *trpsrv* (Reliant UNIX) ist ein weiterer, umfassenderer Trap-Verteiler enthalten, dem Sie den Vorzug gegenüber *nmtrapd* geben sollten (siehe Kapitel „Trap-Server für Solaris und Reliant UNIX“ auf Seite 439).

Ein Trap-Verteiler erfüllt zwei Aufgaben:

- Er multipliziert die am System eingehenden Traps
  - für die verschiedenen Console Monitor-Anwendungen,
  - für andere Anwendungen, die Traps empfangen.
- Er erlaubt auch nicht privilegierten Anwendungen das Abhören des root-privilegierten Port 162.

Die Nutzung eines Trap-Verteilers ist dann sinnvoll, wenn die Console Monitor-Anwendung nicht exklusiv unter *root* gestartet wird. In allen anderen Fällen wird kein Trap-Verteiler benötigt.

Mit der Umgebungsvariablen TNM_TRAPD können Sie festlegen,

- ob ein Trap-Verteiler eingesetzt werden soll, und wenn ja,
- welcher Trap-Verteiler eingesetzt werden soll.

Die Umgebungsvariable TNM_TRAPD kann folgende Werte annehmen:

Wert	Bedeutung
NMTRAPD	Es wird der Trapverteiler *nmtrapd* verwendet.
TRPSRV	Es wird der Trapverteiler *trpsrv* verwendet.
TRPTCC	Es wird der Trapverteiler *trd_distr* von TransView verwendet.
NO	Es wird kein Trapverteiler verwendet; der Port wird über die Oberfläche von CMBS2 eingestellt (Default-Wert: 162).

3.5.2 Installation auf Windows NT

Installation des Interpreters Tcl-Set für Tcl/Tk-Anwendungen

Das Paket *tclset* ist das Basispaket für die Nutzung der Managementanwendungen BCAM-Monitor, Performance-Monitor und Console Monitor auf Windows NT.

Das Paket *tclset* umfasst:

– Verzeichnis *Bin* mit dem Hauptprogramm und dynamischen Bibliotheken,
– Verzeichnis *Inst* mit Installationsprozeduren,
– Verzeichnis *Lib* mit den Tcl-Scripten.

Im Verlauf des Installationsverfahrens kann bestimmt werden, in welchem Verzeichnis das Produkt installiert werden soll. Vorgeschlagen wird die Installation im Verzeichnis *C:\Programme\Tcl*. Dort werden die oben genannten Verzeichnisse *Bin*, *Inst* und *Lib* angelegt.

Installation der Anwendungen

Voraussetzung für den Betrieb von BMBS2, CMBS2 und PMBS2 ist das Paket *tclset*, Version ≥ 05.0A.00, das den Interpreter enthält.

Die Anwendung umfasst jeweils

– das Verzeichnis *Asn1* mit den MIB-Dateien,
– das Verzeichnis *Bin* mit dem Hauptprogramm,
– das Verzeichnis *Bitmaps* mit Bitmapdateien,
– das Verzeichnis *Help* mit den Hilfetexten,
– das Verzeichnis *Inst* mit Installations- und Deinstallationsprogrammen und dem Installationslogfile,
– das Verzeichnis *Lib* mit den Tcl-Scripten,
– das Verzeichnis *config* mit der Konfigurationsdatei *cmon_cnf.prt* bzw. *pmon_cnf.prt*.

Im Verlauf des Installationsverfahrens kann bestimmt werden, in welchem Verzeichnis die Anwendung BMBS2, CMBS2 bzw. PMBS2 installiert werden soll. Die Installationspfade dürfen keine Blanks enthalten.

Vorgeschlagen wird die Installation im Basisverzeichnis des Produktes *tclset* unter dem Verzeichnis *appl*. Ist dieses Verzeichnis nicht vorhanden, wird es angelegt.

Angelegt werden im Verzeichnis BMBS2, CMBS2 bzw. PMBS2 die oben genannten Unterverzeichnisse. Existiert im Installationsverzeichnis noch keine Datei *cmon.cnf*, so wird die Prototypdatei *cmon_cnf.prt* nach *cmon.cnf* kopiert. Analoges gilt für die Datei *pmon.cnf.*

4 Betrieb

Die Liefereinheit SBA-BS2 V5.0 enthält den Masteragenten, den Supervisor Subagenten, den HTML-Subagenten, den Application Monitor Subagenten und den Console Monitor Subagenten. Mit SSC-BS2 V5.0 wird ein Set von Subagenten für BS2000/OSD-spezifische Management-Aufgaben ausgeliefert. Außerdem stehen mit SSA-SM2-BS2 und SSA-OUTM-BS2 zwei additive Subagenten zur Performance-Überwachung bzw. *open*UTM-Anwendungsüberwachung zur Verfügung. *open*Net Server stellt einen MIB-II-Subagenten gemäß RFC 1213 und einen Subagenten mit einer BCAM-spezifischen MIB zur Verfügung. In diesem Kapitel werden die In- und Außerbetriebnahme der einzelnen Komponenten in BS2000/OSD sowie die Kommandos zum Versenden von Traps beschrieben. Der letzte Abschnitt informiert über das Verhalten im Fehlerfall.

4.1 In- und Außerbetriebnahme

Die Subagenten sind nur bei gestartetem Masteragenten funktionsfähig, sie können mit Ausnahme des Supervisor Subagenten jederzeit einzeln gestartet und beendet werden.

Voraussetzung für das Starten der Agenten sind

- eine betriebsbereite LAN1-Verbindung zwischen BS2000/OSD-Rechner und Management-Plattform,
- ein gestartetes POSIX-Subsystem,
- ein installiertes Subsystem SNMP,
- Privilegien (siehe nächste Seite).

Folgende Privilegien werden zum Starten der einzelnen Agenten benötigt:

Kommando	**Privileg**
START-SNMP-MASTER	NET-ADMINISTRATION
START-SNMP-APPMON	NET-ADMINISTRATION
START-SNMP-CONSMON	NET-ADMINISTRATION
START-SNMP-HTML	NET-ADMINISTRATION
START-SNMP-AVAS	NET-ADMINISTRATION
START-SNMP-FT	FT-ADMINISTRATION
START-SNMP-HIPLEX-AF	NET-ADMINISTRATION
START-SNMP-HOSTRES	NET-ADMINISTRATION
START-SNMP-HSMS	HSMS-ADMINISTRATION
START-SNMP-OMNIS	NET-ADMINISTRATION
START-SNMP-PRINTSERVICE	PRINT-SERVICE-ADMINISTRATION
START-SNMP-SESAM	NET-ADMINISTRATION
START-SNMP-STORAGE	NET-ADMINISTRATION
START-SNMP-PERFMON	SW-MONITOR-ADMINISTRATION
START-SNMP-UTM	NET-ADMINISTRATION
START-SNMP-MIB-MIB2	NET-ADMINISTRATION
START-SNMP-MIB-BCAM	NET-ADMINISTRATION

Um den Masteragenten zu starten, muss die BS2000/OSD-Kennung die POSIX-UserID 0 (SYSROOT) besitzen.

Das Stoppen der Agenten muss entweder unter der Kennung TSOS erfolgen oder unter derselben Kennung, unter der das Startkommando abgegeben wurde.

rc-Scripte

Mit der Version V5.0 werden rc-Skripte installiert, die ein automatisches Starten der Agenten beim Hochfahren von POSIX bzw. ein automatisches Stoppen beim Beenden von POSIX erlauben. Diese Prozeduren werden im Verzeichnis */etc/rc0.d* bzw. */etc/rc2.d* abgelegt. Bis auf den Start des Masteragenten sind alle Aufrufe auskommentiert. Damit haben Sie die Möglichkeit, die Prozeduren an Ihre Konfiguration individuell anzupassen.

Name der Prozedur	Funktion
S90snmpsba	Starten der Agenten von SBA-BS2
S91snmpssc	Starten der Agenten von SSC-BS2
S91snmputm	Starten des *open*UTM-Agenten (SSA-OUTM-BS2)
S91snmpsm2	Starten des SM2-Agenten (SSC-SM2-BS2)
K10snmpsba	Stoppen der Agenten von SBA-BS2
K11snmpssc	Stoppen der Agenten von SSC-BS2
K11snmputm	Stoppen des *open*UTM-Agenten (SSA-OUTM-BS2)
K11snmpsm2	Stoppen des SM2-Agenten (SSC-SM2-BS2)

Trace-Dateien

Während des Betriebs der Agenten werden unter der Kennung, unter der der Agent gestartet wurde, Trace-Dateien erzeugt. Die Trace-Dateien werden mit dem Namen *SYSTRC.SNMP.<agent>.<datum>.<uhrzeit>* angelegt und können, sofern sie nicht mehr benötigt werden, nach Beendigung des entsprechenden Agenten gelöscht werden. Die Meldungen der Agenten werden standardmäßig in diesen Trace-Dateien im BS2000/OSD-Dateisystem abgelegt.

Der Name einer Trace-Datei *SYSTRC.SNMP.<agent>.<datum>.<uhrzeit>* ist folgendermaßen aufgebaut:

`<agent>`	ist der Name des Agentenprogramms.
`<datum>`	ist das aktuelle Datum in der Form: JJJJ-MM-TT
`<uhrzeit>`	ist die aktuelle Zeit in der Form: SSMMSS

Beispiel:

```
/FS SYSTRC.SNMP.
%       9 :2DC1:$DC14.SYSTRC.SNMP.AVASAGT.1999-02-19.101643
%       9 :2DC1:$DC14.SYSTRC.SNMP.AVASAGT.1999-03-07.165625
%      78 :2DC1:$DC14.SYSTRC.SNMP.AVASAGT.1999-03-07.171451
```

4.1.1 Masteragent

Vor dem ersten Start des Masteragenten muss im BS2000/OSD die Datei */etc/snmp/agt/snmpd.cnf* an die eigene Konfiguration angepasst werden (siehe Seite 57).

Starten des Masteragenten im BS2000/OSD:

/START-SNMP-MASTER
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54 without-gen-vers> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

oder in der POSIX-Shell mit:

```
snmpdm
```

Der Start des Masteragenten, wie auch aller anderen Agenten, sollte im Hintergrund erfolgen, da sonst die Shell blockiert wird.

Stoppen des Masteragenten im BS2000/OSD:

/STOP-SNMP-MASTER
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
snmpdmcmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.
Das Intervall wird vom Supervisor Subagenten zur Überprüfung seiner Subagenten-Tabelle genutzt. Wurde vom Subagenten während der letzten fünf Minuten keine Nachricht empfangen, überprüft der Supervisor diesen Subagenten durch eine Anfrage.

4.1.2 Subagenten des BASIC-AGENT

Neben dem Supervisor Subagent zur Überwachung der am Masteragenten angemeldeten Subagenten existieren als weitere Subagenten des BASIC-AGENT der Application Monitor Subagent, der Console Monitor Subagent und der HTML-Subagent. Der Application Monitor dient zur Überwachung von Subsystemen, BCAM- und User-Anwendungen sowie Jobvariablen und Logging-Dateien. Zur Überwachung der Konsole steht Ihnen der Console Monitor zur Verfügung. Er dient einerseits zum Erfassen von Konsolmeldungen und gestattet andererseits auch die Eingabe von Konsolkommandos. Der HTML-Subagent wird benötigt, wenn SNMP-basierte Management-Informationen in benutzerspezifischen Seiten über das WWW bereit gestellt werden sollen.

4.1.2.1 Supervisor Subagent

Bedingt durch seine enge Verknüpfung mit dem Masteragenten gibt es für den Supervisor Subagenten kein eigenes Start- bzw. Stop-Kommando. Der Start des Supervisor Subagenten wird initiiert durch einen entsprechenden Eintrag in der Datei */etc/snmp/agt/snmpd.cnf*. Solange dieser Eintrag existiert, wird der Supervisor Subagent immer automatisch mit dem Masteragenten gestartet und beendet.

4.1.2.2 Application Monitor Subagent

Der Application Monitor Subagent wird in der POSIX-Shell oder im BS2000/OSD gestartet.

1. Starten im BS2000/OSD:

/START-SNMP-APPMON

VERSION=***STD** / <product-version>
, **MONJV**=***NONE** / <filename 1 .. 54 without-gen-vers>
, **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO**
, **JOB-CLASS**=***STD** / <name 1 .. 8>
, **FILE-NAME**=***NONE** / <filename 1 .. 54 without-gen-vers>
, **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

2. Starten in der POSIX-Shell mit:

```
appmonagt [-f <inputfile>]
          [-t <int>]
```

Beendet wird der Application Monitor (unabhängig von der Umgebung, in der er gestartet wurde) im BS2000/OSD mit:

/STOP-SNMP-APPMON
VERSION=**<u>*STD</u>** / <product-version>

oder in der POSIX-Shell mit:

```
appmoncmd T
```

Beschreibung der Operanden:

VERSION=<u>*STD</u> / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=<u>*NONE</u> / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=<u>*STD</u> / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=<u>*STD</u> / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

FILE-NAME=<u>*NONE</u> / <filename 1..54 without-gen-vers>
Beim Start des Application Monitor kann eine Konfigurationsdatei angegeben werden (siehe Seite 58). Wird keine Konfigurationsdatei angegeben, werden all diejenigen Subsysteme überwacht, die beim Starten des Application Monitor Subagenten dem BS2000/OSD bekannt waren. Die Konfigurationsdatei, definiert durch die Angabe <*filename*> bzw. <*input-file*>, muss im BS2000/OSD-Filesystem abgespeichert sein

TIMER-INTERVAL=<u>5</u> / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.
Die Dateiüberwachung wird bei Ablauf des Zeitintervalls durchgeführt.
Das Überwachungsintervall für Subsysteme errechnet sich aus dem fünffachen Wert des eingestellten Zeitintervalls, also im Standardfall 25 Sekunden.
Zustandsänderungen von Anwendungen bzw. Jobvariablen werden u.U. erst bei Ablauf des Zeitintervalls gemeldet.
Das Überwachungsintervall für DCAM-Anwendungen errechnet sich aus dem 60-fachen Wert des eingestellten Zeitintervalls, beträgt also im Standardfall 5 Minuten.

4.1.2.3 Console Monitor Subagent

Der Console Monitor Subagent wird in der POSIX-Shell oder im BS2000/OSD gestartet.

1. Starten im BS2000/OSD:

/START-SNMP-CONSMON
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **OPERATOR-ID**= <name 1 .. 8> , **PASSWORD**=***NONE** / <c-string 1 .. 8> / ***SECRET** , **OPERATOR-ROLE**= **list-poss(10)** <name 1 .. 8> , **MSG-FILTER**=***NONE** / <filename 1 .. 54> / <posix-pathname> , **SUPPRESS-MSG-FILE** = ***NONE** / <filename 1 .. 54> / <posix-pathname> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

2. Starten in der POSIX-Shell mit:

```
consmonagt  -o <operid>
            [-t <int>]
            [-p <password>]
            [-f <msg-filter>]
            [-n <negative-msg-filter>]
            <op-role1> [,<op-role2>, ...., <op-role10>]
```

Beendet wird der Console Monitor (unabhängig von der Umgebung, in der er gestartet wurde) im BS2000/OSD mit:

/STOP-SNMP-CONSMON
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
consmoncmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

OPERATOR-ID=<name 1 .. 8>
Benutzerkennung, mit der sich der Subagent bei $CONSOLE anmeldet.

PASSWORD=*NONE / <c-string 1 .. 8> / *SECRET
Definition des das Passworts, das den Subagenten zum Zugriff auf $CONSOLE berechtigt. Die Standardangabe *NONE sorgt dafür, dass kein Passwort angegeben werden muss. *SECRET bewirkt, dass das Feld zur Passworteingabe dunkel gesteuert ist.

OPERATOR-ROLE=list-poss(10) <name 1 .. 8>
Name der Operator-Rolle, die die zur Konsolüberwachung relevanten Routingcodes enthält.

MSG-FILTER=*NONE / <filename 1 .. 54>
Name der Datei (<filename> bzw. <posix-pathname>), die die relevanten Meldungsschlüssel enthält.*NONE (Standardwert) bedeutet, es wird keine Datei mit Meldungsschlüsseln zugewiesen.

SUPPRESS-MSG-FILE=*NONE / <filename 1 .. 54> / <posix-pathname>
Die mit <filename> bzw. <posix-pathname> definierte Datei enthält die zu unterdrückenden Konsolmeldungsschlüssel. *NONE (Standardwert) bedeutet, es wird keine Datei mit zu unterdrückenden Meldungsschlüsseln zugewiesen.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.1.2.4 HTML-Subagent

Der HTML-Subagent ist ein Subagent, der in der POSIX-Shell oder im BS2000/OSD gestartet wird.

1. Starten im BS2000/OSD:

/START-SNMP-HTML
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54 without-gen-vers> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

2. Starten in der POSIX-Shell mit:

```
htmlagt [-t <int>]
```

Beendet wird der HTML-Subagent (unabhängig von der Umgebung, in der er gestartet wurde) im BS2000/OSD mit:

/STOP-SNMP-HTML
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
htmlcmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.1.3 Subagenten der STANDARD-COLLECTION

Die SNMP-STANDARD-COLLECTION-BS2000 enthält in der Version V5.0 die Subagenten für AVAS, FT-BS2000 bzw. *open*FT (BS2000), HIPLEX-AF, HSMS, OMNIS, Host Resources, PrintService, SESAM, Storage-Management und zur SM2-basierten Performance-Basisüberwachung. Detaillierte Beschreibungen dieser Subagenten befinden sich im Kapitel „Funktionen der STANDARD-COLLECTION“ (siehe Seite 211).

Weitere Subagenten werden mit *open*Net Server (MIB-II und Private MIB) bzw. als additive Subagenten (SM2 und UTM) ausgeliefert. Informationen zu diesen Subagenten finden Sie ab Seite 159.

4.1.3.1 Subagent für AVAS

Vor dem Start des AVAS-Subagenten nötige Konfigurationsarbeiten sind auf Seite 79 beschrieben.

Starten des AVAS-Subagenten im BS2000/OSD:

/START-SNMP-AVAS
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **FILE-NAME**=<filename 1 .. 54> , **DELAY-TIME**=60 / <integer 0 .. 3600> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

Stoppen des AVAS-Subagenten im BS2000/OSD:

/STOP-SNMP-AVAS
VERSION=***STD** / <product-version>

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

FILE-NAME=<filename 1 .. 54>
Mit FILE-NAME wird der Name der AVAS-Generierungsdatei GENPAR zugewiesen.

DELAY-TIME=60 / <integer 0 .. 3600>
Hat der Subagent keine Verbindung zu AVAS, versucht er bei neuen Requests diese Verbindung herzustellen. Mit DELAY-TIME wird die Zeit (Angabe in Sekunden) angegeben, die zwischen zwei Verbindungsversuchen vergehen muss. Sie haben die Möglichkeit, weitere Verbindungsversuche zu unterdrücken, indem Sie DELAY-TIME=0 setzen.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.1.3.2 Subagent für *open*FT

Starten des FT-Subagenten im BS2000/OSD:

/START-SNMP-FT
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

oder in der POSIX-Shell mit:

```
ftagt [-t <int>]
```

Beendet wird der Subagent unabhängig von der Umgebung, in der er gestartet wurde, mit dem BS2000/OSD-Kommando:

/STOP-SNMP-FT
VERSION=***STD** / <product-version>

oder in der POSIX-Shell ab BS2000/OSD V2.0 mit:

```
ftcmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.1.3.3 Subagent für HIPLEX-AF

Der HIPLEX-AF-Subagent wird in der POSIX-Shell oder im BS2000/OSD gestartet.

1. Starten im BS2000/OSD:

/START-SNMP-HIPLEX-AF
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54 without-gen-vers> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **USER-ID**=**TSOS** / <name 1..8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

2. Starten in der POSIX-Shell mit:

```
hiplexAFagt [-t <int>][ -u <user-id>]
```

Beendet wird der HIPLEX-AF-Subagent (unabhängig von der Umgebung, in der er gestartet wurde) im BS2000/OSD mit:

/STOP-SNMP-HIPLEX-AF
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
hiplexAFcmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

USER-ID=TSOS / <name 1..8>
Benutzerkennung, die als Ablaufkennung für HIPLEX AF benötigt wird.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.1.3.4 Subagent für HSMS

Der HSMS-Subagent kann im BS2000/OSD oder in der POSIX-Shell gestartet werden.

1. Starten im BS2000/OSD:

/START-SNMP-HSMS
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54 without-gen-vers> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767> , **HSMS-LIBRARY = *STD** / <filename 1 .. 54>

2. Starten in der POSIX-Shell:

```
hsmsagt [-t <int>] -l <HSMS-library>
```

Beendet wird der HSMS-Subagent (unabhängig von der Umgebung, in der er gestartet wurde) im BS2000/OSD mit:

/STOP-SNMP-HSMS
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
HSMScmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

HSMS-LIBRARY=*STD / <full-filename 1..54>
Pfadname der HSMS-SYSLIB. Bei Angabe von *STD wird der Name über IMON ermittelt**.**

4.1.3.5 Host Resources Subagent

Der Subagent kann in BS2000/OSD oder in der POSIX-Shell gestartet werden.

Starten in BS2000/OSD:

/START-SNMP-HOSTRES
VERSION = ***STD** / <product-version> , **MONJV** = ***NONE** / <filename 1 .. 54> , **CPU-LIMIT** = =***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS** = ***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

oder in der POSIX-Shell mit:

```
hostresagt [-t <int>]
```

Stoppen des Subagenten im BS2000/OSD:

/STOP-SNMP-HOSTRES
VERSION = ***STD** / <product-version>

oder in der POSIX-Shell mit:

```
hostrescmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.1.3.6 Subagent für OMNIS

Der Subagent kann in BS2000/OSD oder in der POSIX-Shell gestartet werden.

Starten im BS2000/OSD:

/START-SNMP-OMNIS
VERSION = ***STD** / <product-version> , **MONJV** = ***NONE** / <filename 1 .. 54> , **CPU-LIMIT** = =***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS** = ***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767> , **CONFIGURATION-FILE** = <filename 1 .. 54>

oder in der POSIX-Shell mit:

```
omnisagt –f <filename>
        [–t <int>]
```

Stoppen des Subagenten im BS2000/OSD:

/STOP-SNMP-OMNIS
VERSION = ***STD** / <product-version>

oder in der POSIX-Shell mit:

```
omniscmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.
Bei sechsfachem Ablauf des Timers - also standardmäßig alle 30 Sekunden - werden an der DCAM-Schnittstelle alle vorhandenen OMNIS-Meldungen abgeholt und als Trap an die Management-Station geschickt werden.

CONFIGURATION-FILE-=<filename 1 .. 54>
Beim Start muss dem Subagenten die mit CONFIGURATION-FILE=<*filename*> bezeichnete Datei zugewiesen werden, die die Namen mit dem/den zu überwachenden OMNIS/en enthält.

4.1.3.7 Subagent für SESAM

Der Subagent kann in BS2000/OSD oder in der POSIX-Shell gestartet werden.

Starten im BS2000/OSD:

/START-SNMP-SESAM
VERSION = ***STD** / <product-version> , **MONJV** = ***NONE** / <filename 1 .. 54> , **CPU-LIMIT** = =***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS** = ***STD** / <name 1 .. 8> , **FILE-NAME** = <filename 1 .. 54> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

oder in der POSIX-Shell mit:

```
sesamagt –f <inputfile>
        [–t <int>]
```

Stoppen des Subagenten im BS2000/OSD:

/STOP-SNMP-SESAM
VERSION = ***STD** / <product-version>

oder in der POSIX-Shell mit:

```
sesamcmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

FILE-NAME=<filename 1 .. 54>
Beim Start muss dem Subagenten die mit FILE-NAME=<*filename*> bzw. <*inputfile*> bezeichnete Konfigurationsdatei zugewiesen werden. Die Konfigurationsdatei muss unabhängig vom Start-Kommando immer im BS2000/OSD-Filesystem katalogisiert sein (siehe Seite 81).

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.
Bei jedem Ablauf des Zeitintervalls wird auch die Beziehung zwischen Server und Datenbank überprüft.

4.1.3.8 Subagent für Spool & Print Service

Starten im BS2000/OSD:

/START-SNMP-PRINTSERVICE
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

oder in der POSIX-Shell mit:

```
printagt [-t <int>]
```

Stoppen des Subagenten im BS2000/OSD:

/STOP-SNMP-PRINTSERVICE
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
printcmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.1.3.9 Subagent für Storage-Management

Der Subagent kann im BS2000/OSD oder in der POSIX-Shell gestartet werden.

Starten im BS2000/OSD:

/START-SNMP-STORAGE
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **FILE-NAME**=***NONE** / <filename 1 .. 54> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

In der POSIX-Shell mit:

```
storageagt [-f <inputfile>]
           [-t <int>]
```

Beendet wird der Subagent unabhängig von der Umgebung, in der er gestartet wurde, mit dem BS2000/OSD-Kommando:

/STOP-SNMP-STORAGE
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
storagecmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

FILE-NAME=<filename 1 .. 54>
Name der Input-Datei, falls Pubsets oder Platten überwacht werden sollen.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

Pubsets oder Platten überwacht der Subagent für das Storage Management in einem Abstand von 6 * TIMER-INTERVALL Sekunden.

4.1.3.10 Subagent zur Performance-Basisüberwachung

Voraussetzung für den Start des Subagenten zur Performance-Überwachung mit SM2 (PerfMonB) ist ein gestartetes Subsystem SM2 (in BS2000/OSD V2.0 muss SM2 explizit gestartet werden).

Starten des SM2-Subagenten im BS2000/OSD:

/START-SNMP-PERFMON
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

Stoppen des SM2-Subagenten im BS2000/OSD:

/STOP-SNMP-PERFMON
VERSION=***STD** / <product-version>

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.1.4 Additive Subagenten

Weitere Subagenten, die SNMP-basiertes Management im BS2000/OSD ermöglichen, sind zum einen in *open*Net Server enthalten und zum anderen als additive Subagenten zu SM2 und *open*UTM mit den Produkten SSA-SM2-BS2 und SSA-OUTM-BS2 erhältlich.

4.1.4.1 Subagenten für *open*Net Server und *inter*Net Services

Mit dem BS2000/OSD-Transportsystem *open*Net Server werden zwei Subagenten ausgeliefert. Zum einen der MIB-II-Subagent, der den Zugriff auf die MIB-II gemäß RFC 1213 unterstützt. Zum anderen der BCAM-Subagent, der über eine Private MIB Auskunft über BCAM-spezifische Werte und Einstellungen gibt (siehe Handbuch „SNMP-Management für *open*Net Server“).

Starten des MIB-II-Subagenten im BS2000/OSD:

/START-SNMP-MIB-MIB2
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8>

oder in der POSIX-Shell mit:

```
mib2agt
```

Stoppen des MIB-II-Subagenten im BS2000/OSD:

/STOP-SNMP-MIB-MIB2
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
mib2cmd T
```

Starten des BCAM-Subagenten im BS2000/OSD:

/START-SNMP-MIB-BCAM
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8>

oder in der POSIX-Shell mit:

```
bcamagt
```

Stoppen des BCAM-Subagenten im BS2000/OSD:

/STOP-SNMP-MIB-BCAM
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
bcamcmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

4.1.4.2 Subagent SSA-SM2-BS2 zur Performance-Überwachung

Für den Start des Subagenten zur Performance-Überwachung mit SM2 (PerfMonF) sind Voraussetzung:

– ein gestartetes Subsystem SM2 (in BS2000/OSD V2.0 muss SM2 explizit gestartet werden) und

– die vollständige und erfolgreiche Installation von SSA-SM2-BS2

Beispiel

```
/EXEC $SM2
*call-admin-part
%//set-periodic-task-parameter log-tasks=*none
%//start-measurement-program per
%//start-measurement-program utm
%//call-eval-part
*end
```

Zur Messung von *open*UTM-Anwendungen muss in *open*UTM die SM2-Messung eingeschaltet werden:

```
kdcappl sm2=on
```

Starten des Performance-Subagenten im BS2000/OSD:

/START-SNMP-PERFMON
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

oder in der POSIX-Shell mit:

```
perfagt
```

Stoppen des Performance-Subagenten im BS2000/OSD:

/STOP-SNMP-PERFMON
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
perfcmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.1.4.3 Subagent SSA-OUTM-BS2 für *open*UTM-Anwendungen

Starten des *open*UTM-Subagenten im BS2000/OSD:

/START-SNMP-UTM
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO** , **JOB-CLASS**=***STD** / <name 1 .. 8> , **TIMER-INTERVAL** = 5 / <integer 1 .. 32767>

oder in der POSIX-Shell mit:

```
utmagt [-t <int>]
```

Stoppen des *open*UTM-Subagenten im BS2000/OSD:

/STOP-SNMP-UTM
VERSION=***STD** / <product-version>

oder in der POSIX-Shell mit:

```
utmcmd T
```

Beschreibung der Operanden:

VERSION=*STD / <product-version>
definiert die zu startende bzw. stoppende Version des Agenten. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die den Agenten überwachen soll. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

JOB-CLASS=*STD / <name 1..8>
Jobklasse, mit der der Agent gestartet wird. Bei Angabe von *STD wird die generierte Standard-Jobklasse verwendet.

TIMER-INTERVAL=5 / <integer 1 .. 32767>
Zeitintervall, in dem der Agent überprüft, ob Anforderungen vom Kommandoprogramm vorliegen. Das Zeitintervall ist standardmäßig auf fünf Sekunden eingestellt.

4.2 Trap-Sende-Kommandos

Mit den in SBA-BS2 enthaltenen Trap-Sende-Kommandos können Traps vom BS2000/OSD an einen Zielrechner versandt werden. Die Kennung, unter der der das Kommando abgesetzt wird, benötigt das Privileg NET-ADMINISTRATION.

4.2.1 START-SNMP-TRAPSEND

Mit dem Kommando START-SNMP-TRAPSEND wird ein beliebiger SNMP-Trap an einen Zielrechner versandt.

START-SNMP-TRAPSEND

VERSION=*STD
, **MONJV=*NONE** / <filename 1 .. 54 without-gen-vers>
, **CPU-LIMIT=*STD** / <integer 1 .. 32767> / ***NO**
, **SOURCE-IP-ADDR=*NONE** / <c-string 1..15>
, **DESTINATION-IP-ADDR=*NONE** / <c-string 4..15>
, **COMMUNITY**=<c-string 1..15_with-lower-case>
, **GENERIC-TRAP=0** / <integer_0..6>
, **SPECIFIC-TRAP=0** / <integer 0..2147483647>
, **ENTERPRISE=*1.3.6.1.4.1.231.1.6** / <c-string 3..55 _with-lower-case>
, **SYSUPTIME=0** / <integer -2147483648..2147483647>
, **TRAP-VARIABLE-NAME=*NONE** / <c-string 3..1800_with-lower-case>
, **TRAP-VARIABLE-TYPE=D**/ <c-string 1..3_with-lower-case>
, **TRAP-VARIABLE-VALUE=*NONE** / <c-string ..1800_with-lower-case>

Beschreibung der Operanden:

VERSION=*STD
definiert die Version des Programms. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1 .. 54 without-gen-vers>
Name der Jobvariable, die das Programm überwacht. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

SOURCE-IP-ADDR=*NONE / <c-string 1..15>
IP-Adresse des absendenden Rechners. Verfügt der Rechner über mehrere IP-Adressen, wird im Standardfall die Erste verwendet.

DESTINATION-IP-ADDR=*NONE / <c-string 4 .. 15>
IP-Adresse des Zielrechners. Fehlt diese Angabe (*NONE), wird der Trap an alle in der Datei */etc/snmp/mgr/trap.cnf* definierten Rechner gesendet.

COMMUNITY=<c-string 1..15_with-lower-case>
Community String, mit dem der Trap versandt werden soll.

GENERIC-TRAP=0 / <integer 0 .. 6>
Generic Trap (0 - 6), entspricht den Angaben in RFC 1215

SPECIFIC-TRAP=0 / <integer 0..2147483647>
Spezifische Trapnummer, sofern GENERIC-TRAP=6 angegeben wurde.

ENTERPRISE=*1.3.6.1.4.1.231.1.6 / <c-string 3..55_with-lower-case>
Object Identifier von ENTERPRISE

SYSUPTIME=0 / <integer -2147483648..2147483647>
SYSUPTIME kann zur weiteren Identifikation des Traps verwendet werden. Angabe in Sekunden.

TRAP-VARIABLE-NAME=*NONE / <c-string 3..1800_with-lower-case>
Object Identifier des Objekts, das mitgeschickt werden soll.

TRAP-VARIABLE-TYPE='D' / <c-string 1..3_with-lower-case>
Definiert den Typ des mitgeschickten Wertes. Standardwert: i. Mögliche Angaben:

i	Integer
o	Octet String
d	Object Identifier
a	IP-Adresse
D	Display String

TRAP-VARIABLE-VALUE=*NONE / <c-string 1..1800_with-lower-case>
Mitgeschickter Wert den Angaben unter TRAP-VARIABLE-TYPE entsprechend.

Einträge in der Datei trap.cnf

Die Datei *trap.cnf* enthält Einträge der Form:

```
trap <community-string> <IP-Adresse(Ziel)>
```

Bedeutung:

– <community-string>: frei wählbarer Community-String
– <IP-Adresse(Ziel)>: IP-Adresse des Zielrechners

4.2.2 SEND-TCC-MSG

Mit dem Kommando SEND-TCC-MSG wird ein SNMP-Trap im Format des Objekts *tccGenTrap* an einen Zielrechner versandt. Das Objekt *tccGenTrap* ist in der von TV Control Center definierten MIB *Tcc-MIB* beschrieben. Das Kommando steht im Zusammenhang mit den Management-Stationen TV Control Center und CMBS2, die dieses Trap-Format benötigen.

SEND-TCC-MSG

VERSION=***STD**
, **MONJV**=***NONE** / <filename 1 .. 54 without-gen-vers>
, **CPU-LIMIT**=***STD** / <integer 1 .. 32767> / ***NO**
, **SOURCE-IP-ADDR**=***NONE** / <c-string 1..15>
, **DESTINATION-IP-ADDR**=***NONE** / <c-string 4..15>
, **OBJECT**=***NONE** / <c-string 1..1800_with-lower-case>
, **ANWENDUNG**=<c-string 1..1800_with-lower-case>
, **TEXT**=<c-string 1..1800_with-lower-case>

Beschreibung der Operanden:

VERSION=*STD
definiert die Version des Programms. Diese Angabe wird derzeit nicht ausgewertet.

MONJV=*NONE / <filename 1..54 without-gen-vers>
Name der Jobvariable, die das Programm überwacht. Die Angabe *NONE - keine Überwachung durch eine Jobvariable - ist Standard.

CPU-LIMIT=*STD / <integer 1 .. 32767> / *NO
Angabe der maximalen CPU-Laufzeit in Sekunden. Bei Angabe von *STD wird der generierte Standardwert verwendet.

SOURCE-IP-ADDR=*NONE / <c-string 1..15>
IP-Adresse des absendenden Rechners. Verfügt der Rechner über mehrere IP-Adressen, wird im Standardfall die erste verwendet.

DESTINATION-IP-ADDR=*NONE / <c-string 4..15>
IP-Adresse des Zielrechners. Fehlt diese Angabe (*NONE), wird der Trap an alle in der Datei */etc/snmp/mgr/trap.cnf* definierten Rechner gesendet.

OBJECT=*NONE / <c-string 1..1800_with-lower-case>
Name des Objekts im Netzbild. Dieser wird als Community verwendet und in $DEVC$ eingetragen.

ANWENDUNG=<c-string 1..1800_with-lower-case>
Name der Anwendung, die bei $SOURCE$ eingetragen wird.

TEXT=<c-string 1..1800_with-lower-case>
Text, der bei MSG eingetragen wird.

Einträge in der Datei trap.cnf

Die Datei *trap.cnf* enthält Einträge der Form:

```
trap <community-string> <IP-Adresse(Ziel)>
```

Bedeutung:

– <community-string>: frei wählbarer Community-String
– <IP-Adresse(Ziel)>: IP-Adresse des Zielrechners

4.3 Verhalten im Fehlerfall

Jeder Agent führt Trace-Dateien, in denen standardmäßig Fehlermeldungen protokolliert werden (siehe Seite 131). Zur Verwaltung der Trace-Funktionalität steht jedem Agenten ein eigenes Kommandoprogramm zur Verfügung. Die Kommandoprogramme der einzelnen Agenten dürfen nur dann gestartet werden, wenn auch der entsprechende Agent erfolgreich gestartet wurde. Die vom Kommandoprogramm gebotene Funktionalität erlaubt Ihnen, Trace-Dateien anzuzeigen bzw. zu schließen und den Agenten zu beenden.

Festlegen des Trace-Umfangs

Standardmäßig werden in der Trace-Datei nur Fehlermeldungen protokolliert. Sollte dies zur Diagnose nicht ausreichen, muss der betroffene Agent beendet und mit dem üblichen Startkommando, ergänzt durch die Angabe *TRACE=*APALL*, wieder gestartet werden. In POSIX wird der ausführliche Trace mit dem Schalter *-apall* angefordert, außerdem ist mit *-termout* auch eine zusätzliche Ausgabe des Traces auf Terminal möglich.

Starten des Kommandoprogramms

Voraussetzung für den Betrieb des Kommandoprogramms ist der erfolgreiche Start des entsprechenden Agenten. Die folgende Tabelle listet die Start-Anweisungen der einzelnen Kommandoprogramme auf:

BS2000/OSD-Kommando	POSIX-Kommando	Agent
/START-MASTERCMD	snmpdmcmd	Masteragent / Supervisor
/START-APPMONCMD	appmoncmd	Application Monitor
/START-CONSMONCMD	consmoncmd	Console Monitor
/START-HTMLCMD	htmlcmd	HTML-Subagent
/START-HOSTRESCMD	hostrescmd	Host Resources-Subagent
/START-AVASCMD	avascmd	AVAS-Subagent
/START-FTCMD	ftcmd	FT-Subagent
/START-HIPLEX-AFCMD	hiplexAFcmd	HIPLEX-AF-Subagent
/START-HSMSCMD	hsmscmd	HSMS-Subagent
/START-OMNISCMD	omniscmd	Subagent für OMNIS
/START-SESAMCMD	sesamcmd	SESAM-Subagent
/START-PRINTCMD	printcmd	Subagent für Print- und Spool-Management
/START-STORAGECMD	storagecmd	Subagent für Storage-Management
/START-PERFMONCMD	perfmoncmd	Subagent für den Performance-Monitor

Die Parameter VERSION, MONJV und CPU-LIMIT gelten nur für BS2000/OSD-Kommandos.

BS2000/OSD-Kommando	POSIX-Kommando	Agent
/START-UTMCMD	utmcmd	UTM-Subagent
/START-MIB2CMD	mib2cmd	MIB-II-Subagent (*open*Net Server)
/START-BCAMCMD	bcamcmd	BCAM-Subagent (*open*Net Server)
VERSION=***STD** / <product-version> , **MONJV**=***NONE** / <filename 1 .. 54> , **CPU-LIMIT**=***JOB-REST** / <integer 1 .. 32767>		

Die Parameter VERSION, MONJV und CPU-LIMIT gelten nur für BS2000/OSD-Kommandos.

Nach dem Start des Kommandoprogramms werden zuerst die aktuellen Daten des Subagenten ausgegeben, im folgenden Beispiel sind es die eines AVAS-Subagenten.

Beispiel

```
INFO of AVAS-Subagent
Version :   50A00        FileOut : Yes             Errors  :        0
PID     :      517       TermOut : No              Warnings:        1
LogLevel: APERROR
LogFile : ':2DC1:$DC14.SYSTRC.SNMP.AVASAGT.1999-02-19.101643'
```

Element	Bedeutung
Version	Version der Subagenten
PID	Prozessidentifikation des POSIX-Subsystems (517)
LogLevel	Zu tracende Meldungsklassen (APERROR oder APALL)
LogFile	Absoluter Pfadname der aktuellen Tracedatei
FileOut	Trace-Ausgabe in Datei aktiviert/deaktiviert
TermOut	Trace-Ausgabe auf das Terminal aktiviert/deaktiviert
Errors	Anzahl der bisher aufgetretenen ERROR-Meldungen
Warnings	Anzahl der bisher aufgetretenen WARNING-Meldungen

Wenn das Kommandoprogramm gestartet ist, werden nach dem Drücken der RETURN-Taste im MAIN MENU folgende Optionen zur Trace-Funktionalität angeboten:

s	show trace file	Trace-Datei anzeigen
c	save trace file	Trace-Datei sichern
x	agent executes command	Diese Funktion wird derzeit nur vom Masteragenten und den folgenden Subagenten genutzt: Application Monitor Subagent Console Monitor Subagent SESAM-Subagent
T	terminate agent	Agent beenden
q	quit command program	Kommandoprogramm beenden

Falls beispielsweise der AVAS-Subagent nicht gestartet wurde, beendet sich das entsprechende Kommandoprogramm, in diesem Fall also *avascmd*, sogleich wieder mit folgender Fehlermeldung:

```
--- avascmd: ERROR  14:03:23  08/03/1999
Agent is not running
```

Sollte die folgende Fehlermeldung beim Start eines Subagenten auftreten, obwohl der Agent schon beendet wurde, rufen Sie bitte das entsprechende Kommandoprogramm auf und geben bei Eingabeaufforderung -*CLEAN* an.

```
--- avasagt: ERROR  16:04:23  08/03/1998
Another Agent is probably yet running
Please use command program to terminate that agent correctly
```

5 Funktionen des BASIC-AGENT

5.1 System- und SNMP-Management (Masteragent)

Der Masteragent unterstützt das System- und SNMP-Management mithilfe von zwei Gruppen der MIB-II:

– Gruppe zur Überwachung des Systems
– Gruppe zur SNMP-Überwachung

Darüber hinaus stehen eine Reihe standardisierter und proprietärer MIBs für die SNMP-Administration zur Verfügung.

Der Masteragent unterstützt einzelne, für das SNMP-Management in BS2000/OSD relevante Objekte anderer MIBs.

5.1.1 MIB-II-Werte für die Systemgruppe

MIB-Definition	Zugriff	Erläuterung
sysDescr	read-only	sysDescr definiert den Namen des Geräts, die Software-Version und den Hardware-Typ. Die Beschreibung erfolgt nur in ASCII-Zeichen.
sysObjectID	read-only	sysObjectID definiert exakt die Position des zu managenden Geräts im SMI Enterprise Subtree.
sysUpTime	read-only	sysUpTime definiert die Zeit (Angabe in 1/100 Sekunden) seit der letzten Reinitialisierung der Netzwerkmanagement-Softwarwe.
sysContact	read-write	sysContact enthält einen Text-String, der die Kontaktperson und die Kontaktadresse der Person enthält, die für diesen managebaren Knoten verantwortlich ist.

Gruppe zur Überwachung des Systems

MIB-Definition	Zugriff	Erläuterung
sysName	read-write	sysName enthält einen logischen Namen für das zu administrierende Gerät, der zugleich dem vollen Domain-Namen entspricht.
sysLocation	read-write	sysLocation beschreibt den Standort des Geräts.
sysServices	read-only	sysServices definiert genau die Services (ISO-Schichten), die dieses Gerät unterstützt, wobei das Service-Objekt dem Wert einer Summe - vom Basis wert 0 ausgehend - entspricht.

Gruppe zur Überwachung des Systems

Der in BCAM definierte Hostname wird automatisch als *sysName* abgelegt. Die Werte für *sysContact* und *sysLocation* werden in der Initial System Group festgelegt (siehe Seite 57).

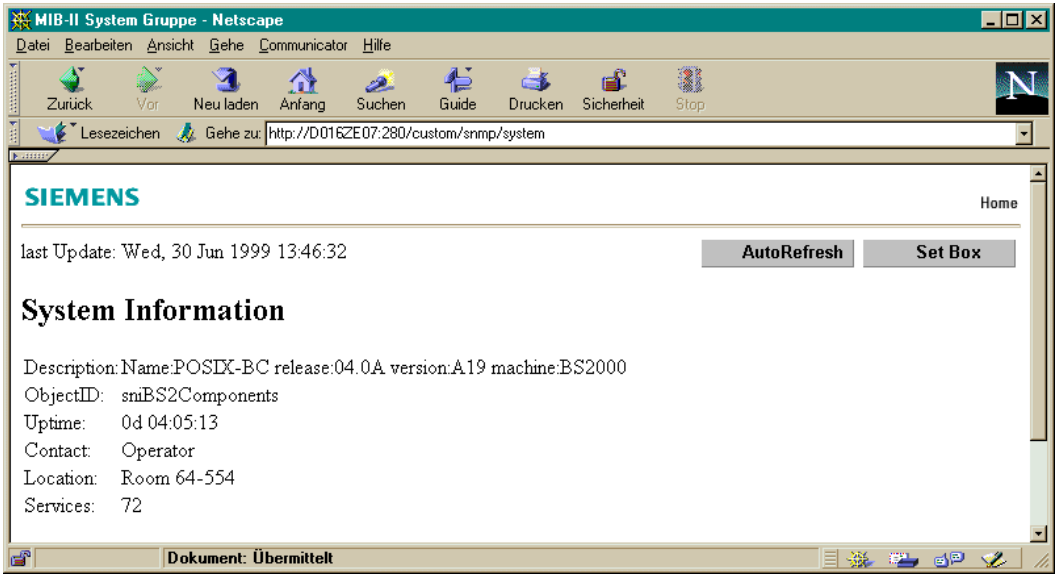


Bild 12: Anzeige der MIB-II-Werte für die Systemgruppe

5.1.2 MIB-II-Werte für die SNMP-Gruppe

Objektname	Zugriff	Erläuterung
snmpInPkts	read-only	Gesamtzahl der Nachrichten, die vom Transportdienst an die SNMP-Entity übermittelt wurden.
snmpOutPkts	read-only	Gesamtzahl der SNMP-Nachrichten, die von der SNMP-Protocol-Entity an den Transportdienst übermittelt wurden.
snmpInBadVersions	read-only	Die Gesamtzahl der SNMP-Nachrichten, die an die SNMP-Protocol-Entity übermittelt wurden und die für eine nicht unterstützte SNMP-Version konzipiert waren.
snmpInBadCommunityNames	read-only	Die Gesamtzahl der SNMP-Nachrichten, die an die SNMP-Protocol-Entity mit einem SNMP-Community-Name übermittelt wurden, der der besagten Entität nicht bekannt ist.
snmpInBadCommunityUses	read-only	Die Gesamtzahl der SNMP-Nachrichten, die an die SNMP-Protocol-Entity übermittelt wurde, die eine SNMP-Operation repräsentierten, die von der SNMP-Community nicht anerkannt wurde, die in der Nachricht genannt wurde.
snmpInASNParseErrs	read-only	Die Gesamtzahl der ASN.1- oder BER-Fehler, die von der SNMP-Protocol-Entity beim Dekodieren der empfangenen SNMP-Nachrichten entdeckt wurden.
snmpInTooBigs	read-only	Die Gesamtzahl der SNMP-PDUs, die an die SNMP-Protocol-Entity übermittelt wurden und für die das Fehlerstatusfeld den Wert "tooBig" aufweist.
snmpInNoSuchNames	read-only	Die Gesamtzahl der SNMP-PDUs, die an die SNMP-Protocol-Entity übermittelt wurden und für die das Fehlerstatusfeld den Wert "noSuchName" aufweist.
snmpInBadValues	read-only	Die Gesamtzahl der SNMP-PDUs, die an die SNMP-Protocol-Entity übermittelt wurden und für die das Fehlerstatusfeld den Wert "badValue" aufweist.

SNMP-Gruppe

Objektname	Zugriff	Erläuterung
snmpInReadOnlys	read-only	Die Gesamtzahl gültiger SNMP-PDUs, die an die SNMP-Protocol-Entity übermittelt wurden und für die das Fehlerstatusfeld den Wert "readOnly" aufweist. Dabei sollte beachtet werden, dass das Erstellen von SNMP-PDUs mit dem Wert "readOnly" im Fehlerstatusfeld einen Fehler darstellt, da solche Objekte als Hilfsmittel beim Erkennen ungültiger Implementierungen von SNMP dienen.
snmpInGenErrs	read-only	Die Gesamtzahl der SNMP-PDUs, die an die SNMP-Protocol-Entity übermittelt wurden und für die das Fehlerstatusfeld den Wert "genErr" aufweist.
snmpInTotalReqVars	read-only	Die Gesamtzahl der MIB-Objekte, die von der SNMP-Protocol-Entity als Ergebnis des Empfangs gültiger SNMP-Get-Request- und Get-Next-PDUs erfolgreich abgerufen wurden.
snmpInTotalSetVars	read-only	Die Gesamtzahl der MIB-Objekte, die von der SNMP-Protocol-Entity als Ergebnis des Empfangs gültiger Set-Request-PDUs erfolgreich geändert wurden.
snmpInGetRequests	read-only	Die Gesamtzahl der SNMP-Get-Request-PDUs, die von der SNMP-Protocol-Entity angenommen und verarbeitet wurden.
snmpInGetNexts	read-only	Die Gesamtzahl der SNMP-Get-Next-PDUs, die von der SNMP-Protocol-Entity angenommen und verarbeitet wurden.
snmpInSetRequests	read-only	Die Gesamtzahl der SNMP-Set-Request-PDUs, die von der SNMP-Protocol-Entity angenommen und verarbeitet wurden.
snmpInGetResponses	read-only	Die Gesamtzahl der SNMP-Set-Response-PDUs, die von der SNMP-Protocol-Entity angenommen und verarbeitet wurden.
snmpInTraps	read-only	Die Gesamtzahl der SNMP-Trap-PDUs, die von der SNMP-Protocol-Entity angenommen und verarbeitet wurden.
snmpOutTooBigs	read-only	Die Gesamtzahl der SNMP-PDUs, die von der SNMP-Protocol-Entity erstellt wurden und für die im Fehlerstatusfeld der Wert "tooBig" angezeigt wird.
snmpOutNoSuchNames	read-only	Die Gesamtzahl der SNMP-PDUs, die von der SNMP-Protocol-Entity erstellt wurden und deren Fehlerstatus den Wert "noSuchName" aufweist.

SNMP-Gruppe

Objektname	Zugriff	Erläuterung
snmpOutBadValues	read-only	Die Gesamtzahl der SNMP-PDUs, die von der SNMP-Protocol-Entity erstellt wurden und für die das Fehlerstatusfeld den Wert "badValue" aufweist.
snmpOutGenErrs	read-only	Die Gesamtzahl der SNMP-PDUs, die von der SNMP-Protocol-Entity erstellt wurden und für die das Fehlerstatusfeld den Wert "genErr" aufweist.
snmpOutGetRequests	read-only	Die Gesamtzahl der SNMP-Get-Request-PDUs, die von der SNMP-Protocol-Entity erstellt wurden.
snmpOutGetNexts	read-only	Die Gesamtzahl der SNMP-Get-Next-PDUs, die von der SNMP-Protocol-Entity erstellt wurden.
snmpOutSetRequests	read-only	Die Gesamtzahl der SNMP-Set-Request-PDUs, die von der SNMP-Protocol-Entity erstellt wurden.
snmpOutGetResponses	read-only	Die Gesamtzahl der SNMP-Get-Response-PDUs, die von der SNMP-Protocol-Entity erstellt wurden.
snmpOutTraps	read-only	Gesamtzahl der SNMP-Trap-PDUs, die von der SNMP-Protocol-Entity erstellt wurden.
snmpEnableAuthenTraps	read-write	Gibt an, ob die SNMP-Agentenverarbeitung in der Lage ist, Alarmnachrichten auf Grund von Berechtigungsfehlern zu erstellen. Der Wert dieses Objekts überschreibt alle Konfigurationsdaten. Er stellt somit eine Möglichkeit dar, alle Alarmnachrichten auf Grund von Berechtigungsfehlern zu inaktivieren. Eingabe: enabled (1) - Ein unberechtigter Zugriff löst das Versenden eines Traps aus. disabled (2) - Ein unberechtigter Zugriff löst keine Trap-Versendung aus.
snmpSilentDrops	read-only	Gesamtzahl der an die SNMP-Entity übergebenen GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs und InformRequest-PDUs, die unbemerkt verloren gingen, weil der Umfang einer Antwort mit der entsprechenden, eine leere Liste von Variable Bindings enthaltenden GetResponse-PDU gegen eine lokale Einschränkung verstieß oder größer war als die für den Absender des Get...Request vereinbarte Meldungslänge

SNMP-Gruppe

Objektname	Zugriff	Erläuterung
snmpProxyDrops	read-only	Gesamtzahl der an die SNMP-Entity übergebenen GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs und InformRequest-PDUs, die unbemerkt verloren gingen, weil die Übertragung der Nachricht an einen Proxy-Server aus anderen Gründen als einer Zeitüberschreitung misslang, sodass keine GetResponse-PDU zurückgesendet werden konnte.

SNMP-Gruppe

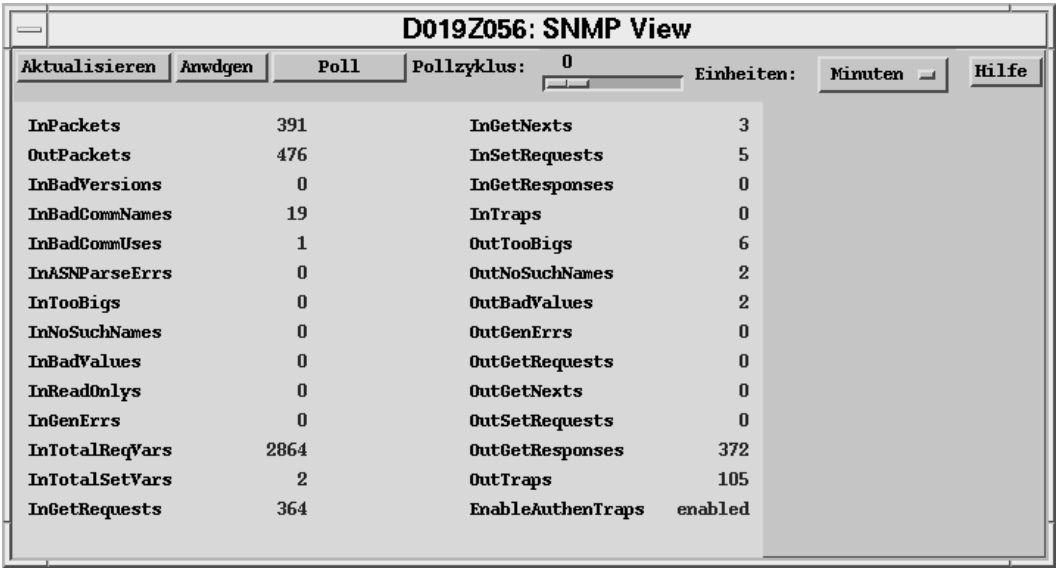


Bild 13: Anzeige der MIB-II-Werte der SNMP-Gruppe

5.1.3 SNMP-Framework-MIB (SNMP Engine)

Objektname	Zugriff	Erläuterung
snmpEngineID	read-only	eindeutiger Administrationsname der SNMP-Engine
snmpEngineBoots	read-only	Anzahl der (Re-)Initialisierungen der SNMP-Engine seit ihrer Start-Konfigurierung
snmpEngineTime	read-only	Anzahl der Sekunden seit der letzten Inkrementierung des Objekts *snmpEngineBoots* durch die SNMP Engine
snmpEngineMaxMessageSize	read-only	maximale Länge (in byte) einer SNMP-Nachricht, die von dieser SNMP-Engine gesendet / empfangen und verarbeitet werden kann.

SNMP Engine

5.1.4 Vom Masteragenten unterstützte Objekte anderer MIBs

Neben den MIBs für das System- und SNMP-Management unterstützt der Masteragent weitere, für das SNMP-Management in BS2000/OSD relevante Objekte der nachfolgend aufgelisteten MIBs.

Standardisierte MIBs

SNMP-MPD-MIB	RFC 2272	snmpModules.3
SNMP-TARGET-MIB	RFC 2273	snmpModules.12
SNMP-NOTIFY-MIB	RFC 2273	snmpModules.13
SNMP-USER-BASED-SM-MIB	RFC 2274	snmpModules.15
SNMP-VIEW-BASED-ACM-MIB	RFC 2275	snmpModules.16

Private MIBs

SR-COMMUNITY-MIB	snmpResearchMIBs.33
TGT-ADDRESS-MASK-MIB	snmpResearchMIBs.36
HTTPSEC-MIB	srExperimentalMIBs.1

5.2 SNMP-Management für Subagenten (Supervisor Subagent)

Der Supervisor Subagent dient der Überwachung aller am Masteragenten angemeldeten Subagenten.

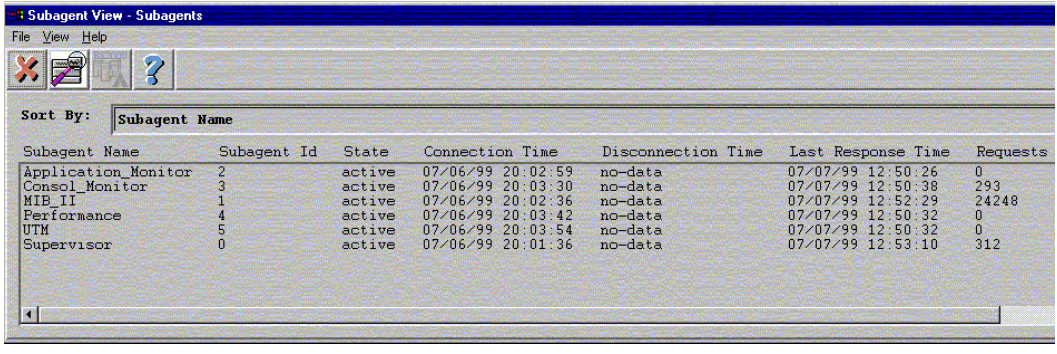


Bild 14: Überwachung der Subagenten

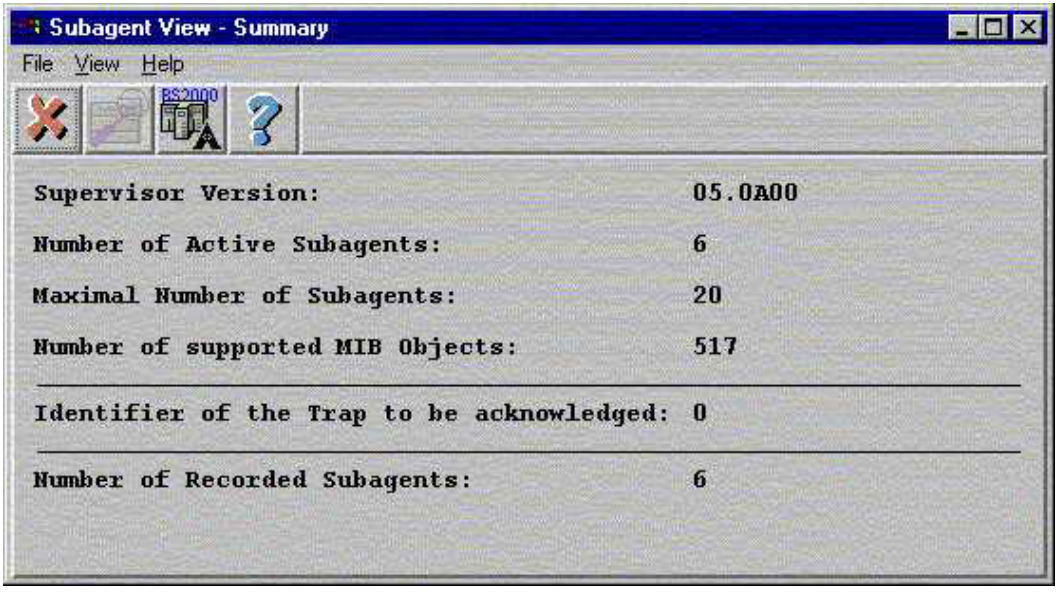


Bild 15: Summary-View des Supervisor Subagenten

Objektname	Zugriff	Erläuterung
superVisVersion	read-only	Version des Supervisor-Subagenten
superVisActiveNumber	read-only	Anzahl aktiver Subagenten
superVisMaxSubagent Number	read-only	Maximale Anzahl Subagenten
superVisObjectNumber	read-only	Anzahl Objekte, die derzeit vom SNMP-Agenten des BS2000 unterstützt werden.
superVisTrapAckId	read-write	ID des letzten Trap, der vom Manager bestätigt werden muss. Wenn dieses Objekt mit dem aktuellen Wert gesetzt wird, bedeutet dies Bestätigung des letzten Trap.
superVisSubagentNumber	read-only	Anzahl Einträge in Subagenten-Tabelle
Subagenten Tabelle		
superVisSubagentName	read-only	Name des Subagenten (nur für BS2000-Subagenten)
superVisSubagentSID	read-only	SID der Subagenten: Index, den der Masteragent zur Verwaltung des Subagenten verwendet.
superVisSubagentStatus	read-only	Status des Subagenten: active (1): Die Verbindung zum Subagenten ist aufgebaut und funktioniert normal. disconnected (2): Der Subagent hat ein Disconnect-Ereignis gesendet und steht nicht mehr zur Verfügung. undefined (3): Vom Subagenten wurde seit 5 Minuten keine Antwort empfangen, aber auch kein Disconnect gesendet.
superVisSubagentConnTime	read-only	Zeitpunkt des letzten Verbindungsaufbaus zum Subagenten
superVisSubagent Disconn Time	read-only	Zeitpunkt des letzten Verbindungsabbaus vom Subagenten
superVisSubagentLast ResponseTime	read-only	Zeitpunkt der letzten Antwort vom Subagenten
superVisSubagentRequests Done	read-only	Anzahl Anforderungen an den Subagenten
superVisSubagentTrapsSent	read-only	Anzahl Traps durch den Subagenten

Objektname	Zugriff	Erläuterung
superVisSubagentOID	read-only	Erste vom Subagenten unterstützte Objekt-ID
superVisSubagentProcessID	read-only	Prozess-ID des Subagenten
superVisSubagentUserId	read-only	User-ID, die zur Prozess-ID gehört
superVisSubagentCpuTime	read-only	Vom Subagenten benötigte CPU-Zeit
superVisSubagentCommand	read-only	In der Ausgabe des Kommandos PS vorhandene Kommandofolge, die zur Prozess-ID gehört.

TrapAcknowledge-Gruppe

Objektname	Zugriff	Erläuterung
superVisTrpAckState	read-write	Status der Trap-Bestätigung am Agenten: active (1): der Bestätigungsmechanismus ist aktiv inactive (2): der Bestätigungsmechanismus ist nicht aktiv undefined (3)
superVisTrpAckId	read-write	ID des bisher letzten vom Manager zu bestätigenden Traps. Das Setzen dieses Objekts mit dem aktuellen Wert bedeutet die Bestätigung des letzten Traps.
superVisTrpAckQueueCnt	read-write	Anzahl der aktuell in die Warteschlange eingereihten Traps. Evtl. überzählige Traps werden aus der Warteschlange entfernt.

Trap-Objekte

Objektname	Trap-Nr	Erläuterung
Enterprise = 1.3.6.1.4.1.231.2.34.2		
superVisSubAgentConnected	301	Der Trap bedeutet, dass die Verbindung zu diesem Subagenten aufgebaut wurde.
superVisSubAgent Disconnected	302	Der Trap bedeutet, dass die Verbindung vom Masteragenten abgebaut wurde.
superVisSubAgentNoAnswer	303	Der Trap bedeutet, dass dieser Subagent 5 Minuten lang nicht auf eine Anforderung geantwortet hat.

5.3 Application Monitor Subagent

Der Application Monitor Subagent gestattet die Überwachung von

– Benutzer-Anwendungen,
– BCAM-Anwendungen,
– DCAM-Anwendungen
– Subsystemen,
– Jobvariablen und
– Protokolldateien.

Logisch zusammengehörige Bestandteile eines Prozesses (Anwendungen, Protokolldateien, Subsysteme und Jobvariablen) können gemeinsam als Gruppe überwacht werden.

Unter dem Begriff Anwendungen werden hier Programme und Tasks verstanden. Art und Umfang der Anwendungsüberwachung werden über die Konfigurationsdatei individuell gesteuert. Hinweise zur Erstellung der Konfigurationsdatei entnehmen Sie bitte dem entsprechenden Abschnitt auf Seite 58.

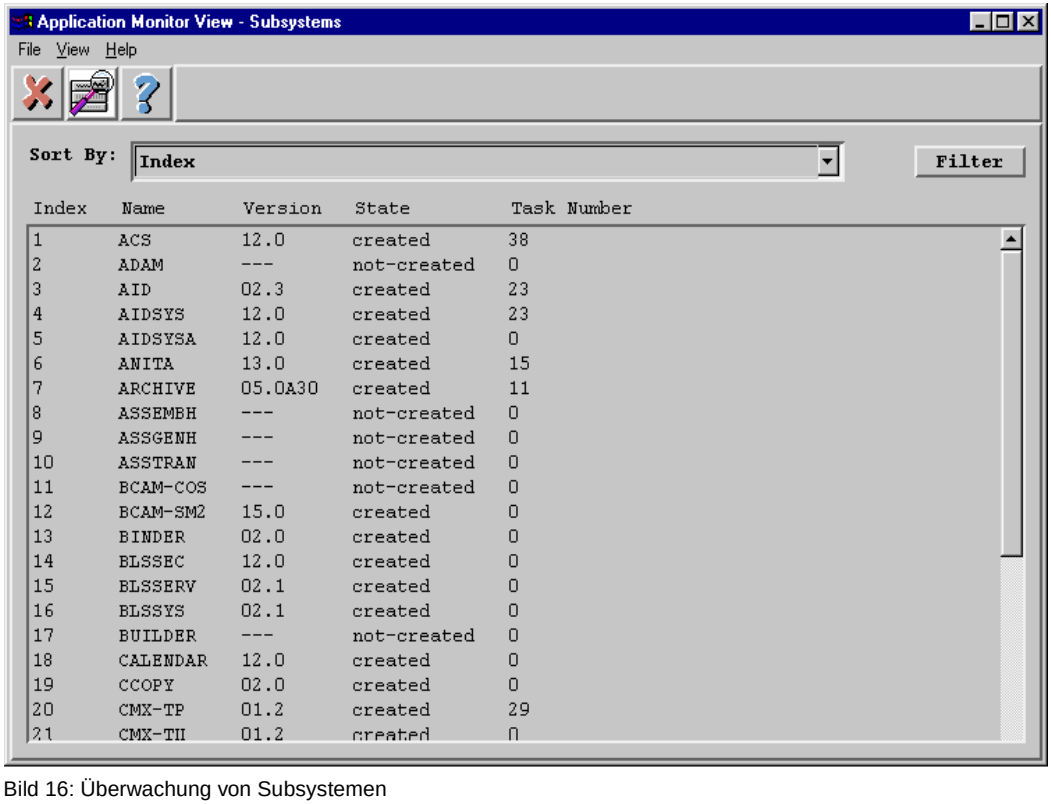


Bild 16: Überwachung von Subsystemen

5.3.1 Private MIB des Application Monitor Subagenten

Die Überwachung von Anwendungen (Programme und Tasks) und Jobvariablen setzen das Softwarepaket Jobvariablen voraus. Die zu überwachenden Anwendungen und Tasks müssen in der Konfigurationsdatei eingetragen sein. Falls der Application Monitor Subagent ohne Konfigurationsdatei gestartet wird, werden nur die Subsysteme angezeigt.

Globale Daten des Application Monitor Subagenten

Folgende Objekte zeigen die globalen Daten des Application Monitor Subagenten:

MIB-Definition	Zugriff	Erläuterung
appMonVersion	read-only	Version des Application Monitor Subagenten
appMonConfFile	read-write	Pfadname der Konfigurationsdatei
appMonTrapFormat	read-write	verwendete Trap-Struktur

5.3.1.1 Trap-Struktur

Der Application Monitor Subagent unterstützt folgende Traps:

– Application Monitor-spezifischer Trap
– Trap aus der TV-CC-MIB (wird aus Kompatibilitätsgründen noch unterstützt)

Standardmäßig wird der Application Monitor-spezifische Trap unterstützt.

Struktur des Application Monitor-spezifischen Traps

1. Community: appMonDevice oder <standard>

2. Enterprise: 1.3.6.1.4.1.231.2.23.20.2 (Trap muss nicht bestätigt werden)
bzw.
1.3.6.1.4.1.231.2.23.20.3 (Trap muss bestätigt werden)

3. Trapnummer: 6 / <weight>

4.Variablen-Bindung:

appMonSource	1.3.6.1.4.1.231.2.23.20.1.1 (OCTET STRING)
appMonDevice	1.3.6.1.4.1.231.2.23.20.1.2 (OCTET STRING)
appMonMsg	1.3.6.1.4.1.231.2.23.20.1.3 (OCTET STRING)
appMonWeight	1.3.6.1.4.1.231.2.23.20.1.4 (INTEGER)

appMonSource, appMonDevice und appMonMsg sind abhängig von der Art der überwachten Anwendung (siehe Seiten 186 - 195).

Struktur des Traps aus der TV-CC-MIB

1. Community: <device> oder <standard>

2. Enterprise: 1.3.6.1.4.1.231.2.14

3. Trapnummer: 6 / 1

4.Variablen-Bindung:

tccTrapString: 1.3.6.1.4.1.231.2.14.1.3 (OCTET STRING)

"$DATE$: <datum> $HOST$: <system> $SOURCE$: <source> $DEVC$: <device> MSG: <msg>"

<source> und <device> sind abhängig von den jeweiligen Angaben in der Konfigurationsdatei. <msg> ist abhängig von der Art der Anwendung. Siehe nachfolgende Abschnitte!

tccApplTrapAck: 1.3.6.1.4.1.231.2.14.1.1.2.1.6.1 (INTEGER)

0 der Trap muss nicht bestätigt werden.
1 der Trap muss bestätigt werden.

Der Wert ist ebenfalls abhängig von den Angaben in der Konfigurationsdatei.

5.3.1.2 Überwachung der BCAM- und Benutzer-Anwendungen

BCAM-Anwendungsgruppe

MIB-Definition	Zugriff	Erläuterung
appMonBcamApplTabNum	read-only	Anzahl der Tabellenelemente
appMonBcamApplIndex	read-only	Index
appMonBcamApplName	read-only	Name
appMonBcamApplVersion	read-only	Version
appMonBcamApplState	read-only	Status*
appMonBcamApplMonJV	read-only	Name der Monitor-Jobvariablen

*Die entsprechenden Statuswerte entnehmen Sie bitte der Tabelle auf der nächsten Seite.

Benutzer-Anwendungsgruppe

MIB-Definition	Zugriff	Erläuterung
appMonUserApplTabNum	read-only	Anzahl der Tabellenelemente
appMonUserApplIndex	read-only	Index
appMonUserApplName	read-only	Name
appMonUserApplVersion	read-only	Version
appMonUserApplState	read-only	Status*
appMonUserApplMonJV	read-only	Name der Monitor-Jobvariablen

*Die entsprechenden Statuswerte entnehmen Sie bitte der Tabelle auf der nächsten Seite.

Status der einzelnen BCAM- und Benutzer-Anwendungen

Wert	Bedeutung
running	Die Anwendung läuft.
terminated	Die Anwendung wurde regulär beendet.
aborted	Die Anwendung wurde abnormal beendet.
scheduled	Die Task befindet sich noch in der Warteschlange.
unknown	Der aktuelle Zustand der Anwendung kann nicht ermittelt werden.

Die Zustandsänderung einer Anwendung kann, abhängig von den Trap-Bedingungen für diese Anwendung in der Konfigurationsdatei, zur Versendung eines Traps an die Management-Station führen.

Variablenbindung

Bei Application Monitor-spezifischem Trap-Format

appMonSource	appMonDevice	appMonMsg
"BS2-MonJV"	<appl-name>	"Application has entered state: <jv-contents>"

Bei TV-CC-MIB-Trap-Format

Der Trap-String hat folgenden Aufbau:

Trap-String
...$SOURCE$: <appl-name> $DEVC$: MSG: Application has entered state: <jv-contents>

5.3.1.3 Überwachung von DCAM-Anwendungen

Für DCAM-Anwendungen werden folgende Werte geliefert:

MIB-Definition	Zugriff	Erläuterung
appMonDcamApplTabNum	read-only	Anzahl der Tabellenelemente
appMonDcamApplIndex	read-only	Index
appMonDcamApplName	read-only	Name
appMonDcamApplHost	read-only	Rechner
appMonDcamApplState	read-only	Status*

*Die entsprechenden Statuswerte entnehmen Sie bitte der folgenden Tabelle.

Status der einzelnen DCAM-Anwendungen

Wert	Bedeutung
running	Die DCAM-Anwendung läuft.
terminated	Die DCAM-Anwendung wurde regulär beendet.
unknown	Der aktuelle Zustand der DCAM-Anwendung kann nicht ermittelt werden.

Die Zustandsänderung einer DCAM-Anwendung kann, abhängig von den Trap-Bedingungen für diese Anwendung in der Konfigurationsdatei, zur Versendung eines Traps an die Management-Station führen.

Variablenbindung

Bei Application Monitor-spezifischem Trap-Format

appMonSource	appMonDevice	appMonMsg
"BS2-DCAM"	<appl-name>	"DCAM application no longer available. Reason <fdb1> <fdb2>"*

Bei TV-CC-MIB-Trap-Format

Der Trap-String hat folgenden Aufbau:

Trap-String
...$SOURCE$: <appl-name> $DEVC$: MSG: application no longer available. Reason <fdb1> <fdb2>*

*) <fdb1> und <fdb2> entsprechen den beiden ersten Bytes des DCAM-Returncodes (siehe Seite 465).

5.3.1.4 Überwachung von Subsystemen

Für Subsysteme werden folgende Werte geliefert:

MIB-Definition	Zugriff	Erläuterung
appMonSubsysTabNum	read-only	Anzahl der Tabellenelemente
appMonSubsysIndex	read-only	Index
appMonSubsysName	read-only	Name
appMonSubsysVersion	read-only	Version
appMonSubsysState	read-only	Status*
appMonSubsysTasks	read-only	Taskanzahl

*Die entsprechenden Statuswerte entnehmen Sie bitte der Tabelle auf der nächsten Seite.

Die Versionsanzeige ist abhängig von den Angaben in der Konfigurationsdatei. Wenn Informationen über alle Subsysteme bzw. über ein Subsystem ohne explizite Versionsangabe gefordert werden, wird pro definiertem Subsystem (Zustand ungleich „not-created“) die höchste Version angezeigt. Sollten sich alle Versionen eines Subsystems im Zustand „not-created“ befinden, wird ein Eintrag ohne Version geliefert. Erfolgt die Informationsanforderung für ein Subsystem mit Versionsangabe, dann erfolgt die Anzeige unabhängig vom Zustand.

Status der Subsysteme

Wert	Bedeutung
created	Das angegebene Subsystem ist geladen und initialisiert.
not-created	Das angegebene Subsystem ist zwar deklariert, aber derzeit nicht aktiviert.
in-delete	Das angegebene Subsystem befindet sich nach einem STOP-SUBSYSTEM-Kommando im Deaktivierungsprozess. Bereits an das Subsystem angeschlossene Prozesse werden noch abgearbeitet.
in-create	Das angegebene Subsystem befindet sich derzeit in der Lade - und Initialisierungsphase.
in-resume	Das angebene Subsystem wird durch ein RESUME-SUBSYSTEM-Kommando fortgesetzt. Der Reinitialisierungsprozess ist noch nicht abgeschlossen.
in-hold	Das angegebene Subsystem wurde durch ein HOLD-SUBSYSTEM-Kommando angehalten. Der Deinitialisierungsprozess ist noch nicht abgeschlossen. Bereits an das Subsystem angeschlossene Prozesse werden noch abgearbeitet.
not-resumed	Das angegebene Subsystem wurde durch ein HOLD-SUBSYSTEM-Kommando angehalten. Der Deinitialisierungsprozess ist abgeschlossen.
locked	Ein nicht behebbarer Fehler ist aufgetreten, während das angegebene Subsystem aktiv war bzw. akitiviert, deaktiviert, fortgesetzt oder angehalten wurde. Ein weiterer Versuch, die entsprechenden Kommandos abzusetzen, wird abgewiesen.
unknown	Das angegebene Subsystem bzw. die angegebene Version existieren nicht.

Informationen zum Status der Subsysteme können von der Management-Station angefordert werden. Es wird ein Trap verschickt, wenn das Subsystem in den Zustand wechselt, der mit TRAP-CONDITION definiert wurde. Standardmäßig werden Subsysteme alle 25 Sekunden vom Subagenten überprüft.

Variablenbindung

Bei Application Monitor-spezifischem Trap-Format

appMonSource	appMonDevice	appMonMsg
"BS2-Subsys"	<subsystem>	"Subsystem has entered state: <state>"

Bei TV-CC-MIB-Trap-Format

Der Trap-String hat folgenden Aufbau:

Trap-String
...$SOURCE$: <ss-name(vers)> $DEVC$: MSG: Subsystem has entered state: <state>

5.3.1.5 Überwachung von Jobvariablen

Die zu überwachenden Jobvariablen müssen in der Konfigurationsdatei mit ADD-JV-RECORD (siehe Seite 67) bekannt gegeben werden.

Für jede Jobvariable werden folgende Werte geliefert:

MIB-Definition	Zugriff	Erläuterung
appMonJVName	read-only	Name der Jobvariablen
appMonJVAppl	read-only	Anwendungsname
appMonJVValue	read-only	aktueller Wert der Jobvariablen
appMonJVPattern	read-only	Muster, bei denen ein Trap gesendet werden soll

Ändert sich der Inhalt einer Jobvariablen, dann wird ein Trap erzeugt. Der Trap enthält Datum, Rechner- und Applikationsname, sofern angegeben, und eine Meldung, die den Jobvariablen-Status enthält.

Variablenbindung

Bei Application Monitor-spezifischem Trap-Format

appMonSource	appMonDevice	appMonMsg
"BS2-JV"	<appl-name>	"Job variable has changed to: <jv-contents>"

Bei TV-CC-MIB-Trap-Format

Der Trap-String hat folgenden Aufbau:

Trap-String
...$SOURCE$: <appl-name> $DEVC$: MSG: Jobvariable has changed to: <jv-contents>

5.3.1.6 Überwachung von Protokolldateien

Die Überwachung durch Protokolldateien ist für diejenigen Anwendungen vorgesehen, die selbst keinen Trap an die Management-Station senden können. Stattdessen legen diese Anwendungen Meldungen in einer Protokolldatei ab, die durch den Application Monitor Subagent überwacht wird. Der Application Monitor Subagent wertet diese Meldungen aus und sendet jeden Eintrag als Trap an die Management-Station.

BS2000-Protokolldateien müssen vom Typ ISAM und SHAREUPD=YES sein. NFS- bzw. POSIX-Protokolldateien können ASCII- oder EBCDIC-Format haben, EBCDIC-Format ist Standard, das ASCII-Format muss in der Konfigurationsdatei entsprechend gekennzeichnet werden. Die Angabe des Dateinamens in der Konfigurationsdatei muss die Benutzerkennung im Fall BS2000 bzw. den absoluten Pfadnamen im NFS-/ POSIX-Fall enthalten. Der Subagent ist sonst nicht in der Lage, zwischen BS2000- und NFS-/ POSIX-Datei zu unterscheiden.

Für jede überwachte Protokolldatei können folgende Objekte angezeigt werden:

MIB-Definition	Zugriff	Erläuterung
appMonLogfName	read-only	Pfadname der Datei
appMonLogfAppl	read-only	Name der zugehörigen Anwendung
appMonLogfState	read-write	Anzeige, ob die Überwachung aktiv ist oder nicht
appMonLogfPattern	read-only	Muster, bei denen ein Trap gesendet werden soll

Das Objekt *appMonLogfState* kann auch gesetzt werden:

Wert	Bedeutung
deactive	beendet die Überwachung.
start-begin	aktiviert die Überwachung am Anfang der Datei.
start-new	aktiviert die Überwachung am Anfang der Datei ohne Berücksichtigung des ursprünglichen Inhalts.
start-end	aktiviert die Überwachung am Ende der Datei.

Standardmäßig werden Protokolldateien alle 5 Sekunden vom Subagenten überprüft, eine Änderung dieses Wertes ist im Startkommando mit dem Operanden TIMER-INTERVAL und im laufenden Betrieb mit dem Kommando *appmoncmd* möglich. Werden vom Subagenten Dateiänderungen erkannt, wird für jede neue Meldung ein Trap an die Management-Station geschickt.

Variablenbindung

Der Aufbau dieses Trap-Strings ist vom Inhalt eines Eintrags in der Protokolldatei abhängig. Beginnt eine neue Meldung mit `$<DEVICE=devc>$`, dann verwendet der Application Monitor Subagent <devc> für Device.

Bei Application Monitor-spezifischem Trap-Format

appMonSource	appMonDevice	appMonMsg
"BS2-LogF"	<appl-name>	<logfile entry>
"BS2-LogF"	<devc>	<logfile entry>

Bei TV-CC-MIB-Trap-Format

Im Trap-String selbst wird DEVC mit <devc> versorgt.

Eintrag in die Datei	Trap-String
$<DEVICE=devc>$ text	...$SOURCE$: <appl-name> $DEVC$: <devc> MSG: text
text	...$SOURCE$: <appl-name> $DEVC$: MSG: text

5.3.1.7 Steuerung der Dateiüberwachung

Das Kommando /START-APPMONCMD (BS2000/OSD) bzw. appmoncmd (POSIX) bietet neben den Standard-Optionen auch folgende Optionen zur Dateiüberwachung:

i	print information	Information ausgeben
a	activate monitoring	Aktivieren der Überwachung
d	deactivate monitoring	Deaktivieren der Überwachung
p	set time period [sec]	Zeitintervall festlegen

Optionen zur Dateiüberwachung

Option	Erläuterung
[**i**]	Gibt Informationen über die Protokolldateien nach stderr aus.
[**a**] <logfile-id> <position>	Aktiviert die Überwachung der Protokolldatei mit der ID <logfile-id>. Mit der Angabe <position> wird der Dateizeiger in der Datei positioniert: b Anfang der Datei p letzte Leseposition, falls die Überwachung bereits aktiv war e Ende der Datei Die Überwachung wird nur temporär eingeschaltet, es erfolgt keine Änderung der Konfigurationsdatei.
[**d**] <logfile-id>	Die Überwachung wird nur temporär ausgeschaltet, es erfolgt keine Änderung der Konfigurationsdatei.
[**p**] <seconds>	Definiert den Zyklus (Angabe in Sekunden), in dem die Protokolldateien überprüft werden.

Beispiel:

```
ID APPL      S FSYS PATHNAME             FILE   ERR SIZE  MTIME
1  ROBAR.025 A ISAM $SYSROBAR.LOGFILE3   open   0   78    15:41:05 11.Oct(UTC)
2  APPL1     A UFSE /tmp/logfile4        closed 8   0     unknown
3  APPLICATI D ISAM $TSOS.APPL2.LOGFILE  closed 0   0     unknown
4  unknown   A UFS  /home/snmp/Logfile2  open   0   196   16:42:35 12.Oct
5  SNMP      A ISAM :2OS6:$DC14.SNMP.LOG open   0   335   17:48:57 12.Oct(UTC)
```

Ausgabe	Bedeutung
ID	Der Application Monitor Subagent ordnet jeder Protokolldatei eine Zahl zu. Diese ID wird beim Aktivieren bzw. Deaktivieren einer Dateiüberwachung angegeben.
APPL	Angabe der ersten neun Zeichen des Anwendungsnamens.
S	Status der Überwachung: "A" für aktiviert und "D" für deaktiviert.
FSYS	Angabe des Dateiformats: "UFS" (UNIX-File-System, ASCII-Datei) "UFSE" (UNIX-File-System, EBCDIC-Datei) "ISAM" (BS2000-Datei)
PATHNAME	Die ersten 20 Zeichen des Namens der Protokolldatei.
FILE	Angabe des Dateizustands: mögliche Werte sind open und closed.
ERR	Fehlernummer, falls beim Dateizugriff ein Fehler auftritt. Bedeutung siehe /usr/include/sys/errno.h
SIZE	aktuelle Dateigröße in Byte
MTIME	Uhrzeit und Tag der letzten Dateiänderung Hinweis: Für BS2000-Dateien wird die UTC-Zeit ausgegeben (Kennzeichen: (UTC)).

5.3.1.8 Überwachung von Gruppen zusammengehöriger Elemente

Logisch zusammengehörige Bestandteile eines Prozesses (Anwendungen, Protokolldateien, Subsysteme und Jobvariablen) können als Gruppe (Objekt) zusammengefasst und gemeinsam überwacht werden (DEFINE-OBJECT, siehe Seite 69).

Alle Elemente (Anwendungen, Subsysteme etc.), die zu einem Objekt zusammengefasst sind, müssen in der Konfigurationsdatei mit den entsprechenden Anweisungen konfiguriert sein.

Für Objekte werden folgende Werte geliefert:

MIB-Definition	Zugriff	Erläuterung
appMonObjectName	read-only	Name des Objekts
appMonObjectBcamAppl	read-only	Name aller BCAM-Anwendungen, die zu diesem Objekt gehören
appMonObjectUserAppl	read-only	Name aller Benutzeranwendungen
appMonObjectDcamAppl	read-only	Name aller DCAM-Anwendungen
appMonObjectSub	read-only	Name aller Subsysteme
appMonObjectLogfile	read-only	Name aller Protokolldateien
appMonObjectJV	read-only	Name aller Jobvariablen

Tritt ein Ereignis ein, für das der Application Monitor Subagent einen Trap an die Management-Station schickt, dann wird der Trap-Inhalt wie beschrieben aufgebaut, mit folgenden Abweichungen:

– Beim Application Monitor-spezifischen Trap wird in der Variablenbindung appMonSource mit BS2-Object: <object> versorgt.

– Im Trap-String des TV-CC-Traps wird DEVC mit dem Objektnamen versorgt:

Trap-String
.... $SOURCE$: ... $DEVC$:<obj-name>MSG: ...

5.4 Console Monitor Subagent

Der Console Monitor Subagent überwacht die Konsolschnittstelle. Er dient zur Erfassung von Konsolmeldungen sowie zur Eingabe von Konsolkommandos. Dem Console Monitor Subagenten ist mit den Integrationspaketen SMAWcmbs2 (Solaris) bzw. CMBS2 (Reliant UNIX, Windows NT) eine eigene Management-Anwendung CMBS2 zugeordnet. Sollten Sie CMBS2 nutzen wollen, beachten Sie bitte die entsprechende Beschreibung ab Seite 354.

5.4.1 Erfassung von Konsolmeldungen

Konsolmeldungen werden vom Console Monitor Subagenten empfangen und einzeln mit Rechnername und Uhrzeit versehen als Trap an die Management-Station versandt. Abhängig von Anzahl, Auslastung und Größe der Rechner, die Sie vom Console Monitor Subagent überwachen lassen, haben Sie eine mehr oder weniger große Meldungsflut zu bewältigen. Es wird jedoch in den seltensten Fällen sinnvoll sein, alle Konsolmeldungen zur Management-Station durchzureichen. Daher bietet der Console Monitor Subagent zwei Möglichkeiten zum Filtern von Konsolmeldungen. Es werden positive und negative Meldungsfilter angeboten.

positive Meldungsfilter

1. Jeder Konsolmeldung ist ein bestimmter Routingcode zugeordnet. Durch die Auswahl bestimmter Routingcodes, die in Operator-Rollen festgelegt werden, definieren Sie die auf der Management-Station auszugebenden Meldungen anhand ihres Routingcodes.
2. Der Meldungsschlüssel der Konsolmeldung bzw. -frage oder TYPE I/Os ist ein weiteres Auswahlkriterium, mit dem Sie festlegen können, welche Meldungen der Management-Station zugestellt werden sollen. Dazu werden die relevanten Meldungsschlüssel in einer Meldungsfilter-Datei hinterlegt, die vom Console Monitor Subagent beim Start bzw. im Falle einer Aktualisierung auch im laufenden Betrieb ausgewertet wird.

negativer Meldungsfilter

Der Console Monitor Subagent bietet die Möglichkeit, bereits bei der Anmeldung an UCON bestimmte Meldungen zu unterdrücken.

Die Erstellung der Meldungsfilter-Datei, die beim Start des Subagenten angegeben werden muss, ist ab Seite 72 beschrieben. Änderungen an der Meldungsfilter-Datei im laufenden Betrieb sind durch Schreiben des MIB-Objekts *consMonMsgFilter* (positiver Meldungsfilter) und über das Kommandoprogramm möglich.

Kann die neu zugewiesene Meldungsfilter-Datei nicht geöffnet werden, wird dies mit dem Returncode *General Error* abgewiesen, und die alte Datei weiter benutzt. Enthält die Meldungsfilter-Datei keine bzw. keine gültigen Meldungsschlüssel, so werden der Management-Station keine Traps zugestellt. Der negative Meldungsfilter *consMonNegMsgFilter* kann im laufenden Betrieb nicht geändert werden.

Die MIB des Console Monitor Subagenten enthält folgende, intern verwendete Objekte:

Objektname	**Zugriff**	**Erläuterung**
consMonVersion	read-only	Version des Console Monitor Subagent
consMonMsgFilter	read-write	Name der Meldungsfilterdatei
consMonNegMsgFilter	read-only	Name der negativen Meldungsfilterdatei
consMonCmdFreeIndex	read-only	nächster freier Index in der Kommandotabelle
consMonCmdTabNum	read-only	Anzahl der Einträge in der Kommandotabelle
Kommando-Tabelle		
consMonCmdIndex	read-only	Kommando-Index
consMonCmd	read-write	BS2000/OSD-Konsol-Kommando
consMonCmdResult	read-only	Ergebnis des BS2000/OSD-Konsol-Kommandos
consMonCmdMainRetco	read-only	Main Returncode des BS2000/OSD-Konsol-Kommandos
Tabelle der Kommando-Ausgaben		
consMonOutCmdIndex	read-only	Kommando-Index des zugehörigen Kommandos
consMonOutLineNo	read-only	Anzahl der Zeilen für ein Kommando
consMonOutContents	read-only	eine Zeile der Kommandoausgabe
consMonBS2Ans	read-write	Antwort auf eine BS2000/OSD-Konsol-Meldung

Nutzen Sie bitte zur Bedienung des Console Monitor Subagenten die Management-Anwendung CMBS2 aus dem Integrationspaket SMAWcmbs2 (Solaris) bzw. CMBS2 (Reliant UNIX). Näheres zur Management-Anwendung CMBS2 finden Sie ab Seite 344.

Trap-Struktur

Der Console Monitor Subagent unterstützt folgende Trap-Formate:

– Application Monitor-spezifischer (generischer) Trap

– TV Control Center-Trap (Trap aus der TV-CC-MIB)

Das gewünschte Trap-Format für den Console Monitor legen Sie in der Meldungsfilterdatei des Console Monitor Subagenten fest (siehe Seite 73, „Auswahlkriterium Trap-Struktur“).

Standardmäßig wird der Application Monitor-spezifische Trap verwendet.

Application Monitor-spezifischer Trap

Der Application Monitor-spezifische Trap ist auf Seite 184 beschrieben. Die Variablenbindung wird entsprechend den Einträgen in der Konfigurationsdatei versorgt.

TV Control Center-Trap (TV-CC-MIB-Trap)

Der Aufbau des TV Control Center Trap-String hängt von den Einträgen für SOURCE und DEVICE in der Konfigurationsdatei ab:

SOURCE=	**DEVICE=**	**Trap-String**	**COMMUNITY**
<src>	<dev>	...$SOURCE$: BS2-<src> DEV: <dev> MSG:...	<dev>
---	<dev>	...$SOURCE$: BS2Console DEV: <dev> MSG:...	<dev>
<src>	---	...$SOURCE$: BS2-<src> DEV: MSG:...	*std
---	---	...$SOURCE$: BS2Console DEV: MSG:...	*std

5.4.2 Symmetrix-Überwachung

Symmetrix ist ein mächtiges Plattensteuerungssubsystem der EMC Corporation, das es gestattet, die Plattenperipherie verschiedener Systeme, seien es Mainframes oder Open Systems, in komfortabler Weise zu verwalten und zentral zu überwachen. Darüber hinaus ermöglicht Symmetrix mit seinen Zusatzfunktionen ein unternehmensweites Speicherverwaltungskonzept.

Funktionalität

Ein BS2000-System erhält von jeder Symmetrix Ereignismeldungen, die in Konsolmeldungen - NJD0010 bis NJD0013 - umgesetzt werden. Der Console Monitor Subagent filtert diese Meldungen und sendet entsprechende Traps an die Management-Station. Das Paket SMBS2 enthält Elemente für eine einfache Überwachung, die den Eingang einer Konsolmeldung zu einem Symmetrix-Ereignis durch eine Verfärbung im Netzbild signalisiert. Die Überwachungsfunktion besteht aus den auf Seite 111 beschriebenen Erweiterungen des TransView Control Center und den auf Seite 350 beschriebenen Alarmen.

Die an der Konsole gemeldeten Symmetrix- Ereignisse sind in vier Klassen aufgeteilt, denen vier Meldungsschlüssel entsprechen:

NJD0010 Die Verbindung zum Serviceprozessor oder zum EMC Customer Support Center (CSC) ist verloren. Die Symmetrix sollte weiterhin normal arbeiten.

NJD0011 Ein Fehler ist aufgetreten, der einen Funktionsausfall oder Datenverlust nach sich ziehen kann.

NJD0012 Ein Fehler ist aufgetreten, der durch eine redundante Funktion behoben werden kann.

NJD0013 Symmetrix meldet ein Ereignis. Teilweise handelt es sich dabei um die Behebung eines Problemzustandes.

Der Meldungstext enthält verschiedene Zusatzinformationen, welche das betroffene Gerät und die Art des Ereignisses näher bezeichnen:

– die aus den mnemotechnischen Namen von Kanal, Steuerung und Gerät gebildete Geräteadresse.
– den Steuerungstyp
– die Seriennummer der Steuerung
– den Referenzcode zur genaueren Bezeichnung des aufgetretenen Problems oder Ereignisses
– einen Indikator, der Wiederholungsmeldungen kennzeichnet

Referenzcodes zu den Meldungen NJD0010 - NJD0013

Referenz-code	Meldung und Bedeutung	Meldungs-schlüssel	betroffene Kom-ponente
460	*dynamic spare invoked* Ersatzplatte aktiviert	NJD0012	Platte
461	*resyncronisation completed* Die Resynchronisation zwischen einer Platte und ihrer "Spiegelplatte" ist abgeschlossen.	NJD0013	Platte
462	*resyncronisation completed* ähnliche Bedeutung wie x461.	NJD0013	Platte
463	*dual initiator failed* Die Steuerung für eine Platte ist ausgefallen. Die zweite Steuerung übernimmt die Aufgabe.	NJD0012	Plattensteuerung
464	*data migration for all volumes completed* Die Datenmigration ist auf allen Geräten abge-schlossen.	NJD0013	Platte
465	*resyncronisation started* Eine Resynchronisation für eine Platte wurde ge-started. Die Meldung erscheint in der Regel in Fol-ge der Meldung x460.	NJD0013	Platte
466	*dynamic spare invoked for remote disk* Eine Ersatzplatte mu?te an einer Partner-Symme-trix aktieviert werden. Die Meldung kommt parallel zur Meldung von x460 durch SRDFverbundenen Symmetrix-Steuerungen.	NJD0012	Partner-Symmetrix
467	*error/event posted by SRDF partner box* Eine Partner Symmetrix meldet einen Fehler oder ein Ereignis. Diese Meldung kommt parallel von den durch SRDF verbundenen Symmetrix-Steue-rungen.	NJD0011	Partner-Symmetrix
46D	*remote links not operational* Alle SRDF-Verbindungen zu den Partner-Symme-trix sind verloren gegangen. Die darüber verbunde-nen Platten können nicht mehr synchron gehalten werden.	NJD0012	SRDF-Verbindung
46E	*all remote links operational again* Alle SRDF-Verbindungen sind wieder betriebsbe-reit.	NJD0013	SRDF-Verbindung
470	*over temperature* Die Steuerung ist zu heiß geworden und droht aus-zufallen.	NJD0011	Steuerung

Referenz-code	Meldung und Bedeutung	Meldungs-schlüssel	betroffene Kom-ponente
471	*low battery / high charge state* Problem mit der Stromversorgung und der Batterie.	NJD0011	Steuerung
472	*power subsystem alarm* Problem mit der Stromversorgung. Die Steuerung droht auszufallen.	NJD0011	Steuerung
473	*local mirrored device not ready* Eine Spiegelplatte ist ausgefallen. Die Verfügbarkeit einer Platte ist eingeschränkt.	NJD0012	Platte
474	*local mirrored device write disabled* Eine Spiegelplatte kann nicht geschrieben werden. Es liegt ein ähnliches Problem wie bei x474 vor. Der Schaden an der Platte ist aber schwerwiegender.	NJD0012	Platte
475	*remote mirrored device not ready* Eines der Probleme x474 oder x475 ist an einer Partner-Symmetrix aufgetreten.	NJD0012	Partner-Symmetrix
476	*service processor not responding* Der Serviceprozessor ist ausgefallen. Es können keine Meldungen mehr an das EMC-Customer-Support-Center versandt werden.	NJD0010	Serviceprozessor
477	*autocall (to EMC-CSC) failed* Der Serviceprozessor hat keine Verbindung zum EMC-Customer-Support-Center.	NJD0010	Serviceprozessor
478	*12 V on* Problem mit der Stromversorgung von außen	NJD0011	Steuerung
479	*enviroment cable missing* Physikalischer Anschluss nach außen nicht vorhanden.	NJD0011	Steuerung
47A	*AC line failure/interruption* Ausfall der Wechselstromversorgung.	NJD0011	Steuerung
47B	*battery, clock, director without power* Problem mit der Stromversorgung einzelner Komponenten.	NJD0011	Steuerung
47C	*latched alarm* Problem mit der Steuerungsumgebung.	NJD0011	Steuerung
47D	*remote link not operational* Eine einzelne SRDF-Verbindung ist ausgefallen. Mit den dort angeschlossenen Platten kann nicht mehr synchronisiert werden.	NJD0012	SRDF-Verbindung

Referenz-code	Meldung und Bedeutung	Meldungs-schlüssel	betroffene Kom-ponente
47E	*remote link(s) operational again* Eine ausgefallene SRDF-Verbindung ist wieder intakt.	NJD0013	SRDF-Verbindung

Beispiel:

Das folgende Beispiel zeigt die Umwandlung der Konsolmeldung NJD0013 mit dem Referenzcode 46E in einen Trap-String:

```
% P26-000.144244  %  NJD0013 -INFORMATION- #EZM  5100
MT=3860-43 SER=03-00434 REFCODE=146E-1E134-0000
- READ HELP TEXT FOR DETAILLED INFORMATION ABOUT REFCODE
```

Trap-String:

```
$DATE$: Feb 16 14:42:50 $HOST$: D016ZE07 $SOURCE$: BS2-SYMMETRIX $DEVC$:
 Symmetrix $MSG$: <000> % P26-000.144244  %  NJD0013 -INFORMATION- #EZM
 5100 MT=3860-43 SER=03-00434 REFCODE=146E-1E134-0000 - READ HELP TEXT FOR
 DETAILLED INFORMATION ABOUT REFCODE
```

In der folgenden Abbildung des Event-Managers finden Sie in der ersten Zeile die Fehlermeldung mit dem Referenzcode 46E wieder:

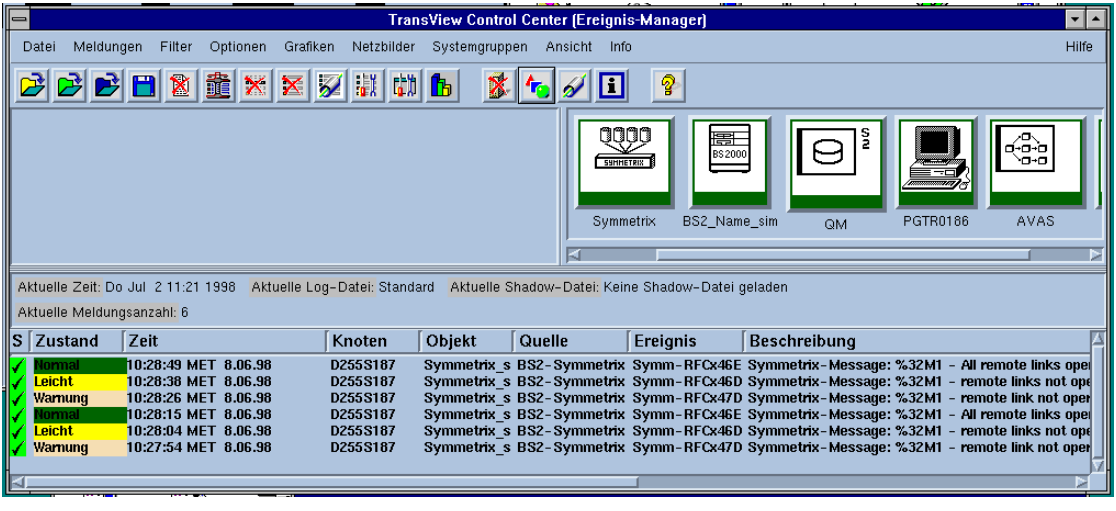


Bild 17: Symmetrix-Überwachung

5.5 Kundenspezifische Web-Seiten (HTML-Subagent)

Der HTML-Subagent wird benötigt für die Bearbeitung kundenspezifischer DR-Web-Seiten (Custom-Pages, siehe Seiten 418 und 427) mithilfe von SNMP-Requests. Die Informationen über die kundenspezifischen DR-Web-Seiten sind in den Variablen der HTML-MIB hinterlegt.

Die HTML-MIB enthält folgende Gruppen und Tabellen:

– htmlGlobals-Gruppe
– htmlPages-Gruppe
– htmlPageTable
– htmlPageParameterTable
– htmlPageContentTable

htmlGlobals-Gruppe

MIB-Definition	Zugriff	Erläuterung
htmlConsistencyCheck	read-write	*htmlConsistencyCheck* wird verwendet zur Speicherbereinigung hinsichtlich unreferenzierter Zeilen in der *htmlPageParameterTable* und der *htmlPageContentTable*. Beim Lesen der Variable wird stets ein Wert *konsistent* (1) zurückgeliefert. Durch Setzen der Variable auf den Wert *verify* (2) wird der Check ausgelöst.

htmlPages-Gruppe

Die Objekte in der *htmlPages*-Gruppe enthalten Informationen über die vom BS2000/OSD-Web-Agenten (DR-Web-Entity) unterstützten Custom-Pages. Auf Custom-Pages kann zugegriffen werden über die Menü-Seite der DR-Web-Schnittstelle (siehe Seite 407).

MIB-Definition	Zugriff	Erläuterung
htmlPageSetSerialNo	read-write	*htmlPageSetSerialNo* realisiert eine in die HTML-MIB integrierte Sperre, die es einer Vielzahl von Management-Stationen ermöglicht, miteinander zu kooperieren und störende Wechselwirkungen zu vermeiden.

htmlPageTable

Die Tabelle htmlPageTable enthält allgemeine (Meta-)Informationen über die Custom-Pages. Jeder Custom-Page, auf die ein Hyperlink in der DR-Web-Menü-Seite existiert, ist eine Zeile in der htmlPageTable zugeordnet.

MIB-Definition	Zugriff	Erläuterung
htmlPageTitle	read-create	*htmlPageTitle* spezifiziert den Titel der zugehörigen HTML-Seite. Der Text in diesem DisplayString-Objekt wird in der HTML-Seite zwischen den Tags <title>...<\title> eingefügt. Ein String der Länge 0 bedeutet, dass die Custom-Page keinen Titel hat.
htmPageAddressInfo	read-create	*htmlPageAddressInfo* spezifiziert Adressinformation der zugehörigen HTML-Seite. Der Text in diesem DisplayString-Objekt wird unten auf der HTML-Seite zwischen den Tags <address>...<\address> eingefügt. Ein String der Läng 0 bedeutet, dass die Custom-Page keine Adressinformation enthält.
htmlPageLastUpdated	read-create	*htmlPageLastUpdated* spezifiziert den Zeitpunkt der letzten Änderung der HTML-Seite. Diesem Objekt ist kein spezielles Format zugeordnet.
htmlPageBodyArgs	read-create	*htmlPageBodyArgs* enthält die Argumente für den <body>-Tag. Z.B. kann dieses DiplayString-Objekt den den Wert bgcolor='EFEFEF' haben, der dem <body>-Tag <body bgcolor='#EFEFEF' entspricht. Der Defaultwert von *htmlPageBodyArgs* ist der String der Läng 0. *htmlPageBodyArgs* wird außerdem für die Einstellung der Refresh-Zeit verwendet (siehe Seite 414).
htmlPageOwner	read-create	*htmlPageOwner* spezifiziert den Eigentümer der Custom-Page. Mithilfe dieses Objekts wird der Zugriff mehrerer Management-Plattformen auf die Custom-Page koordiniert. In *htmlPageOwner* können beliebige Daten abgelegt werden. Eine Instanz des Objekts sollte mindestens die snmpID des SNMP-Managers sowie die User-ID enthalten. Beim Erzeugen einer neuen Tabellenzeile bzw. beim Ändern einer vorhandenen Zeile sollte der Manager das Objekt *htmlPageSetSerialNo* der *htmlPages*-Gruppe verwenden, um den Zugriff auf die gesamte *htmlPageTable* kontrollieren zu können.
htmlPageStorageType	read-create	*htmlPageStorageType* spezifiziert, wie die zugehörige Tabellenzeile abgespeichert werden soll. Dieses Objekt ist vom Typ StorageType und als TEXTUAL-CONVENTION beschrieben im RFC 1903.

MIB-Definition	Zugriff	Erläuterung
htmlPageStatus	read-create	*htmlPageStatus* enthält den Status der Instanz in der der *htmlPageTable*. Dieses Objekt ist vom Typ *RowStatus* und als TEXTUAL-CONVENTION im RFC 1903 beschrieben. Zu beachten ist, dass das Löschen einer Zeile keine Auswirkung auf die zugeordneten Zeilen der *htmlPageTable* und der *htmlPagContentTable* hat. Vielmehr wird die Speicherbereinigung mithilfe des Objekts *htmlConsistencyCheck* der *htmlGlobals*-Gruppe durchgeführt.

htmlPageParameterTable

Die Objekte der *htmlPageParameterTable* enthalten Informationen über die Parameter, die durch die Inhalte der zugeordneten Custom-Pages referenziert werden können. Die *htmlPageParameterTable* wird gefunden über den Namen *htmlPageName* der Custom-Page, die den Parameter referenziert.

MIB-Definition	Zugriff	Erläuterung
htmlPageParameterName	read-create	Name des Parameters in der HTML-Seite
htmlPageParameterDefault	read-create	Default-Wert für für einen speziellen Parameter in einer speziellen HTML-Seite
htmlPageParameterStorageType	read-only	*htmlPageParameterStorageType* spezifiziert, wie die Tabellenzeile gespeichert werden soll. Dieses Objekt ist vom Typ StorageType als TEXTUAL-CONVENTION beschrieben im RFC 1903.
htmlPageParameterStatus	read-only	Status der zugeordneten Instanz in der *htmlPageParameterTable.*

htmlPageContentTable

Die Objekte der *htmlPageContentTable* enthalten Informationen über die Inhalte von Custom-Pages. Die *htmlPageContentTable* wird gefunden über den durch *htmlPageName* spezifizierten Namen der Custom-Page, die den Parameter spezifiziert.

MIB-Definition	Zugriff	Erläuterung
htmlPageContentIndex	not-accessible	Index für einen Textabschnitt, der auf einer HTML-Seite angezeigt werden soll. Zu beachten ist, dass die Index-Werte in der *htmlPageContentTable* nicht fortlaufend angeordnet sein müssen. So können Tabellenzeilen z.B in 5er- oder 10er-Schritten indiziert sein. Dies ist sinnvoll, da der durch die zunächst nicht belegten Index-Werte gewonnene Platz für zusätzliche Zeilen verwendet werden kann. Dies erleichtert Modifikation und Ergänzung einer Custom-Page.
htmlPageContentText	read-create	*htmlPageContentText* spezifiziert einen Textabschnitt, der auf der Custom-Page dargestellt werden soll.
htmlPageContentStorageType	read-create	*htmlPageContentStorageType* spezifiziert, wie die zugehörige Tabellenzeile abgespeichert werden soll.
htmlPageContentStatus	read-create	*htmlPageContentStatus* enthält den Status der zugeordneten Tabellezeile.

5.6 Trap-Sicherung

Die asynchrone Meldung von Problemen über Traps des Agenten ist äußerst performant, da die Netzbelastung auf ein Minimum reduziert wird. Problematisch dagegen ist, dass die Information verloren geht, wenn zum Zeitpunkt des Trap-Sendens keine Management-Station eingeschaltet oder die Kommunikation zu ihr fehlerhaft war. Eine wesentliche Verbesserung dieses Verhaltens wird durch das hier beschriebene Konzept der Trap-Bestätigung erreicht.

Einem Trap, der als *zu bestätigen* deklariert ist, wird eine interne Information mitgegeben. Die Management-Station erkennt diese Information und sendet daraufhin automatisch einen Set-Request an den Agenten. Erhält der Agent den Request, gilt für ihn der Trap als bestätigt.

Das Konzept setzt neben der in diesem Handbuch beschriebenen Version der Agenten vor allem ein TransView Control Center ab Version V4.3 voraus. Die Console Monitor-Anwendung kann ebenfalls Traps bestätigen (siehe Seite 356).

Es können nur Traps des Console Monitor Subagenten und des Application Monitor Subagenten, die im Application Monitor-spezifischen Trap-Format gesendet werden, als *zu bestätigen* deklariert werden.

Funktionalität

Zu bestätigende Traps werden streng sequenziell gesendet, d.h. ein zu bestätigender Trap wird vom Agenten nur dann gesendet, wenn die Bestätigung des vorherigen Traps eingetroffen ist.

Nicht zu bestätigende Traps werden in jedem Fall gesendet.

Zu bestätigende Traps werden bis zu ihrer Bestätigung im Agenten zwischengespeichert.

Trifft die Bestätigung nicht innerhalb der Toleranzzeit von 30 Sekunden ein, wird ein Information-Trap mit folgender Meldung gesendet:

```
<number> messages left in SNMP Master-Agent agent buffer;
```

Dabei ist <number> die Anzahl der Traps, die nicht bestätigt wurden oder nicht gesendet werden konnten, weil die Bestätigung ausbleibt. Dieser Information-Trap selbst ist auch ein zu bestätigender Trap. Im Gegensatz zu einem Nutz-Trap wird ein Information-Trap aber nicht zwischengespeichert. Er wird bis zu einer Bestätigung im Abstand von 90 Sekunden wiederholt. Damit wird periodisch die Kommunikation auf ihre Funktionsfähigkeit geprüft.

Trifft eine Bestätigung beim Agenten ein, werden die zwischengespeicherten Traps erneut und im Originalformat, also auch mit dem Flag *zu bestätigen*, gesendet.

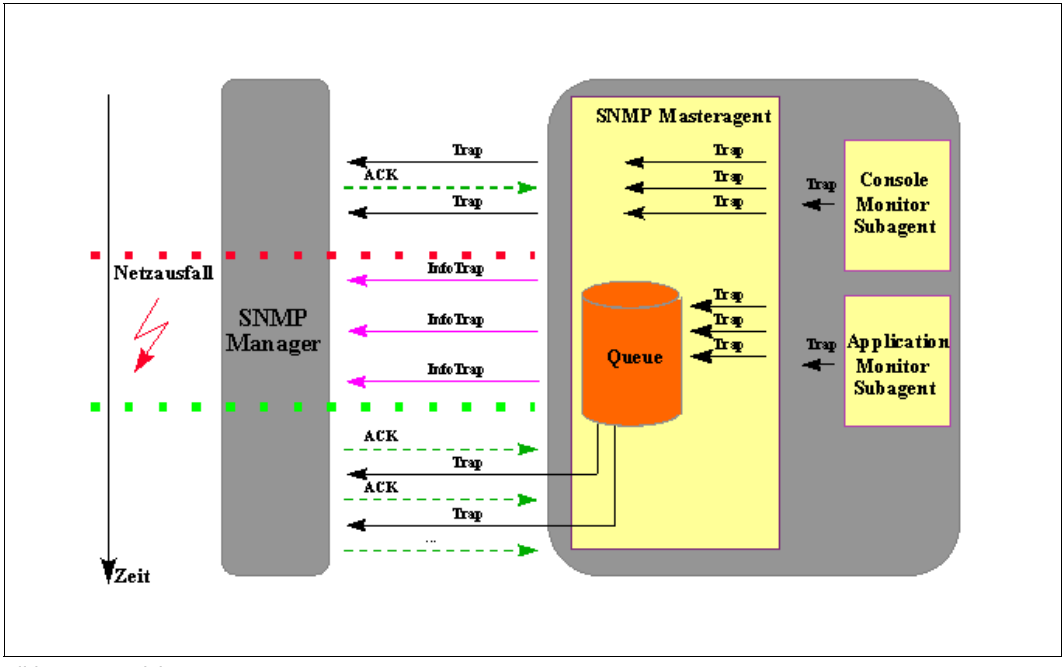


Bild 18: Trap-Sicherung

Konfiguration

Welche Traps durch den Manager zu bestätigen sind, wird wie folgt festgelegt:

– im Console Monitor Subagenten durch die Angabe `ACKNOWLEDGE=YES` in Meldungsfilterdatei (siehe Seite 76)

– im Application Monitor Subagenten durch die Angabe `ACKNOWLEDGE=YES` in den Anweisungen der Konfigurationsdatei (siehe Seite 60)

Damit ist eine differenzierte Festlegung des Acknowledge bis auf die Ebene von Meldungsnummern bzw. von Anwendungen möglich.

Steuerung der Trap-Sicherung

Die Trap-Sicherung ist auf der BS2000-Seite eingeschaltet, sobald der Supervisor Subagent gestartet wird. Das gesamte Bestätigungsverfahren kann mit dem Kommandoprogramm des Masteragenten und der Console Monitor-Anwendung SMAWcmbs2 (Solaris) bzw. CMBS2 (Reliant UNIX) gesteuert werden (siehe Abschnitt „Fenster zur Trap-Bestätigung“ auf Seite 372):

/START-MASTERCMD	
x	agent executes command
getTrapAckState	1 oder 2: Bestätigung eingeschaltet 3 oder 4: Bestätigung ausgeschaltet
startTrapAck	schaltet Bestätigungsverfahren ein.
stopTrapAck	schaltet Bestätigungsverfahren aus.

1. Es ist zu empfehlen, nur wenige wichtige Traps mit dem Flag *zu bestätigen* zu senden.
2. Die Bestätigung durch eine Management-Station genügt dem Agenten.
3. Ist keine der Management-Stationen in der Lage, zu bestätigen, so werden alle als *zu bestätigen* deklarierten Traps zurückgehalten und gespeichert.

6 Funktionen der STANDARD-COLLECTION

Die in der STANDARD-COLLECTION enthaltenen Subagenten werden in diesem Kapitel beschrieben. Neben Funktionsbeschreibungen finden Sie hier auch vollständige Auflistungen der MIBs.

6.1 SNMP-Management für AVAS

Die AVAS-MIB besteht aus vier Gruppen für folgende Aufgaben:

– Information über Basisdaten

– Überwachung der zentralen Prozesse und Ablaufsteuerungen

– Überwachung der Netze

– Überwachung der Netzstrukturelemente

Basisdaten

MIB-Definition	Zugriff	Erläuterung
avasagtVersion	read-only	Version des AVAS-Subagenten
avasSystemID	read-only	AVAS System-ID

Prozesse und Ablaufsteuerungen

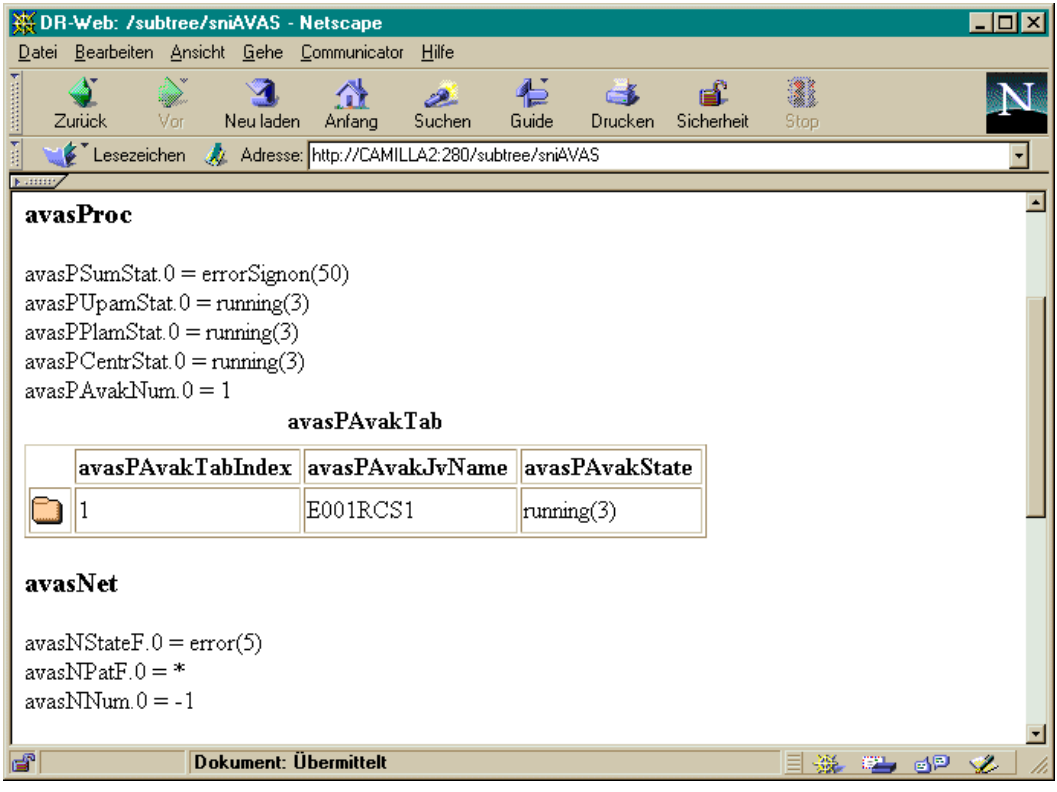


Bild 19: AVAS: Status der zentralen Prozesse

Gruppe zur Überwachung der zentralen Prozesse und Ablaufsteuerungen

MIB-Definition	Zugriff	Erläuterung
avasPSumStat	read-only	Systemstatus AVAS*
avasPUpamStat	read-only	Prozessstatus UPAM-ZD
avasPPlamStat	read-only	Prozessstatus PLAM-ZD
avasPCentrStat	read-only	Zentral-Prozessstatus
avasPAvakNum	read-only	Anzahl der Ablaufsteuerungen
Tabelle:		
avasPAvakTabIndex	read-only	Index
avasPAvakJvName	read-only	Name
avasPAvakState	read-only	Status

*Die entsprechenden Werte entnehmen Sie bitte der folgenden Tabelle.

Der AVAS-Systemstatus wird aus einer Kombination der Zustände der Verarbeitungsprozesse gebildet und liefert eine Gesamtinformation zum Zustand des AVAS-Systems.

Wert	Bedeutung
missing	Einer der Prozesse UPAM-ZD und PLAM-ZD ist weder im Zustand "ready" noch "running".
ready	Die Prozesse UPAM-ZD und PLAM-ZD sind im Zustand "ready".
running	Die Prozesse UPAM-ZD und PLAM-ZD sind im Zustand "ready“ und mindestens 1 RCS ist im Zustand "running".
error-net	Mindestens 1 Netz befindet sich im Status "error"
error-system	Einer der Prozesse UPAM-ZD und PLAM-ZD ist ausgefallen
error-signon	Die Verbindungsaufnahme über die Programmschnittstelle war erfolglos.

Systemstatus AVAS

Außerdem werden Informationen zum Zentral-Prozessstatus, zum Status der Prozesse PLAM-ZD und UPAM-ZD und zur Anzahl der Ablaufsteuerungen geliefert. Die Interpretation der möglichen Ausgaben entnehmen Sie bitte den entsprechenden AVAS-Handbüchern.

Anzeigen der Jobnetze

Die Gruppe zur Überwachung der Netze liefert tabellarisch Informationen über AVAS-Netze. Auswahlkriterium für den Umfang der gelieferten Information sind entweder Netzstatus oder Netzname. Bei Angabe eines Netzstatus werden nur diejenigen Objekte angezeigt, die sich im angegebenen Zustand befinden. Auswahlkriterium Netzname: die Eingabe erfolgt in Großbuchstaben, am Ende dieser Eingabe ist ein "*" zulässig. "*" ist die Default-Einstellung für den Netznamen. Die Angabe des Benutzerkreises ist nicht nötig. Bei vollqualifizierter Eingabe des Netznamens werden Einschränkungen hinsichtlich des Netzstatus ignoriert.

Gruppe zur Überwachung der AVAS-Netze

MIB-Definition	Zugriff	Erläuterung
avasNStateF	read-write	Anzeigeeinschränkung Netzstatus
avasNPatF	read-write	Anzeigeeinschränkung Netzname
avasNNum	read-only	Anzahl der Netze
Tabelle:		
avasNTabIndex	read-only	Tabellenindex
avasNName	read-only	Netzname
avasNState	read-only	Netzstatus*
avasNStateOfError	read-only	Netzstatus-Switch : Fehler
avasNStateOfRestart	read-only	Netzstatus-Switch : Restart
avasNStateOfCondwait	read-only	Netzstatus-Switch : Condwait
avasNStateOfHold	read-only	Netzstatus-Switch : Hold
avasNAvak	read-only	zum Netz gehörende Ablaufsteuerung

*Die entsprechenden Werte entnehmen Sie bitte der folgenden Tabelle.

Die Interpretation der Ausgaben finden Sie in den entsprechenden AVAS-Handbüchern.

Statusflag zur Anzeigeeinschränkung der AVAS-Netze:

Wert	Bedeutung
problem	Es werden die Netze angezeigt, die sich im Zustand "error", "hold", "waiting" oder "condwait" befinden. Dies ist die Standardeinstellung.
error	Es werden nur die Netze angezeigt, die sich im Zustand "error" befinden.
hold	Es werden nur die Netze angezeigt, die sich im Zustand "hold" befinden.
running	Es werden nur die Netze angezeigt, die sich im Zustand "running" befinden.
waiting	Es werden nur die Netze angezeigt, die sich im Zustand "waiting" befinden.
condwait	Es werden nur die Netze angezeigt, die sich im Zustand "condwait" befinden.

Netzstatus AVAS

Anzeigen der Strukturelemente

Die Gruppe zur Überwachung der Strukturelemente liefert tabellarisch Informationen über AVAS-Strukturelemente. Mögliche Auswahlkriterien für den Umfang der gelieferten Information sind

– Netzstatus,
– Netzname,
– Elementstatus,
– Elementtyp oder
– Elementfunktion.

Bei Angabe eines Netzstatus werden diejenigen Elemente angezeigt, deren Netze sich im angegebenen Zustand befinden. Auswahlkriterium Netzname: die Eingabe erfolgt in Großbuchstaben, am Ende dieser Eingabe ist ein "*" zulässig. "*" ist die Default-Einstellung für den Netznamen. Die Angabe des Benutzerkreises ist nicht nötig. Bei vollqualifizierter Eingabe des Netznamens werden Einschränkungen hinsichtlich des Netzstatus ignoriert. Das Auswahlkriterium Elementstatus liefert Informationen über Elemente, die sich im angegebenen Zustand befinden (siehe Tabelle). Wird nach Elementtyp ausgewählt, werden die Elemente entsprechenden Typs ausgegeben, Standardwert für Elementtyp ist "all". Eine Ausgabe, eingeschränkt auf Elementfunktionen, ist mit dem Auswahlkriterium Elementfunktion möglich. Voreingestellt ist der Wert "all". Die ausführliche Beschreibung der Werte für Elementtyp und -funktionen entnehmen Sie bitte den entsprechenden AVAS-Handbüchern.

Gruppe zur Überwachung der AVAS-Strukturelemente

MIB-Definition	Zugriff	Erläuterung
avasENStateF	read-write	Anzeigeeinschränkung Netzstatus [1)]
avasENPatF	read-write	Anzeigeeinschränkung Netzname
avasEEStateF	read-write	Anzeigeeinschränkung Elementstatus [2)]
avasEEFuncF	read-write	Anzeigeeinschränkung Elementfunktion
avasEETypeF	read-write	Anzeigeeinschränkung Elementtyp
avasENum	read-only	Anzahl der Elemente
Tabelle:		
avasETabIndex	read-only	Tabellenindex
avasEName	read-only	Name des Strukturelements
avasEFu	read-only	Funktion des Strukturelements
avasEType	read-only	Typ des Strukturelements
avasEInd	read-only	Indexstufe des Strukturelements
avasESynInd	read-only	Synchronisationsstufe des Strukturelements
avasEState	read-only	Status des Strukturelements
avasENet	read-only	zugehöriges Netz
avasEDelSolution	read-only	DELAY-Solution für das Strukturelement
avasELatest	read-only	spätester Startzeitpunkt

[1)] siehe Tabelle „Netzstatus der AVAS-Strukturelemente“ auf der nächsten Seite
[2)] siehe Tabelle „Elementstatus der AVAS-Strukturelemente“ auf der nächsten Seite

Die Interpretation der Ausgaben finden Sie in den entsprechenden AVAS-Handbüchern.

Netzstatusflag zur Anzeigeeinschränkung der AVAS-Strukturelemente

Wert	Bedeutung
problem	Es werden nur die Elemente angezeigt, deren Netz sich im Zustand "error", "hold", "running", "waiting" oder "condwait" befindet. Dies ist die Standardeinstellung.
error	Es werden nur die Elemente angezeigt, deren Netz sich im Zustand "error" befindet.
hold	Es werden nur die Elemente angezeigt, deren Netz sich im Zustand "hold" befindet.
running	Es werden nur die Elemente angezeigt, deren Netz sich im Zustand "running" befindet.
waiting	Es werden nur die Elemente angezeigt, deren Netz sich im Zustand "waiting" befindet.
condwait	Es werden nur die Elemente angezeigt, deren Netz sich im Zustand "condwait" befindet.

Netzstatus der AVAS-Strukturelemente

Elementstatusflag zur Anzeigeeinschränkung der AVAS-Strukturelemente

Wert	Bedeutung
all	Es erfolgt keine Einschränkung über den Status. Dies ist die Standardeinstellung.
abended	Es werden nur die Elemente angezeigt, die sich im Zustand "abended" befinden.
error	Es werden nur die Elemente angezeigt, die sich im Zustand "error" befinden
hold	Es werden nur die Elemente angezeigt, die sich im Zustand "hold" befinden.
running-exec	Es werden nur die Elemente angezeigt, die sich im Zustand "running-exec" befinden.
skipped	Es werden nur die Elemente angezeigt, die sich im Zustand "skipped" befindet.
waiting	Es werden nur die Elemente angezeigt, die sich im Zustand "waiting" befinden.
noOccure	Es werden nur die Elemente angezeigt, die sich im Zustand "no-Occure" befinden.

Elementstatus der AVAS-Strukturelemente

Traps

Objektname	**Trap-Nr**	**Erläuterung**
avasLastMsg		Last Trap Message
avasStateTraps (Enterprise = 1.3.6.1.4.1.231.2.24.11.10)		
avasMissing	301	(UPAMZD || PLAMZD) not ready
avasReady	302	(UPAMZD && PLAMZD) ready
avasRunning	303	min1 RCS (ready || running)
avasErrorSystem	304	(UPAMZD || PLAMZD) abended
avasErrorNet	305	min1 net in error
avasErrorSignon	350	SIGNON != ok
avasProblemTraps (Enterprise = 1.3.6.1.4.1.231.2.24.11.11)		
avasNetAbended	311	Net abended
avasNetError	312	Net error
avasNetRestarted	313	Net Restarted
avasNetCancelled	314	Net Cancelled
avasJobAbended	321	Job abended
avasJobError	322	Job error
avasJobRestarted	323	Job restarted
avasJobCancelled	324	Job cancelled
avasProcAbended	331	Procedure abended
avasProcError	332	Procedure error
avasProcRestarted	333	Procedure restarted
avasProcCancelled	334	Procedure cancelled
avasUJobAbended	341	Unix or NT Job abended
avasUJobError	342	Unix or NT Job error
avasUJobRestarted	343	Unix or NT Job restarted
avasUJobCancelled	344	Unix or NT Job cancelled

6.2 SNMP-Management für *open*FT (BS2000)

Der Filetransfer-Subagent dient
- zum Starten und Stoppen von *open*FT (BS2000)
- zur Informationsbeschaffung über Systemparameter
- zum Ändern des Public-Key zur Verschlüsselung
- zur Ausgabe von Statistikdaten
- zur Steuerung der Diagnose
- zur Ausgabe von Partner-Informationen

Die proprietäre MIB zu *open*FT (BS2000) bietet Objekte zu den oben genannten Management-Aufgaben. Die Objekte zum Starten und Stoppen, zur Verschlüsselung des Public-Key und zur Steuerung der Diagnose bieten auch schreibende Zugriffe.

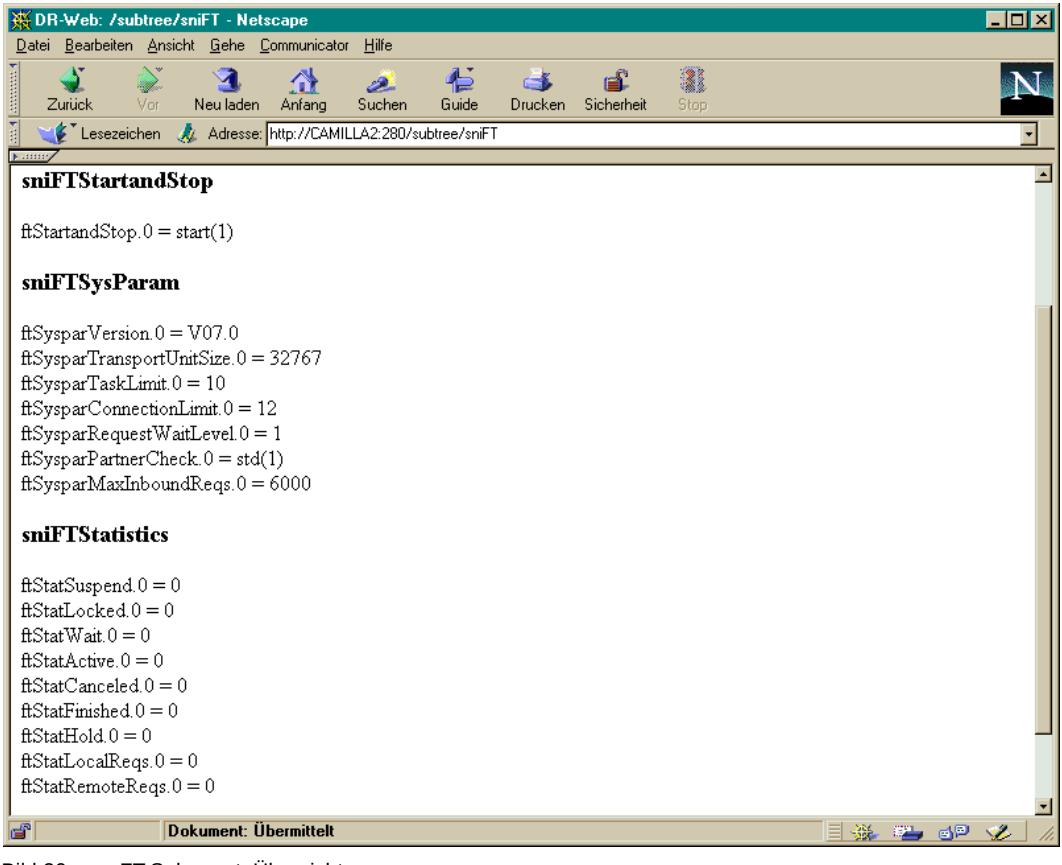


Bild 20: *open*FT-Subagent: Übersicht

Starten und Stoppen von FT

MIB-Definition	Zugriff	Erläuterung
ftStartandStop	read-write	Start / Stop start (1) stop (2) on (3) off (4) undefined (255)

Mit Setzen der Werte *START* bzw. *STOP* wird durch den FT-Subagenten das Starten bzw. Stoppen von FT veranlasst.

– Ein lesender Zugriff liefert Informationen über den aktuellen Zustand von FT (STARTED/NOT STARTED) .

– Mit schreibendem Zugriff kann FT gestartet oder beendet werden.

Systemparameter

MIB-Definition	Zugriff	Erläuterung
ftSysparVersion	read-only	Version
ftSysparTransportUnitSize	read-write	Transport Unit Size
ftSysparTaskLimit	read-write	Task Limit
ftSysparConnectionLimit	read-write	Maximale Anzahl von Transportverbindungen, die für die Ausführung von FT-Requests reserviert werden können.
ftSysparRequestWaitLevel	read-write	Anzahl der wartenden Requests, die für den Aufbau einer Verbindung zum entfernten System erforderlich sind (Request Wait Level)
ftSysparPartnerCheck	read-write	Partner Check
ftSysparProcessorName	read-write	Prozessorname des Zielsystems
ftSysparStationName	read-write	Stationsname des Zielystems
ftSysparMaxInboundReqs	read-write	Maximalzahl der pro Partnersystem eingehenden (inbound) Requests
ftSysparMaxLifeTime	read-write	Maximale Lebensdauer (in Tagen) in der Warteschlange der Requests (maximal 400 Tage)

Die Erklärung der ausgegebenen Werte finden Sie im *open*FT (BS2000) Systemverwalter-Handbuch.

Public-Key zur Verschlüsselung

MIB-Definition	Zugriff	Erläuterung
ftEncryptKey	write-only	Die Eingabe "create-new-key" bzw. "1" bewirkt die Erzeugung eines neuen Public-Key.

Statistik-Informationen

MIB-Definition	Zugriff	Erläuterung
ftStatSuspend	read-only	Requests im Status: SUSPEND
ftStatLocked	read-only	Requests im Status: LOCKED
ftStatWait	read-only	Requests im Status: WAIT
ftStatActive	read-only	Requests im Status: ACTIVE
ftStatCanceled	read-only	Requests im Status: CANCELED
ftStatFinished	read-only	Requests im Status: FINISHED
ftStatHold	read-only	Requests im Status: HOLD
ftStatLocalReqs	read-only	Async Requests im lokalen System
ftStatRemoteReqs	read-only	Requests im fernen System

Die Erklärung der ausgegebenen Werte befindet sich im *open*FT (BS2000) Systemverwalterhandbuch im Abschnitt zum Kommando SHOW-FILE-TRANSFER.

Steuerung der Diagnose

MIB-Definition	Zugriff	Erläuterung
ftDiagStatus	read-write	Diagnose Management

Die folgende Tabelle zeigt die Eingabemöglichkeiten - Syntax oder Integer - zur FT-Diagnose-Steuerung:

Eingabe:		Bedeutung für:		
Syntax	**Integer**	**FTNEA=**	**FTAM=**	**SESSION=**
off	1	TRACE=OFF - schaltet alle FT-Traces aus		
snn	2	*STD	*NONE	*NONE
pnn	3	*BY-PARTNER	*NONE	*NONE
mnn	4	*MINIMUM	*NONE	*NONE
nnn	5	*NONE	*NONE	*NONE

Eingaben zur Steuerung der FT-Diagnose

Eingabe:		**Bedeutung für:**		
Syntax	**Integer**	**FTNEA=**	**FTAM=**	**SESSION=**
ssn	6	*STD	*STD	*NONE
sns	7	*STD	*NONE	*STD
sss	8	*STD	*STD	*STD
psn	9	*BY-PARTNER	*STD	*NONE
pns	10	*BY-PARTNER	*NONE	*STD
pss	11	*BY-PARTNER	*STD	*STD
msn	12	*MINIMUM	*STD	*NONE
mns	13	*MINIMUM	*NONE	*STD
mss	14	*MINIMUM	*STD	*STD
nsn	15	*NONE	*STD	*NONE
nns	16	*NONE	*NONE	*STD
nss	17	*NONE	*STD	*STD
on	18	TRACE=ON - schaltet alle FT-Traces an		
Die folgenden Angaben bewirken eine Trace-Speicherung im Hauptspeicher:				
smnn	19	*STD	*NONE	*NONE
smsn	20	*STD	*STD	*NONE
smns	21	*STD	*NONE	*STD
smss	22	*STD	*STD	*STD
pmnn	23	*BY-PARTNER	*NONE	*NONE
pmsn	24	*BY-PARTNER	*STD	*NONE
pmns	25	*BY-PARTNER	*NONE	*STD
pmss	26	*BY-PARTNER	*STD	*STD
mmnn	27	*MINIMUM	*NONE	*NONE
mmsn	28	*MINIMUM	*STD	*NONE
mmns	29	*MINIMUM	*NONE	*STD
mmss	30	*MINIMUM	*STD	*STD

Eingaben zur Steuerung der FT-Diagnose

Die gebräuchlichsten Eingaben sind "off" (1) und "sss" (8).
Beachten Sie bitte zusätzlich den Abschnitt zum Kommando MODIFY-FT-OPTIONS im Systemverwalterhandbuch zu *open*FT (BS2000).

Partner-Informationen

MIB-Definition	Zugriff	Erläuterung
ftPartnerName	read-only	Name des FT-Partners
ftPartnerType	read-only	vom Partner verwendetes FT-Protokoll: openft (1), ftam (2)
ftPartnerState	read-write	Status des FT-Partners: act (1), inact (2), nocon (3), lunk (4), runk (5), adeact (6), ainact (7)
ftPartnerNetworkAddr	read-only	Layer 3 Adresse des Partners
ftPartnerTransportSel	read-only	Layer 4 Adresse des Partners
ftPartnerSessionSel	read-only	Layer 5 Adresse des Partners
ftPartnerPresentationSel	read-only	Layer 6 Adresse des Partners

Derzeit wird nur die Statusänderung für einen Partner unterstützt.

Traps

Objektname	Trap-Nr	Erläuterung
Enterprise = sniFTTraps		
ftStopTrap	1	TRAP wird gesendet, wenn der File Transfer verloren ging oder mit Fehler beendet wurde.
ftPartnerStateTrap	4	TRAP wird gesendet, wenn sich der Zustand des Partners geändert hat.
ftPartnerUnreachableTrap	5	Partner ist möglicherweise nicht erreichbar.
ftStartTrap	6	TRAP wird nach dem Start von *open*FT gesendet.
ftRequestQueueUpperLimitTrap	7	TRAP wird gesendet, wenn die Warteschlange der FT-Requests zu mindestens 85 % gefüllt ist.
ftRequestQueueLowerLimitTrap	8	TRAP wird gesendet, wenn mindestens 20 % der Warteschlange der FT-Requests noch nicht belegt sind.
ftRequesrSuccessfulTrap	9	TRAP wird bei erfolgreicher Ausführung eines FT-Requests gesendet.
ftRequestErrorTrap	10	TRAP wird gesendet, wenn ein FT-Auftrag mit Fehler beendet wurde.
ftSubsystemStartTrap	11	TRAP wird gesendet, wenn das Subsystem FT gestartet wurde.
ftSubsystemStopTrap	12	TRAP wird gesendet, wenn das Subsystem FT gestoppt wurde.

*open*FT-Traps

Trap-Gruppen und Trap-Steuerung

Die Traps des *open*FT-Subagenten können in Gruppen zusammengefasst werden, die durch die nachfolgenden MIB-Objekte repräsentiert werden. Auf diese Weise können Sie für die einzelnen Trap-Gruppen das Senden von Traps wie folgt veranlassen oder unterbinden (Trap-Sendezustand "on" bzw. "off"):

– Angabe von 2 ("on"): Die Traps der betreffenden Gruppe werden gesendet.
– Angabe von 1 ("off"): Die Traps der betreffenden Gruppe werden nicht gesendet.

MIB-Definition	Zugriff	betroffene Traps
ftTrapsSubsystemState	read-write	– ftSubsystemStartTrap – ftSubsystemStopTrap
ftTrapsFTState	read-write	– ftStartTrap – ftStopTrap
ftTrapsPartState	read-write	– ftPartnerStateTrap
ftTrapsPartnerUnreachable	read-write	– ftPartnerUnreachableTrap
ftTrapsRequestQueueState	read-write	– ftRequestQueueLowerLimitTrap – ftRequestQueueUpperLimitTrap
ftTrapsTransSucc	read-write	– ftRequestSuccesfulTrap
ftTrapsTransFail	read-write	– ftRequestErrorTrap

Trap-Informationen

In der MIB des *open*FT-Subagenten sind MIB-Objekte definiert, die zusammen mit den Traps versendet werden.

MIB-Definition	Zugriff	Erläuterung
ftRequestID	not-accessible	Transfer-ID des Auftrags
ftRequestInitiator	not-accessible	Initiator des Auftrags: local (1), remote (2)
ftRequestPartnerName	not-accessible	Partner des Auftraggebers
ftRequestUserID	not-accessible	Benutzerkennung des Auftraggebers
ftRequestFileName	not-accessible	Name der zu übertrageneden Datei
ftRequestError	not-accessible	Fehler im Auftrag

6.3 SNMP-Management für HIPLEX-AF

Die HIPLEX-AF-MIB enthält Informationen zu den an einem HIPLEX-AF-Verbund beteiligten Systemen und zu den definierten Umschalteinheiten. Wichtige Ereignisse im Verbund, wie z.B. das Starten und Beenden oder das Umschalten, werden durch Traps gemeldet.

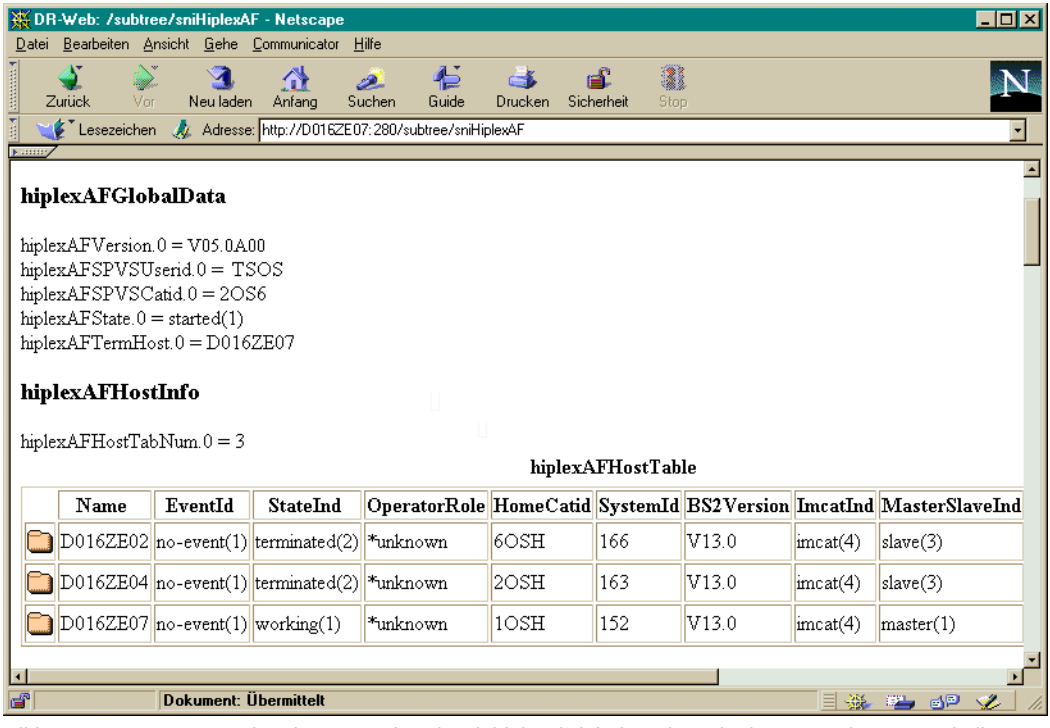


Bild 21: HIPLEX-AF: Anzeige der Werte der Einzelobjekte (GlobalData) sowie der Werte der Host-Tabelle

HIPLEX-AF-Einzelobjekte

Objektname	Zugriff	Erläuterung
hiplexAFVersion	read-only	Version des HIPLEX-AF-Subagenten
hiplexAFSPVSUserid	read-only	HIPLEX-AF-Benutzerkennung (in der Regel TSOS)
hiplexAFSPVSCatid	read-write	Katalog-Kennung des Shared Pubset, das die Jobvariablen und Dateien von HIPLEX-AF enthält
hiplexAFStatus	read-write	Status von HIPLEX-AF: – *started*: mindestens eine Haupt-Prozedur wurde auf einem Host gestartet. – *stopped*: HIPLEX-AF wurde beendet. Auf keinem Host wird eine HIPLEX-AF-Prozedur ausgeführt. – *undefined*: Der Status von HIPLEX-AF ist unbekannt. Es konnten keine Job-Variablen mit korrekten Werten gefunden werden. Vom Status *started* kann in den Status *stopped* gewechselt werden.
hiplexAFTermHost	read-only	BCAM-Name des Systems, auf dem die Anforderung zum Beenden von HIPLEX-AF ausgelöst wurde.

Host-Tabelle

Objektname	Zugriff	Erläuterung
hiplexAFHostTabNum	read-only	Anzahl der Hosts im Availability-Cluster
Tabelle:		
hiplexAFHostName	read-only	BCAM-Name des Systems
hiplexAFHostEventId	read-only	Request-Indikator für die Hauptprozedur: – no-request – termination-requested – undefined
hiplexAFHostStateInd	read-write	Status der Hauptprozedur, der die Beteiligung des Host anzeigt: – working – terminated – undefined Status *working* kann nur vom Status *terminated* aus erreicht werden.
hiplexAFHostOperatorRole	read-write	Status des Operator-Role-Parameters des START-XAF-Kommandos
hiplexAFHostHomeCatid	read-only	Home-CatID des Systems
hiplexAFHostSystemId	read-only	Systemkennung
hiplexAFHostBS2Version	read-only	BS2000/OSD-Version auf dem System
hiplexAFHostImcatInd	read-only	Status des Host: – check – crash – exact – imcat – mchange – readerr – shutdown – wrterr – undefined
hiplexAFHostMasterSlaveInd	read-only	Typ des Host im Shared-Pubset-Verbund: – master – backup – slave – undefined
hiplexAFHostSnmpAgentStatusInd	read-only	Status des SNMP-Subagenten auf dem System: – working – not-working – undefined

Tabelle für die Umschalteinheiten

Objektname	Zugriff	Erläuterung
hiplexAFSWUTabNum	read-only	Anzahl der Umschalteinheiten im Availability-Cluster
Tabelle:		
hiplexAFSWUName	read-only	Name der Umschalteinheit
hiplexAFSWUCreaTime	read-only	Erstellungsdatum der Umschalteinheit
hiplexAFSWUWorkSystem	read-write	BCAM-Name des Systems, das derzeit das Worksystem für die Umschalteinheit ist
hiplexAFSWUVirtHost	read-only	BCAM-Name des virtuellen Host für die Umschalteinheit
hiplexAFSWUVirtHostAct	read-only	Name der Prozedur zur Aktivierung des virtuellen Host
hiplexAFSWUVirtHostDeact	read-only	Name der Prozedur zur Deaktivierung des virtuellen Host
hiplexAFSWUFEPNumber	read-only	Anzahl der Front-End-Prozessoren
hiplexAFSWUPubsetNumber	read-only	Anzahl der Datenträger, die von Anwendungen der Umschalteinheit benutzt werden
hiplexAFSWUApplicationNumber	read-only	Anzahl der in der Umschalteinheit enthaltenen Anwendungen

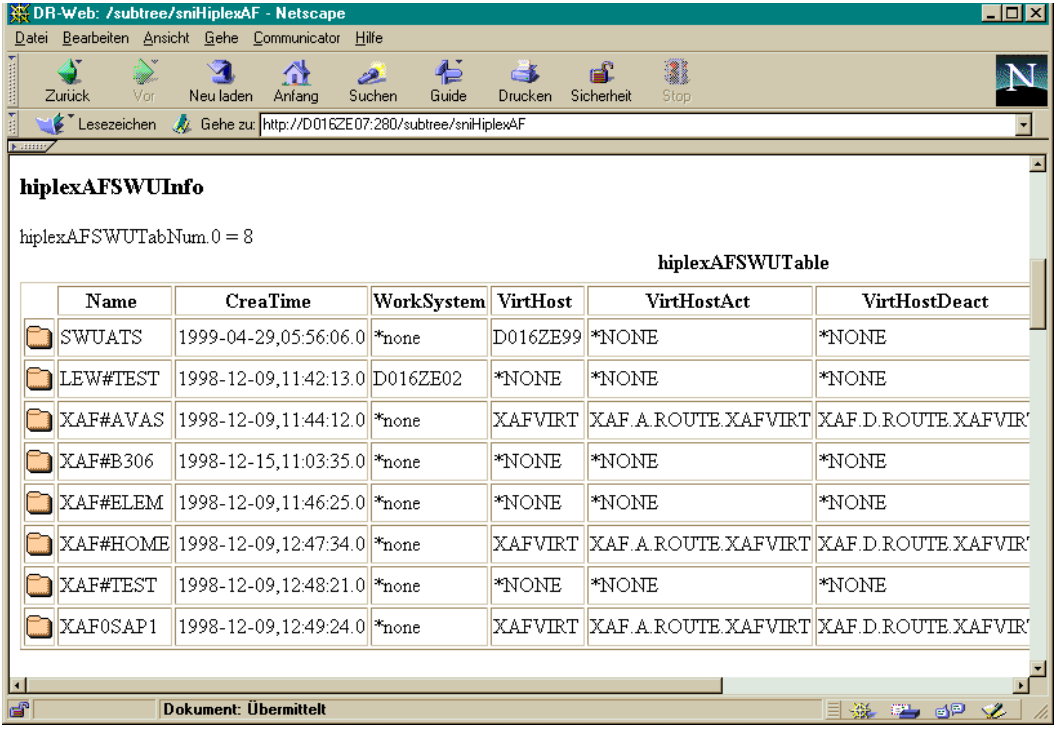


Bild 22: HIPLEX-F: Informationen zu den Umschalteinheiten

Tabelle der host-spezifischen Parameter für die Umschalteinheiten

Objektname	Zugriff	Erläuterung
hiplexAFSWUHostParamEventId	read-only	Letzte Aktion der Umschalteinheit: – no-action – pass-over – take-over – terminate – undefined
hiplexAFSWUHost ParamStat Ind	read-write	Status der Umschalteinheit: – work – standby – crashed – terminated – undefined
hiplexAFSWUHostParamPriority	read-write	Priorität des Host beim automatischen Umschalten
hiplexAFSWUHostParamOperatorRole	read-write	Beim START-SWITCH-UNIT-Kommando angegebener Wert des Parameters „Operator-Role“

Tabelle der Front-End-Prozessoren

Objektname	Zugriff	Erläuterung
hiplexAFSWUHostFEPTabNum	read-only	Anzahl der FEP-Einträge
Tabelle:		
hiplexAFSWUHostFEPIndex	read-only	Index des Front-End-Prozessors
hiplexAFSWUHostFEPName	read-write	BCAM-Name des Front-End-Prozessors
hiplexAFSWUHostFEPPortnumber	read-write	Anzahl der für das System benutzten Ports

Datenträgertabelle

Objektname	Zugriff	Erläuterung
hiplexAFSWUVolumeTabNum	read-only	Anzahl der Datenträger
Tabelle:		
hiplexAFSWUVolumeName	read-only	Name des Datenträgers
hiplexAFSWUVolumeType Name	read-only	Name des Datenträger-Typs
hiplexAFSWUVolumeType	read-only	Datenträger-Typ: – shared-pubset – pubset – private-disk – by-user – undefined
hiplexAFSWUVolumeImportProc	read-only	Name der Prozedur zum Importieren des Datenträgers
hiplexAFSWUVolumeExportProc	read-only	Name der Prozedur zum Exportieren des Datenträgers

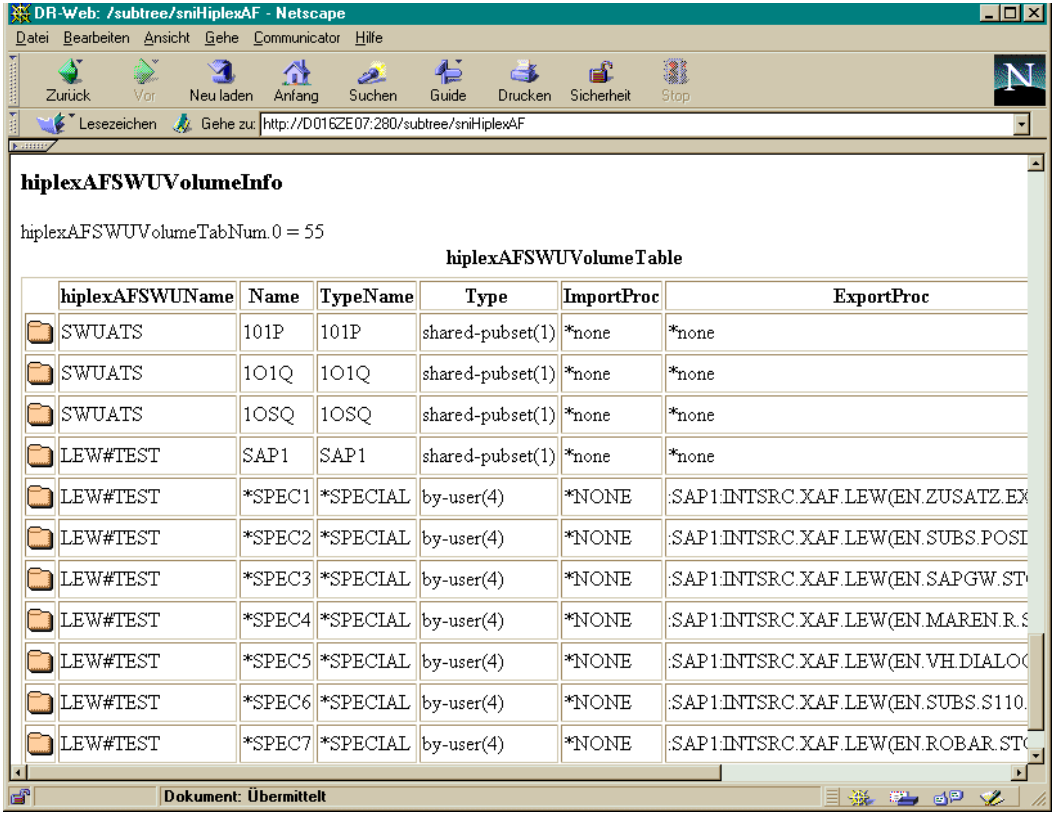


Bild 23: HIPLEX-AF: Anzeige der Datenträgertabelle

Tabelle der Anwendungen

Objektname	Zugriff	Erläuterung
hiplexAFSWUApplicationTabNum	read-only	Anzahl der Anwendungen
Tabelle:		
hiplexAFSWUApplicationMonJVName	read-only	Name der Jobvariablen für die Überwachung der Anwendung
hiplexAFSWUApplicationType	read-only	Typ der Anwendung: – job – utm – bcam – by-user – undefined
hiplexAFSWUApplicationStartProc	read-only	Prozedur zum Starten der Anwendung
hiplexAFSWUApplicationStopProc	read-only	Prozedur zum Beenden der Anwendung

Tabelle der Trap-Filter

Objektname	Zugriff	Erläuterung
hiplexAFTrapFilterHost1Name	read-only	BCAM-Name des Systems, auf dem der HIPLEX-AF-Subagent läuft
hiplexAFTrapFilterHost2Name	read-only	BCAM-Name eines überwachten Systems im HIPLEX-AF-Cluster
hiplexAFTrapSendInd	read-write	Sendebestätigung: – yes: Ereignisse auf dem überwachten System werden durch einen Trap gemeldet. – no : Ereignisse auf dem überwachten System werden nicht durch Traps gemeldet. – undefined

Traps

Objektname	Trap-Nr.	Erläuterung
hiplexAFStart	301	HIPLEX-AF-Hauptprozedur wurde gestartet.
hiplexAFSWUStart	302	Die Prozedur für die Umschalteinheit wurde gestartet.
hiplexAFStop	303	Das Beenden von HIPLEX-AF wurde eingeleitet.
hiplexAFCrash	304	Das System hat sich abnormal beendet.
hiplexAFSWUAppStop	305	Die Anwendungen einer Umschalteinheit werden gestoppt.
hiplexAFSWUAppStart	306	Die Anwendungen einer Umschalteinheit werden gestartet.
hiplexAFSWUStop	307	Die Umschalteinheit-Prozedur wurde gestoppt.

6.4 SNMP-Management für Host Resources

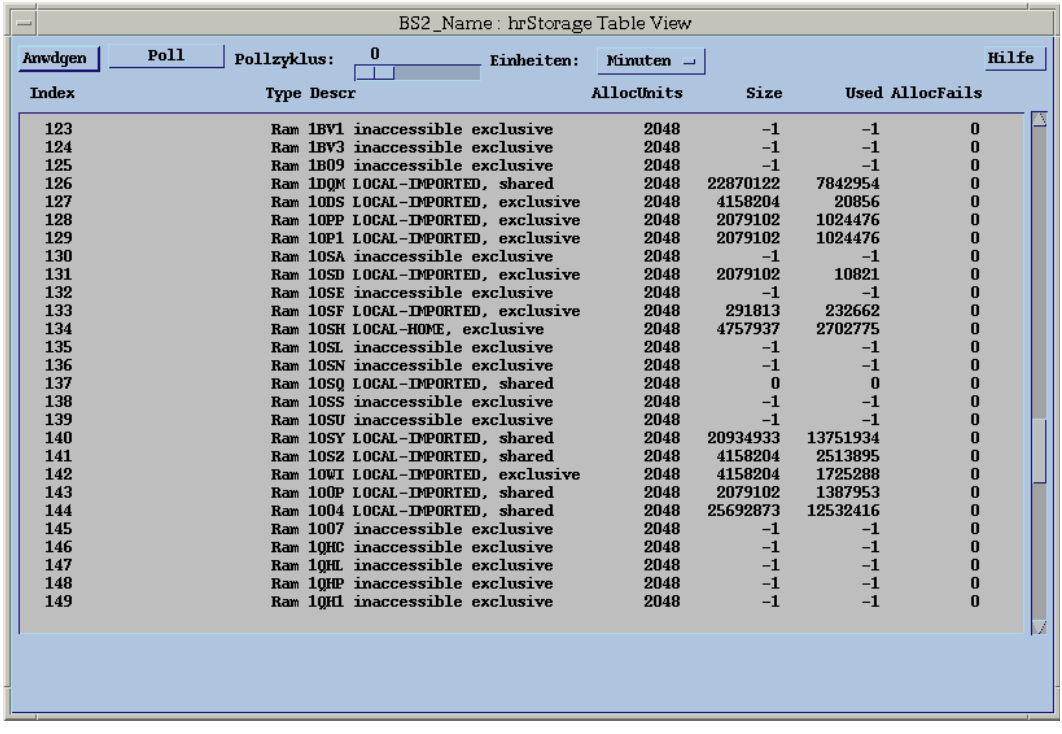
Der Subagent Host Resources liefert Informationen über das System, über Geräte und Datei-Systeme sowie über die installierte Software entsprechend dem Standard RFC 1514.

Host Resources System-Gruppe

Objektname	Zugriff	Erläuterung
hrSystemUptime	read-only	Zeitspanne seit der letzten Initialisierung dieses Hosts.
hrSystemDate	read-write	Lokales Datum und Uhrzeit des Hosts.
hrSystemInitialLoadDevice	read-write	Anzeige = -1
hrSystemInitialLoad Parameters	read-write	Anzeige = '-'
hrSystemNumUsers	read-only	Anzahl der Anwender-Tasks, für die dieser Host-Status-Informationen speichert. Eine Sitzung ist eine Gruppe von Prozessen, für die eine einzige Anwenderidentifikationsüberprüfung erforderlich ist; gegebenenfalls mit einer gemeinsamen Jobsteuerung.
hrSystemProcesses	read-only	Anzahl der Task-Kontexte, die derzeit in diesem System geladen sind oder ausgeführt werden.
hrSystemMaxProcesses	read-only	Maximale Anzahl Prozess-Kontexte, die von diesem System unterstützt werden können. Wenn kein Höchstwert festgelegt ist, muss dieser Wert Null sein. In Systemen mit einem festgelegten Höchstwert sind mit diesem Objekt Fehler diagnostizierbar, die beim Erreichen des Höchstwertes auftreten. In BS2000/OSD derzeit 4096.

Host Resources Storage-Gruppe

Objektname	Zugriff	Erläuterung
hrMemorySize	read-only	Größe des physikalischen Hauptspeichers im Host.
hrStorageIndex	read-only	Ein eindeutiger Wert für jeden logischen Speicherbereich im Host. INTEGER (1..2147483647)
hrStorageType	read-only	Die Art des Speichers, der durch diesen Eintrag dargestellt wird.
hrStorageDescr	read-only	Eine Beschreibung von Art und Ausprägung des Speichers in diesem Eintrag.
hrStorageAllocationUnits	read-only	Die Größe der von diesem Pool zugeordneten Datenobjekte in Byte. Wenn dieser Eintrag z.B. Sektoren, Blöcke, Puffer oder Pakete überwacht, ist diese Zahl gewöhnlich größer als Eins. Ansonsten ist diese Zahl üblicherweise Eins. Für Pubsets beträgt der Wert 2048.
hrStorageSize	read-write	Die Größe des dargestellten Speichers in Einheiten von *hrStorageAllocationUnits*. INTEGER (0..2147483647)
hrStorageUsed	read-only	Belegter Speicherbereich in Einheiten von *hrStorageAllocationUnits*. INTEGER (0..2147483647)
hrStorageAllocationFailures	read-only	Anzeige = ’0’

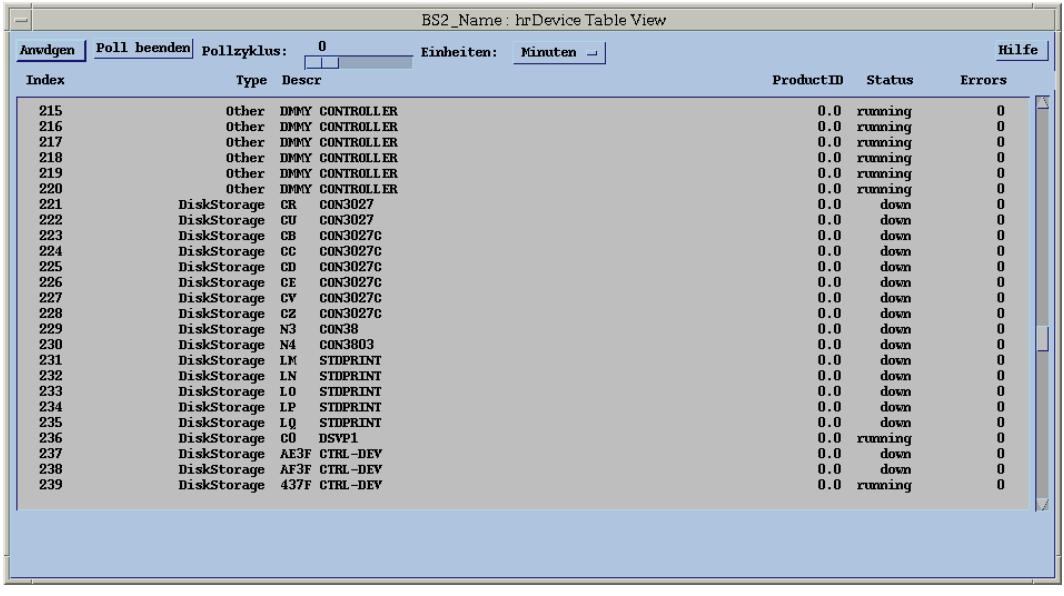


Index	Type Descr	AllocUnits	Size	Used	AllocFails
123	Ram 1BV1 inaccessible exclusive	2048	-1	-1	0
124	Ram 1BV3 inaccessible exclusive	2048	-1	-1	0
125	Ram 1B09 inaccessible exclusive	2048	-1	-1	0
126	Ram 1DQM LOCAL-IMPORTED, shared	2048	22870122	7842954	0
127	Ram 1ODS LOCAL-IMPORTED, exclusive	2048	4158204	20856	0
128	Ram 1OPP LOCAL-IMPORTED, exclusive	2048	2079102	1024476	0
129	Ram 1OP1 LOCAL-IMPORTED, exclusive	2048	2079102	1024476	0
130	Ram 1OSA inaccessible exclusive	2048	-1	-1	0
131	Ram 1OSD LOCAL-IMPORTED, exclusive	2048	2079102	10821	0
132	Ram 1OSE inaccessible exclusive	2048	-1	-1	0
133	Ram 1OSF LOCAL-IMPORTED, exclusive	2048	291813	232662	0
134	Ram 1OSH LOCAL-HOME, exclusive	2048	4757937	2702775	0
135	Ram 1OSL inaccessible exclusive	2048	-1	-1	0
136	Ram 1OSN inaccessible exclusive	2048	-1	-1	0
137	Ram 1OSQ LOCAL-IMPORTED, shared	2048	0	0	0
138	Ram 1OSS inaccessible exclusive	2048	-1	-1	0
139	Ram 1OSU inaccessible exclusive	2048	-1	-1	0
140	Ram 1OSY LOCAL-IMPORTED, shared	2048	20934933	13751934	0
141	Ram 1OSZ LOCAL-IMPORTED, shared	2048	4158204	2513895	0
142	Ram 1OWI LOCAL-IMPORTED, exclusive	2048	4158204	1725288	0
143	Ram 1OOP LOCAL-IMPORTED, shared	2048	2079102	1387953	0
144	Ram 1OO4 LOCAL-IMPORTED, shared	2048	25692873	12532416	0
145	Ram 1OO7 inaccessible exclusive	2048	-1	-1	0
146	Ram 1QHC inaccessible exclusive	2048	-1	-1	0
147	Ram 1QHL inaccessible exclusive	2048	-1	-1	0
148	Ram 1QHP inaccessible exclusive	2048	-1	-1	0
149	Ram 1QH1 inaccessible exclusive	2048	-1	-1	0

Bild 24: Host Resources-Subagent: Host Resources Storage-Gruppe

Host Resources Device-Gruppe

Objektname	Zugriff	Erläuterung
hrDeviceIndex	read-only	Ein eindeutiger Wert für jedes Gerät innerhalb des Host. Der Wert der einzelnen Geräte muss mindestens von einer Reinitialisierung des Agenten zur nächsten Reinitialisierung konstant bleiben. INTEGER (1..2147483647)
hrDeviceType	read-only	Angabe des Gerätetyps. Ist dieser Wert *hrDeviceProcessor* { *hrDeviceTypes 3* }, dann gibt es einen Eintrag in *hrProcessorTable*, der zu diesem Gerät gehört.
hrDeviceDescr	read-only	Eine Textbeschreibung dieses Gerätes.
hrDeviceID	read-only	Produkt-ID für dieses Gerät.
hrDeviceStatus	read-only	Der aktuelle Betriebsstatus des Gerätes, das in dieser Zeile der Tabelle beschrieben wird. Der Wert unknown (1) gibt an, dass der aktuelle Status des Gerätes nicht bekannt ist. running (2) gibt an, dass das Gerät aktiv ist (attached) und keine ungewöhnlichen Fehlerbedingungen bekannt sind. Der Status warning (3) (detached-pending) Der Status down (5) (detached) wird nur verwendet, wenn der Agent informiert wurde, dass das Gerät überhaupt nicht zur Verfügung steht.
hrDeviceErrors	read-only	Anzahl der Fehler an diesem Gerät. Derzeit immer 0.
hrProcessorFrwID	read-only	Die Produkt-ID der Firmware, die dem Prozessor zugeordnet ist.
hrProcessorLoad	read-only	Anzeige = ’0’



Index	Type	Descr	ProductID	Status	Errors
215	Other	DMMY CONTROLLER	0.0	running	0
216	Other	DMMY CONTROLLER	0.0	running	0
217	Other	DMMY CONTROLLER	0.0	running	0
218	Other	DMMY CONTROLLER	0.0	running	0
219	Other	DMMY CONTROLLER	0.0	running	0
220	Other	DMMY CONTROLLER	0.0	running	0
221	DiskStorage	CR CON3027	0.0	down	0
222	DiskStorage	CU CON3027	0.0	down	0
223	DiskStorage	CB CON3027C	0.0	down	0
224	DiskStorage	CC CON3027C	0.0	down	0
225	DiskStorage	CD CON3027C	0.0	down	0
226	DiskStorage	CE CON3027C	0.0	down	0
227	DiskStorage	CV CON3027C	0.0	down	0
228	DiskStorage	CZ CON3027C	0.0	down	0
229	DiskStorage	N3 CON38	0.0	down	0
230	DiskStorage	N4 CON3803	0.0	down	0
231	DiskStorage	LM STDPRINT	0.0	down	0
232	DiskStorage	LN STDPRINT	0.0	down	0
233	DiskStorage	LO STDPRINT	0.0	down	0
234	DiskStorage	LP STDPRINT	0.0	down	0
235	DiskStorage	LQ STDPRINT	0.0	down	0
236	DiskStorage	C0 DSVP1	0.0	running	0
237	DiskStorage	AE3F CTRL-DEV	0.0	down	0
238	DiskStorage	AF3F CTRL-DEV	0.0	down	0
239	DiskStorage	437F CTRL-DEV	0.0	running	0

Bild 25: Host Resources-Subagent: Host Resources Device-Gruppe

Host Resources Partition-Tabelle

Objektname	Zugriff	Erläuterung
hrPartitionIndex	read-only	Ein eindeutiger Wert für jede Partition auf dieser Speichereinheit für langfristige Speicherung. Der Wert für jede Speichereinheit für langfristige Speicherung muss mindestens von einer Reinitialisierung des Agenten bis zur nächsten Reinitialisierung konstant bleiben. INTEGER (1..2147483647)
hrPartitionLabel	read-only	Eine Textbeschreibung dieser Partition.
hrPartitionID	read-only	Ein Deskriptor, mit dem diese Partition gegenüber dem Betriebssystem eindeutig dargestellt wird. In einigen Systemen kann dies durch Binärdarstellung geschehen.
hrPartitionSize	read-only	Die Größe dieser Partition.
hrPartitionFSIndex	read-only	Der Index des Dateisystems in dieser Partition. Wenn kein Dateisystem in dieser Partition vorhanden ist, muss dieser Wert Null sein. Mehrere Partitionen können auf ein gemeinsames Dateisystem zeigen. Dies bedeutet, das Dateisystem ist auf diesen Partitionen resident. Mehrere Dateisysteme können nicht auf einer Partition resident sein. INTEGER (0..2147483647)

File System-Tabelle

Objektname	Zugriff	Erläuterung
hrFSIndex	read-only	Ein eindeutiger Wert für jedes lokale Dateisystem auf diesem Host. Die Werte für die einzelnen Dateisysteme müssen mindestens von einer Reinitialisierung des Agenten zur nächsten Reinitialisierung konstant bleiben. INTEGER (1..2147483647)
hrFSMountPoint	read-only	Der Pfadname für den Root dieses Dateisystems.
hrFSRemoteMountPoint	read-only	Beschreibung für den Namen und/oder die Adresse des Servers, von dem dieses Dateisystem eingehängt wurde. Dazu können auch Parameter wie Mount-Punkt des fernen Dateisystems gehören. Wenn dies kein fernes Dateisystem ist, ist dieses Objekt leer.
hrFSType	read-only	Der Wert dieses Objekts gibt den Typ dieses Dateisystems an.
hrFSAccess	read-only	Meldung, wie dieses Dateisystem vom Betriebssystem logisch konfiguriert wurde: lesbar und beschreibbar oder nur lesbar. Dies ist keine Maßnahme der lokalen Zugriffssteuerung, es betrifft das Dateisystem als Ganzes. readWrite (1), readOnly (2)
hrFSBootable	read-only	Flag bezüglich der Bootfähigkeit dieses Dateisystems.
hrFSStorageIndex	read-only	Der Index des *hrStorageEntry*, der Informationen zu diesem Dateisystem darstellt. Wenn solche Informationen nicht zur Verfügung stehen, muss dieser Wert Null sein. Mit dem entsprechenden Speichereintrag ist die prozentuale Auslastung dieses Dateisystems feststellbar, und Fehler auf Grund von Platzmangel sind diagnostizierbar. INTEGER (0..2147483647)

Objektname	Zugriff	Erläuterung
hrFSLastFullBackupDate	read-write	Datum, an dem dieses vollständige Dateisystem zuletzt auf eine andere Speichereinheit gesichert wurde. Mit dieser Information lässt sich sicherstellen, dass regelmäßig Sicherungen durchgeführt werden. Wenn diese Information nicht bekannt ist, muss diese Variable einen Wert haben, der dem 1. Januar entspricht, mit der Jahresangabe 0000, 00:00:00.0, codiert als (hex) '00 00 01 01 00 00 00 00'.
hrFSLastPartialBackupDate	read-write	Datum, an dem dieses Dateisystem zuletzt teilweise auf eine andere Speichereinheit gesichert wurde. Mit dieser Information lässt sich sicherstellen, dass regelmäßig Sicherungen durchgeführt werden. Wenn diese Information nicht bekannt ist, muss diese Variable einen Wert haben, der dem 1. Januar entspricht, mit der Jahresangabe 0000, 00:00:00.0, codiert als (hex) '00 00 01 01 00 00 00 00'.

Host Resources Installed Software-Tabelle

Objektname	Zugriff	Erläuterung
hrSWInstalledLastChange	read-only	Der Wert von sysUpTime zu dem Zeitpunkt, als zuletzt ein Eintrag in hrSWInstalledTable hinzugefügt, umbenannt oder gelöscht wurde. Da diese Tabelle wahrscheinlich zahlreiche Einträge enthält, kann eine Management-Station beim Polling dieses Objekts bestimmen, wann erneutes Laden der Tabelle nützlich ist. Wert ist immer die sysUpTime zum Zeitpunkt der Initialisierung des HR-Agenten.
hrSWInstalledLastUpdateTime	read-only	Der Wert von sysUpTime zu dem Zeitpunkt, als hrSWInstalledTable zuletzt vollständig aktualisiert wurde. Beim Implementieren dieser Daten ist Caching üblich. Beim Abrufen dieses Objekts bedeutet dies für die Management-Station, dass die Daten in dieser Tabelle höchstens so alt sind wie die angegebene Zeit. Wert ist immer die sysUpTime zum Zeitpunkt der Initialisierung des HR-Agenten.
Tabelle:		
hrSWInstalledIndex	read-only	Ein eindeutiger Wert für jedes Softwareprogramm auf dem Host. Dieser Wert muss im Bereich von 1 bis zur Anzahl der auf dem Host installierten Softwareprogramme liegen. INTEGER (1..2147483647)
hrSWInstalledName	read-only	Eine Textbeschreibung dieses installierten Softwareprogramms einschließlich Hersteller, Überarbeitung, üblichem Namen und wahlweise Seriennummer.
hrSWInstalledID	read-only	Produkt-ID dieses installierten Softwareprogramms.
hrSWInstalledType	read-only	Der Typ dieses Softwareprogramms unknown (1), operatingSystem (2), deviceDriver (3), application (4)
hrSWInstalledDate	read-only	Letztes Änderungsdatum dieser Anwendung (entspricht Anzeige in einer Verzeichnisliste). Enthält immer den Wert für unknown: ’00 00 01 01 00 00 00 00’, dies steht für 1. Januar, Jahr: 0000, Time: 00:00:00.0

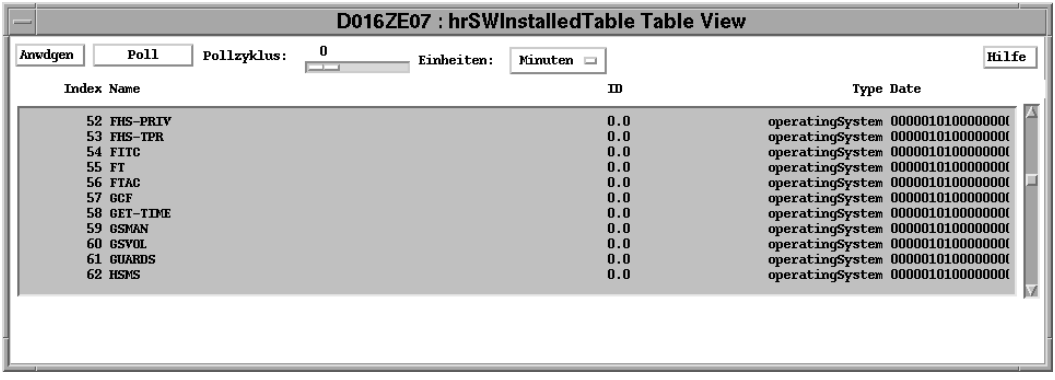


Bild 26: Host Resources-Subagent: Host Resources Installed Software-Tabelle

6.5 SNMP-Management für HSMS

Der HSMS-Subagent ermöglicht das Lesen und Ändern von globalen HSMS-Daten. Darüber hinaus liefert er detaillierte Informationen über HSMS-Aufträge und deren Zustände. Den Umfang der Anzeige können Sie durch die Auswahlkriterien "Zustand" und "Herkunftsort" einschränken. Der HSMS-Subagent sendet selbst keine Traps.

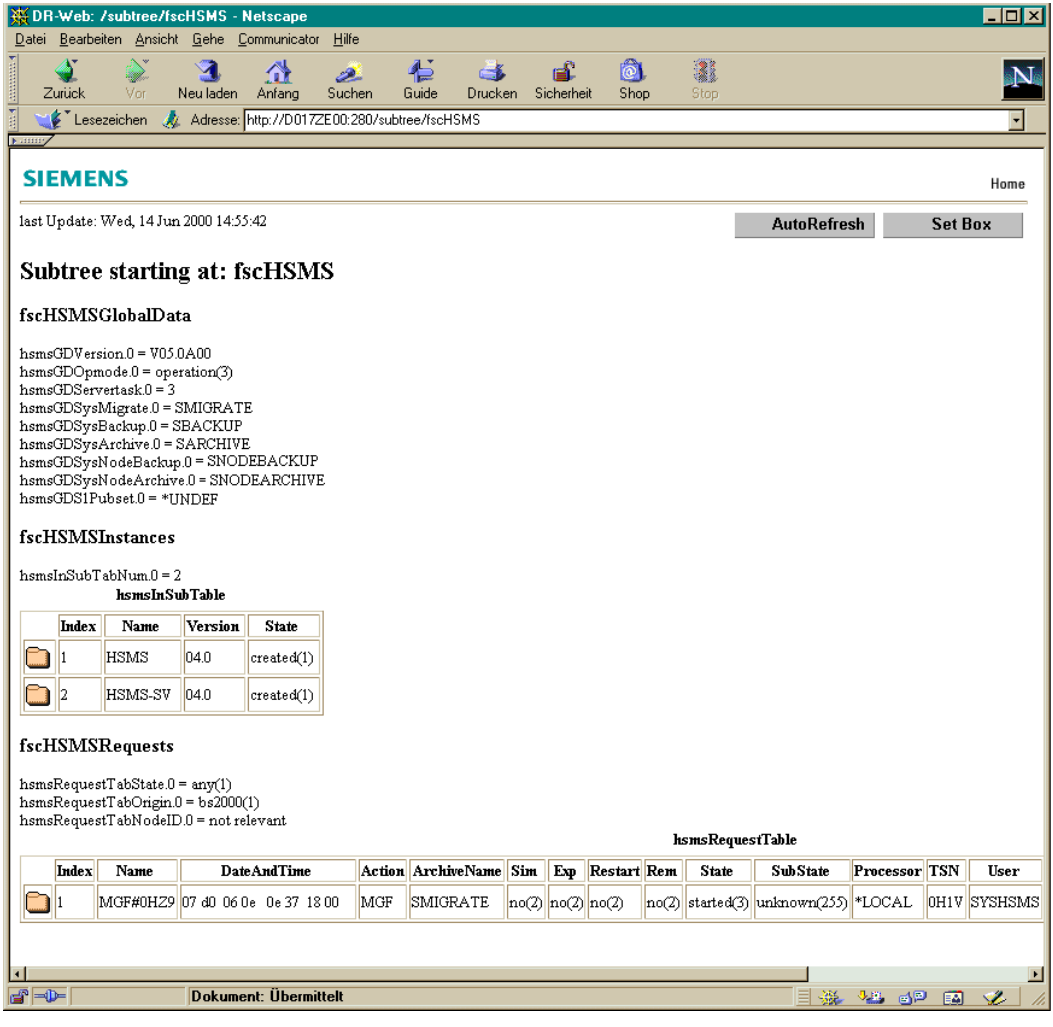


Bild 27: HSMS-Übersicht

Globale Daten

Objektname	Zugriff	Erläuterung
hsmsGDVersion	read-only	Version des Subagenten
hsmsGDOpmode	read-write	Betriebsweise von HSMS
hsmsGDServertask	read-write	Anzahl der laufenden Server-Tasks
hsmsGDSysMigrate	read-only	Name des HSMS-Standard-Archivs für Verdrängung
hsmsGDSysBackup	read-only	Name des HSMS-Standard-Archivs für Datensicherung
hsmsGDSysArchive	read-only	Name des HSMS-Standard-Archivs für Langzeitarchivierung
hsmsGDSysNodeBackup	read-only	Name des HSMS-Standard-Archivs für die Sicherung von Knoten
hsmsGDSysNodeArchive	read-only	Name des HSMS-Standard-Archivs für die Archivierung von Knoten
hsmsGDS1Pubset	read-only	Kennung des Pubsets, das als Standard-S1-Pubset genutzt wird

Instanzen

Für die beiden Subsysteme HSMS und HSMS-SV werden fogende Werte geliefert:

Objektname	Zugriff	Erläuterung
hsmsInSubIndex	read-only	Index
hsmsInSubName	read-only	Name
hsmsInSubVersion	read-only	Version
hsmsInSubState	read-only	Status

HSMS-Aufträge

In einer Tabelle werden alle HSMS-Aufträge angezeigt, die vom betreffenden BS2000/OSD-Rechner bearbeitet werden. Der HSMS-Subagent ermittelt diese Information durch Auswerten einer OPS-Variablen.

Pro Auftrag werden folgende Informationen geliefert:

Objektname	Zugriff	Erläuterung
hsmsRequestIndex	read-only	Index
hsmsRequestName	read-only	Name des Auftrags
hsmsRequestDateAndTime	read-only	Datum und Uhrzeit der Erstellung des Auftrags
hsmsRequestAction	read-only	Aktionsanweisung*
hsmsRequestArchiveName	read-only	Archivname*
hsmsRequestSim	read-only	Auftrag simuliert (yes/no)
hsmsRequestExp	read-only	Expressauftrag (yes/no)
hsmsRequestRestart	read-only	Auftrag nach Wiederanlauf (yes/no)
hsmsRequestRem	read-only	Remote Auftrag (Master-Bearbeitung für Shared-Pubset)
hsmsRequestState	read-only	Status
hsmsRequestSubstate	read-only	Substatus
hsmsRequestProcessor	read-only	BCAM-Name des Rechners, der den Auftrag bearbeitet (*LOCAL, wenn lokal).
hsmsRequestTSN	read-only	TSN der ausführenden Servertask

*) erst ab HSMS V4.0

Darüber hinaus gibt es rechner-abhängig noch folgende Informationen

Nur für BS2000/OSD:

hsmsRequestUser	read-only	Benutzerkennung, unter der der Auftrag erstellt wurde

Nur für Workstations

hsmsRequestUserNo	read-only	UNIX-Benutzernummer
hsmsRequestNodeId	read-only	Kennung des Knotens
hsmsRequestIPAddr	read-only	IP-Adresse des Knotens
hsmsRequestIPPort	read-only	IP-Port-Nummer des Knotens
hsmsRequestBspId	read-only	Auftragskennzeichen am Client

Damit der Subagent die Aufträge auch nach deren Beendigung anzeigen kann, dürfen die Aufträge nicht per Kommando gelöscht werden. Aufträge mit dem Status *COMPLETED* werden jedoch zu Beginn jeder HSMS-Session automatisch durch die implizite Recovery gelöscht.

Die Anzahl der angezeigten Aufträge kann eingeschränkt werden, abhängig vom

– Bearbeitungsstand der Aufträge,
– Rechner, von dem der Auftrag stammt.

Objektname	**Zugriff**	**Erläuterung**
hsmsRequestTabState	read-write	Einschränken der angezeigten HSMS-Aufträge, abhängig vom Bearbeitungsstand der einzelnen Aufträge. Folgende Auswahlkriterien stehen zur Verfügung: – ANY – COMPLETED – ACCEPTED – STARTED – INTERRUPTED
hsmsRequestTabOrigin	read-write	Einschränkung der angezeigten HSMS-Aufträge, abhängig vom Rechner, von dem der Auftrag stammt. Der Rechner kann durch folgende Angaben spezifiziert werden: – *BS2000 (zentraler BS2000/OSD-Host) – *NODE-CL (ein Client, auf dem HSMS-CL aktiv ist)
hsmsRequestTabNodeID	read-write	Name des Client. Das Setzen dieses Objekts wird abgewiesen, wenn *hsmsRequestTabOrigin* den Wert *BS2000 hat.

6.6 SNMP-Management für OMNIS

Der Subagent für OMNIS ermöglicht die Administration von OMNIS über SNMP. Mit dem OMNIS-Subagenten lassen sich Datenstationen, Partner und Anwendungen überwachen. Außerdem können OMNIS-Kommandos abgesetzt werden. Beim Eintreffen von kritischen Ereignissen versendet der OMNIS-Subagent Traps.

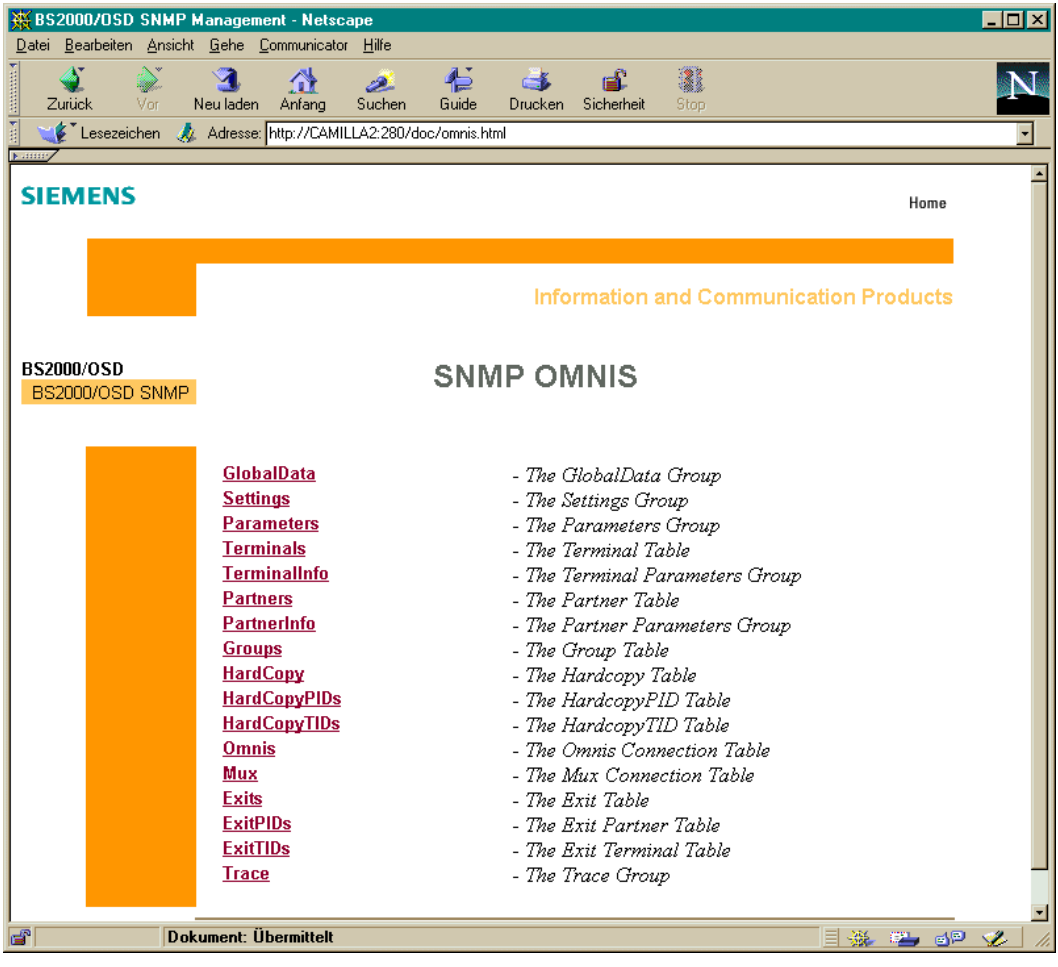


Bild 28: OMNIS-Übersicht

Globale OMNIS-Informationen

Objektname	**Zugriff**	**Erläuterung**
omnisGlobalDataSubagent Version	read-only	Version des OMNIS-Subagenten
omnisGlobalDataTabNum	read-only	Gesamtanzahl aller OMNIS
omnisGlobalDataActID	read-write	Index des aktuell eingestellten OMNIS. Alle weiteren Daten beziehen sich auf dieses OMNIS. Das Setzen dieser ID führt im Folgenden zur Anzeige des OMNIS mit der angegebenen ID.
omnisGlobalDataActName	read-write	Name des aktuell eingestellten OMNIS. Alle weiteren Daten beziehen sich auf dieses OMNIS. Das Setzen dieses Namens führt im Folgenden zur Anzeige des OMNIS mit dem angegebenen Namen.
Tabelle der konfigurierten OMNIS:		
omnisGlobalDataOmnID	read-only	OMNIS-Index
omnisGlobalDataVersion	read-only	OMNIS-Version
omnisGlobalDataOmnName	read-only	OMNIS-Name
omnisGlobalDataState	read-write	OMNIS-Status Verbindung zu OMNIS wird aufgebaut / abgebaut. open (1), close (2)

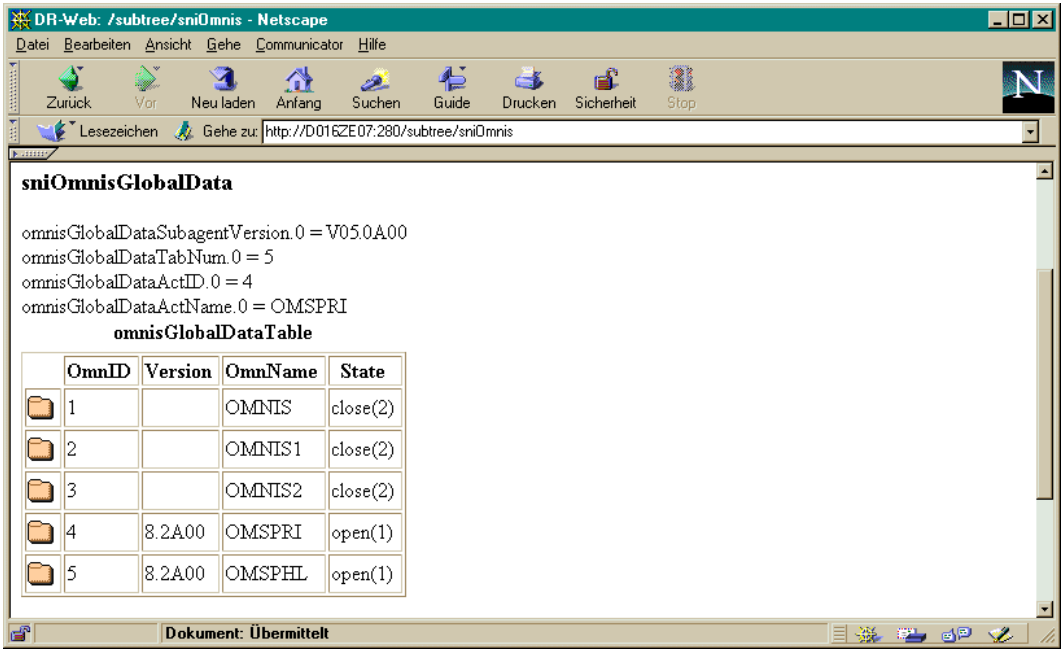


Bild 29: OMNIS-Subagent: Anzeige der globalen OMNIS-Informationen

OMNIS-Settings

Objektname	Zugriff	Erläuterung
omnisSettingsAppName	read-only	NEA-Name der OMNIS-Anwendung
omnisSettingsAppNameISO	read-only	ISO-Name der OMNIS-Anwendung
omnisSettingsNumPartners	read-only	Momentane Anzahl Partner
omnisSettingsNumTerminals	read-only	Momentane Anzahl Terminals
omnisSettingsDSTMax	read-write	Maximale Anzahl DSTs
omnisSettingsPTNMax	read-write	Maximale Anzahl Partner
omnisSettingsPACMax	read-write	Maximale Anzahl Partner für eine DST
omnisSettingsState	read-only	Verbindung zum Subagenten aufgebaut open (1), close (2), end (3), unknown (99)
omnisSettingsAPASS	read-write	Administratorkennwort
omnisSettingsHOLD	read-write	Verbindung aufrechterhalten yes (1), no (2), std (3), auto (4), unknown (99)
omnisSettingsHcyForm	read-write	Formular des Druckers
omnisSettingsHCopy	read-write	Route der Druckerausgabe
omnisSettingsLogging	read-write	Protokollieren in Logging-Datei yes (1), no (2), unknown (99)
omnisSettingsChangeLogging	read-write	Umschalten der Logging-Datei change (1), unknown (99)
omnisSettingsACK	read-write	Bildschirmüberlaufsteuerung yes (1), no (2), std (3), unknown (99)
omnisSettingsMTAB	read-write	Meldungstabelle
omnisSettingsEXIT	read-write	Adresscode von EXIT

Objektname	Zugriff	Erläuterung
omnisSettingsOpncon	read-write	Verbindungsberechtigung std (1), free (2), dcl (3), unknown (99)
omnisSettingsBreakKey	read-write	K-Taste zum Hervorrufen einer Unterbrechung in einem $DIALOG-Partner: k1 (1) ... k14 (14), no (98), unknown (99)
omnisSettingsCallKey	read-write	K-Taste für Anrufe k1 (1) ... k14 (14), no (98), unknown (99)
omnisSettingsCallInf	read-write	Anruf-Statusinformation mitteilen yes (1), no (2), std (3), unknown (99)
omnisSettingsPac	read-write	Adresscode des Partners line (1), prefix (2), no (3), std (4), unknown (99)
omnisSettingsInputLog	read-write	Protokoll für die Terminaleingabe rec (1), send (2), both (3), std (4), unknown (99)
omnisSettingsOutputLog	read-write	Protokoll für die Terminalausgabe rec (1), send (2), both (3), std (4), unknown (99)
omnisSettingsLine25	read-write	Die 25. Anzeigezeile verwenden yes (1), no (2), std (3), unknown (99)

Objektname	Zugriff	Erläuterung
omnisSettingsDisMod	read-write	Anzeigemodus system (1), omnis (2), mixed (3), unknown (99)
omnisSettingsKPAC	read-write	K-Taste zum Umschalten in Kommandomodus / zum Wechseln des Partners k1 (1) ... k14 (14), no (98), unknown (99)
omnisSettingsExitPri	read-write	Definiert die Priorität der Kommandos SET, PARAM und OPTION bezüglich des Operanden EXIT. set-opt (1), opt-set (2), std (3), unknown (99)
omnisSettingsReply	read-write	Antworten zur UCON-Anwendung restricted (1), all (2), unknown (99)
omnisSettingsExitAuth	read-write	Berechtigung für Kommando EXIT all (1), adm (2), unknown (99)
omnisSettingsLoggPri	read-write	Definiert die Priorität der Kommandos SET, PARAM und OPTION bezüglich des Operanden LOGGING. set-opt (1), opt-set (2), unknown (99)
omnisSettingsAudit	read-write	OMNIS-Audit on (1), off (2), unknown (99)
omnisSettingsMDefAuth	read-write	Berechtigung für Kommando MDEF all (1), adm (2), unknown (99)

Objektname	Zugriff	Erläuterung
omnisSettingsHoldPri	read-write	Definiert die Priorität der Kommandos SET und OPTION bezüglich des Operanden HOLD=AUTO. set-opt (1), opt-set (2), unknown (99)
omnisSettingsInsave	read-write	Gesicherte K-Taste k1 (1) ... k14 (14), f1 (21) ... f24 (44), no (97), std (98), unknown (99)
omnisSettingsOpnStart	read-write	Start-Sequenz erlaubt yes (1), no (2), unknown (99)
omnisSettingsExclPartner	read-write	Steuerung des Nachrichtenflusses an die Partner yes (1), no (2), std (3), unknown (99)
omnisSettingsSave	read-write	Sicherung nach Verbindungsabbau pkey (1), screen (2), all (3), no (4), std (5), unknown (99)
omnisSettingsMessageALL	read-write	Keine Anzeige. Das Setzen dieses Objekts sendet die spezifizierte Nachricht an alle OMNIS-Anwender.
omnisSettingsMessageADM	read-write	Keine Anzeige. Das Setzen dieses Objekts sendet die spezifizierte Nachricht an den OMNIS-Administrator.

OMNIS-Parameter

Objektname	Zugriff	Erläuterung
omnisParametersAppName	read-only	Name der OMNIS-Anwendung
omnisParametersAppName ISO	read-only	ISO-Name der OMNIS-Anwendung
omnisParametersPrefix	read-only	Präfix der Standby-Anwendung
omnisParametersProName	read-only	Prozessorname
omnisParametersVirtPro Name	read-only	Virtueller Prozessorname
omnisParametersLoggingFile	read-only	Name der Logging-Datei
omnisParametersStartupFile	read-only	Name der Startdatei
omnisParametersConfigFile	read-only	Name der Konfigurationsdatei
omnisParametersConfUpdate	write-only	Durch das Setzen dieses Objektes erfolgt das Neu-einlesen der OMNIS-Konfigurationsdatei (keine Anzeige). start (1)
omnisParametersModulFile	read-only	Name der Moduldatei
omnisParametersBulletinFile	read-only	Name der Bulletindatei
omnisParametersTextFile	read-only	Name der Textdatei
omnisParametersPagePool	read-only	Name der PagePool-Datei
omnisParametersIOArea Length	read-only	Länge des E/A-Bereichs
omnisParametersTWork Length	read-only	Länge des Terminal-Arbeitsbereichs
omnisParametersPWork Length	read-only	Länge des Partner-Arbeitsbereichs
omnisParametersTextKey Length	read-only	Länge des Textschlüssels
omnisParametersSecurity Level	read-only	Sicherheitsstufe high (1), medium (2), low (3), unknown (99)
omnisParametersDCAMInt Vers	read-only	Version des DCAM-Interface
omnisParametersVTSUBVers	read-only	Version des lokalen VTSU-B

Objektname	Zugriff	Erläuterung
omnisParametersVTSUCB Vers	read-only	Version des lokalen VTSUCB
omnisParametersCMD	read-write	BS2000-Kommando für OMNIS-Task
omnisParametersDump	read-write	Kommando /DUMP start (1), unknown (99)
omnisParametersDumpMsgNr	read-write	OMNIS-Meldungsnummer
omnisParametersDumpInsert	read-write	Kommando /DUMP
omnisParametersDumpInsertNr	read-write	Nummer des Insert

OMNIS Terminal-Tabelle

Objektname	Zugriff	Erklärung
omnisTerminalsStatus	read-write	Status Flag legt den Ausgabe-Umfang für die Terminal-Tabelle fest. all (1), active (2), -- Standardwert hold (3), inactive (4)
omnisTerminalsTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisTerminalsTable*
Terminal-Tabelle:		
omnisTerminalsTID	read-write	Terminal-ID
omnisTerminalsPtnName	read-only	Partnername
omnisTerminalsProName	read-only	Prozessorname
omnisTerminalsTyp	read-only	Terminal-Typ term (1), appl (2), skp (3), cons (4), unknown (99)
omnisTerminalsState	read-write	Terminal-Status / Wert *cancel* nur für *write* decl (1), opn (2), act (3), los (4), cls (5), hold (6), inact (7), cancel (8), unknown (99)
omnisTerminalsRoute	read-only	Route ind (1), dir (2), unknown (99)
omnisTerminalsKPAC	read-only	K-Taste zum Umschalten in Kommandomodus / zum Wechseln des Partners k1 (1) ... k14 (14), no (97), std (98), unknown (99)
omnisTerminalsUser	read-only	Anwender

Objektname	Zugriff	Erklärung
omnisTerminalsMessage	write-only	Meldung an eine TID

OMNIS Terminal-Info

Objektname	Zugriff	Erläuterung
omnisTerminalInfoTID	read-write	Terminal-ID
omnisTerminalInfoPtnName	read-only	Partnername
omnisTerminalInfoProName	read-only	Prozessorname
omnisTerminalInfoTyp	read-only	Terminal-Typ term (1), appl (2), skp (3), cons (4), unknown (99)
omnisTerminalInfoState	read-only	Terminal-Status decl (1), opn (2), act (3), los (4), cls (5), hold (6), inact (7), unknown (99)
omnisTerminalInfoRoute	read-only	Route ind (1), dir (2), unknown (99)
omnisTerminalInfoKPAC	read-only	K-Taste zum Umschalten in Kommandomodus / zum Wechseln des Partners k1 (1) ... k14 (14), no (97), std (98), unknown (99)
omnisTerminalInfoUser	read-only	Anwender

Objektname	Zugriff	Erläuterung
omnisTerminalInfoPAC	read-only	Art der Bildschirmausgabe für PAC no (1), line (2), prefix (3), std (4), unknown (99)
omnisTerminalInfoADM	read-only	Administration erlaubt no (1), yes (2), unknown (99)
omnisTerminalInfoOPass	read-only	Passwort für das Kommando OCCUPY no (1), yes (2), unknown (99)
omnisTerminalInfoMTAB	read-only	Report-Tabelle
omnisTerminalInfoExit	read-only	Adresscode von EXIT
omnisTerminalInfoHold	read-only	Verbindung aufrechterhalten yes (1), no (2), std (3), auto (4), unknown (99)
omnisTerminalInfoChange	read-only	CHANGELOG erlaubt yes (1), no (2), unknown (99)
omnisTerminalInfoHcopy	read-only	Hardcopy-Drucker
omnisTerminalInfoAck	read-only	Bestätigung erforderlich yes (1), no (2), std (3), unknown (99)
omnisTerminalInfoListening	read-only	Weiteres „mithörendes“ Terminal

Objektname	Zugriff	Erläuterung
omnisTerminalInfoColour	read-only	Anzeigefarbe blue (1), cyan (2), green (3), yellow (4), magenta (5), red (6), white (7), unknown (99)
omnisTerminalInfoLogging	read-only	Protokollieren in Logging-Datei yes (1), no (2), std (3), unknown (99)
omnisTerminalInfoBerID	read-only	Passwort/Erlaubnis in SKP generiert yes (1), no (2), unknown (99)
omnisTerminalInfoDeclared	read-only	Festgelegt yes (1), no (2), unknown (99)
omnisTerminalInfoBreakKey	read-only	K-Taste zum Hervorrufen einer Unterbrechung in einem $DIALOG-Partner: k1 (1) ... k14 (14), no (97), std (98), unknown (99)
omnisTerminalInfoCallKey	read-only	K-Taste für Anrufe k1 (1) ... k14 (14), no (97), std (98), unknown (99)
omnisTerminalInfoCallInf	read-only	Anruf-Statusinformation mitteilen yes (1), no (2), std (3), unknown (99)

Objektname	Zugriff	Erläuterung
omnisTerminalInfoDisMod	read-only	Anzeigemodus std (1), system (2), omnis (3), mixed (4), unknown (99)
omnisTerminalInfoConnect	read-only	Status der Verbindung logon (1), start (2), unknown (99)
omnisTerminalInfoOpncon	read-only	Verbindungsberechtigung std (1), free (2), dcl (3), unknown (99)
omnisTerminalInfoPacAnz	read-only	Anzahl aktiver Partner
omnisTerminalInfoInput Logging	read-only	Protokoll für die Terminaleingabe std (1), both (2), rec (3), send (4), unknown (99)
omnisTerminalInfoOutput Logging	read-only	Protokoll für die Terminalausgabe std (1), both (2), rec (3), send (4), unknown (99)
omnisTerminalInfoAutoLogoff	read-only	Automatisches Logoff std (1), yes (2), no (3), unknown (99)
omnisTerminalInfoLine25	read-only	Die 25. Anzeigezeile verwenden yes (1), no (2), std (3), unknown (99)

Objektname	Zugriff	Erläuterung
omnisTerminalExclPartner	read-only	Steuerung des Nachrichtenflusses an die Partner yes (1), no (2), std (3), unknown (99)
omnisTerminalInfoSave	read-only	Gesichert nach Verbindungsabbau std (1), screen (2), pkey (3), all (4), no (5), unknown (99)
omnisTerminalInfoReply	read-only	Route-Daten zur UCON-Anwendung restricted (1), all (2), std (3), unknown (99)
omnisTerminalInfoUserProt	read-only	Anwender-Protokoll no (1), omnis (2), vtsucb (3), unknown (99)
omnisTerminalInfoTestmode	read-only	Testmodus no (1), yes (2), unknown (99)
omnisTerminalInfoInsave	read-only	Gesicherte K-Taste k1 (1) ... k14 (14), f1 (21) ... f24 (44), no (97), std (98), unknown (99)
omnisTerminalInfoSNMP	read-only	SNMP-Überwachung no (1), yes (2), unknown (99)
omnisTerminalInfoTransProt	read-only	Transport-Protokoll
omnisTerminalInfoHcyForm	read-only	Formular des Druckers

OMNIS Partner-Tabelle

Objektname	Zugriff	Erklärung
omnisPartnerStatus	read-write	Status Flag legt den Ausgabeumfang für die Partner-Tabelle fest. all (1), active (2), -- Standardwert hold (3), inactive (4)
omnisPartnerTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisPartnerTable*
omnisPartnerSelectTID	read-write	Terminal-ID, für die die Partner-Tabelle angezeigt werden soll
OMNIS Partner-Tabelle:		
omnisPartnerPID	read-write	Partner-ID
omnisPartnerPAC	read-only	Partner-Adresscode
omnisPartnerPtnName	read-only	Partnername
omnisPartnerProName	read-only	Prozessorname
omnisPartnerTyp	read-only	Terminal-Typ tiam (1), dcam (2), ucon (3), utm (4), svp (5), skp (6), unknown (99)
omnisPartnerState	read-write	Partnerstatus opn (1), act (2), los (4), cls (5), hold (6), inact (7), cancel (8), unknown (99)
omnisPartnerRoute	read-only	Route ind (1), dir (2), mux (3), unknown (99)

Objektname	Zugriff	Erklärung
omnisPartnerKPAC	read-only	K-Taste zum Wechseln des Partners k1 (1) ... k14 (14), no (97), std (98), unknown (99)
omnisPartnerTid	read-only	Terminal-ID

OMNIS Partner-Info

Objektname	Zugriff	Erläuterung
omnisPartnerInfoPID	read-write	Partner-ID
omnisPartnerInfoPAC	read-only	Partner-Adresscode
omnisPartnerInfoPtnName	read-only	Partnername
omnisPartnerInfoProName	read-only	Prozessorname
omnisPartnerInfoTyp	read-only	Partner-Typ tiam (1), dcam (2), ucon (3), utm (4), svp (5), skp (6), unknown (99)
omnisPartnerInfoState	read-only	Partner-Status opn (1), act (2), los (3), cls (4), hold (5), inact (6), unknown (99)
omnisPartnerInfoRoute	read-only	Route ind (1), dir (2), mux (3), unknown (99)
omnisPartnerInfoKPAC	read-only	K-Taste zum Wechseln des Partners k1 (1) ... k14 (14), no (97), std (98), unknown (99)
omnisPartnerInfoRepApp Name	read-only	Name der Partner-Anwendung
omnisPartnerInfoOPass	read-only	Passwort für das Kommando OCCUPY no (1), yes (2), unknown (99)
omnisPartnerInfoMTAB	read-only	Report-Tabelle
omnisPartnerInfoExit	read-only	Adresscode von EXIT

Objektname	Zugriff	Erläuterung
omnisPartnerInfoHold	read-only	Verbindung aufrechterhalten yes (1), no (2), std (3), unknown (99)
omnisPartnerInfoChange	read-only	CHANGELOG erlaubt yes (1), no (2), unknown (99)
omnisPartnerInfoHcopy	read-only	Hardcopy-Drucker
omnisPartnerInfoClass	read-only	Nachrichtenklasse für den Partner sav (1), out (2), del (3), unknown (99)
omnisPartnerInfoColour	read-only	Anzeigefarbe blue (1), cyan (2), green (3), yellow (4), magenta (5), red (6), white (7), unknown (99)
omnisPartnerInfoProtocol	read-only	Protokolltyp für eine DCAM-Verbindung dssim (1), omnis (2), unknown (99)
omnisPartnerInfoLogging	read-only	Protokollieren in Logging-Datei yes (1), no (2), std (3), unknown (99)
omnisPartnerInfoLPass	read-only	Verbindungspasswort erforderlich yes (1), no (2), unknown (99)
omnisPartnerInfoDeclared	read-only	Festgelegt yes (1), no (2), unknown (99)

Objektname	Zugriff	Erläuterung
omnisPartnerInfoAutoLogoff	read-only	Automatisches Logoff std (1), yes (2), no (3), unknown (99)
omnisPartnerInfoLine25	read-only	Die 25. Anzeigezeile verwenden yes (1), no (2), std (3), unknown (99)
omnisPartnerStartSequ	read-only	Nummer der Start-Sequenz
omnisPartnerInfoCMsg	read-only	Verbindungsnachricht yes (1), no (2), unknown (99)
omnisPartnerInfoLCase	read-only	Kleinbuchstaben an Partner erlaubt yes (1), no (2), unknown (99)
omnisPartnerInfoSave	read-only	Gesichert nach Verbindungsabbau std (1), screen (2), pkey (3), all (4), no (5), unknown (99)
omnisPartnerInfoTid	read-only	Terminal-ID
omnisPartnerInfoSNMP	read-only	SNMP-Überwachung no (1), yes (2), unknown (99)
omnisPartnerInfoPACPrefix	read-only	Typ der Bildschirmausgabe für PAC no (1), std (2), line (3), prefix (4), unknown (99)
omnisPartnerInfoBerid	read-only	Passwort/Erlaubnis in SKP generiert no (1), yes (2), unknown (99)

Objektname	Zugriff	Erläuterung
omnisPartnerInfoConnect	read-only	Status der Verbindung opncon (1), logon (2), start (3), unknown (99)

OMNIS Group-Tabelle

Objektname	Zugriff	Erläuterung
omnisGroupsTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisGroupsTable*
omnisGroupsSelectTID	read-write	Terminal-ID, für die die Gruppen-Tabelle angezeigt werden soll
OMNIS Gruppen-Tabelle:		
omnisGroupsGAC	read-only	Adresscode der Gruppe
omnisGroupsPAC	read-only	Adresscode des Partners
omnisGroupsTid	read-only	Terminal-ID

OMNIS Hardcopy-Tabelle

Objektname	Zugriff	Erläuterung
omnisHardCopyStatus	read-write	Status Flag legt den Ausgabeumfang für die Hardcopy-Tabelle fest. all (1), active (2), -- Standardwert inactive (4)
omnisHardCopyTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisHardCopyTable*
Hardcopy-Tabelle:		
omnisHardCopyHAC	read-write	Adresscode des Druckers
omnisHardCopyHID	read-write	ID des Druckers
omnisHardCopyPtnName	read-write	Partnername
omnisHardCopyProName	read-write	Prozessorname
omnisHardCopyState	read-write	Drucker-Status Der Wert *cancel* kann gesetzt werden. Es wird die Verbindung zu dem Drucker abgebaut. cls-p (1), opn (2), act (3), los (4), cls (5), inact (6), cancel (7), unknown (99)
omnisHardCopyINOP	read-only	Adresscode des Ersatzdruckers
omnisHardCopyConnect	read-write	Startzeit für die Verbindung zu einem Drucker s (1), u (2), unknown (99)
omnisHardCopyRestart	read-write	Hardcopy-Verbindung neu starten start (1), unknown (99)

OMNIS HAC/PID-Tabelle

Objektname	Zugriff	Erläuterung
omnisHardCopyPIDsTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisHardCopyPIDsTable*
omnisHardCopyPIDsSelect Hid	read-write	Hardcopy-ID, für die die HAC/PID-Tabelle angezeigt werden soll.
HAC/PID-Tabelle:		
omnisHardCopyPIDsHID	read-only	ID des Druckers (HID)
omnisHardCopyPIDsID	read-only	ID des Partners (PID)

OMNIS HAC/TID-Tabelle

Objektname	Zugriff	Erläuterung
omnisHardCopyTIDsTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisHardCopyTIDsTable*
omnisHardCopyTIDsSelect Hid	read-write	Hardcopy-ID, für die die HAC/TID-Tabelle angezeigt werden soll.
HAC/TID-Tabelle:		
omnisHardCopyTIDsHID	read-only	ID des Druckers (HID)
omnisHardCopyTIDsHAC	read-only	Adresscode des Druckers (HAC)
omnisHardCopyTIDsID	read-only	ID des Terminals (TID)

OMNIS Hardcopy Create

Objektname	Zugriff	Erläuterung
omnisHardCopyCreateHAC	read-write	Adresscode für einen neuen Drucker
omnisHardCopyCreateHID	read-only	ID für einen generierten Drucker
omnisHardCopyCreatePtn Name	read-write	Terminalname für einen neuen Drucker
omnisHardCopyCreatePro Name	read-write	Prozessorname für einen neuen Drucker
omnisHardCopyCreateInop	read-write	Adresscode des Ersatzdruckers
omnisHardCopyCreate Connect	read-write	Startzeit für die Verbindung zu einem neuen Drucker s (1), u (2), unknown (99)

OMNIS-OMNIS-Tabelle

Objektname	Zugriff	Erläuterung
omnisOmnisStatus	read-write	Status Flag legt den Ausgabeumfang für die OMNIS-Tabelle fest. all (1), active (2), -- Standardwert inactive (4)
omnisOmnisTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisOmnisTable*
OMNIS-Tabelle:		
omnisOmnisOAC	read-write	OMNIS-Adresscode
omnisOmnisID	read-only	ID von OMNIS
omnisOmnisPtnName	read-only	Partnername
omnisOmnisProName	read-only	Prozessorname
omnisOmnisState	read-only	OMNIS-Status cls-p (1), opn (2), act (3), los (4), cls (5), inact (6), cancel (7), unknown (99)
omnisOmnisConnect	read-only	Status der Verbindung start (1), opncon (2), unknown (99)
omnisOmnisTime	read-only	Verbindungsdauer
omnisOmnisLPass	read-only	Verbindungspasswort yes (1), no (2), unknown (99)
omnisOmnisOpncon	read-only	Verbindungsberechtigung dcl (1), free (2), unknown (99)
omnisOmnisRestart	write-only	OMNIS-OMNIS-Verbindung neu starten start (1), unknown (99)

OMNIS Mux-Tabelle

Objektname	Zugriff	Erläuterung
omnisMuxStatus	read-write	Status Flag legt den Ausgabeumfang für die OMNIS-Tabelle fest. all (1), active (2), -- Standardwert inactive (4)
omnisMuxTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisMuxTable*
Mux-Tabelle:		
omnisMuxID	read-only	ID von MUX
omnisMuxPtnName	read-only	Partnername
omnisMuxProName	read-only	Prozessorname
omnisMuxState	read-only	Status der MUX-Verbindung cls-p (1), opn (2), act (3), los (4), cls (5), inact (6), cancel (7), unknown (99)
omnisMuxConnect	read-only	Status der Verbindung start (1), opncon (2), unknown (99)
omnisMuxLPass	read-only	Verbindungspasswort yes (1), no (2), unknown (99)
omnisMuxSessions	read-only	Anzahl momentaner Sitzungen
omnisMuxAvailability	read-only	Verfügbarkeit yes (1), no (2), unknown (99)

OMNIS EXIT-Tabelle

Objektname	Zugriff	Erläuterung
omnisExitTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisExitTable*
EXIT-Tabelle:		
omnisExitEAC	read-write	Adresscode von EXIT
omnisExitID	read-only	ID von EXIT
omnisExitModul	read-write	Modul EXIT

OMNIS EXIT/TID-Tabelle

Objektname	Zugriff	Erläuterung
omnisExitTIDsTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisExitTable*
omnisExitTIDsSelectEac	read-write	EXIT-Adresscode, für den die EXIT/TID-Tabelle angezeigt werden soll.
EXIT/TID-Tabelle:		
omnisExitTIDsEAC	read-only	Adresscode von EXIT
omnisExitTIDsID	read-only	ID des Terminals (TID)

OMNIS EXIT/PID-Tabelle

Objektname	Zugriff	Erläuterung
omnisExitPIDsTabNum	read-only	Anzahl der Einträge in der Tabelle *omnisExitTable*
omnisExitPIDsSelectEac	read-write	Terminal-ID, für die die EXIT/PID-Tabelle angezeigt werden soll
EXIT/PID-Tabelle:		
omnisExitPIDsEAC	read-only	Adresscode von EXIT
omnisExitPIDsID	read-only	ID des Partners (PID)

OMNIS Exit Create

Objektname	Zugriff	Erläuterung
omnisExitCreateEAC	read-write	Adresscode für neuen EXIT
omnisExitCreateModul1	read-write	1. Modul für neuen EXIT
omnisExitCreateModul2	read-write	2. Modul für neuen EXIT
omnisExitCreateModul3	read-write	3. Modul für neuen EXIT
omnisExitCreateModul4	read-write	4. Modul für neuen EXIT
omnisExitCreateModul5	read-write	5. Modul für neuen EXIT
omnisExitCreateModul6	read-write	6. Modul für neuen EXIT
omnisExitCreateModul7	read-write	7. Modul für neuen EXIT
omnisExitCreateModul8	read-write	8. Modul für neuen EXIT
omnisExitCreateModul8	read-write	9. Modul für neuen EXIT
omnisExitCreateModul10	read-write	10. Modul für neuen EXIT
omnisExitCreateModul11	read-write	11. Modul für neuen EXIT
omnisExitCreateModul12	read-write	12. Modul für neuen EXIT
omnisExitCreateModul13	read-write	13. Modul für neuen EXIT
omnisExitCreateModul14	read-write	14. Modul für neuen EXIT
omnisExitCreateOption	read-write	Definiert die auszuführende Operation create (1), modify (2), delete (3), unknown (99)

OMNIS-Trace

Objektname	Zugriff	Erläuterung
omnisTraceConnection	read-write	Trace der DCAM-Verbindung yes (1), no (2), unknown (99)
omnisTraceExit	read-write	EXIT-Trace yes (1), no (2), unknown (99)
omnisTraceTransport	read-write	DCAM-Transport-Trace yes (1), no (2), select (3), unknown (99)
omnisTraceTransportTrm	read-write	DCAM-Transport-Trace für ein ausgewähltes Terminal
omnisTraceTransporthcy	read-write	DCAM-Transport-Trace für einen ausgewählten Drucker
omnisTraceTransportmux	read-write	DCAM-Transport-Trace für ausgewählte MUX-Verbindung
omnisTraceTransportoms	read-write	DCAM-Transport-Trace für ausgewähltes OMNIS

Traps

Objektname	Trap-Nr	Erläuterung
Enterprise = 1.3.6.1.4.1.231.2.31.20		
omnisStopTrap	301	TRAP wird gesendet, wenn ein OMNIS beendet wurde.
omnisStartTrap	302	TRAP wird gesendet, wenn ein OMNIS aktiviert wurde.
omnisConnStopTrap	303	TRAP wird gesendet, wenn eine kritische Verbindung inaktiviert wurde.
omnisDstConnStopTrap	304	TRAP wird gesendet, wenn eine OMNIS-Sitzung normal beendet wurde.
omnisEventTrap	305	TRAP wird gesendet, wenn eine kritische OMNIS-Meldung empfangen wurde.
omnisDstLevelTrap	306	TRAP wird gesendet, wenn DSTMAX erreicht wurde.
omnisPacLevelTrap	307	TRAP wird gesendet, wenn PACMAX erreicht wurde.
omnisPtnLevelTrap	308	TRAP wird gesendet, wenn PTNMAX erreicht wurde.
omnisMuxConnStopTrap	309	TRAP wird gesendet, wenn eine kritische Mux-Verbindung deaktiviert wurde.
omnisOmnConnStopTrap	310	TRAP wird gesendet, wenn eine kritische OMNIS-OMNIS-Verbindung deaktiviert wurde.
omnisHcConnStopTrap	311	DCAM-Verbindung-Trace
omnisDumpWriteTrap	312	TRAP wird gesendet, wenn eine kritische Hardcopy-Verbindung deaktiviert wurde.
omnisDumpEndTrap	313	TRAP wird gesendet, wenn OMNIS die Dump-Erstellung beendet hat.
omnisEndTrap	314	TRAP wird gesendet, wennOMNIS sich normal beendet hat.

OMNIS Trap-Gruppe

Benutzerdefiniertes Trap-Objekt

Objektname	Zugriff	Erläuterung
Enterprise = 1.3.6.1.4.1.231.2.31.21		
omnisTrapMsgText	read-only	OMNIS-Meldungstext generiert einen Trap.

Benutzerdefinierter Trap

Objektname	Trap-Nr	Erläuterung
Enterprise = 1.3.6.1.4.1.231.2.31.21		
omnisGeneralTrap	320	TRAP wird in allen benutzerdefinierten Fällen gesendet.

6.7 SNMP-Management zur Performance-Basisüberwachung mit SM2

Der Subagent zur Performance-Basisüberwachung mit SM2 liefert Durchschnittswerte zur Überwachung des CPU-Verbrauchs und der I/O-Raten.

Objektname	**Zugriff**	**Erläuterung**
Gruppe SM2 Params		
sm2Status	read-only	Status des Mess-Subsystems SM2
sm2Interval	read-write	Online-Zyklus des Mess-Subsystems SM2 in Sekunden, auch Messintervall genannt (Standardwert: 120)
Gruppe SM2 Basic		
sm2BasicStatus	read-only	Status, der dem BASIC-Puffer zugeordnet ist
sm2BasicTime	read-only	Zeit beim Abschluss des letzten Messintervalls DateAndTime gemäß RFC 1514
sm2BasicTimeString	read-only	Zeit beim Abschluss des letzten Messintervalls. Datum und Uhrzeit in einem direkt anzeigbaren Format: YYYY-MM-DD,hh:mm:ss.d[,shh:mm] Dabei steht YYYY-MM-DD für das lokale Datum in der Reihenfolge Jahr-Monat-Tag, hh:mm:ss.d steht für die lokale Zeit als Stunde-Minuten-Sekunden.Dezisekunden, shh:mm gibt die Abweichung in (-|+)Stunden:Minuten von UTC an
Gruppe der I/O-Werte		
sm2TimeIOStatus	read-only	Status, der dem TIME IO-Puffer zugeordnet ist (data-supported, data-invalid, prg-inactive, no-subsystem, sm2-not-running, unkown)
sm2TimeIOMachTabNumber	read-only	Anzahl der Einträge in der folgenden Rechnertabelle
sm2TimeIOMachTabIdleTime	read-only	Zeit, in der der logische Rechner nicht aktiv war (nicht angehalten) als o/oo (Anteil der Zeit in Promille)
sm2TimeIOMachTabTUTime	read-only	TU Time des logischen Rechners als o/oo (Anteil der Zeit in Promille)
sm2TimeIOMachTabTPRTime	read-only	TPR Time des logischen Rechners als o/oo (Anteil der Zeit in Promille)

Objektname	Zugriff	Erläuterung
sm2TimeIOMachTabSIHTime	read-only	SIH Time des logischen Rechners als o/oo (Anteil der Zeit in Promille)
sm2TimeIOMachTabStopTime	read-only	Stop Time des logischen Rechners als o/oo (Anteil der Zeit in Promille)
sm2TimeIOMachTabPagingIO	read-only	Rate des Paging IO in Bezug auf den logischen Rechner als (Anzahl der Paging IOs pro Sekunde) * 10
sm2TimeIOMachTabDiskIO	read-only	Rate des Disk IO in Bezug auf den logischen Rechner als (Anzahl der Disk IOs pro Sekunde) * 10
sm2TimeIOMachTabTapeIO	read-only	Rate des Tape IO bezogen auf den logischen Rechner als (Anzahl der Tape IOs pro Sekunde) * 10
sm2TimeIOMachTabPrinterIO	read-only	Rate des Drucker IO bezogen auf den logischen Rechner als (Anzahl der Drucker IOs pro Sekunde) * 10
sm2TimeIOMachTabOtherIO	read-only	Rate des sonstigen IO bezogen auf den logischen Rechner als (Anzahl des sonstigen IO pro Sekunde) * 10

6.8 SNMP-Management für SESAM-Datenbanken

Der Subagent zum Management von SESAM-Datenbanken liefert Informationen über SESAM-Datenbanken und SESAM-DBHs, mit denen diese Datenbanken prozessiert werden. Er unterstützt die RDBMS-MIB gemäß RFC 1697.

Tabelle der installierten Datenbanken

Objektname	Zugriff	Erläuterung
rdbmsDbVendorName	read-only	Der Name des Anbieters, dessen RDBMS diese Datenbank verwaltet (zur Information).
rdbmsDbName	read-only	Der Name dieser Datenbank in einem produktspezifischen Format. Unter Umständen muss das Produkt den Namen qualifizieren, um Konflikte zu lösen, falls der Datenbankname auf einem Host dupliziert werden kann. Es kann notwendig sein, einen hierarchischen Namen zu konstruieren, der die RDBMS-Instanz/Installation auf dem Host bzw. den Eigentümer der Datenbank einbettet. Beispiel: "/test-installation/database-owner/database-name".
rdbmsDbContact	read-write	Die Identifikation des Ansprechpartners für diese verwaltete Datenbank als Text sowie Informationen, wie diese Person zu erreichen ist.

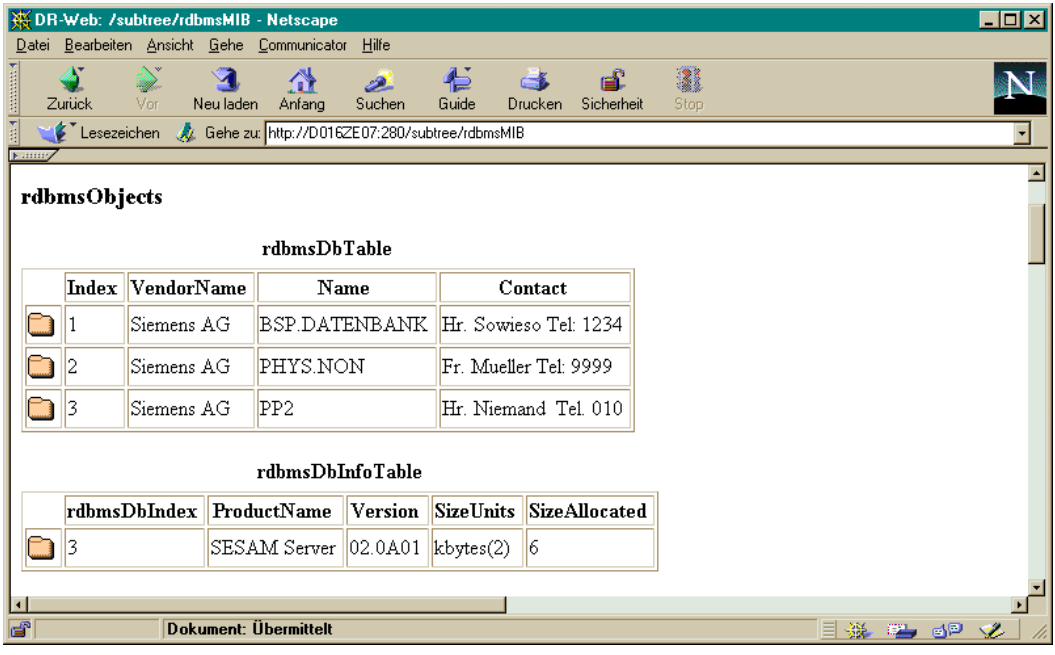


Bild 30: Übersicht über die installierten SESAM-Datenbanken

Zusätzliche Informationen über derzeit an einem Server prozessierte Datenbanken

Objektname	Zugriff	Erläuterung
rdbmsDbInfoProductName	read-only	Der Produktname des Servers, der diese Datenbank erstellt bzw. zuletzt neu strukturiert hat, als Text. Das Format ist produktspezifisch.
rdbmsDbInfoVersion	read-only	Die Versionsnummer des Servers, der diese Datenbank erstellt bzw. zuletzt neu strukturiert hat. Das Format ist produktspezifisch.
rdbmsDbInfoSizeUnits	read-only	INTEGER bytes(1), kbytes(2), mbytes(3), gbytes(4), tbytes(5) Identifikation der Einheiten, mit denen die Größe dieser Datenbank in rdbmsDbInfoSizeAllocated und rdbmsDbInfoSizeUsed gemessen wird. bytes(1) steht für einzelne Bytes, kbytes(2) steht für Einheiten an Kilobyte, mbytes(3) steht für Megabyte, gbytes(4) steht für Gigabyte und tbytes(5) steht für Terabyte. Alle Werte sind binäre Vielfache -- 1K = 1024. Sofern Werte überschreibbar sind, spiegeln sich Änderungen in den get-Werten der entsprechenden Objekte wieder.
rdbmsDbInfoSizeAllocated	read-write	Die geschätzte Größe dieser Datenbank (in rdbmsDbInfoSizeUnits). Dies entspricht dem Plattenplatz, der zugewiesen wurde und den Benutzern an diesem Host nicht mehr zur Verfügung steht. rdbmsDbInfoSize gibt nicht in jedem Fall den Platz wider, der tatsächlich durch Daten der Datenbank belegt ist. Einige Datenbanken unterstützen möglicherweise die Erweiterung des zugeordneten Platzes, andere wiederum nicht. Bitte beachten Sie, dass der SESAM-Subagent keinen Schreibzugriffauf dieses Objekt zulässt.

Tabelle der installierten Server (SESAM-DBH)

Objektname	Zugriff	Erläuterung
rdbmsSrvVendorName	read-only	Der Name des Anbieters, dessen RDBMS diese Datenbank verwaltet (zur Information).
rdbmsSrvProductName	read-only	Der Produktname dieses Servers. Dabei handelt es sich in der Regel um den formalen Namen des Anbieters für das Produkt. (Das Format ist produktspezifisch.)
rdbmsSrvContact	read-write	Die Identifikation des Ansprechpartners für diesen verwalteten Server als Text sowie Informationen, wie diese Person zu erreichen ist.

Zusätzliche Information über derzeit aktive Server

Objektname	Zugriff	Erläuterung
rdbmsSrvInfoStartupTime	read-only	Datum und Uhrzeit, als dieser Server zuletzt gestartet wurde.
rdbmsSrvInfoFinishedTransactions	read-only	Die Anzahl der Transaktionen, die für diesen Server sichtbar sind und die entweder durch commit oder abort abgeschlossen wurden. Einige Datenbankoperationen, wie zum Beispiel read-only-Abfragen, führen u.U nicht zur Erstellung einer Transaktion.
rdbmsSrvInfoDiskReads	read-only	Die Gesamtzahl der Lesevorgänge (Reads) von Datenbankdateien, die seit dem Start von diesem Server an das Betriebssystem abgesetzt wurden. Die Zahlen sind nicht über Produktgrenzen hinweg vergleichbar. Die Berechnung von Reads und Festlegung, was ein Read ist, ist produktspezifisch.
rdbmsSrvInfoLogicalReads	read-only	Die Gesamtzahl der logischen Lesevorgänge (Reads) von Datenbankdateien, die seit dem Start von diesem Server intern vorgenommen wurden. Die Werte dieses Objekts und von rdbmsSrvInfoDiskReads verdeutlichen die Wirkung des Caching bei Read-Operationen. Die Zahlen sind nicht über Produktgrenzen hinweg vergleichbar. Sie können nur dann Aussagekraft haben, wenn sie für alle Server berechnet werden, die einen Cache gemeinsam nutzen.

Objektname	Zugriff	Erläuterung
rdbmsSrvInfoDiskWrites	read-only	Die Gesamtzahl der Schreibvorgänge (Writes) in Datenbankdateien, die seit dem Start von diesem Server an das Betriebssystem abgesetzt wurden. Die Zahlen sind nicht über Produktgrenzen hinweg vergleichbar.
rdbmsSrvInfoLogicalWrites	read-only	Gibt an, wie oft Teile der Datenbankdateien als "dirty" markiert wurden und die Notwendigkeit erkannt wurde, sie auf Platte zu schreiben. Dieser Wert sowie rdbmsSrvInfoDiskWrites liefern einen Hinweis über die Wirkung von "write-behind"-Strategien bei der Reduzierung der Häufigkeit von Schreibvorgängen auf Platte (im Vergleich zu Datenbankoperationen). Da die Schreibvorgänge (Writes) von anderen Servern vorgenommen werden können als denen, die die Teile der Datenbankdateien als „dirty“ markiert haben, können diese Werte nur aussagekräftig sein, wenn sie für alle Server ermittelt werden, die einen Cache gemeinsam nutzen. Die Zahlen sind nicht über Produktgrenzen hinweg vergleichbar.
rdbmsSrvInfoHandledRequests	read-only	Die Gesamtzahl der Anforderungen an den Server bezüglich ankommender Zuordnungen. Die Bedeutung des Begriffs "Anforderungen" ist hier jedoch produktspezifisch zu sehen. Dies ist nicht über Produktgrenzen hinweg vergleichbar. Hiermit ist eine Kapselung semantischer Operationen auf hoher Ebene zwischen Clients und Servern (oder zwischen Peers) beabsichtigt. So kann eine Anforderung zum Beispiel einer Anweisung "select" oder "insert" entsprechen. Die Erfassung von Disk I/O, die von rdbmsSrvInfoDiskReads und rdbmsSrvInfoDiskWrites beschrieben wird, ist nicht beabsichtigt.

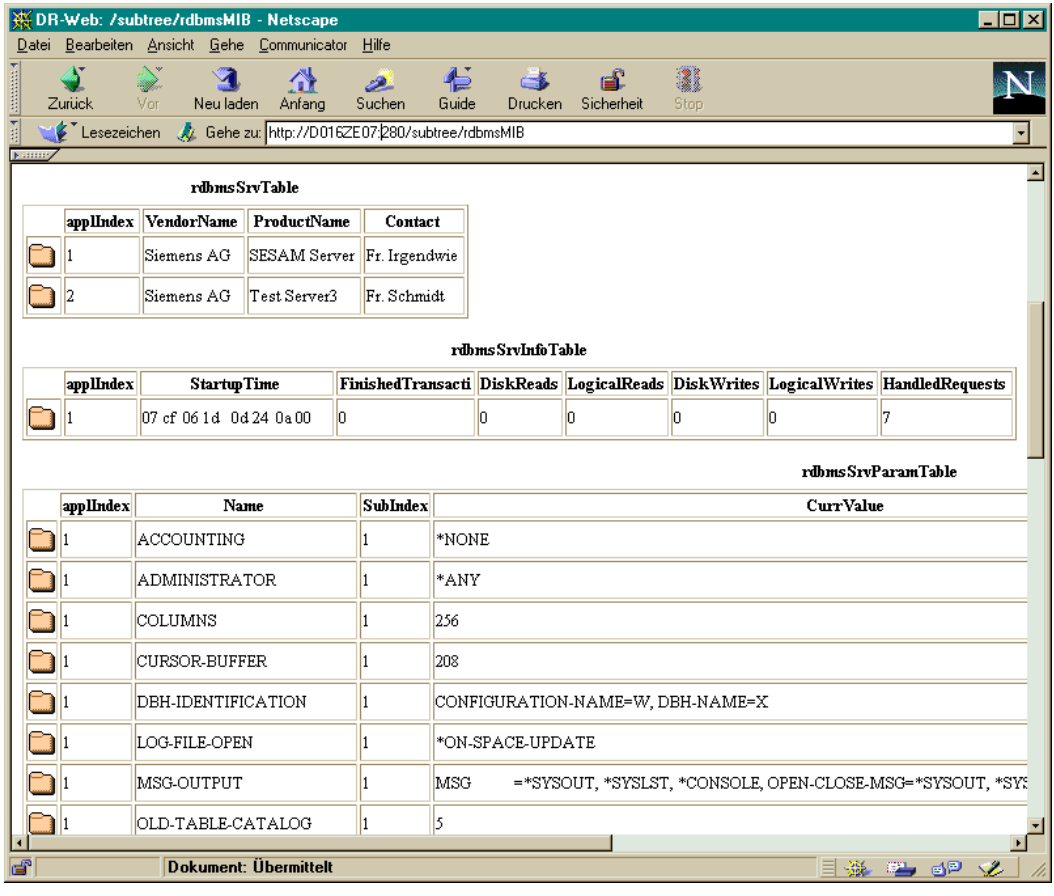


Bild 31: Anzeige der derzeit installierten Server mit zusätzlichen Informationen über die zurzeit aktiven Server

Grenzwerte

Objektname	Zugriff	Erläuterung
rdbmsSrvLimitedResourceLimit	read-write	Der maximale Wert, den die Ressourcennutzung erreichen kann. Der SESAM-Subagent lässt keinen Schreibzugriff auf dieses Objekt zu.
rdbmsSrvLimitedResourceCurrent	read-only	Der aktuelle Wert für die Ressource.
rdbmsSrvLimitedResourceHighwater	read-only	Maximaler Wert der Ressource seit Zurücksetzen von applUpTime.

Grenzwerte

Resourcename	**ResourceLimit**	**ResourceCurrent**	**ResourceHighwater**
CURSORS	X	X	
PLANS	X	X	
SERVICE-TASKS	X	X	
SPACES		X	
SUBORDERS	X	X	X
THREADS		X	
USERS		X	

Für jeden in der Konfigurationsdatei eingetragenen und gerade aktiven Server (SESAM-DBH) werden die durch die oben aufgeführten DBH-Ladeparameter beschriebenen Grenzwerte unterstützt.

Anzeige der aktuellen DBH-Ladeparameter für aktive Server

Objektname	Zugriff	Erläuterung
rdbmsSrvParamCurrValue	read-write	Der Wert für einen jetzt aktiven Konfigurationsparameter (Einstellung für den Server). In der entsprechenden temporären Domäne können zwar mehrere Werte relevant sein (z.B. der Wert, der beim nächsten Neustart wirksam wird), dies ist jedoch die aktuelle Einstellung. Der SESAM-Subagent lässt keinen Schreibzugriff auf dieses Objekt zu.
rdbmsSrvParamComment	read-write	Anmerkung, die den Zweck eines Konfigurationsparameters oder den Grund für eine bestimmte Parametereinstellung beschreibt. Der SESAM-Subagent lässt keinen Schreibzugriff auf dieses Objekt zu.

Anzeige der aktuellen DBH-Ladeparameter für aktive Server

Beziehung zwischen Datenbanken und Servern

Objektname	Zugriff	Erläuterung
rdbmsRelState	read-only	INTEGER other(1), active(2), available(3), restricted(4), unavailable(5) Status des Zugriffs dieses Servers auf diese Datenbank. Active(2) bedeutet, dass der Server die Datenbank aktiv nutzt. Available(3) bedeutet, dass der Server die Datenbank bei Bedarf nutzen könnte. Restricted(4) bedeutet, dass sich die Datenbank in einem verwaltungstechnisch bestimmten Status befindet, in dem eine vollständige Verfügbarkeit nicht gegeben ist. Unavailable(5) bedeutet, dass die Datenbank über diesen Server nicht zur Verfügung steht. Other(1) bedeutet, dass für Datenbank/Server eine andere Bedingung vorliegt, die möglicherweise in der privaten MIB des Anbieters beschrieben ist.

Traps

Objektname	Trap-Nr	Erläuterung
Enterprise = rdbmsMIB.2		
rdbmsStateChange	1	Ein rdbmsStateChange Trap bedeutet, dass einer der Datenbankserver/eine der Datenbanken, die von diesem Agenten verwaltet werden, einen veränderten rdbmsRelState hat, auf Grund dessen die Verfügbarkeit für die Nutzung eingeschränkt ist. Für diese Zwecke wird sowohl active(2) als auch available(3) als uneingeschränkt zugriffsfähig betrachtet. Der Status, der mit dem Trap übermittelt wird, ist der neue Status mit der geringeren Verfügbarkeit.

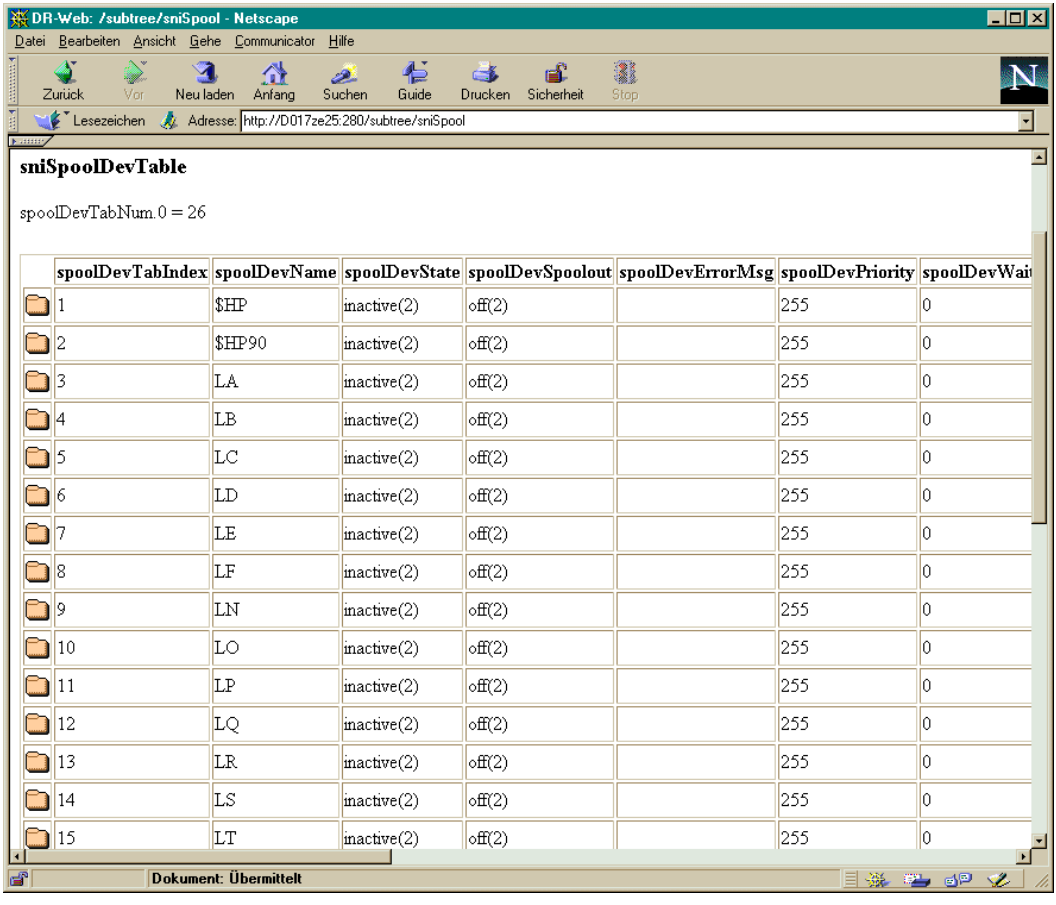
6.9 SNMP-Management für Spool & Print Service

Der Subagent für Spool & Print Service dient zur Überwachung der SPOOL- und RSO-Geräte, er liefert Informationen über Geräte und Druckaufträge. Der PrintService-Agent wird ausgeliefert mit einer proprietären MIB, die mit der SINIX-Spool-MIB identisch ist. Für BS2000/OSD sind von dieser MIB die Device- und die Job-Gruppe realisiert.

Print-Device-Management

MIB-Definition	Zugriff	Erläuterung
spoolDevTabNum	read-only	Anzahl der Tabellenelemente
spoolDevTabIndex	read-only	Index
spoolDevName	read-only	Name
spoolDevState	read-only	Status
spoolDevSpoolout	read-only	Spoolout
spoolDevErrorMsg	read-only	Fehlermeldung
spoolDevPriority	read-only	Priorität
spoolDevWaitingJobs	read-only	wartende Aufträge
spoolDevCurForm	read-only	Formular
spoolDevActJid	read-only	Druckjob
spoolDevHost	read-only	Host
spoolDevAdmin	read-only	Verwalter
spoolDevDftForm	read-only	Default-Form
spoolDevAdmComment	read-only	Anmerkung
spoolDevEnablePoll	read-only	Poll-Option

Device-Gruppe



sniSpoolDevTable

spoolDevTabNum.0 = 26

	spoolDevTabIndex	spoolDevName	spoolDevState	spoolDevSpoolout	spoolDevErrorMsg	spoolDevPriority	spoolDevWait
	1	$HP	inactive(2)	off(2)		255	0
	2	$HP90	inactive(2)	off(2)		255	0
	3	LA	inactive(2)	off(2)		255	0
	4	LB	inactive(2)	off(2)		255	0
	5	LC	inactive(2)	off(2)		255	0
	6	LD	inactive(2)	off(2)		255	0
	7	LE	inactive(2)	off(2)		255	0
	8	LF	inactive(2)	off(2)		255	0
	9	LN	inactive(2)	off(2)		255	0
	10	LO	inactive(2)	off(2)		255	0
	11	LP	inactive(2)	off(2)		255	0
	12	LQ	inactive(2)	off(2)		255	0
	13	LR	inactive(2)	off(2)		255	0
	14	LS	inactive(2)	off(2)		255	0
	15	LT	inactive(2)	off(2)		255	0

Bild 32: Print-Device-Management-Tabelle

Print-Job-Management

MIB-Definition	Zugriff	Erläuterung
spoolJobTabNum	read-only	Anzahl der Tabellenelemente
spoolJobTabIndex	read-only	Index
spoolJobGlobalJid	read-only	Globale-Job-ID
spoolJobComment	read-only	Anmerkung
spoolJobOriginator	read-only	Originator
spoolJobOrigHost	read-only	Origination-Host
spoolJobDestination	read-only	Ziel-Drucker
spoolJobFileList	read-only	File-List
spoolJobPriority	read-only	Priorität
spoolJobTotalSize	read-only	Größe
spoolJobRawMode	read-only	Raw-Modus
spoolJobDevName	read-only	Drucker
spoolJobState	read-only	Status
spoolJobErrorMsg	read-only	Fehler-Meldung
spoolJobRqCopies	read-only	geforderte Kopien
spoolJobPrCopies	read-only	gedruckte Kopien
spoolJobPrPercent	read-only	gedruckt (in Prozent)

Job-Gruppe

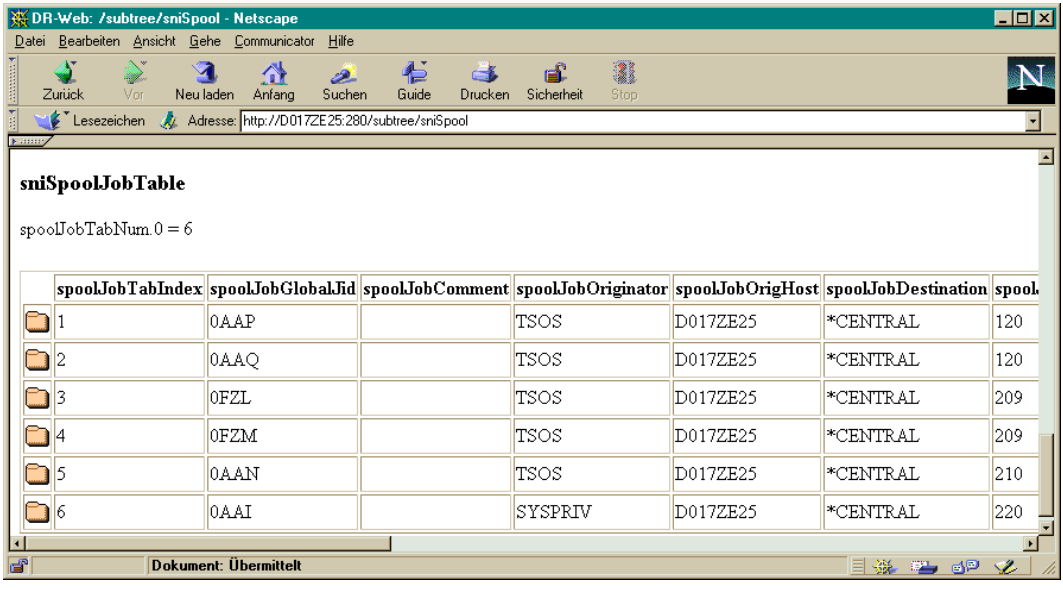


Bild 33: Print-Job-Management-Tabelle

6.10 SNMP-Management für Storage-Management

Der Subagent für das Storage-Management liefert Informationen zu Pubsets und Platten sowie über die Verfügbarkeit der Storage-Management-Produkte HSMS, MAREN, TLS und ROBAR. Dementsprechend wird mit dem Subagenten eine proprietäre MIB ausgeliefert, die neben den globalen Daten des Storage-Management-Subagenten vier Gruppen mit folgenden Informationen enthält:

– allgemeinen Informationen zu HSMS, MAREN, ROBAR und TLS,
– Ressourcen-Informationen,
– Anzeige aller Pubsets in einer Tabelle
– Anzeige aller Platten in einer Tabelle

Globale Daten des Storage-Management-Subagenten

MIB-Definition	Zugriff	Erläuterung
storMgmtGlobalDataVersion	read-only	Version des Subagenten
storMgmtGlobalDataInputFile	read-write	Name der Eingabedatei

Allgemeine Informationen zu HSMS, MAREN, ROBAR und TLS

MIB-Definition	Zugriff	Erläuterung
storMgmtProductTabNum	read-only	Anzahl der Tabellenelemente
storMgmtProductIndex	read-only	Index
storMgmtProductName	read-only	Name
storMgmtProductVersion	read-only	Version
storMgmtProductState	read-only	Subsystem-Status

Produktgruppe

Die Anzeige der Produktinformation erfolgt in einer Tabelle, in der für die Produkte HSMS, MAREN, TLS und ROBAR Aussagen über Index, Name, Version und Status gemacht werden. Für ROBAR wird zusätzlich der Name des Roboterarchivs (Lagerort) mit ausgegeben.

Folgende Werte für den Subsystem-Status (siehe Seite 189) werden unterschieden:

- created
- not-created
- in-delete
- in-create
- in-resume
- in-hold
- not-resumed
- locked
- not-installed

Für die Subsysteme MAREN, HSMS und TLS wird jeweils die höchste Version angezeigt, deren Zustand ungleich not-created ist. Sind für ein Subsystem alle Versionen im Status not-created, wird ein Eintrag ohne Version zurückgegeben.

Der Ausfall eines der Subsysteme HSMS, MAREN oder TLS kann derzeit nicht über Traps an die Management-Station gemeldet werden.

Falls sich der Zustand eines überwachten Pubsets oder einer überwachten Platte ändert, wird ein Trap an die Management-Station geschickt.

Beispiel:

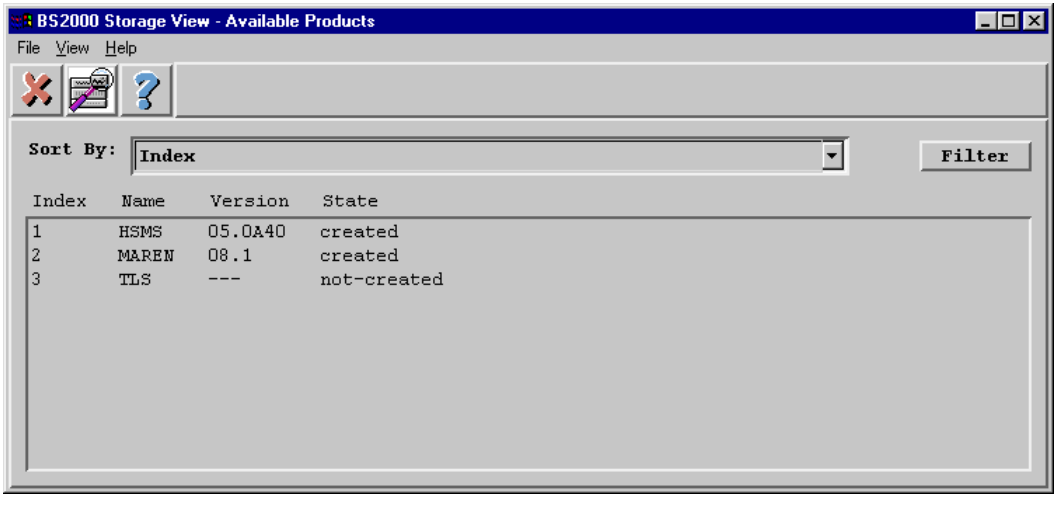


Bild 34: Übersicht über die verfügbaren Produkte

Ressourcen-Informationen

MIB-Definition	Zugriff	Erläuterung
storMgmtResourcePubset	read-write	Pubset (Cat-ID)
storMgmtResourceSaturation	read-only	derzeitiger Sättigungsgrad level-0 bis level-5 oder unknown-level*
storMgmtResourceCapacity	read-only	Kapazität (in Half Pages (HP)
storMgmtResourceSpaceAllocated	read-only	belegter Speicher (Anzahl der belegten HPs)
storMgmtResourceFragment	read-only	Grad der Fragmentierung
storMgmtResourceReusableS1	read-only	Anzahl der Sicherungsdateien; Anzahl der von diesen Sicherungsdateien belegten PAM-Seiten; Anzahl der nicht-belegten PAM-Seiten
storMgmtResourceSecureQueue	read-only	Anzahl der in der SECURE-Queue wartenden Tasks

Ressourcengruppe
*Der Wert "unknown-level" wird ausgegeben, wenn keine Information zu dem angegebenen Pubset ermittelt werden kann. *storMgmtResourceCapacity.0* und *storMgmtResourceSpaceAllocated.0* haben in diesem Fall den Wert 1.

Für ein ausgewähltes Pubset können bestimmte Informationen abgefragt werden. Die Auswahl eines Pubsets erfolgt durch Angabe der Cat-ID in Großbuchstaben für das Objekt *storMgmtResourcePubset.0*. Die Anzeige der Pubset-Information erfolgt in einer Tabelle.

Anzeige aller Pubsets in einer Tabelle

Der Storage-Management-Subagent ermöglicht die Anzeige aller Pubsets in einer Tabelle. Außerdem lässt sich der Saturation-Level einzelner Pubsets überwachen. Hierzu müssen diese Pubsets bei der Konfiguration des Storage-Management-Subagenten in dessen Input-Datei definiert werden (siehe Seite 88). Bei Änderung des Saturation-Levels sendet der Storage-Management-Subagent einen Trap mit dem spezifizierten Community-String (siehe Seite 303).

MIB-Definition	Zugriff	Erläuterung
storMgmtPubsetTabNum	read-only	Anzahl der Tabelleneinträge
storMgmtPubsetTabState	read-write	Status der Pubsets in der Pubset-Tabelle: all paging local remote accessible local-accessible shared exclusive remote-accessible local-accessible-speedcat xcs-pubset hsms-supported single-feature system-managed volume-sets unused-volsets master-change-error Durch Setzen dieser Werte kann die Tabellenausgabe modifiziert werden:
Tabelle:		
storMgmtPubsetIndex	read-only	Eindeutiger Wert für jeden Tabellen-Eintrag (CatID des zugehörigen Pubset)
storMgmtPubsetTyp	read-only	Typ des Pubsets: single-featured system-managed volumeset unknown
storMgmtPubsetLocal	read-only	Anzeige, ob der Pubset *local* oder *remote* ist
storMgmtPubsetHome	read-only	Anzeige, ob der Pubset *home* oder *imported* ist

MIB-Definition	Zugriff	Erläuterung
storMgmtPubsetShared	read-only	Anzeige, ob der Pubset *shared* oder *exclusive* ist
storMgmtPubsetMaster	read-only	Anzeige, ob es sich um einen Master- oder Slave-Pubset handelt
storMgmtPubsetAccessible	read-only	Anzeige, ob der Pubset zugreifbar oder nicht zugreifbar ist
storMgmtPubsetQuiet	read-only	Anzeige, ob es sich um einen „Quiet Pubset“ handelt
storMgmtPubsetPaging	read-only	Anzeige, ob es sich um einen „Paging Pubset“ handelt
storMgmtPubsetSize	read-only	Größe des Pubset
storMgmtPubsetUsedSize	read-only	belegter Speicherplatz des Pubset
storMgmtPubsetSaturationLevel	read-write	Saturation-Level für das Pubset

Pubset-Tabelle

Beispiel:

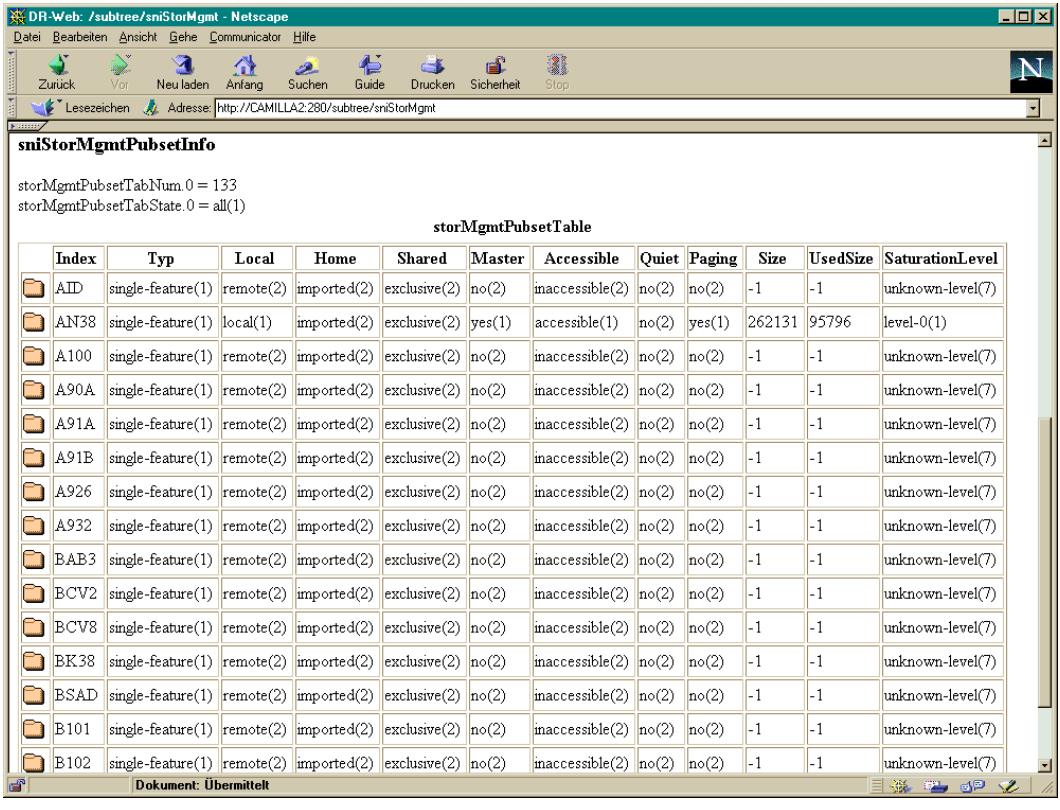


Bild 35: Anzeige aller Pubsets

Anzeige aller Platten in einer Tabelle

Der Storage-Management-Subagent ermöglicht die Anzeige aller Platten in einer Tabelle. Außerdem lässt sich der Reconfiguration-State einzelner Platten überwachen. Hierzu müssen diese Platten bei der Konfiguration des Storage-Management-Subagenten in dessen Input-Datei definiert werden (siehe Seite 88). Bei Änderung des Reconfiguration-State sendet der Storage-Management-Subagent einen Trap mit dem spezifizierten Community-String (siehe Seite 303).

MIB-Definition	Zugriff	Erläuterung
storMgmtDiskTabNum	read-only	Anzahl der Tabelleneinträge
storMgmtDiskTabReconfState	read-write	Reconfiguration-State der angezeigten Platte: all attached detached other Durch Setzen dieser Werte kann die Tabellenausgabe modifiziert werden.
storMgmtDiskIndex	read-only	Eindeutiger Wert für jeden Tabellen-Eintrag (mnemonischer Name der Platte)
storMgmtDiskVSN	read-only	Volume Serial Number (vsn) der Platte
storMgmtDiskDeviceAllocState	read-only	Device Allocation State der Platte
storMgmtDiskSystemUse	read-only	Typ der Platte
storMgmtDiskPoolAttribut	read-only	Anzeige, ob es sich um eine *lokale* oder *remote* Platte handelt
storMgmtDiskReconfState	read-only	Reconfiguration State der Platte
storMgmtDiskVolAllocState	read-only	Volume Allocation State der Platte
storMgmtDiskPrivDiskRunState	read-only	Private Disk Run State der Platte
storMgmtDiskPhaseSet	read-only	Phase Set der Platte
storMgmtDiskActionState	read-only	Action State der Platte
storMgmtDiskUse	read-only	Verwendungszweck (Disk Use) der Platte
storMgmtDiskAssignTime	read-only	Assign Time der Platte
storMgmtDiskUserAllocation	read-only	User Allocation der Platte
storMgmtDiskOperatorControl	read-only	Operator Control der Platte
storMgmtDiskSystemAllocation	read-only	System Allocation der Platte
storMgmtDiskAccess	read-only	Disk Access der Platte
storMgmtDiskRecordingMode	read-only	Disk Recording Mode der Platte

Beispiel:

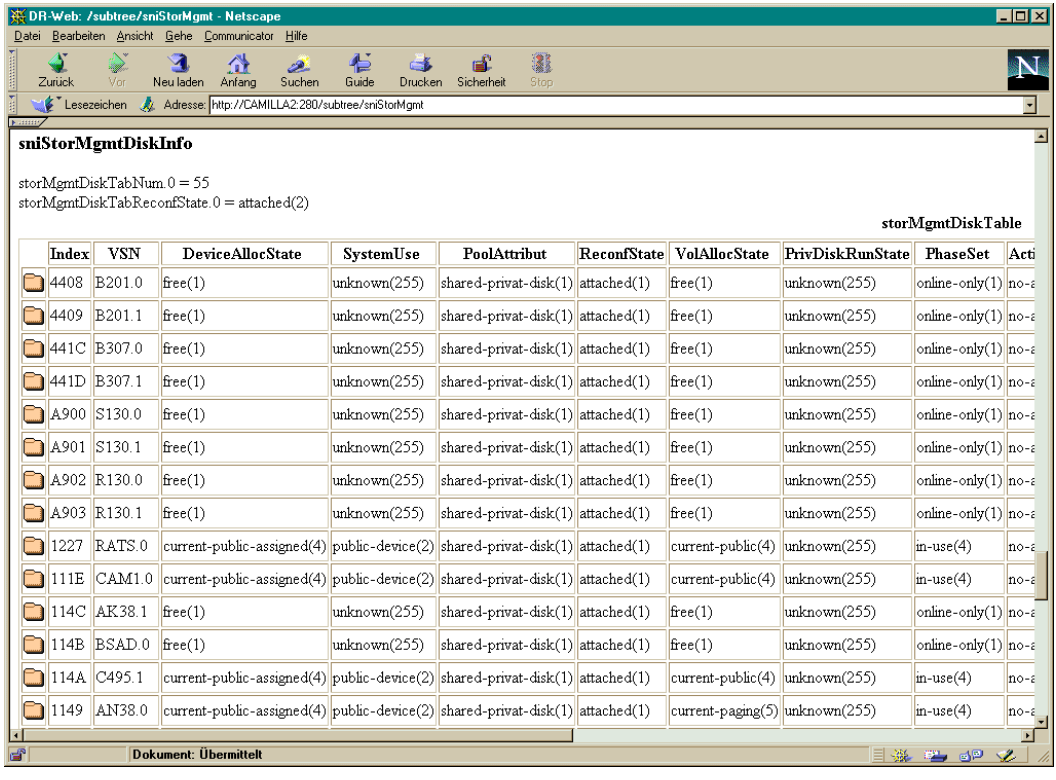


Bild 36: Anzeige aller Platten

Traps

Es gibt je einen Trap zu

– Saturation-Level (Pubset-Überwachung)
– Reconfiguration-State (Platten-Überwachung)

Trap zu Saturation-Level (Pubset-Überwachung)

Objektname	**Trap-Nr.**	**Erläuterung**
sniStorMgmtPubsetTraps (Enterprise=1.3.6.1.4.1.231.1.20.20)		
storMgmtPubsetSatLevTrap	301	Saturation-Level *x* erreicht

Trap zu Reconfiguration-State (Platten-Überwachung)

Objektname	**Trap-Nr.**	**Erläuterung**
sniStorMgmtDiskTraps (Enterprise=1.3.6.1.4.1.231.1.20.21)		
storMgmtDiskReconfStateTrap	301	Disk Reconfiguration State *x* erreicht

7 SNMP-Management zur erweiterten Performance-Überwachung mit SM2

Der SM2-basierte Performance-Subagent SSA-SM2-BS2 steht für BS2000-Systeme ab BS2000/OSD V2.0 zur Verfügung. SSA-SM2-BS2 liefert Basisinformationen zum SM2 selbst, d.h. zum Status des Subsystems, zur Version, zur Größe des Messintervalls und zum Stichprobenzyklus. Die eigentlichen Messwerte entsprechen den SM2-bekannten Reportgruppen und informieren über

- die CPU-Auslastung,
- I/O-Aktivitäten,
- die Auslastung des Hauptspeichers und des virtuellen Adressraums,
- die Belegung des Hauptspeichers durch die vier Standardkategorien von Tasks,
- Ein- und Ausgabeoperationen auf periphere Geräte während eines Messintervalls,
- applikationsspezifische Daten von *open*UTM-Anwendungen,
- Verbrauchswerte einzelner Tasks.

Zur Darstellung und Bewertung der gelieferten Messwerte auf der Management-Station steht die Management-Anwendung PMBS2 in den Integrationspaketen PMBS2 (Reliant UNIX, Windows NT) und SMAWpmbs2 (Solaris) zur Verfügung. PMBS2 ermöglicht ferner die gleichzeitige Überwachung mehrerer BS2000/OSD-Systeme. Die Integrationspakete PMBS2 und SMAWpmbs2 sind auf der dem Produkt SBA-BS2 beigefügten CD-ROM enthalten. Eine ausführliche Beschreibung von PMBS2 finden Sie ab Seite 385.

SM2-Parameter und Basiswerte

Objektname	Zugriff	Erläuterung
Gruppe SM2 Params		
sm2Status	read-only	Status des Mess-Subsystems SM2
sm2Version	read-only	Version des Mess-Subsystems SM2: Format Vnn.nAnn
sm2Interval	read-write	Online-Zyklus des Mess-Subsystems SM2 in Sekunden, auch Messintervall genannt Bereich: 10 - 3600 (Standardwert: 120)
sm2SamplingCycle	read-write	Beispielzyklus des Mess-Subsystems SM2 in Millisekunden Bereich: 200 - 10000 (Standardwert: 800)
Gruppe SM2 Basic		
sm2BasicStatus	read-only	Status, der dem BASIC-Puffer zugeordnet ist
sm2BasicTime	read-only	Zeit beim Abschluss des letzten Messintervalls DateAndTime gemäß RFC 1514
sm2BasicTimeString	read-only	Zeit beim Abschluss des letzten Messintervalls. Datum und Uhrzeit in einem direkt anzeigbaren Format: YYYY-MM-DD,hh:mm:ss.d[,shh:mm] Dabei steht YYYY-MM-DD für das lokale Datum in der Reihenfolge Jahr-Monat-Tag, hh:mm:ss.d steht für die lokale Zeit als Stunde-Minuten-Sekunden.Dezisekunden, shh:mm gibt die Abweichung in (-|+)Stunden:Minuten von UTC an
sm2BasicSamples	read-only	Anzahl der Beispiele innerhalb des letzten Messintervalls
sm2BasicMaxLogMach	read-only	Anzahl der logischen Rechner
sm2BasicVM2000	read-only	Info über VM2000-Aktivität (no-data, inactive, active)

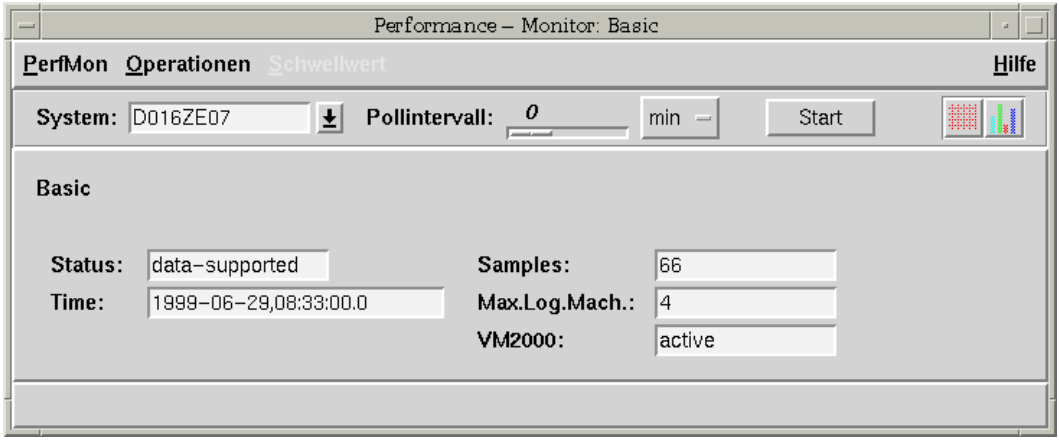
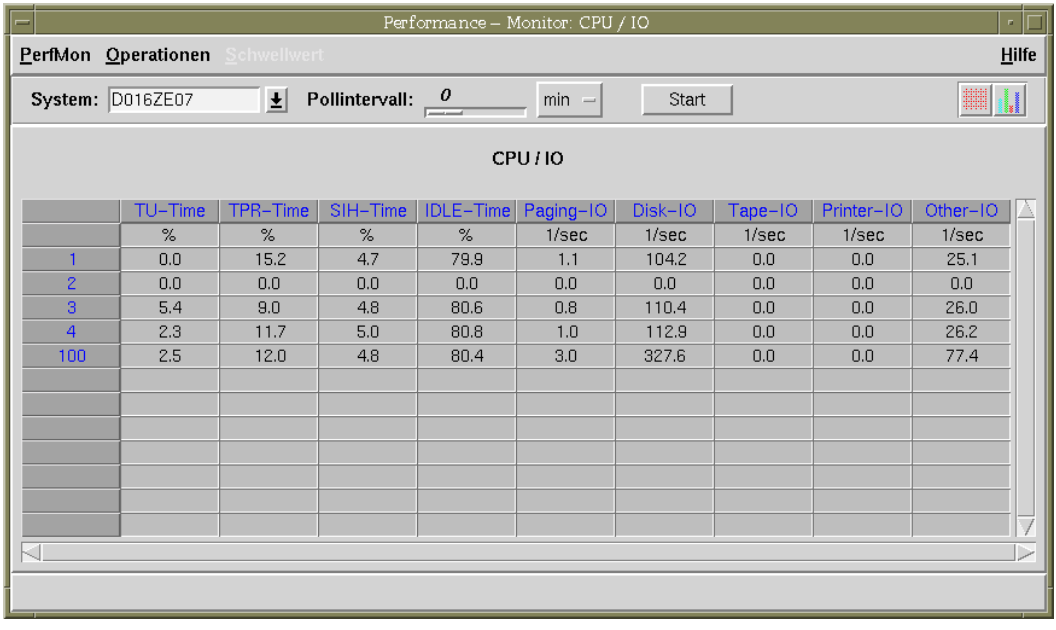


Bild 37: Anzeige der SM2-Parameter durch den Performance-Monitor

I/O-Werte

Objekt	Zugriff	Erläuterung
sm2TimeIOStatus	read-only	Status, der dem TIME IO-Puffer zugeordnet ist (data-supported, data-invalid, prg-inactive, no-subsystem, sm2-not-running, unkown)
sm2TimeIOActMach	read-only	Anzahl der aktiven logischen Rechner
sm2TimeIOMachTabNumber	read-only	Anzahl der Einträge in der folgenden Rechnertabelle
sm2TimeIOMachTabIndex	read-only	Der Index startet mit 1 und identifiziert jeden Wert eindeutig. Die Instanz 100 der Objektgruppe TIMEIO beschreibt die Durchschnittswerte aller gelieferten Messwerte und die Summen der verbleibenden I/O-Zähler über alle generierten logischen Maschinen.
sm2TimeIOMachTabIdleTime	read-only	Zeit, in der der logische Rechner nicht aktiv war (nicht angehalten) (Anteil der Zeit in Promille)
sm2TimeIOMachTabTUTime	read-only	TU Time des logischen Rechners (Anteil der Zeit in Promille)
sm2TimeIOMachTabTPRTime	read-only	TPR Time des logischen Rechners als (Anteil der Zeit in Promille)
sm2TimeIOMachTabSIHTime	read-only	SIH Time des logischen Rechners (Anteil der Zeit in Promille)
sm2TimeIOMachTabStopTime	read-only	Stop Time des logischen Rechners als (Anteil der Zeit in Promille)
sm2TimeIOMachTabPagingIO	read-only	Rate des Paging IO bezogen auf den logischen Rechner als (Anzahl der Paging IOs pro Sekunde) * 10
sm2TimeIOMachTabDiskIO	read-only	Rate des Disk IO bezogen auf den logischen Rechner als (Anzahl der Disk IOs pro Sekunde) * 10
sm2TimeIOMachTabTapeIO	read-only	Rate des Tape IO bezogen auf den logischen Rechner als (Anzahl der Tape IOs pro Sekunde) * 10
sm2TimeIOMachTabPrinterIO	read-only	Rate des Drucker IO bezogen auf den logischen Rechner als (Anzahl der Drucker IOs pro Sekunde) * 10
sm2TimeIOMachTabOtherIO	read-only	Rate des sonstigen IO in Bezug auf den logischen Rechner als (Anzahl des sonstigen IO pro Sekunde) * 10



	TU-Time	TPR-Time	SIH-Time	IDLE-Time	Paging-IO	Disk-IO	Tape-IO	Printer-IO	Other-IO
	%	%	%	%	1/sec	1/sec	1/sec	1/sec	1/sec
1	0.0	15.2	4.7	79.9	1.1	104.2	0.0	0.0	25.1
2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
3	5.4	9.0	4.8	80.6	0.8	110.4	0.0	0.0	26.0
4	2.3	11.7	5.0	80.8	1.0	112.9	0.0	0.0	26.2
100	2.5	12.0	4.8	80.4	3.0	327.6	0.0	0.0	77.4

Bild 38: Anzeige von CPU-Auslastung und IO-Rate

Auslastung des Hauptspeichers und des virtuellen Adressraums

Objekt	Zugriff	Erläuterung
sm2MemoryStatus	read-only	Status, der dem Memory-Puffer zugeordnet ist (data-supported, data-invalid, prg-inactive, no-subsystem, sm2-not-running, unkown)
sm2MemorySize	read-only	Gesamtgröße des Hauptspeichers in Kilobyte (KB)
sm2MemoryPageableSize	read-only	Größe des Speichers (pageable) in Kilobyte (KB)
sm2MemoryFreeReadSize	read-only	Größe des freien read-only Speichers (pageable) in Kilobyte (KB)
sm2MemoryFreeReadWriteSize	read-only	Größe des freien read/write Speichers (pageable) in Kilobyte (KB)
sm2MemoryPagingAreaTotal	read-only	Gesamtgröße des Paging-Bereichs (inkl. ES/GS) in Kilobyte (KB)
sm2MemoryPagingAreaESGS	read-only	Größe des ES/GS Paging-Bereichs in Kilobyte (KB)
sm2MemoryPagingAreaFree	read-only	Größe des freien Paging-Bereichs in Kilobyte (KB)
sm2MemoryPageFaults	read-only	Gesamtzahl der Page Faults Interrupts pro Sekunde * 10
sm2MemoryPage1stFaults	read-only	Anzahl der Page Faults Interrupts pro Sekunde für den ersten Zugriff auf eine Page * 10
sm2MemoryPageReclaims	read-only	Anzahl der Page Faults Interrupts pro Sekunde, für die die adressierte Page noch im Speicher vorliegt, * 10
sm2MemoryPageReads	read-only	Anzahl der Pages pro Sekunde, die aus dem Hintergrundspeicher gelesen werden, * 10 (PAGE READS)
sm2MemoryPageWrites	read-only	Anzahl der Pages pro Sekunde, die in den Hintergrundspeicher geschrieben werden, * 10 (PAGE WRITES)
sm2MemoryPageReadESGS	read-only	Anzahl der Pages pro Sekunde, die aus dem erweiterten (ES) oder globalen Speicher (GS) gelesen werden, * 10
sm2MemoryPageWriteESGS	read-only	Anzahl der Pages pro Sekunde, die in den erweiterten (ES) oder globalen Speicher (GS) geschrieben werden, * 10

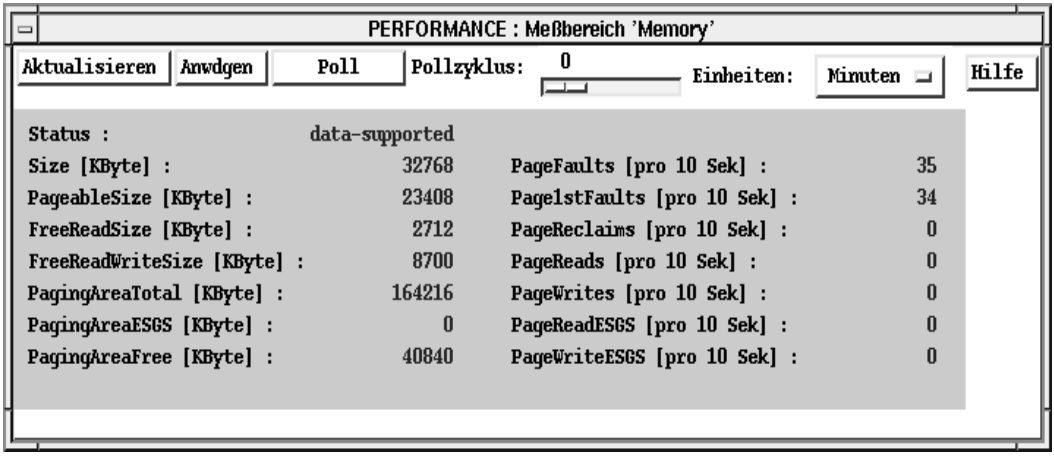


Bild 39: Performance-Monitor: Messbereich „Memory“

Hauptspeicherbelegung duch Standardkategorien von Tasks

Objekt	Zugriff	Erläuterung
sm2CategoryStatus	read-only	Status, der dem Category-Puffer zugeordnet ist (data-supported, data-invalid, prg-inactive, no-subsystem, sm2-not-running, unkown)
sm2CategorySystemTasks	read-only	Durchschnittliche Anzahl der Systemtasks *10
sm2CategoryDialogTasks	read-only	Durchschnittliche Anzahl der Dialogtasks *10
sm2CategoryBatchTasks	read-only	Durchschnittliche Anzahl der Batch-Tasks *10
sm2CategoryTPTasks	read-only	Durchschnittliche Anzahl der TP-Tasks *10

Gerätespezifische Werte

Objektname	Zugriff	Erläuterung
sm2SDeviceStatus	read-only	Status, der dem Device-Puffer zugeoednet ist.
sm2SDeviceRealNumber	read-only	Tatsächliche Anzahl der verfügbaren Geräte
sm2SDeviceTabNumber	read-only	Anzahl der Einträge in der folgenden Tabelle; derzeit sind maximal 10 Einträge möglich.
sm2SDeviceTabIndex	read-only	Eindeutige Identifikation der einzelnen Einträge dieser Tabelle
sm2SDeviceTabVSN	read-only	Volume Sequence Number (VSN; Volume-Name) Die Instanzen der Objektgruppe DEVICES sind zu jedem Messzeitpunkt nach der Anzahl der IO-Operationen sortiert. Die erste Instanz entspricht dem Gerät mit den meisten IO-Operationen im Messintervall.
sm2SDeviceTabMnemonic	read-only	Mnemonischer Gerätename
sm2SDeviceTabType	read-only	Gerätetyp (mit Makro NKGTYPE)
sm2SDeviceTabIO	read-only	Anzahl der IO-Operationen, die physisch pro Sekunde durchgeführt werden, * 10
sm2SDeviceTabBusyDms	read-only	Geräteaktivität (ohne Paging) (Anteil der Zeit in Promille)
sm2SDeviceTabBusyPaging	read-only	Geräteaktivität auf Grund des Pagings (Anteil der Zeit in Promille)

Applikationsspezifische Daten von *open*UTM-Anwendungen

Objekt	Zugriff	Erläuterung
sm2UTMStatus	read-only	Status, der dem UTM-Puffer zugeordnet ist
sm2UTMTabNumber	read-only	Anzahl der Einträge in der folgenden Tabelle
sm2UTMTabIndex	read-only	Eindeutige Identifikation der einzelnen Einträge dieser Tabelle Die Instanzen der Objektgruppe UTM sind zu jedem Messzeitpunkt nach der Anzahl der Dialogschritte sortiert. Die erste Instanz entspricht dem Gerät mit den meisten Dialogschritten im Messintervall.
sm2UTMTabApplName	read-only	Name der UTM-Anwendung
sm2UTMTabUTMVersion	read-only	Version des Subsystems. Format: Vnn.nAnn
sm2UTMTabApplMode	read-only	UTM-Anwendungsmodus
sm2UTMTabTasksRunning	read-only	Anzahl der Tasks, die für diese UTM-Anwendung laufen
sm2UTMTabMaxAsyncTasks	read-only	Maximal Anzahl der Tasks für die asynchrone Verarbeitung
sm2UTMTabConnectedUsers	read-only	Anzahl der derzeit angeschlossenen Benutzer
sm2UTMTabCurrConvDial	read-only	Anzahl der aktiven Dialogkonversationen
sm2UTMTabCurrConvAsync	read-only	Anzahl der aktiven asynchronen Konversationen
sm2UTMTabWaitingATACS	read-only	Anzahl der wartenden asynchronen Transaktionen, die gepuffert, aber noch nicht verarbeitet sind
sm2UTMTabCacheHitRate	read-only	UTM Cache-Trefferquote (Angabe in Promille)
sm2UTMTabFreePagePool	read-only	freie Pages im UTM Pagepool *10 (Angabe in
sm2UTMTabDialTACS	read-only	Anzahl der (beendeten) Dialogtransaktionen pro Sekunde *10
sm2UTMTabAsyncTACS	read-only	Anzahl der (beendeten) asynchronen Transaktionen (ATACS) pro Sekunde *10
sm2UTMTabDialTotalTime	read-only	Durchschnittszeit eines Dialogschritts (UTM-Antwortzeit) in Sekunden *10
sm2UTMTabDialTotalTimeDB	read-only	Durchschnittszeit eines Dialogschritts (UTM-Antwortzeit) in Sekunden *10. Es werden nur Dialogschritte mit Datenbankzugriff berücksichtigt.

Objekt	Zugriff	Erläuterung
sm2UTMTabDialDBTime	read-only	Durchschnittszeit pro Dialogschritt in Sekunden, die UTM auf Datenbankantworten wartet, *10. Es werden nur Dialogschritte mit Datenbankzugriff berücksichtigt.
sm2UTMTabDialDBCall	read-only	Durchschnittliche Anzahl der Datenbankaufrufe pro Dialogschritt. Es werden nur Dialogschritte mit Datenbankzugriff berücksichtigt.
sm2UTMTabDialDBCpuTime	read-only	Durchschnittliche CPU-Zeit in Sekunden pro Dialogschritt für die Datenbankverarbeitung *10. Es werden nur Dialogschritte mit Datenbankzugriff berücksichtigt.
sm2UTMTabDialDBIO	read-only	Durchschnittliche Anzahl der Datenbank-IOs pro Dialogschritt. Es werden nur Dialogschritte mit Datenbankzugriff berücksichtigt.
sm2UTMTabDialUTMCpuTime	read-only	Durchschnittliche CPU-Zeit in Sekunden pro Dialogschritt, die von UTM-Tasks benötigt wird, *10
sm2UTMTabDialUTMIO	read-only	Durchschnittliche Anzahl der IOs durch UTM-Tasks pro Dialogschritt
sm2UTMTabAsyncTotalTime	read-only	Durchschnittszeit einer asynchronen Konversation (UTM-Antwortzeit) in Sekunden *10
sm2UTMTabAsyncTotalTimeDB	read-only	Durchschnittszeit einer asynchronen Konversation in Sekunden *10. Es werden nur asynchrone Konversationen mit Datenbankzugriff berücksichtigt.
sm2UTMTabAsyncDBTime	read-only	Durchschnittszeit pro asynchroner Konversation in Sekunden, die UTM auf Datenbankantworten wartet, *10. Es werden nur asynchrone Konversationen mit Datenbankzugriff berücksichtigt.
sm2UTMTabAsyncDBCall	read-only	Durchschnittliche Anzahl der Datenbankaufrufe pro asynchroner Konversation. Es werden nur asynchrone Konversationen mit Datenbankzugriff berücksichtigt.
sm2UTMTabAsyncDBCpuTime	read-only	Durchschnittliche CPU-Zeit in Sekunden pro asynchroner Konversation für die Datenbankverarbeitung *10. Es werden nur asynchrone Konversationen mit Datenbankzugriff berücksichtigt.

Objekt	Zugriff	Erläuterung
sm2UTMTabAsyncDBIO	read-only	Durchschnittliche Anzahl der Datenbank-IOs pro asynchroner Konversation. Es werden nur asynchrone Konversationen mit Datenbankzugriff berücksichtigt.
sm2UTMTabAsyncUTMCpuTime	read-only	Durchschnittliche CPU-Zeit in Sekunden pro asynchroner Konversation, die für UTM-Tasks benötigt wird, *10
sm2UTMTabAsyncUTMIO	read-only	Durchschnittliche Anzahl der IOs, die von UTM-Tasks pro asynchroner Konversation durchgeführt werden

Verbrauchswerte einzelner Tasks

Objekt	Zugriff	Erläuterung
sm2PerTaskStatus	read-only	Status, der dem Periodic Task-Puffer zugeordnet ist (data-supported, data-invalid, prg-inactive, no-subsystem, sm2-not-running, unkown)
sm2PerTaskRealNumber	read-only	Tatsächliche Anzahl der verfügbaren Tasks
sm2PerTaskTabNumber	read-only	Anzahl der Einträge in der folgenden Tabelle; derzeit sind maximal 10 Einträge möglich
sm2PerTaskTabIndex *	read-only	Eindeutige Identifikation der einzelnen Einträge dieser Tabelle. Die Instanzen der Objektgruppe PERTASK sind zu jedem Messzeitpunkt nach dem CPU-Verbrauch sortiert. Die erste Instanz entspricht dem Gerät mit dem höchsten CPU-Verbrauch im Messintervall.
sm2PerTaskTabTSN	read-only	Task Sequence Number (TSN)
sm2PerTaskTabUserID	read-only	Benutzer-ID, unter der der Task läuft
sm2PerTaskTabJobName	read-only	Auftragsname
sm2PerTaskTabType	read-only	Tasktyp (no-data, system, dialog, batch, tp)
sm2PerTaskTabCPU	read-only	CPU-Nutzung (Anteil der Zeit in Promille)
sm2PerTaskTabIO	read-only	Anzahl der IO-Operationen pro Sekunde * 10
sm2PerTaskTabUPG	read-only	Durchschnittliche Anzahl der Used Pages
sm2PerTaskTabServiceUnits	read-only	Anzahl der pro Sekunde genutzten Service Units * 10
sm2PerTaskTabPageRead	read-only	Anzahl der pro Sekunde gelesenen Pages * 10

8 SNMP-Management zur Überwachung von *open*UTM und *open*UTM-Anwendungen

Der *open*UTM-Subagent SSA-OUTM-BS2 bietet folgende Leistungen:

- Überwachung und Steuerung ausgewählter *open*UTM-Anwendungen
- Informationen über Systemparameter, physikalische und logische Terminals, Terminal-Pools, Transaktionscodes, Transaktionsklassen, Benutzerdaten, Verbindungen und Statistikdaten
- Änderung von Anwendungseigenschaften und Systemparametern
- Sperren bzw. Entsperren von UTM-Datenstationen
- Beenden einer *open*UTM-Anwendung

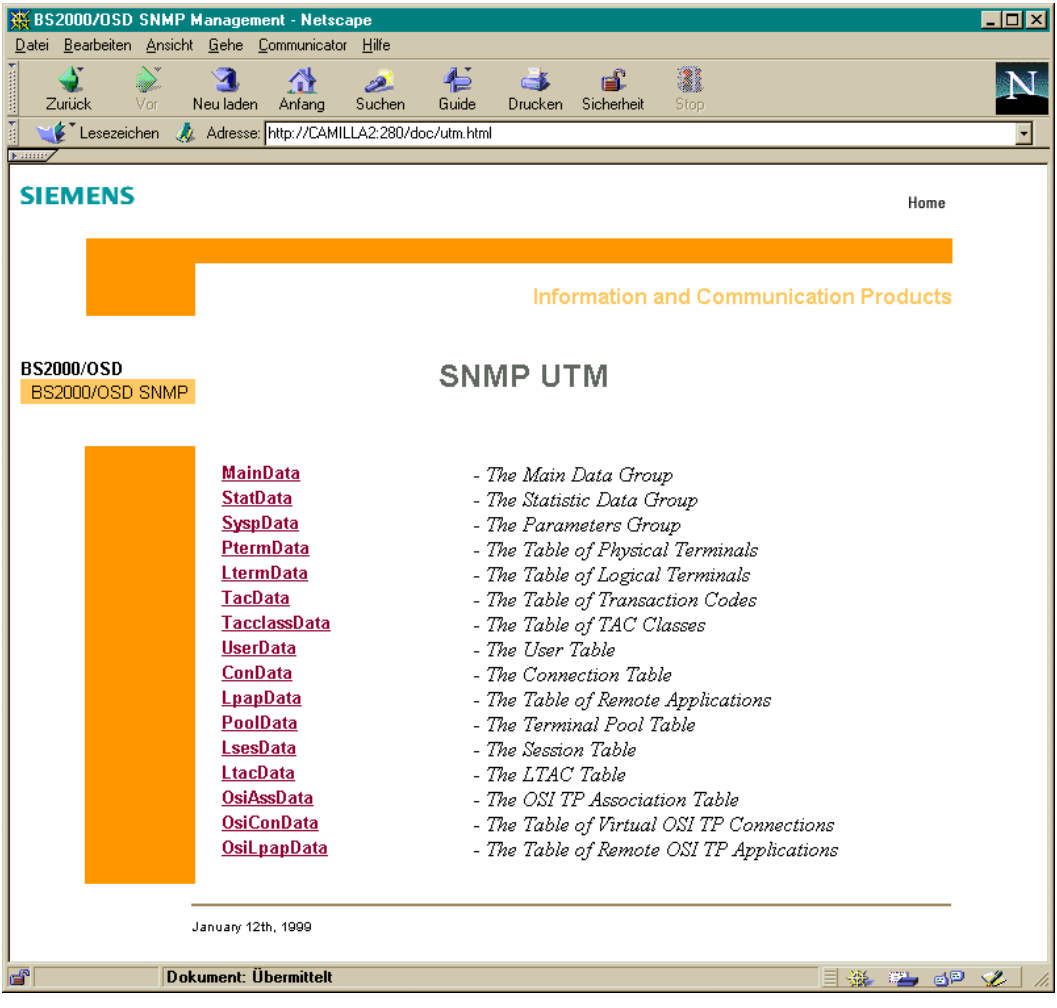


Bild 40: *open*UTM-Subagent: Übersicht

Globale Daten des *open*UTM-Subagenten

Objektname	Zugriff	Erläuterung
utmMainApplName	read-write	Name der ausgewählten UTM-Anwendung
utmMainBCAMAppl	read-write	BCAM-Anwendungsname der ausgewählten UTM-Anwendung
utmMainUTMversion	read-only	UTM-Version
utmMainApplStartStop	read-write	Read: Status der ausgewählten UTM-Anwendung; Write: Beenden (STOP) der ausgewählten UTM-Anwendung (start, stop, undefined)
utmMainSubagentVersion	read-only	Versionsnummer des SNMP-Subagenten und Art des Betriebssystems

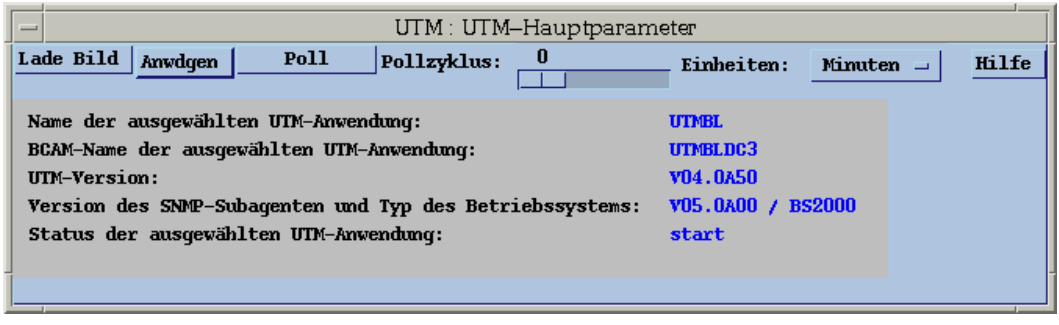


Bild 41: *open*UTM-Hauptparameter

Allgemeine Statistik-Informationen

Objektname	Zugriff	Erläuterung
utmStatStartDateAndTime	read-only	Datum und Uhrzeit des letzten Kaltstarts der Anwendung (im DateAndTime-Format)
utmStatStartDateAndTimeString	read-only	Datum und Uhrzeit des letzten Kaltstarts der Anwendung (abdruckbar)
utmStatTermInMsgs	read-only	Anzahl der Meldungen, die seit der letzten vollen Stunde an allen Terminals eingegeben wurden
utmStatTermOutMsgs	read-only	Anzahl der Meldungen, die seit der letzten vollen Stunde an allen Terminals abgesetzt wurden
utmStatCurrTasks	read-only	Anzahl der aktuellen Tasks in dieser Anwendung
utmStatConnUsers	read-only	Anzahl der angeschlossenen Benutzer
utmStatOpenDialConv	read-only	Anzahl der aktiven Dialogkonversationen
utmStatOpenAsynConv	read-only	Anzahl der aktiven asynchronen Konversationen
utmStatDialTAperSec	read-only	Anzahl der Dialogtransaktionen pro Sekunde
utmStatAsynTAperSec	read-only	Anzahl der asynchronen Transaktionen pro Sekunde

Objektname	Zugriff	Erläuterung
utmStatDialStepSec	read-only	Anzahl der Dialogschritte pro Sekunde
utmStatMaxPoolSize	read-only	Maximale Belegung des Pagepools in Prozent
utmStatActPoolSize	read-only	Aktuelle Belegung des Pagepools in Prozent
utmStatAvgPoolSize	read-only	Durchschnittliche Belegung des Pagepools in Prozent
utmStatCacheHitRate	read-only	Trefferquote in Prozent beim Durchsuchen einer Cache Page
utmStatCacheWaits	read-only	Prozentsatz der Cache-Pufferanforderungen, die zu Wartezeiten führen
utmStatUnprocAtacs	read-only	Anzahl der asynchronen Transaktionsaufträge, die noch nicht verarbeitet sind
utmStatUnprocPrints	read-only	Anzahl der wartenden Druckaufträge
utmStatWaitDPUTs	read-only	Anzahl der offenen zeitgesteuerten Aufträge
utmStatAbTermConv	read-only	Anzahl der abnormal beendeten Konversationen
utmStatResourcWaits	read-only	Beziehung zwischen der Anzahl der wartenden Ressourcenanforderungen und der Gesamtzahl der Ressourcenanforderungen (Angabe in Promille)
utmStatDeadlocks	read-only	Anzahl der erkannten und beseitigten Deadlocks
utmStatPeriodWrites	read-only	Anzahl der periodischen Schreiboperationen
utmStatPagesPWrite	read-only	Anzahl der 2 KB Pages, die durchschnittlich durch eine periodische Schreiboperation gesichert werden
utmStatLogWrites	read-only	Anzahl der Schreibaufträge in die Benutzerprotokolldatei seit der letzten vollen Stunde
utmStatActJR	read-only	Aktuelle Anzahl der auftragsempfangenden Konversationen, die gleichzeitig adressiert werden
utmStatMaxJR	read-only	Maximale Anzahl der auftragsempfangenden Konversationen, die seit der KDCDEF-Generierung gleichzeitig adressiert wurden

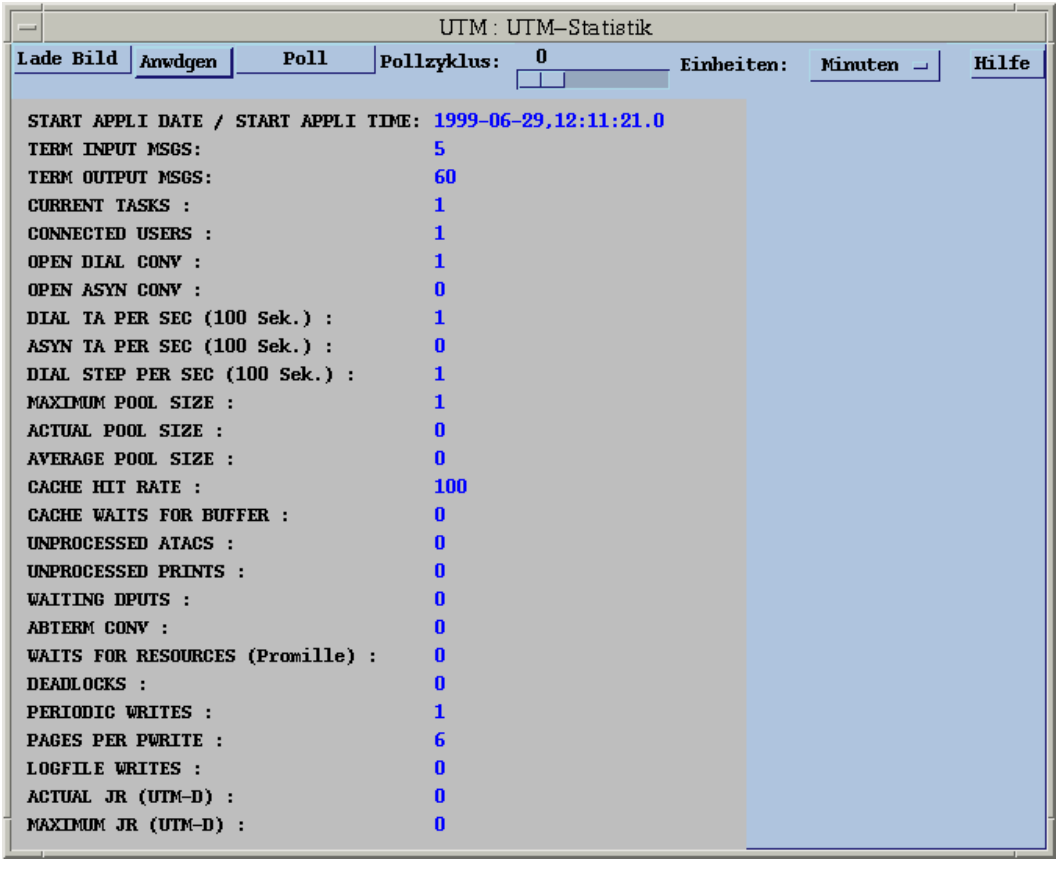


Bild 42: *open*UTM-Statistik

Systemparameter

Objektname	Zugriff	Erläuterung
utmSyspAccount	read-write	UTM-Accounting ist entweder aktiviert (ON) oder nicht aktiviert (OFF) (ON, OFF)
utmSyspCalcAccount	read-write	Die Berechnungsphase für das UTM-Accounting ist entweder aktiviert (ON) oder nicht aktiviert (OFF) (ON, OFF)
utmSyspSM2	read-write	Die Lieferung von Daten an SM2 ist entweder aktiviert (ON) oder nicht aktiviert (OFF) (ON, OFF)
utmSyspKDCMON	read-write	KDCMON ist entweder aktiviert (ON) oder nicht aktiviert (OFF) (ON, OFF)
utmSyspTestmode	read-write	Der Testmodus ist entweder aktiviert (ON) oder nicht aktiviert (OFF) (ON, OFF)
utmSyspMaxPagRate	read-write	Prozentsatz der Cache Pages, die bei einem Engpass nach KDCFILE geschrieben werden
utmSyspProgFGG	read-write	Read: Nummer der aktuellen Dateigenerierung des Programms Write: -1 => alt (Laden einer niedrigeren Programmgenerierung) +1 => neu (Laden einer höheren Programmgenerierung)
utmSyspTermWait	read-write	Maximal verstrichene Zeit (in Sekunden) zwischen Terminalausgabe und der folgenden Eingabe des Terminalbenutzers während einer Konversation aus mehreren Schritten
utmSyspUsLogFGG	read-write	Nummer der aktuellen Dateigenerierung der Benutzerprotokolldatei
utmSyspResWaitTA	read-write	Maximale Wartezeit in Sekunden für eine Ressource, die von einer anderen Transaktion gesperrt wurde
utmSyspMaxTasks	read-write	Maximale Anzahl der Tasks, die in dieser Anwendung zulässig sind
utmSyspResWaitPr	read-write	Maximale Wartezeit in Sekunden für eine Ressource, die von einem anderen Prozess gesperrt wurde
utmSyspCurrTasks	read-only	Anzahl der aktuellen Arbeitsprozesse der Anwendung

Objektname	Zugriff	Erläuterung
utmSyspConRTime	read-write	Zyklus in Minuten, in dem *open*UTM die Erstellung einer logischen Verbindung erneut versucht
utmSyspMaxAsynTasks	read-write	Maximale Anzahl der Tasks für asynchrone Programme
utmSyspLogAckwait	read-only	Maximale Wartezeit in Sekunden für eine Druck- oder eine Transportbestätigung
utmSyspPTCTime	read-write	Maximale Wartezeit in Sekunden einer auftragsempfangenden Konversation in PTC auf die Bestätigung
utmSyspConcTime	read-write	Zeit in Sekunden, die für die Erstellung einer Session oder eine Zuordnung zulässig ist
utmSyspPGWTTime	read-write	Maximale Zeit in Sekunden, die für den KDCS-Aufruf PGWT zulässig ist
utmSyspTasksWaitPGWT	read-only	Aktuelle Anzahl der Tasks, die in einem Wartestatus sind (PGWT-Aufruf)
utmSyspTasksinPGWT	read-write	Maximale Anzahl der Tasks für PGWT-Aufrufe

Tabelle der physischen Datenstationen

Objektname	Zugriff	Erläuterung
utmPtermTabNum	read-only	Die Anzahl der Einträge in der Tabelle der physischen Datenstationen
utmPtermIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmPtermTabNum)
utmPtermName	read-only	Name des ausgewählten physischen Terminals
utmPtermProname	read-write	Prozessorname des physischen Terminals (oder Blank für lokale Geräte)
utmPtermLterm	read-write	Name des logischen UTM-Terminals, das zum physischen Terminal gehört
utmPtermBCAMAppl	read-write	BCAM-Name der UTM-Anwendung
utmPtermPtyp	read-only	Partnertyp des UTM-Terminals
utmPtermStatus	read-write	Das UTM-Terminal ist entweder gesperrt (OFF) oder nicht gesperrt (ON) (ON, OFF)
utmPtermConnected	read-write	Das UTM-Terminal ist entweder verbunden (Y), nicht verbunden (N) oder wartet auf eine Verbindung (yes, no, waiting)
utmPtermConnectStatus	read-write	Status = 'A' bedeutet: automatische Verbindung beim Start der Anwendung, Status = 'P' bedeutet: Terminalpool-Verbindung (automaticCon, terminalPool, na)
utmPtermConnectForced	read-only	Wie bei der automatischen Verbindung, jedoch wird außerdem eine bestehende Verbindung zum Terminal zwangsweise unterbrochen (yes, no)
utmPtermConnectMultiplexed	read-only	Das Terminal verwendet eine Multiplex-Verbindung, oder es verwendet keine Multiplex-Verbindung (yes, no)
utmPtermConTime	read-only	Dauer der bestehenden Verbindung in Minuten
utmPtermLett	read-only	Anzahl für den Meldungs-Input und -Output am Terminal seit dem Start der Anwendung
utmPtermConb	read-only	Anzahl der Zusammenbrüche der physischen oder virtuellen Verbindung zwischen diesem Terminal und der Anwendung seit dem Start der Anwendung

Tabelle der logischen Datenstationen

Objektname	Zugriff	Erläuterung
utmLtermTabNum	read-only	Die Anzahl der Einträge in der Tabelle der logischen Datenstationen
utmLtermIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmLtermTabNum)
utmLtermName	read-only	Name des ausgewählten logischen UTM-Terminals
utmLtermPterm	read-write	Name des physischen Terminals, das zum logischen UTM-Terminal gehört
utmLtermUser	read-only	Kennung des Benutzers, der derzeit mit dem logischen UTM-Terminal verbunden ist
utmLtermKset	read-only	Key Set des UTM-Terminals
utmLtermLock	read-only	Sperre des UTM-Terminals
utmLtermUsageType	read-only	Typ ist 'D' (Dialogterminal) oder 'O' (Output-Terminal) (dialog, output)
utmLtermUsageBundle	read-only	Das UTM-Terminal ist ein Pool ('Bundle'), wenn 'B' gesetzt ist (yes, no)
utmLtermUsageTermPool	read-only	Das UTM-Terminal wird für einen Terminalpool generiert, wenn 'P' gesetzt ist (yes, no)
utmLtermStatus	read-write	Der Status des UTM-Terminals ist entweder 'ON' oder 'OFF' (ON, OFF)
utmLtermOutq	read-only	Anzahl der Meldungen, die noch an dieses Terminal ausgegeben werden müssen
utmLtermInCnt	read-only	Anzahl der Meldungen, die seit dem Start der Anwendung an diesem Terminal eingegeben wurden; bei Druckern ist es die Anzahl der Druckbestätigungen
utmLtermSecCnt	read-only	Anzahl der Sicherheitsverletzungen an diesem logischen Terminal seit dem Start der Anwendung

Tabelle der Transaktionscodes

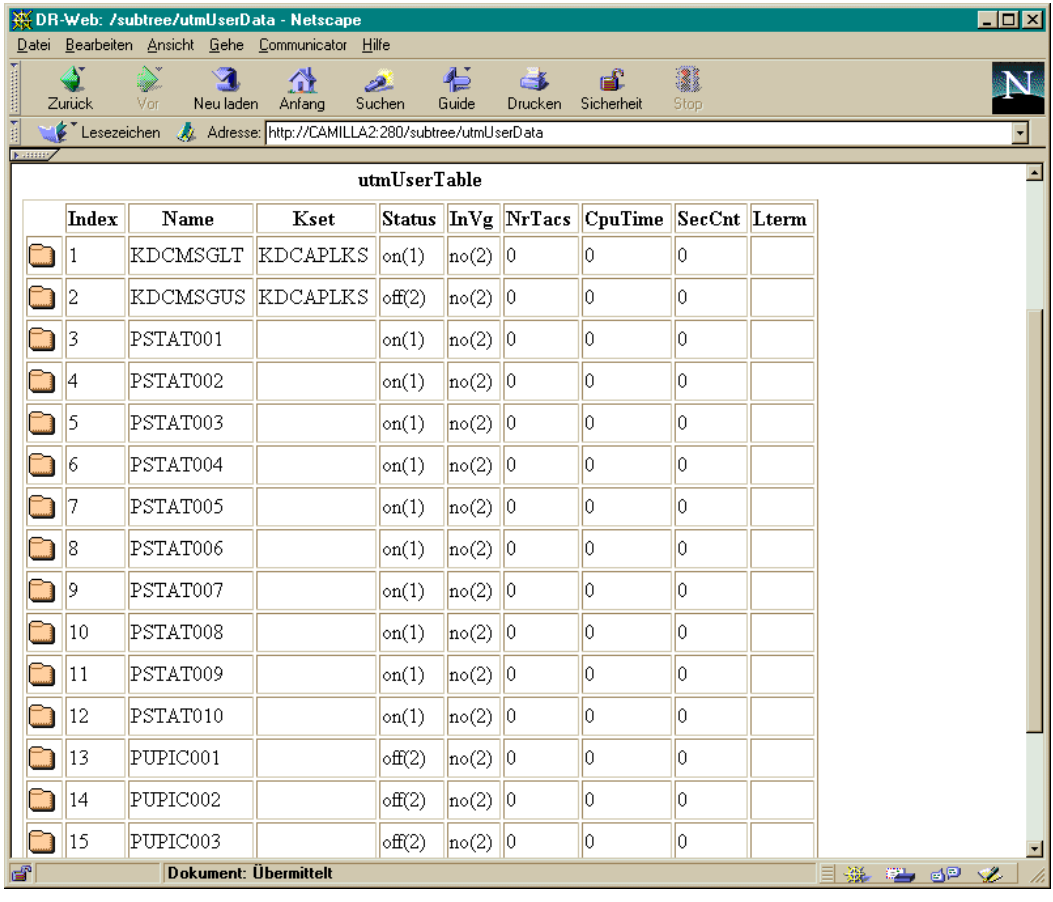
Objektname	Zugriff	Erläuterung
utmTacTabNum	read-only	Die Anzahl der Einträge in der Tabelle der Transaktionscodes
utmTacIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmTacTabNum)
utmTacName	read-only	Name des ausgewählten Transaktionscodes
utmTacLock	read-only	Sperre des Transaktionscodes (0 bis 255)
utmTacStatus	read-write	Der Status des Transaktions codes ist entweder 'ON', 'OFF' oder 'HALT' (ON,OFF, HALT)
utmTacTcl	read-only	TAC-Klasse dieses Transaktionscodes
utmTacInq	read-only	Anzahl der Meldungen, die noch von dem Programmeinheitendurchlauf verarbeitet werden müssen, der vom Transaktionscode angegeben ist
utmTacUsed	read-only	Anzahl der Programmeinheitendurchläufe mit diesem Transaktionscode, die seit dem Erststart der Anwendung verarbeitet wurden (nur für asynchrone TAC's)
utmTacError	read-only	Anzahl der Programmeinheitendurchläufe mit diesem Transaktionscode, die seit dem Erststart der Anwendung mit Fehlern beendet wurden
utmTacDbcnt	read-only	Mittlere Anzahl der Datenbankaufrufe der zugehörigen Teilprogrammläufe. Immer '0', wenn die XA-Schnittstelle verwendet wird
utmTacElap	read-only	Durchschnittliche Laufzeit in Millisekunden für die Programmeinheiten mit diesem Transaktionscode
utmTacDbElap	read-only	Durchschnittliche Zeit in Millisekunden für die Verarbeitung der Datenbankaufrufe in den Programmeinheitendurchläufen mit diesem Transaktionscode
utmTacCpu	read-only	Durchschnittliche CPU-Zeit in Millisekunden für den UTM-Programmdurchlauf für die Verarbeitung dieses Transaktionscodes

Tabelle der TAC-Klassen

Objektname	Zugriff	Erläuterung
utmTacclassNumber	read-only	TAC-Klassennummer
utmTacclassTasks	read-write	Maximale Anzahl der Tasks, die derzeit für eine bestimmte TAC-Klasse arbeiten können
utmTacclassWtMesg	read-only	Anzahl der Meldungen für eine bestimmte TAC-Klasse, die derzeit gepuffert und noch nicht verarbeitet sind
utmTacclassAvgWtTime	read-only	Durchschnittliche Wartezeit in Millisekunden für alle Dialog-TAC-Klassen (1 bis 8)
utmTacclassPGWT	read-only	Gibt an, ob Programmeinheiten mit einem PGWT-Aufruf in einer bestimmten TAC-Klasse ablaufen können (yes, no)

Benutzertabelle

Objektname	Zugriff	Erläuterung
utmUserTabNum	read-only	Die Anzahl der Einträge in der Tabelle der *open*UTM-Benutzer
utmUserIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmUserTabNum)
utmUserName	read-only	Name des Benutzers
utmUserKset	read-only	Key Set, der der Benutzerkennung zugeordnet ist
utmUserStatus	read-write	Die Kennung ist entweder gesperrt (OFF) oder nicht gesperrt (ON) (ON, OFF)
utmUserInVg	read-only	Stellt fest, ob der Benutzer derzeit eine Konversation verarbeitet (yes, no)
utmUserNrTacs	read-only	Anzahl der Transaktionsaufträge, die vom Benutzer seit dem Erststart der Anwendung eingegeben wurden
utmUserCpuTime	read-only	Anzahl der Sekunden, die für die Verarbeitung der Transaktionsaufträge des Benutzers aufgewandt wurden (ohne Datenbankaufrufe)
utmUserSecCnt	read-only	Anzahl der Sicherheitsverletzungen für die Kennung seit dem Start der Anwendung
utmUserLterm	read-only	Name des logischen Terminals, über das sich der Benutzer der UTM-Anwendung angemeldet hat



utmUserTable

	Index	Name	Kset	Status	InVg	NrTacs	CpuTime	SecCnt	Lterm
	1	KDCMSGLT	KDCAPLKS	on(1)	no(2)	0	0	0	
	2	KDCMSGUS	KDCAPLKS	off(2)	no(2)	0	0	0	
	3	PSTAT001		on(1)	no(2)	0	0	0	
	4	PSTAT002		on(1)	no(2)	0	0	0	
	5	PSTAT003		on(1)	no(2)	0	0	0	
	6	PSTAT004		on(1)	no(2)	0	0	0	
	7	PSTAT005		on(1)	no(2)	0	0	0	
	8	PSTAT006		on(1)	no(2)	0	0	0	
	9	PSTAT007		on(1)	no(2)	0	0	0	
	10	PSTAT008		on(1)	no(2)	0	0	0	
	11	PSTAT009		on(1)	no(2)	0	0	0	
	12	PSTAT010		on(1)	no(2)	0	0	0	
	13	PUPIC001		off(2)	no(2)	0	0	0	
	14	PUPIC002		off(2)	no(2)	0	0	0	
	15	PUPIC003		off(2)	no(2)	0	0	0	

Bild 43: Tabelle der *open*UTM-Benutzer

Tabelle der logischen Verbindungen für die verteilte Verarbeitung über LU6.1

Objektname	Zugriff	Erläuterung
utmConTabNum	read-only	Die Anzahl der Einträge in der Tabelle der Verbindungen
utmConIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmConTabNum)
utmConName	read-only	Name der Verbindung
utmConProname	read-only	Prozessorname
utmConLpap	read-only	Name der fernen Anwendung in der lokalen Anwendung
utmConBcamAppl	read-only	BCAM-Name der *open*UTM-Anwendung
utmConStatus	read-write	Eine Verbindung zur fernen Anwendung besteht bereits oder kann eingerichtet werden (ON) bzw. kann nicht eingerichtet werden (OFF) (ON, OFF)
utmConConnected	read-write	Ein Verbindung ist entweder eingerichtet (yes) oder nicht (no) oder UTM versucht gerade eine Verbindung einzurichten (waiting) (yes, no, waiting)
utmConConnectStatus	read-write	Ein 'A' bedeutet eine automatische Verbindungseinrichtung beim Start der Anwendung (automaticCon, noAutomaticCon)
utmConConTime	read-only	Dauer der Verbindung in Minuten
utmConLett	read-only	Anzahl für den Meldungs-Input und -Output über die Verbindung
utmConConb	read-only	Anzahl der Zusammenbrüche der Verbindung seit dem Start der Anwendung

Tabelle der fernen Anwendungen, mit denen über das LU6.1-Protokoll kommuniziert wird

Die Kommunikation mit fernen Anwendungen erfolgt über das LU6.1-Protokoll.

Objektname	Zugriff	Erläuterung
utmLpapTabNum	read-only	Die Anzahl der Einträge in der Tabelle der über LU6.1 kommunizierenden Applikationen
utmLpapIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmLpapTabNum)
utmLpapName	read-only	Name des LPAP
utmLpapKset	read-only	Key Set der fernen Anwendung
utmLpapStatus	read-write	Eine Verbindung zur fernen Anwendung besteht bereits oder kann eingerichtet werden (ON) bzw. kann nicht eingerichtet werden (OFF) (ON, OFF)
utmLpapQuiet	read-write	Ein 'Q' steht für 'quiet'; d.h., dass keine weiteren Dialogaufträge für die ferne Anwendung angenommen werden (yes, no)
utmLpapOutq	read-only	Anzahl der Meldungen, die noch an diese ferne Anwendung gesendet werden müssen
utmLpapIdleTime	read-write	Zeit für die Überwachung des Leerstatus einer Session in Sekunden

Tabelle der Terminal-Pools

Objektname	Zugriff	Erläuterung
utmPoolTabNum	read-only	Die Anzahl der Einträge in der Tabelle der Terminalpools
utmPoolIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmPoolTabNum)
utmPoolProname	read-only	Prozessorname des Terminalpools
utmPoolBcamAppl	read-only	Name des Zugangspunkts für das Transportsystem (für diesen Terminalpool generiert)
utmPoolPtype	read-only	Physischer Terminaltyp der Terminals, die über diesen Pool mit der Anwendung verbunden werden können
utmPoolStations	read-only	Generierte maximale Anzahl der Terminals, die über diesen Pool mit der Anwendung verbunden werden können
utmPoolStatusOn	read-write	Maximale Anzahl der Terminals mit STATUS=ON
utmPoolActCon	read-only	Anzahl der Terminals, die über diesen Pool mit der Anwendung verbunden sind
utmPoolMaxCon	read-only	Maximale Anzahl der Terminals, die während dieses Anwendungsdurchlaufs über diesen Terminalpool gleichzeitig mit der Anwendung verbunden waren
utmPoolKset	read-only	Key Set der Terminals dieses Terminalpools
utmPoolLock	read-only	Sperre des Terminals dieses Terminalpools Zahlenwert zwischen 1 und dem in der Anwendung erlaubten Maximalwert (255) Standard: 0 (keine Sperre)

Informationen über lokale Sessions (nur bei VTV über das LU6.1-Protokoll)

Objektname	Zugriff	Erläuterung
utmLsesTabNum	read-only	Die Anzahl der Einträge in der Tabelle der LU6.1-Sessions
utmLsesIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmLsesTabNum)
utmLsesName	read-only	Name der Session in der lokalen Anwendung
utmLsesRses	read-only	Name der Session in der fernen Anwendung
utmLsesLpap	read-only	Name der fernen Anwendung, für die die Session generiert wird
utmLsesCon	read-only	Bezeichnet die Transportverbindung, die für die Session eingerichtet wird
utmLsesProname	read-only	Prozessorname
utmLsesBcamAppl	read-only	Bezeichnet die Transportverbindung, die für die Session eingerichtet wird
utmLsesAgUser	read-only	Name des auftragserteilenden Partners, für den die Session reserviert wurde

Tabelle der Transaktionscodes für ferne Anwendungen

Objektname	Zugriff	Erläuterung
utmLtacTabNum	read-only	Die Anzahl der Einträge in der Tabelle der LTACs
utmLtacIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmLtacTabNum)
utmLtacName	read-only	Name des LTAC
utmLtacLock	read-only	Sperre der fernen Konversation
utmLtacStatus	read-write	Der LTAC-Transaktionscode ist entweder gesperrt (OFF) oder nicht gesperrt (ON) (ON, OFF)
utmLtacRtac	read-only	Name des Transaktionscodes in einer fernen Anwendung
utmLtacLpap	read-only	Name der fernen Anwendung in der lokalen Anwendung
utmLtacAccessWait	read-write	Zeit in Sekunden, die auf die Reservierung einer Session oder Zuordnung gewartet wird
utmLtacReplyWait	read-write	Zeit in Sekunden, die auf die Reaktion eines empfangenden Partners gewartet wird
utmLtacUsed	read-only	Anzahl der Aufträge, die seit dem Start der Anwendung für diesen LTAC abgesetzt wurde

Tabelle der OSI-TP-Associations

Objektname	Zugriff	Erläuterung
utmOsiAssTabNum	read-only	Die Anzahl der Einträge in der Tabelle der OSI-TP-Zuordnungen (Association)
utmOsiAssIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmOsiAssTabNum)
utmOsiAssName	read-only	Name der OSI-Zuordnung
utmOsiAssOsiLpap	read-only	Name der fernen Anwendung in der lokalen Anwendung, für die die Zuordnung generiert wird
utmOsiAssOsiCon	read-only	Name der Verbindung, die für die Zuordnung zur fernen Anwendung eingerichtet wird
utmOsiAssAgUser	read-only	Name des Auftragserteilers, für den die Zuordnung reserviert ist. Ab *open*UTM V4.0 wird für dieses Objekt kein gültiger Wert geliefert, sondern *not supported* ausgegeben.
utmOsiAssConTime	read-only	Dauer der Verbindung in Minuten
utmOsiAssLetters	read-only	Anzahl für den Meldungs-Input und -Output seit dem Start der Anwendung. Ab *open*UTM V4.0 wird für dieses Objekt kein gültiger Wert geliefert, sondern *not supported* ausgegeben.

Informationen über logische Verbindungen zur verteilten Verarbeitung über das OSI-TP-Protokoll

Objektname	Zugriff	Erläuterung
utmOsiConTabNum	read-only	Die Anzahl der Einträge in der Tabelle der OSI-Verbindungen
utmOsiConIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmOsiConTabNum)
utmOsiConName	read-only	Name der OSI-Verbindung
utmOsiConOsiLpap	read-only	Name der fernen Anwendung in der lokalen Anwendung
utmOsiConTsel	read-only	BCAM-Anwendungsname des fernen OSI-TP-Partners (Transportauswahl)
utmOsiConNsel	read-only	Name des Prozessors, auf dem der OSI-TP-Partner angeordnet ist (Netzauswahl)
utmOsiConAccPnt	read-only	Lokaler Name eines Zugangspunkts, über den die Kommunikation mit den OSI-TP-Partnern stattfindet
utmOsiConActive	read-write	Die Transportverbindung kann entweder verwendet werden (YES), oder sie ist als Ersatzverbindung reserviert (NO) (yes, no)

Informationen über ferne Partneranwendungen

Objektname	Zugriff	Erläuterung
utmOsiLpapTabNum	read-only	Die Anzahl der Einträge in der Tabelle der OSI-LPAPs
utmOsiLpapIndex	read-only	Ein eindeutiger Wert für jeden Eintrag (Wertebereich zwischen 1 und dem Wert von utmOsiLpapTabNum)
utmOsiLpapName	read-only	Name des OSI LPAP
utmOsiLpapKset	read-only	Key Set der fernen Anwendung
utmOsiLpapStatus	read-write	Eine Verbindung zur fernen Anwendung besteht bereits oder kann eingerichtet werden (ON) bzw. kann nicht eingerichtet werden (OFF) (ON, OFF)
utmOsiLpapQuiet	read-write	Ein 'Q' steht für 'quiet'; d.h., dass keine weiteren Dialogaufträge für die ferne Anwendung angenommen werden (yes, no)
utmOsiLpapOutq	read-only	Anzahl der Meldungen, die noch an diese ferne Anwendung gesandt werden müssen
utmOsiLpapIdleTime	read-write	Zeit für die Überwachung des Leerstatus einer Session
utmOsiLpapOsiCon	read-only	Name der Transportverbindung, die für die Kommunikation mit dem OSI-TP-Partner verwendet wird
utmOsiLpapAssoc	read-only	Anzahl der parallelen Verbindungen, die für den OSI-TP-Partner generiert werden
utmOsiLpapConnect	read-only	Anzahl der eingerichteten Verbindungen
utmOsiLpapAutoCon	read-only	Anzahl der Verbindungen, die zum Partner eingerichtet werden, wenn die Anwendung gestartet wird

9 Betrieb der Management-Station

Die Integrationspakete SMBS2 (für Reliant UNIX und Windows NT) und SMAWsmbs2 (für Solaris) enthalten ergänzende Teile zur Einbindung des Systemmanagements für BS2000/OSD in folgende Management-Plattformen:

- Unicenter TNG
- TransView SNMP
- OpenView NNM (Network Node Manager)

Beschrieben sind die Integrationspakete im Abschnitt „Bedienoberflächen für das SNMP-Management des BS2000/OSD“ (siehe Seite 20).

9.1 Integration in die Bedienoberfläche

Die Installation von SMBS2 bzw. SMAWsmbs2 setzt eine der genannten Management-Plattformen voraus.

9.1.1 Integration in die Bedienoberfläche von Unicenter TNG

BS2000/OSD ist als eigene Objektklasse in das World View Repository von Unicenter TNG integriert. Die BS2000/OSD-Objekte können mit denselben Funktionen verwaltet werden wie alle anderen Objekte im Repository, d.h. in die 2D- und die 3D-Darstellung des Netzbildes können Ikonen für BS2000/OSD-Systeme eingefügt werden (siehe Seiten 95 und 103). Bild 44 auf der nächsten Seite zeigt die 2D-Darstellung eines Netzbildes mit BS2000/OSD-Systemen.

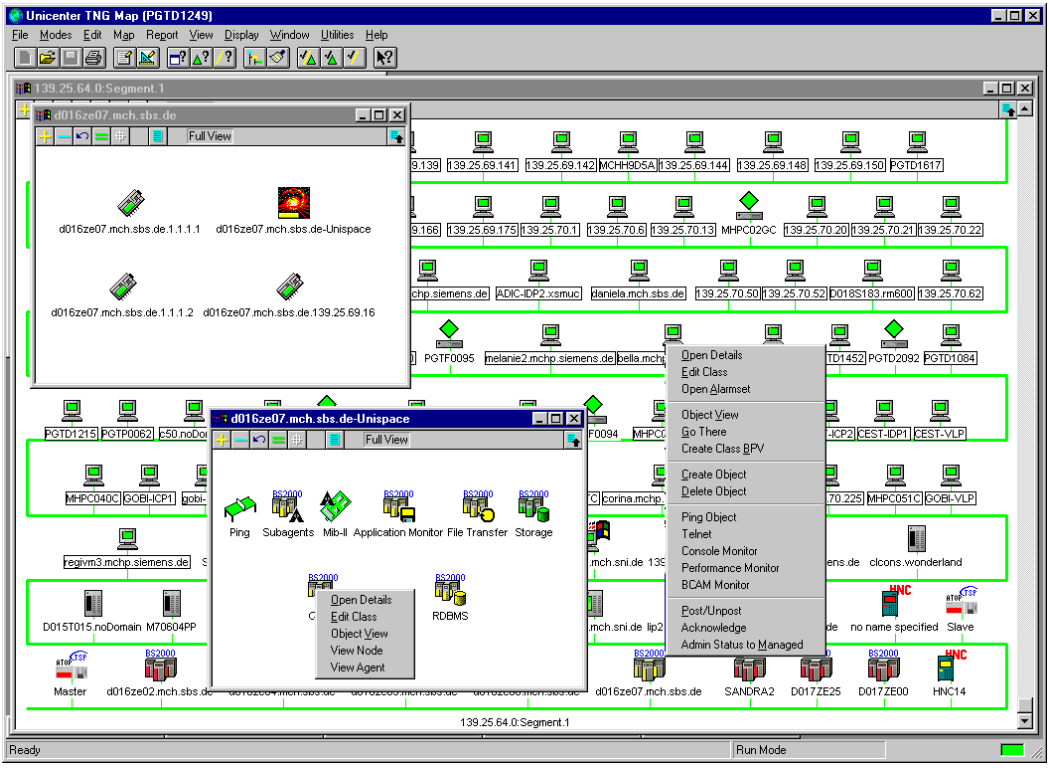


Bild 44: Darstellung der überwachten BS2000/OSD-Systeme in einem Netzbild

Jede Ikone in diesem Netzbild ist mit einem Popup-Menü verknüpft, das per einfachem Klick mit der rechten Maustaste geöffnet werden kann.

Das Menü zur Klasse "SiemensBS2000" gliedert sich in fünf Untergruppen:

- Open Details
- Edit Class
- Open Alarmset

- Object View
- Go There
- Create Class BPV

- Create Object
- Delete Object

– Ping Object
– Telnet
– Console Monitor
– Performance Monitor
– BCAM Monitor

– Post/Unpost
– Acknowledge
– Admin Status to Managed

Mit den Einträgen "BCAM Monitor", "Console Monitor" und "Performance Monitor", rufen Sie die Management-Anwendungen BCAM-Monitor, Console Monitor und Performance Monitor auf. Bei diesen Aufrufen werden einige Voreinstellungen, insbesondere der Name des Systems, aus den Netzbilddaten übernommen.

Die restlichen Einträge entsprechen den Einträgen des Standardmenüs für Objekte der Klasse "Host". Die Funktionen dieser Einträge sind in der Dokumentation zu Unicenter TNG beschrieben.

Doppeltes Anklicken der BS2000/OSD-Ikone mit der linken Maustaste öffnet ein weiteres Subnetzbild. Ab der Version 2.2 von Unicenter TNG kann dieses Fenster Symbole zu den einzelnen Interfaces enthalten. Bei einer Vollversion von Unicenter TNG mit Agent-Technology ist in das Netzbild eine Unispace-Ikone eingetragen.

Ein Doppelklick auf die Unispace-Ikone öffnet ein weiteres Subnetzbild, das Ikonen für alle entdeckten Agenten-Klassen des BS2000/OSD enthält. Dies können die Symbole für die Klassen "Ping", "Mib2", "Supervisor", "Application Monitor", "AVAS", "HSMS", "Storage", "RDBMS" und "OMNIS" sein.

Mit den Ikonen ist das Standard-Popup-Menü für Agenten-Klassen mit den folgenden Einträgen verknüpft:

– Open Details
– Edit Class
– Object View
– View Node
– View Agent

Dieses Menü entspricht dem Standardmenü für Objekte der Klasse "Agent". Die Funktionen der Menüeinträge sind in den Handbüchern zu Unicenter TNG beschrieben.

9.1.1.1 NodeView-Anzeige

Mit dem Eintrag "View Node" kann ein "Node View"-Fenster geöffnet werden, das den Status der MIB-II-Interfaces und der einzelnen Subagenten anzeigt (siehe Bild 45 auf der nächsten Seite).

Für jedes überwachte BS2000/OSD-System können die folgenden zehn DSM-Objekte erzeugt werden:

– Ping
– Mib2
– Application Monitor
– AVAS
– HSMS
– Omnis
– RDBMS
– Storage
– Supervisor

Zustandsänderungen werden durch Polls und durch den Empfang von Traps ausgelöst.

Im Node View gibt es die folgenden Anzeigen für BS2000/OSD-Systeme:

- Application Monitor:

  Statusanzeige aller überwachten Subsysteme sowie aller BCAM-, Benutzer- und DCAM-Anwendungen

- AVAS:

  Gesamt-Status von AVAS

- HSMS:

  Anzeige der Verfügbarkeit des HSMS-Subagenten

- Omnis:

  – Anzeige der Status aller überwachten OMNIS-Systeme
  – Anzeige des Empfangs wichtiger Traps, die ein OMNIS-System betreffen

- RDBMS:

  Anzeige der Verfügbarkeit der Datenbank-Server für die Datenbanken

- Storage:

  Anzeige der Saturation-Levels der Pubsets und der Verfügbarkeit der Privatplatten

- Supervisor:

  Statusanzeige für die Subagenten

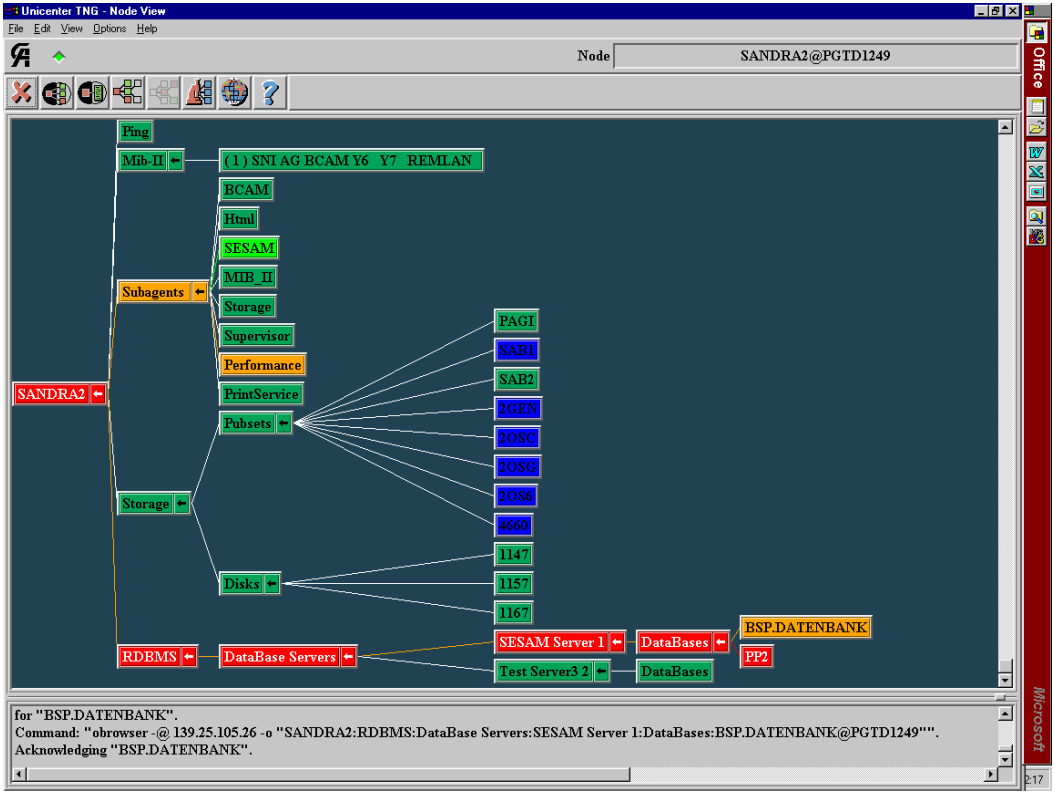


Bild 45: Node View

9.1.2 Integration in die Bedienoberfläche von TransView SNMP

Die Management-Plattform TransView SNMP unterstützt die komfortable Überwachung von BS2000/OSD-Rechnern sowie von Anwendungen des BS2000/OSD in einer heterogenen IT-Landschaft.

9.1.2.1 Überwachung des BS2000/OSD-Rechners

Ein Doppelklick auf die Ikone des BS2000/OSD-Rechners öffnet die Objektübersicht dieses Systems. Hinter dieser Ikone verbirgt sich die Funktionalität des SNMP-Basic-Agents und des Host-Resources-Subagenten.

Im Arbeitsbereich des Fensters werden u.a. angezeigt (siehe Bild 46 auf der nächsten Seite):

– der Name des Systems,
– die Internet-Adresse des Systems,
– der Community-String,
– die Eigenschaftsgruppe.

In den Feldern *sysDescr*, *sysObjectID* und *sysUpTime* wird ein Teil der Informationen aus der Systemgruppe der MIB-II ausgegeben. Die *sysUpTime* beschreibt dabei die Zeit, die der Masteragent an diesem System in Betrieb ist. Der Pollzyklus gibt die Zeit an, nach der Informationen im Fenster durch einen erneuten Request aktualisiert werden. Voraussetzung dafür ist, dass das Polling durch Betätigen des Aktionsknopfes *Poll* eingeschaltet wird. Menüs und Fensterelemente entsprechen jeder anderen Geräteübersicht unter TransView SNMP.

Spezifisch ist das Menü *Objekte*:

– Über die Menüeinträge *MIB II* bzw.*MIB II Sx* werden diejenigen Werte der MIB-II ausgegeben, die vom MIB-II-Subagenten geliefert werden (siehe Bild 46).

– Über die Menüeinträge *RFC1514-HOST-RSC*, *BS2000-APPMON*, *Console-Monitoring* und *Subagentenüberwachung* erhält man Informationen über die Werte der zugeordneten MIBs, die durch die entsprechenden Subagenten geliefert werden.

9.1.2.2 Überwachung der BS2000/OSD-Komponenten

In den Feldern *sysDescr*, *sysObjectID* und *sysUpTime* wird ein Teil der Information aus der Systemgruppe der MIB-II angezeigt. Diese Information ist identisch mit der des BS2000/OSD-Systems. Menü und Fensterelemente entsprechen jeder anderen Geräte-Übersicht unter TransView SNMP.

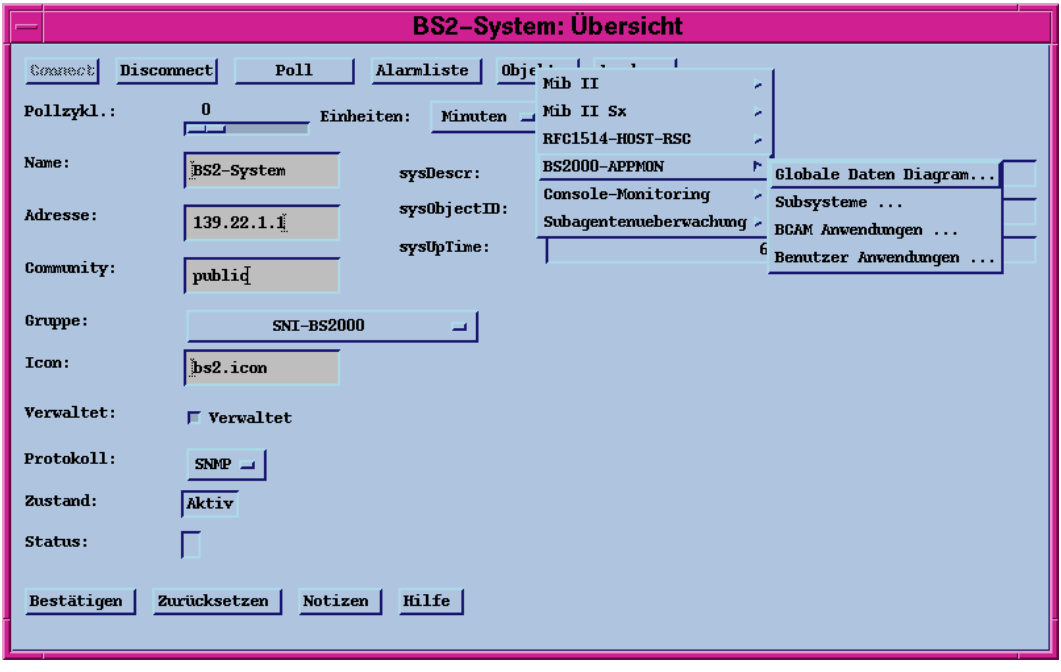


Bild 46: BS2000/OSD Systemübersicht in TransView SNMP

Spezifisch ist das Menü *Objekte.* Dieses Menü enthält einen Eintrag mit dem Namen der genormten oder privaten MIB zu dieser Komponente. Über diesen Eintrag erhält man Zugang zu den Werten der MIB-Objekte, die durch den zugehörigen Subagenten geliefert oder geändert werden.

Anzeigen von Objektwerten

Über das Menü *Objekte* in einer Übersichtsdarstellung erhalten Sie einTabellenfenster oder eine einfache Auflistung der Objekte mit ihren Werten, abhängig davon, ob die Objektgruppe mehrere Instanzen zulässt oder nicht.

Tabellenfenster

Den Arbeitsbereich des Fensters bildet eine Tabelle. Die Tabellenspalten stehen für die Attribute des im Fenster dargestellten Objekttyps, die Tabellenzeilen beschreiben die Objektinstanzen. In einem einzelnenTabellenfeld stehen die Attributwerte. Die Objektinstanzen werden eindeutig über die Indizes adressiert, die in den ersten Tabellenspalten stehen.

Objektfenster

Das Objektfenster dient der Darstellung der Attributwerte von Objekttypen, die lediglich über eine Instanz verfügen können. Die Information wird als Paar, gebildet aus dem Attributnamen und dem Attributwert, dargestellt.

Menüs und Fensterelemente entsprechen jedem anderen Fenster dieses Typs unter TransView SNMP.

Insbesondere beschreibt auch hier der Pollzyklus die Zeit, nach der die Informationen im Fenster durch einen erneuten Request aktualisiert werden. Beim Öffnen des Fensters wird ein einzelner Poll angestoßen. Ein Betätigen des Aktionsknopfes *Poll* ohne einen eingestellten Pollzyklus löst ebenfalls nur einen einzelnen Poll aus, der zur Aktualisierung der Anzeige führt.

In den Tabellen für die Objekte des SESAM-Subagenten bleiben einzelne Spalten leer, weil der SESAM-Subagent die RDBMS-MIB nicht in vollem Umfang unterstützt. Die Tabellen enthalten jedoch grundsätzlich Spalten für alle in der RDBMS-MIB definierten Objekte. Dies ermöglicht die Nutzung derselben Formate bei der Unterstützung anderer Datenbanksysteme.

Einstellen von Objektwerten

Einige Subagenten erlauben die Einstellung von Objektwerten. Mit der Anwendung *Setzen Objekt* können Sie Werte von Attributen ändern. Das Attribut muss als schreibbar definiert sein, und der im Übersichtsfenster angegebene Community-String muss die Schreibberechtigung am Agentensystem besitzen.

1. Wählen Sie *Anwendungen* in der Übersichtsdarstellung oder in einem Tabellen- bzw. Formularfenster aus.
2. Wählen Sie aus der angezeigten Liste *Setzen Objekt* aus.
3. Selektieren Sie in der Dialogbox zunächst das Basisobjekt und dann das Attribut.

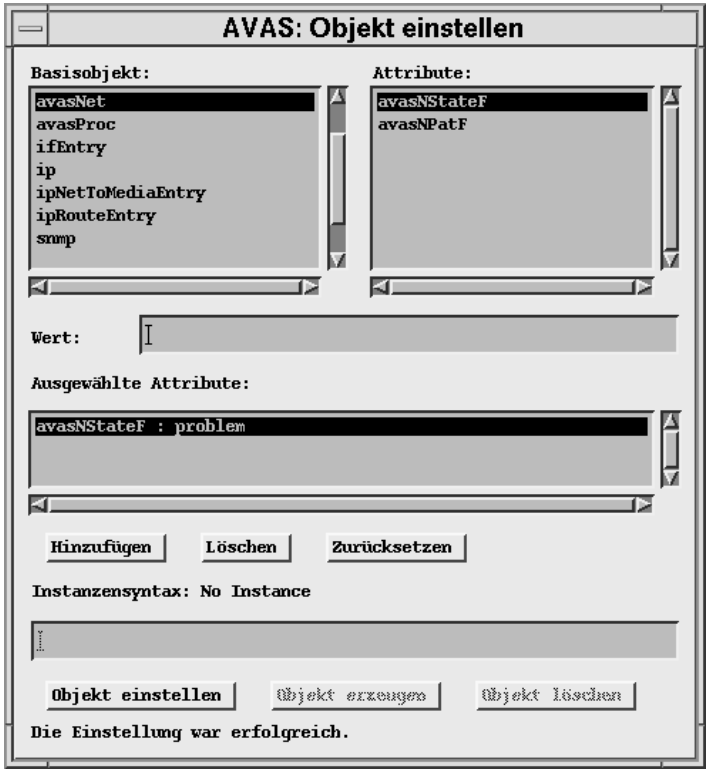


Bild 47: Einstellen von Objektwerten

4. Schreiben Sie den gewünschten Wert in das Feld *Wert*.
5. Klicken Sie den Aktionsknopf *Hinzufügen* an.
6. Geben Sie gegebenenfalls eine Instanz an, für die der Wert eingestellt werden soll.
7. Klicken Sie den Aktionsknopf *Objekt einstellen* an.

TransView SNMP zeigt in einer Meldung an, ob die Werte eingestellt werden konnten. Eine Beschreibung dazu befindet sich im entsprechenden Handbuch.

9.1.2.3 Alarme

Zur automatischen Überwachung von BS2000/OSD-Systemen sind eine Reihe von Alarmen definiert.

RDBMS_relState

Dieser Alarm dient zur Anzeige der Zugriffsmöglichkeit der Datenbankserver auf die Datenbanken. Die Zustände des Alarms entsprechen der Wertemenge des Objektes *rdbmsRelState*. Beim Verlust oder der Einschränkung einer Zugriffsmöglichkeit, versendet der
SESAM-Subagent einen Trap. Einen entgegengesetzten Trap, der die Rückkehr in den Normalzustand einer Datenbank anzeigt, gibt es nicht. Die vollständige, nur auf Traps gestützte Steuerung des Alarms zur Anzeige der Datenbankverfügbarkeiten ist daher nicht möglich. Es müssen Polls verwendet werden. Die Polls sind nach der Installation von SMBS2 eingeschaltet. Das Einschalten aller vier Polls ist die Voraussetzung für die vollständige Funktionsweise des Alarms. Die Polls fragen alle drei Minuten den Wert der Objekte *rdbmsRelState* ab. Es ist deshalb möglich, dass die Veränderung der Zugriffsmöglichkeit auf eine Datenbank erst mit einer Verzögerung angezeigt wird. Durch die Verminderung der Pollfrequenz kann diese Zeitspanne verkürzt werden.

AVASState

Der Alarm zeigt den Empfang einzelner Traps aus der AVAS-MIB an. Er hat die Zustände *Normal*, *Missing*, *Ready, Running*, *ErrorSystem*, *ErrorNet* und *ErrorSignon*. Die ersten vier Zustände haben das Gewicht *normal*. Die übrigen drei zeigen Probleme mit den Gewichten *Schwer* (bzw. *Major*), *leicht* (bzw. *Minor*) oder *Information* an. Der Alarm ist ausschließlich durch Traps gesteuert. Die Zustände *Normal* und *Missing* können nur am Anfang eingenommen werden. Im späteren Betrieb wird nur zwischen den übrigen Zuständen gewechselt. Die Alarmzustände entsprechen in ihrer Bedeutung den angezeigten Traps.

SupervisBasic, SubagentStatus, SubagentStatus_a

Diese Alarme erzeugen eine Anzeige der Status der Subagenten. Während der Status des MIB-II-Subagenten, des Application Monitor Subagenten, des Console Monitor Subagenten und des Host-Resources-Subagenten durch eine Verfärbung der BS2000/OSD-Ikone angezeigt wird, führen Statusänderungen der anderen Subagenten zu einer Verfärbung der Leitungs-Ikone zwischen der BS2000/OSD-Ikone und der zugehörigen Anwendungs-Ikone. Der Status *aktiv* wird durch den Zustand *Normal* angezeigt. Dieser Zustand gilt auch, solange der Subagent für den Master und damit für die Management-Station unbekannt ist. Vor der ersten Anmeldung gibt es keinen Eintrag in der Subagententabelle der Supervisor-MIB. Die Objektinstanzen für den Alarm existieren noch nicht. Die Abmeldung eines Subagenten führt zu einer Blauverfärbung, das heißt zu einem Zustand mit dem Gewicht *Information*. Wenn ein Subagent nicht antwortet und deshalb in den Zustand *undefined*

gesetzt wird, wird in einen Zustand mit dem Gewicht *Leicht* (bzw. *Minor*) gewechselt. Bei einem Statuswechsel kann von jedem Zustand in jeden der zwei anderen Zustände gewechselt werden. Die Alarme sind durch die Traps der Supervisor-MIB und durch Polls gesteuert. Nach dem Empfang eines Traps werden kurzzeitig die Polls eingeschaltet.

OmnisMsg

Dieser Alarm zeigt den Empfang von OMNIS-Traps an. Wenn ein OMNIS-Trap empfangen wird, wird der Zustand *Normal* verlassen und einer der Zustände *Inform* oder *Minor* angenommen, denen die Gewichte *Information* und *Leicht* (bzw. *Minor*) zugeordnet sind. Der Alarm hat nur die Funktion, dem Benutzer den Empfang der Traps anzuzeigen. Die Gewichte entsprechen der Bedeutung der Traps. Die Alarmzustände können nicht automatisch wieder verlassen werden. Der Alarm muss manuell wieder zurückgesetzt werden.

9.1.3 Integration in TransView Control Center

Die Integration in TransView Control Center ermöglicht die Überwachung von Symmetrix-Geräten. Dazu sind die nachfolgend beschriebenen Alarme definiert.

Die folgenden vier Alarme dienen der Anzeige von Symmetrix-Ereignissen. Die Zustandswechsel werden nur durch das TransView Control Center gesteuert.

sym-sp

Dieser Alarm betrifft die durch die Meldung *NJD0010* mitgeteilten Probleme mit dem Serviceprozessor der Symmetrix. Das Alarmdiagramm besteht aus zwei Zuständen: *Normal* (Gewicht: *Normal*) und *SP-Down* (Gewicht: *Leicht*). Die Referenzkodes *x476* und *x477*, welche melden, dass über den Serviceprozessor keine Verbindung zum EMC-Service-Support-Center (EMC-CSC) besteht, bewirken den Übergang in den Zustand *SP-Down*. Durch eine Meldung mit dem Referenzkode *x47F* wird ein erfolgreicher Autocall an das EMC-Service-Support-Center signalisiert. Nach dieser Meldung kann deshalb in den Zustand *Normal* zurückgekehrt werden. Dieser Ereignistyp kann nur registriert werden, wenn die Symmetrix darauf eingestellt ist. Ist der Ereignistyp nicht registriert, dann muss dieser Alarm manuell zurückgesetzt werden.

sym-partner

Die Verfügbarkeit der SRDF-Verbindungen (SRDF=Symmetrix Remote Data Facilty) zu den Partnergeräten wird durch die drei Zustände dieses Alarms angezeigt:

all-connected (Gewicht: *Normal*) bedeutet, dass alle SRDF-Verbindungen funktionieren.

part.-connec. (Gewicht: *Warnung*) bedeutet, dass die SRDF-Verbindungen nur teilweise zur Verfügung stehen. Einzelne Verbindungen sind ausgefallen.

all-disconn. (Gewicht: *Leicht*) bedeutet, dass alle SRDF-Verbindungen ausgefallen sind und kein Kontakt zu den Partnergeräten besteht.

sym-disk

Im Diagramm dieses Alarms gibt es zwei Zustände *Normal* und *Disk_Problem* (Gewicht: *Schwer*) und nur einen Zustandsübergang von *Normal* nach *Disk_Problem*. Er wird durch alle Referenzkodes bewirkt, die ein Plattenproblem signalisieren. Das Zurücksetzen dieses Alarms muss manuell erfolgen.

sym-error

Dieser Alarm betrifft Probleme, die mit der Meldung *NJD0011* angezeigt werden und in der Mehrzahl Hardware-Probleme der Symmetrix sind (z.B. Überhitzung oder Probleme mit der Stromversorgung). Wie im Alarm zur Anzeige der Plattenprobleme gibt es bei diesem Alarm nur zwei Zustände *Normal* und *Error* (Gewicht: *Schwer*). Der Zustandswechsel von *Normal* nach *Error* erfolgt nach der Meldung eines Problems. In den Zustand *Normal* kann nur durch manuelles Zurücksetzen des Alarms zurückgekehrt werden.

9.1.4 Integration in die Bedienoberfläche von HP OpenView

Nach der Installation von SMBS2 stehen die folgenden Erweiterungen an der Oberfläche von OpenView zur Verfügung:

– Die MIB-Struktur ist im MIB-Browser bekannt.

– Die Ikone für BS2000/OSD-Systeme kann in das Netzbild eingefügt werden.

– In die Menüleiste der Netzbilddarstellungen ist das Menü für die BS2000/OSD-Anwendung eingefügt. Mit dem Menü können Fenster zu MIB-Objekten geöffnet werden.

Das BS2000/OSD-Menü wird wie folgt aufgerufen:

1. Die BS2000-Ikone wir durch Einfach-Klick mit der linken Maustaste markiert.
2. Danach kann das Menü für die BS2000/OSD-Anwendung geöffnet werden. Dieses Menü ist sowohl in der Menüleiste als auch als Popup-Menü in der Ikone verfügbar.

Die Struktur der durch SMBS2 hinzugefügten Menüs und Fenster entspricht weitgehend den Menüs und Fenstern, um die TransView-SNMP durch das Paket SMBS2 erweitert wird. Im BS2000/OSD-Menü spiegelt sich im Wesentlichen die Struktur der BS2000/OSD-MIBs wider. Die Einträge in der ersten Stufe entsprechen den Bereichen, die in den Unternetzbildern für BS2000/OSD-Systeme in TransView-SNMP durch die verschiedenen Subagenten-Ikonen repräsentiert werden. Die weitere Struktur der Submenüs und die Gestaltung der Fenster ist, so weit das möglich ist, den Menüs der BS2000/OSD-Oberfläche an TransView-SNMP nachgebildet.

Im Einzelnen gehören zu den Submenüs des BS2000/OSD-Menüs die Fenster für die Objekte aus den folgenden MIBs.

System: Application-Monitoring-MIB, Console-Monitoring-MIB, Supervisor-MIB

AVAS: AVAS-MIB

File-Transfer: File-Transfer-MIB

Host Resources: Host Resources-MIB

HIPLEX-AF: HIPLEX-AF-MIB

OMNIS: OMNIS-MIB

Performance: SNIPERF-MIB

Printservice: Spool-MIB

SESAM: RDBMS-MIB

Storage: Storage-Management-MIB

UTM: UTM-MIB

Eine Besonderheit gibt es im Submenü *Performance* mit dem Eintrag *graphics*. In diesem Submenü können grafische Überwachungen von Performance-Werten aufgerufen werden, wie die CPU-Zeiten und die Häufigkeit der Ein- und Ausgaben. Mit regelmäßigen Polls werden die aktuellen Werte abgefragt und ihre zeitliche Veränderung in einer Kurve dargestellt.

Der SESAM-Subagent unterstützt die RDBMS-MIB nicht im vollen Umfang, daher sind in den Tabellen nur Spalten für den Teil der MIB-Objekte definiert, die auch vom Subagenten unterstützt werden.

Für die OMNIS, Supervisor- und RDBMS-Traps sind Status-Events definiert. Der Eingang dieser Traps wird durch eine Meldung angezeigt.

Nach der Installation ist auch die BCAM-MIB geladen. Formulare und Tabellen zu dieser MIB werden von SMBS2 für OpenView NNM nicht unterstützt.

Allgemeine Informationen über den Betriebszustand eines überwachten BS2000/OSD-Systems sind im Rahmen des *All Event Browsers* verfügbar. Wenn ein Systemausfall gemeldet wird, wird die Ikone mit einem roten Rahmen versehen, im Normalbetrieb ist der Rahmen grün.

9.2 Management-Anwendungen CMBS2 und PMBS2

Für spezielle Subagenten wie den Console Monitor Subagenten und den Performance Monitor Subagenten stehen eigene, auf die speziellen Eigenschaften und Aufgaben des jeweiligen Subagenten zugeschnittene Management-Anwendungen zur Verfügung:

– CMBS2 für den Console Monitor Subagenten
– PMBS2 für den Performance Monitor Subagenten

Diese Management-Anwendungen können in die oben beschriebenen Management-Plattformen integriert werden. Sie ergänzen und verbessern die Darstellung und Handhabung der bestehenden Management-Plattform und bieten insbesondere eine netzweite Übersicht über alle BS2000/OSD-Systeme.

9.2.1 Anwendung CMBS2 für den Console Monitor Subagenten

CMBS2 unterstützt den Console Monitor Subagenten bei der Erfassung, Bearbeitung und Filterung von Console-Meldungen und bietet einen remote Zugang zu den Konsolen aller BS2000/OSD-Systeme im Netz.

Funktionalität

- Darstellen von Konsolmeldungen mit der Möglichkeit, sowohl am Agenten als auch an der Management-Station zu filtern,
- Setzen von Filtern am Agentensystem, um die Netzbelastung zu verringern und die Anzeige übersichtlicher zu gestalten,
- Beantworten von Fragen, die auf der Konsole angezeigt werden,
- Absetzen von Kommandos,
- automatische Reaktionen auf Traps.

Starten und Beenden von CMBS2

CMBS2 wird auf UNIX-Systemen aus der Shell-Ebene durch Aufruf der Prozedur *ConsMon* gestartet. Es erscheint das Hauptfenster der Anwendung.

Auf Windows NT wird die Anwendung aus der Programmgruppe *SNMP Management Applications* heraus gestartet. Alternativ kann sie durch Doppelklick auf den Eintrag *ConsoleMonitor* im Verzeichnis *<tcldir>\appl\Cmbs2* aufgerufen werden.

CMBS2 kann aus jedem Fenster heraus beendet werden, indem im Menü *ConsMon* die Funktion *Beenden* ausgewählt wird. Unbeabsichtigtes Beenden wird durch eine Sicherheitsabfrage vermieden. Je nach Einstellung der Parameter für das *Sichern* werden Veränderungen der Parameter gesichert, verworfen oder abgefragt.

9.2.1.1 Einstellung der Bedienoberfläche

CMBS2 verfügt über verschiedene Darstellungsmodi, um die Aufmerksamkeit des Anwenders auf die wesentlichen Objekte seiner momentanen Tätigkeit zu konzentrieren.

Trap-Fenster oder Kommando-Fenster

Im Hauptfenster von CMBS2 kann über Menü oder Toolbar zwischen der Darstellung eines Trap-Fensters und der eines Kommando-Fensters gewechselt werden. Die Beschreibung der Fenster finden Sie ab Seite 356 bzw. Seite 364.

Anzeige der SNMP-Parameter / Ausblenden der Community

Über das Menü und die Toolbar kann die Anzeige der Community ausgeblendet werden.

SNMP-Parameter

Um eine Nachricht via SNMP korrekt an ein System senden zu können, ist die Angabe der IP-Adresse des Zielsystems, eines Ports und eines Community-Strings nötig. Der Community-String bestimmt die Zugangsberechtigung und den Berechtigungsumfang. Der Console Monitor erzeugt beim Start eine Liste möglicher Zielsysteme mit ihren Namen und SNMP-Parametern. Diese Liste von Systemen kann unter der Menüleiste *Optionen* → *Einstellungen* → *Systeme* bearbeitet werden.

Im Eingabefeld *Adresse* erfolgt die Angabe der IP-Adresse. Wird der Systemname im SNMP-Parameterbereich geändert, so wird die IP-Adresse aus der Systemliste gelesen. Ist das System in der Systemliste nicht erfasst, bleibt die IP-Adresse unverändert.

Das Eingabefeld *Port* definiert den Port. Wird der Systemname im SNMP-Parameterbereich geändert, so wird auch der Port aus der Systemliste gelesen. Ist das System in der Systemliste nicht erfasst, bleibt der Port unverändert.

Das Eingabefeld *Community* enhält die Angaben zu Community.

Der Community bestimmt die Zugangsberechtigung und den Berechtigungsumfang für die SNMP-Requests. Die Anpassung des Community bei Änderung des Systemnamens erfolgt nach der gleichen Regel wie die des Ports.

Anzeige der Filter im Trap-Fenster

Die Anzeige im Trap-Fenster lässt sich übersichtlicher gestalten, indem die lokalen Filter ausgeblendet werden.

9.2.1.2 Trap-Fenster

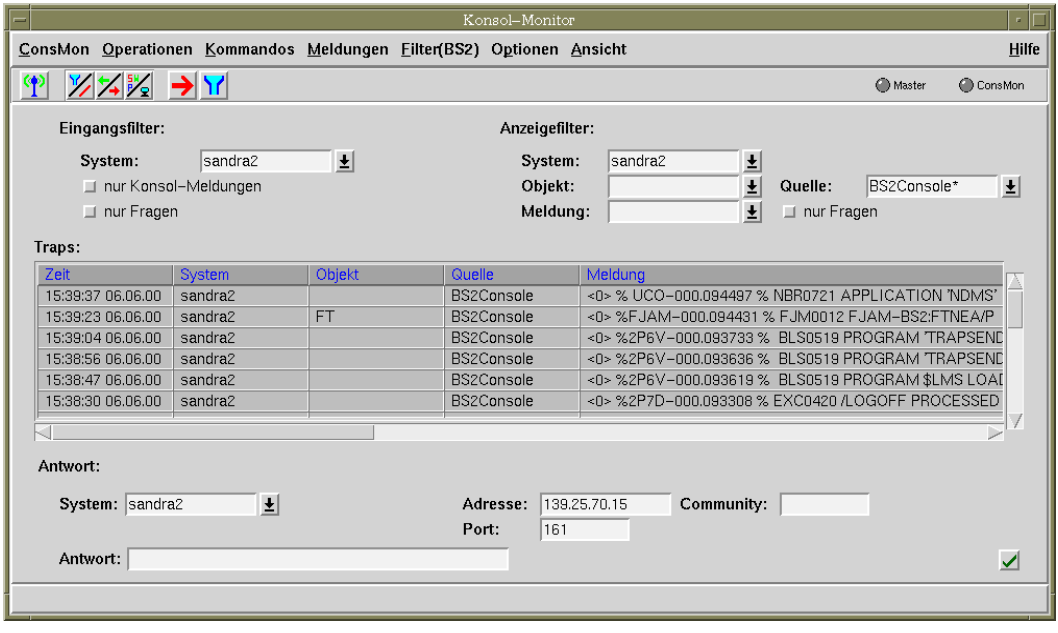


Bild 48: Trap-Fenster

Das Trap-Fenster ist zugleich das Hauptfenster von CMBS2. Von ihm ausgehend, können Fenster für weitere Aktionen geöffnet werden. Wird dieses Fenster geschlossen, wird die Applikation beendet. Über das Menü oder die Toolbar kann aus diesem Fenster in den Modus des Kommando-Fensters gewechselt werden (siehe Seite 355).

Das Fenster gliedert sich in vier Bereiche:

1. die Menüleiste
2. die Toolbar
3. den Arbeitsbereich
4. die Hilfezeile.

Menüleiste des Trap-Fensters

Die Menüleiste umfasst die Menüs *ConsMon*, *Operationen*, *Kommandos*, *Meldungen*, *Filter(BS2)*, *Optionen, Ansicht* und *Hilfe*.

Das Menü *ConsMon* enthält den Eintrag *Beenden*.

Das Menü *Operationen* enthält die Funktion "Test". Mit "Test" können Sie prüfen:

– Erreichbarkeit des angegebenen Systems via ICMP

– Status des SNMP-Masteragenten und des Console Monitor Subagenten mit folgender Ergebnisanzeige:

  Anzeige "Master" in der Toolbar:

  – rot: keine Verbindung über ICMP
  – gelb: *noResponse* über SNMP
  – blau: Community read-only
  – grün: Community read-write

  Anzeige "ConsMon" in der Toolbar:

  – gelb: *noResponse* über SNMP
  – grün: Der Console Monitor Subagent hat Verbindung zum Masteragenten.

In Sekundärfenstern enthält das Menü zusätzlich den Eintrag *Schließen* zum Schließen des Fensters.

Das Menü *Kommandos* enthält den Eintrag *Neues Fenster* zum Öffnen eines separaten Fensters für die Eingabe von BS2000-Kommandos. Die weiteren Einträge beziehen sich auf den Arbeitsbereich im Kommandomodus und sind im Trap-Fenster inaktiv.

Mithilfe der Menüeinträge

– *Meldungen Löschen* → *alle*,
– *Meldungen Löschen* → *angezeigte* und
– *Meldungen Löschen* → *selektierte*

können alle im Ausgabebereich der Traps angezeigten Meldungen bzw. alle selektierten Meldungen gelöscht werden. Eine Meldung wird durch Doppelklick oder durch Ziehen der Maus über den Meldungstext selektiert.

In *Filter(BS2)* wird über den Menüeintrag *Bearbeiten* ein weiteres Fenster geöffnet, über welches der Meldungsfilter für den Console Monitor im BS2000 angezeigt und geändert werden kann.

Optionen enthält die Einträge *Einstellungen*, *Reaktionen*, *Sichern*:

– *Einstellungen* öffnet eine Optionen-Dialogbox, in der Einstellungswerte zu den Bereichen *Systeme*, *Gruppen*, *Ping*, *SNMP*, *Meldungen*, *Kommandos* und *Sichern* berabeitet und gesichert werden können.

– *Reaktionen* öffnet eine Dialogbox, in der Reaktionen auf eintreffende Meldungen definiert werden können.

– *Sichern* → *Einstellungen* + *Reaktionen* speichert alle Werte der Einstellungsbereiche sofort in der Konfigurationsdatei.

– *Sichern* → *Start-Konfiguration* speichert alle Werte der Einstellungsbereiche sowie die Startkonfiguration sofort in der Konfigurationsdatei. Nach einem Neustart des Console Monitors befinden sich alle Einstellungen und Werte des Trap-Fensters in dem Zustand, der beim Aufruf des Menüeintrags vorlag.

  Hinweis: Der Menüeintrag *Sichern* ist nur dann aktiv, wenn alle Diaolgboxen geschlossen sind.

Das Menü *Ansicht* enthält folgende Einträge:

– *Anzeigen Filter* ermöglicht das Ein- und Ausblenden des Filters.

– *Kommandos* wechselt zwischen Trap- und des Kommando-Fenster.

– *Anzeigen Community* ermöglicht das Ein- und Ausblenden des Community-Strings.

Unter *Hilfe* gibt es Informationen zur Version, zu den neuen Funktionen in Version 5.0, zum aktiven Fenster und über den Index.

Toolbar des Trap-Fensters

Die Toolbar enthält eine Auswahl der im Menü angebotenen Funktionen. Sie soll einen schnellen Zugriff auf häufig benötigte Operationen erlauben. Ein Stichwort zu der hinter dem jeweiligen Icon verborgenen Funktionalität erhalten Sie, wenn der Mauszeiger länger als eine Sekunde auf dem Icon verweilt.

Die Toolbar umfasst folgende drei Gruppen:

Die erste Gruppe enthält die Funktion *Test*, mit der Sie die Erreichbarkeit des angegebenen Systems via ICMP sowie die Status des SNMP-Masteragenten und des Console Monitor Subagenten prüfen können.

Die Ergebnisse werden wie folgt angezeigt:

Anzeige "Master" in der Toolbar:

– rot: keine Verbindung über ICMP
– gelb: *noResponse* über SNMP
– blau: Community read-only
– grün: Community read-write

Anzeige "ConsMon" in der Toolbar:

– gelb: *noResponse* über SNMP
– grün: Der Console Monitor Subagent hat Verbindung zum Masteragenten.

Die zweite Gruppe ermöglicht:

– Ausblenden der Filter im Trap-Fenster
– Umschalten des aktuellen Arbeitsbereichs zwischen dem Arbeitsbereich eines Trap-Fensters und dem Arbeitsbereichs eines Kommando-Fensters
– Ausblenden des Community-Strings

Die dritte Gruppe enthält die Funktionen

– zum Öffnen eines weiteren Kommando-Fensters sowie
– zum Öffnen eines Fensters zum Anzeigen und Setzen von Filtern.

Arbeitsbereich eines Trap-Fensters

Der Arbeitsbereich des Trap-Fensters besteht aus drei Teilen:

1. dem Bereich für die Einstellung der lokalen Filter (Eingangsfilter und Anzeigefilter)
2. dem Anzeigebereich für die einlaufenden Traps,
3. dem Bereich zur Beantwortung einer Konsolfrage.

Einstellung eines lokalen Filters

Der lokale Filter gliedert sich in den Eingangs- und den Anzeigefilter.

Eingangsfilter

Die Einstellung des Eingangsfilters erlaubt, die Anzeige einlaufender Traps einzuschränken. Bereits eingegangene Traps werden nicht nachträglich aus der Anzeige entfernt. Ausgefilterte Meldungen werden verworfen. Der Filter wird aus der "UND-Verknüpfung" der folgenden drei Parameter gebildet.

Combobox *System*	Durch die Angabe eines Systems oder einer Systemgruppe kann die Anzeige auf Traps, die von einem bestimmten System oder einer Gruppe von Systemen kommen, eingeschränkt werden. Gruppen werden durch [gruppenname] dargestellt. Bei der Eingabe von Gruppennamen müssen die eckigen Klammern nicht angegeben werden. Die Bearbeitung von Gruppen erfolgt in der Menüleiste *Optionen* → *Einstellungen* → *Gruppen*. Ein Doppelklick auf einen Gruppennamen zeigt in der Hilfezeile die entsprechende Konfiguration. Ein leeres Feld schränkt die Anzeige nicht ein. Die Liste der Combobox ist vorbelegt durch die Systemliste und die bereits definierten Systemgruppen.
Checkbutton *nur Konsolmeldungen*	Die Aktivierung dieses Checkbutton begrenzt die Anzeige auf Traps des Console Monitor.
Checkbutton *nur Fragen*	Die Aktivierung dieses Checkbutton begrenzt die Anzeige auf Fragen der Konsole.

Anzeigefilter

Die Einstellung des Anzeigefilters erlaubt, die Anzeige aller nicht verworfenen Traps einzuschränken. Gefiltert wird stets die Grundmenge, sodass mit der Angabe "*" bzw. "" eine Rückkehr zur vollen Grundmenge möglich ist. Der Filter wird aus der "UND-Verknüpfung" der folgenden fünf Parameter gebildet.

Combobox *System*
: Durch die Angabe eines Systems oder einer Systemgruppe kann die Anzeige auf Traps, die von einem bestimmten System oder einer Gruppe von Systemen kommen, eingeschränkt werden. Gruppen werden durch [gruppenname] dargestellt. Bei der Eingabe von Gruppennamen müssen die eckigen Klammern nicht angegeben werden. Die Bearbeitung von Gruppen erfolgt in der Menüleiste *Optionen* → *Einstellungen* → *Gruppen*. Ein Doppelklick auf einen Gruppennamen zeigt in der Hilfezeile die entsprechende Konfiguration. Ein leeres Feld schränkt die Anzeige nicht ein. Die Liste der Combobox ist vorbelegt durch die Systemliste und die bereits definierten Systemgruppen.

Combobox *Quelle*
: Der Quellenfilter kann direkt in das Textfeld eingetragen werden. Die Anzeige wird auf die entsprechenden Quellen beschränkt. Die Liste der Combobox ist vorbelegt durch die unter *Quellen-Filter Bearbeiten* definierten Einträge (siehe Menüleiste *Optionen* → *Einstellungen* → *Meldungen*).

Combobox *Objekt*
: Der Objektfilter kann direkt in das Textfeld eingetragen werden. Die Anzeige wird auf die entsprechenden Objekte beschränkt. Die Liste der Combobox ist vorbelegt durch die unter *Objekt-Filter Bearbeiten* definierten Einträge (siehe Menüleiste *Optionen* → *Einstellungen* → *Meldungen*).

Combobox *Meldung*
: Der Meldungsfilter kann direkt in das Textfeld eingetragen werden. Dieser Filter wird durch einen Vergleich des angegebenen Strings mit der Nettonachricht nach den "global-style-Regeln" ausgewertet. Damit ist auch eine Einschränkung auf das Gewicht einer Meldung möglich. Die Liste der Combobox ist vorbelegt durch die unter *Meldungs-Filter Bearbeiten* definierten Einträge (siehe Menüleiste *Optionen* → *Einstellungen* → *Meldungen*).

Checkbutton *nur Fragen*
: Die Aktivierung dieses Checkbutton begrenzt die Anzeige auf Fragen der Konsole.

Anzeigebereich einlaufender Traps

In diesem Bereich werden die ankommenden Traps tabellarisch dargestellt. Der zuletzt einlaufende Trap wird in die erste Zeile eingefügt. Überschreitet die Anzahl die in *Optionen → Einstellungen → Meldungen* festgelegte Zahl, werden die ältesten Traps gelöscht.

Ausgabe	**Bedeutung**
Zeit	Uhrzeit und Datum des Trap-Empfangs
System	Absender des Traps. Ist das System in der Systemliste eingetragen, so wird der zur Adresse gehörende Systemname angezeigt, andernfalls die IP-Adresse.
Objekt	Für dieses Feld ausgewertet wird der Text der Nettonachricht zwischen den Schlüsselworten *$DEVC$:* und *MSG:*. Dieser wird der BS2000-Meldungsfilterdatei unter dem Schlüssel DEVICE entnommen.
Quelle	Vermerk, ob der Trap von einem Console Monitor Subagenten des BS2000/OSD stammt. Im Standardfall steht dort *BS2Console*, es sei denn, es wurde, wie auf Seite 75 beschrieben, eine andere Source vereinbart. Für dieses Feld ausgewertet wird der Text der Nettonachricht zwischen den Schlüsselwörtern *$SOURCE$:* und *$DEVC$:*.
Meldung	Nettonachricht des Traps

Ein Klick auf eine Meldungszeile oder Ziehen über einen Bereich der Meldung markiert die Meldung. Eine markierte Meldung kann über das Menü *Traps → Meldungen Löschen → selektierte* gelöscht werden. Ein Doppelklick auf die Meldungszeile einer Frage übernimmt die Angabe des Absenders in das Feld *System* und die TSN in das Eingabefeld des Bereiches *Antwort*.

Ein Doppelklick mit der mittleren Maustaste schaltet die Trap-Bestätigung ein (siehe Abschnitt „Trap-Sicherung“ auf Seite 207), ein weiterer Doppelklick schaltet die Trap-Bestätigung wieder aus. Eingeschaltete Trap-Bestätigung wird durch rot gefärbte Tabellenüberschriften angezeigt.

Bereich zur Beantwortung einer Konsolfrage

In diesem Bereich kann die Antwort auf eine von der Konsole eingetroffene Frage eingegeben werden.

In der Combobox *System* wird das Zielsystem definiert, an das die Antwort gesendet werden soll. Die Liste der Combobox ist vorbelegt durch die Einträge in der Systemliste. Der Name des Systems kann durch den Comboboxmechanismus aus der Liste übernommen oder direkt eingetragen werden. Darüber hinaus kann er durch Doppelklick auf eine Meldungszeile aus dem Ausgabebereich der Traps entnommen werden.

Im zweiten Teil der Parameter werden die SNMP-Parameter ausgegeben.

Das Eingabefeld *Antwort* dient zur Eingabe des Antworttextes. Der notwendige Vorspann durch die TSN kann ebenfalls durch Doppelklick auf die Meldungszeile aus dem Ausgabebereich der Traps entnommen werden.

Aktionsknöpfe:

Bei Betätigen dieses Buttons wird die Antwort an das angegebene System gesendet. Zwischen Eingabefeld und Aktionsknopf wird das Ergebnis der SNMP-Operation angezeigt. Kann die Antwort vom BS2000-System nicht korrekt verarbeitet werden, erscheint eine Konsolmeldung im Trap-Ausgabefenster.

Hilfezeile des Trap-Fensters

In der Hilfezeile erscheint ein Stichwort zur Funktionalität eines Fensterelementes, wenn der Mauszeiger auf dem Element länger als eine Sekunde verweilt.

Wenn im Trap-Fenster ein Doppelklick auf die unter *Eingangs- bzw. Anzeige-Filter* ausgewählte Gruppe durchgeführt wird, werden in der Hilfezeile die zu dieser Gruppe gehörenden Systeme ausgegeben.

9.2.1.3 Kommando-Fenster

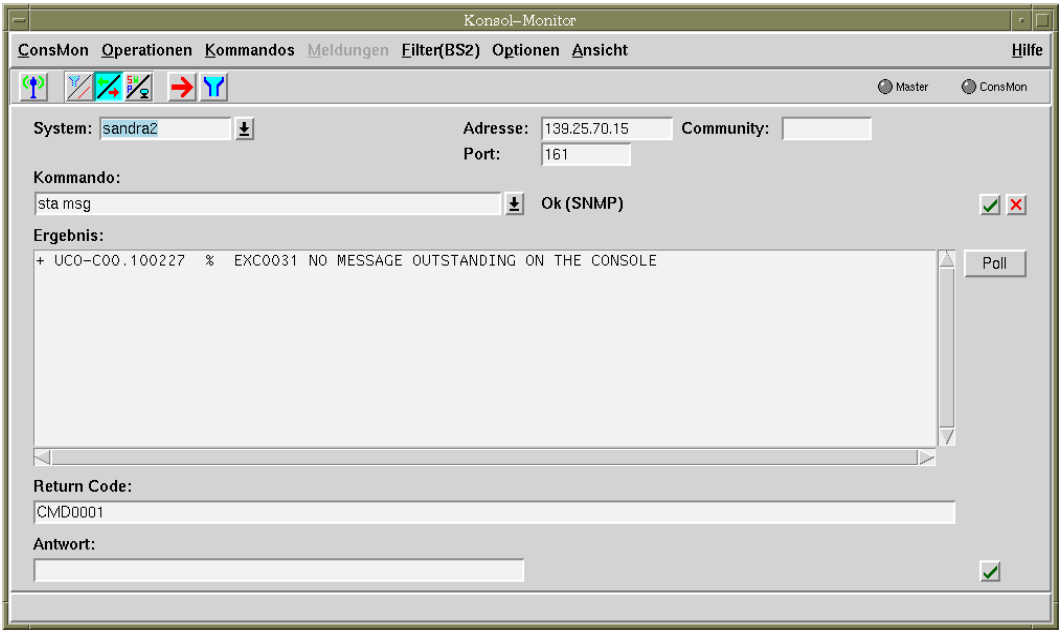


Bild 49: Kommando-Fenster

Das Kommando-Fenster kann als Hauptfenster oder als Nebenfenster entstehen. Im Fall des Hauptfensters können ausgehend von ihm weitere Kommando-Fenster geöffnet werden. Wird es als Hauptfenster geschlossen, wird die Applikation beendet. Ist CMBS2 im Trap-Modus gestartet und das Kommando-Fenster Hauptfenster, so kann über das Menü oder die Toolbar in den Modus des Trap-Fensters gewechselt werden (siehe Seite 355).

Auch das Kommando-Fenster gliedert sich wie das Trap-Fenster in vier Bereiche:

1. die Menüleiste
2. die Toolbar
3. den Arbeitsbereich
4. die Hilfezeile.

Menüleiste des Kommando-Fensters

Die Menüleiste umfasst die Menüs *ConsMon*, *Operationen*, *Kommandos*, *Filter(BS2)*, *Optionen*, *Ansicht* und *Hilfe*.

Das Menü *ConsMon* enthält den Eintrag *Beenden*.

Das Menü *Operationen* enthält die Funktion *Test*, mit der Sie die Erreichbarkeit des angegebenen Systems via ICMP sowie den Status des SNMP-Masteragenten und des Console Monitor Subagenten prüfen können.

Die entsprechenden Beschreibungen entnehmen Sie bitte Seite 357.

Das Menü *Kommandos* enthält folgende Einträge:

– *Neues Fenster* öffnet ein separates Fensters für die Eingabe von BS2000- Kommandos. Diese Funktion steht nur zur Verfügung, wenn das Kommando-Fenster das Hauptfenster ist.

– *Ausführen* sorgt dafür, dass das im Eingabefeld *Kommando* angegebene Kommando zur Ausführung an den Console Monitor gesendet wird. Die Kommandoausgabe erscheint im Bereich Ergebnis. Im Fehlerfall wird hinter dem Eingabefeld die Meldung von SNMP ausgegeben.

– *Stoppen* bricht das Verfahren ab, das das Kommando an den Subagenten liefert und die Kommandoergebnisse holt. Je nach Zustand kann nicht in jedem Fall davon ausgegangen werden, dass das Kommando nicht zur Ausführung kommt. In keinem Fall wird ein bereits vom Console Monitor abgesendetes Kommando abgebrochen!

– Unter *Liste Sortieren* wird die über die Combobox zum Eingabefeld *Kommando* erreichbare Liste sortiert.

Im Menü *Filter(BS2)* wird über den Menüeintrag *Bearbeiten* ein weiteres Fenster geöffnet, über welches der Meldungsfilter für den Console Monitor im BS2000 angezeigt und geändert werden kann.

Optionen enthält die Einträge *Einstellungen*, *Reaktionen*, *Sichern*:

– *Einstellungen* öffnet eine Optionen-Dialogbox, in der Einstellungswerte zu den Bereichen *Systeme*, *Gruppen*, *Ping*, *SNMP*, *Meldungen*, *Kommandos* und *Sichern* berabeitet und gesichert werden können.

– *Reaktionen* öffnet eine Dialogbox, in der Reaktionen auf eintreffende Meldungen definiert werden.

– *Sichern* → *Einstellungen + Reaktionen* speichert alle Werte der Einstellungsbereiche sofort in der Konfigurationsdatei.

– *Sichern* → *Start-Konfiguration* speichert alle Werte der Einstellungsbereiche sofort in der Konfigurationsdatei.

Das Menü *Ansicht* enthält folgende Einträge:

– *Kommandos* wechselt zwischen der Anzeige von Trap- und Kommando-Fenster.

– Die Funktion *Anzeigen Community* ermöglicht das Ein- und Ausblenden des Community String.

Unter *Hilfe* gibt es Informationen zur Version, zu den neuen Funktionen in Version V5.0, zum aktiven Fenster und über den Index.

Toolbar des Kommando-Fensters

Die Toolbar enthält eine Auswahl der im Menü angebotenen Funktionen. Sie soll einen schnellen Zugriff auf häufig benötigte Operationen erlauben. Ein Stichwort zu der hinter dem jeweiligen Icon verborgenen Funktionalität erhalten Sie, wenn der Mauszeiger länger als eine Sekunde auf dem Icon verweilt.

Die Toolbar umfasst die auf Seite 359 beschriebenen Gruppen:

– Die erste Gruppe enthält die Funktion *Test*, mit der Sie die Erreichbarkeit des angegebenen Systems via ICMP sowie die Status des SNMP-Masteragenten und des Console Monitor Subagenten prüfen können.

– Die zweite Gruppe ermöglicht:

  – Umschalten des aktuellen Arbeitsbereichs zwischen dem Arbeitsbereich eines Trap-Fensters und dem Arbeitsbereichs eines Kommando-Fensters

  – Ausblenden des Community-Strings

Die dritte Gruppe enthält die Funktionen zum Öffnen

– eines weiteren Kommando-Fensters sowie
– eines Fensters zum Anzeigen und Setzen von Filtern.

Arbeitsbereich des Kommando-Fensters

Der Arbeitsbereich des Kommando-Fensters besteht aus drei Teilen:

1. Bereich für die Einstellung des Systems und der SNMP-Parameter,
2. Kommandobereich,
3. Bereich zum Beantworten eine Konsolfrage.

Systemeinstellungen und Statuswerte

Im Arbeitsbereich des Kommando-Fensters werden die Parameter für SNMP eingestellt. Wurde das Kommando-Fenster aus einem anderen Fenster heraus aufgerufen, werden die Parameter aus dem aufrufenden Fenster übernommen, andernfalls die Defaultwerte gesetzt.

Mit der Combobox *System* definieren Sie das Zielsystem, an das das Kommando oder die Antwort gesendet werden soll. Die Liste der Combobox ist vorbelegt durch die Einträge in der Systemliste. Im zweiten Teil werden die SNMP-Parameter angegeben.

Kommandobereich

In diesem Bereich kann ein Kommando eingegeben werden. Ergebnis und Main-Return-Code werden angezeigt.

- Combobox *Kommando*

  Eingabe des Kommandos. Kommandos können direkt im Textfeld eingetragen und durch den Combobox-Mechanismus als *Temporäre Kommandos* in die Liste der Combobox übernommen werden. Die Liste der Combobox ist vorbelegt mit *Standard Kommandos*, die in der Menüleiste *Optionen* → *Einstellungen* → *Kommandos* definiert wurden. Dort können die Kommandos auch bearbeitet und *Temporäre Kommandos* in *Standard Kommandos* konvertiert werden

Ausgabe	**Bedeutung**
Ergebnis	Anzeige des Kommandoergebnisses
Return Code	Anzeige des Main Return Code des Kommandos

Aktionsknöpfe:

Bei Betätigen dieses Buttons wird das Kommando zur Ausführung an den Console Monitor Subagenten gesendet. Die Kommandoausgabe erscheint im Bereich Ergebnis. Im Fehlerfall wird hinter dem Eingabefeld die Meldung von SNMP ausgegeben.

Bei Betätigen dieses Buttons wird das Verfahren, das das Kommando an den Subagenten liefert und die Kommandoergebnisse holt, abgebrochen. Je nach Zustand kann nicht unbedingt davon ausgegangen werden, dass das Kommando nicht zur Ausführung kommt. In keinem Fall wird ein bereits vom Console Monitor abgesendetes Kommando abgebrochen.

poll Zeigt das Ergebnis des letzten Kommandos erneut an.

Bereich zur Beantwortung einer Konsolfrage

In diesem Bereich kann die Antwort auf eine von der Konsole eingetroffene Frage eingegeben werden. Als Zielsystem und SNMP-Parameter werden die aus dem ersten Bereich unter Systemeinstellungen angegebenen Werte genutzt.

Weitere Parameter:

Das Eingabefeld *Antwort* dient der Eingabe des Antworttextes.

Aktionsknöpfe:

Bei Betätigen dieses Buttons wird die Antwort an das angegebene System gesendet. Zwischen Eingabefeld und Aktionsknopf wird das Ergebnis der SNMP-Operation angezeigt. Kann die Antwort vom BS2000-System nicht korrekt verarbeitet werden, erscheint eine Konsolmeldung im Trap-Ausgabefenster.

Hilfezeile des Kommando-Fensters

Die Funktionalität der Hilfezeile entspricht derjenigen des Trap-Fensters (vgl. Seite 363).

9.2.1.4 Filter-Fenster

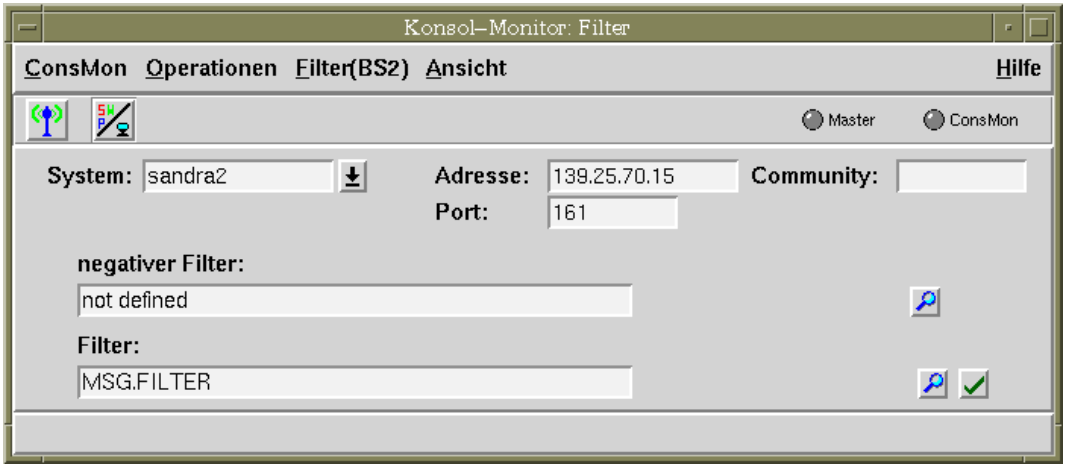


Bild 50: Filter-Fenster

Das Filter-Fenster entsteht bei Aufruf der Funktion *Bearbeiten* im Menü *Filter(BS2)*. Es dient der Anzeige und Änderung der am Console Monitor gesetzten BS2000-Meldungsfilterdatei. Über sie können Traps ausgefiltert werden, bevor sie über das Netz zur Management-Station gesendet werden, was die Netzbelastung verringert.

Auch das Filter-Fenster gliedert sich wie das Trap-Fenster in vier Bereiche:

1. die Menüleiste
2. die Toolbar
3. den Arbeitsbereich
4. die Hilfezeile.

Menüleiste des Filter-Fensters

Die Menüleiste umfasst die Menüs *ConsMon*, *Operationen*, *Ansicht* und *Filter (BS2)*.

Das Menü *Filter(BS2)* enthält:

– die Funktion *Anzeigen* zum Abfragen der am Agenten aktuell eingestellten Werte für den negativen Filter und die Filterdatei sowie

– die Funktion *Ändern* zum Setzen einer neuen Filterdatei.

Das Menü *Ansicht* ermöglicht über die Funktion *Anzeigen Community* das Ein- und Ausblenden des Community-String.

Toolbar des Filter-Fensters

Die Toolbar enthält eine Auswahl der im Menü angebotenen Funktionen. Sie soll einen schnellen Zugriff auf häufig benötigte Operationen erlauben. Ein Stichwort zu der hinter dem jeweiligen Icon verborgenen Funktionalität erhalten Sie, wenn der Mauszeiger länger als eine Sekunde auf dem Icon verweilt.

Die Toolbar umfasst zwei Gruppen:

– Mit der Funktion *Test* der ersten Gruppe können Sie
  – die Erreichbarkeit via ICMP des angegebenen Systems prüfen,
  – die Status von SNMP-Masteragent und Console Monitor Subagent prüfen.
– Mit der zweiten Gruppe können Sie den Community-String ausblenden.

Arbeitsbereich des Filter-Fensters

Der Arbeitsbereich des Filter-Fensters besteht aus drei Teilen:

1. dem Bereich für die Einstellung des Systems und der SNMP-Parameter
2. dem Bereich zur Anzeige des Dateinamens für die negativen Filter und
3. dem Bereich zur Anzeige und Eingabe des Namens der Filterdatei.

Systemeinstellungen und Statuswerte

In diesem Bereich werden die Parameter für SNMP eingestellt. Vorbelegt sind die Eingabefelder mit den Werten aus dem aufrufenden Fenster.

Combobox *System* Zielsystem, an dem die Meldungsfilterdatei gesetzt werden soll. Die Liste der Combobox ist vorbelegt durch die Systemliste.

Im zweiten Teil spezifizieren Sie die SNMP-Parameter.

negativer Filter

In diesem Bereich werden die Namen der aktuell eingestellten BS2000-Datei für die negativen Filter angezeigt.

Im Ausgabefeld *negativer Filter* wird beim Ausführen der Aktion *Anzeigen* der Name der aktuellen Filterdatei angezeigt.

Aktionsknopf:

Bei Betätigen dieses Buttons wird die am angegebenen System eingestellte BS2000-Datei für die negativen Filter angezeigt.

Filter

In diesem Bereich können Sie sich den Namen der aktuell eingestellten BS2000-Meldungsfilterdatei anzeigen lassen und gegebenenfalls einen anderen Meldungsfilter einstellen.

Im Ein-/Ausgabefeld *Filter* wird beim Ausführen der Aktion *Anzeigen* der Name der aktuellen Filterdatei angezeigt. Das Feld ist editierbar. Bei Ausführen der Aktion *Ändern* wird der im Feld eingetragene Name als BS2000-Meldungsfilterdatei im angegebenen System gesetzt.

Aktionsknöpfe:

Bei Betätigen dieses Buttons wird die am angegebenen System eingestellte BS2000-Meldungsfilterdatei angezeigt. Im Fehlerfall wird hinter dem Eingabefeld die Meldung von SNMP angegeben.

Bei Betätigen dieses Buttons wird der eingetragene Filter an den Console Monitor gesendet und von ihm als aktuelle BS2000-Meldungsfilterdatei gesetzt. Im Fehlerfall wird hinter dem Eingabefeld die Meldung von SNMP ausgegeben. *General Error* kann ein Hinweis darauf sein, dass die angegebene Filterdatei nicht gesetzt werden konnte, z.B. weil sie nicht existiert.

Änderungen der Datei können im laufenden Betrieb wirksam gemacht werden, indem der angezeigte Dateiname erneut gesetzt wird.

Hilfezeile des Filter-Fensters

Die Funktionalität der Hilfezeile entspricht derjenigen des Trap-Fensters (vgl. Seite 363).

9.2.1.5 Fenster zur Trap-Bestätigung

Das Fenster *Trap-Bestätigung* wird aktiviert bei Aufruf der Funktion *Bestätigung* im Menü *Meldungen*. Es dient zur Anzeige und Änderung der Trap-Bestätigung.

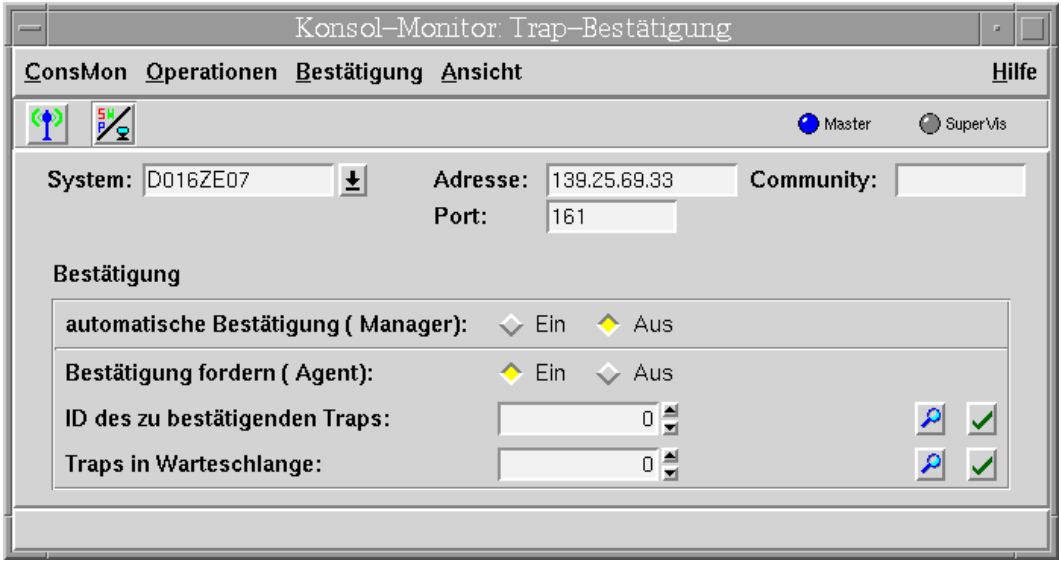


Bild 51: Fenster „Trap-Bestätigung“

Das Fenster *Trap-Bestätigung* gliedert sich in vier Bereiche:

– Menü-Leiste
– Toolbar
– Arbeitsbereich
– Hilfe-Zeile

Aufbau des Arbeitsbereichs

Der Arbeitsbereich des Fensters *Trap-Bestätigung* besteht aus drei Teilen:

– Bereich für die Einstellung des Systems und der SNMP-Parameter

– Bereich zur Einstellung der automatischen Trap-Bestätigung an der Console Monitor-Anwendung

– Bereich zur Einstellung der automatischen Trap-Bestätigung am Agenten

Systemeinstellungen und Statuswerte

In diesem Bereich stellen Sie die SNMP-Parameter ein.

Combobox System

In der Combobox *System* spezifizieren Sie das Zielsystem, an dem die Meldungsfilterdatei eingesetzt werden soll. Die Liste der Combobox ist vorbelegt mit den Einträgen aus der *System*-Liste.

Für den zweiten Teil der Parameter sind zwei Darstellungsarten möglich, die über Menü oder Toolbar eingestellt werden können:

– SNMP-Parameter
– Agentenstatus-Werte

automatische Bestätigung (Manager)

Mit dem Optionsfeld *automatische Bestätigung* können Sie die automatische Trap-Bestätigung am Manager ein- und ausschalten.

Trap-Bestätigung anfordern

Mit dem Optionsfeld *Bestätigung anfordern (Agent)* können Sie die automatische Trap-Bestätigung am Agenten ein- und ausschalten.

ID des zu bestätigenden Traps

Im Dialogfeld *ID des zu bestätigen Traps* wird die ID des Traps angezeigt, der auf eine Bestätigung wartet. Wenn Sie diesen Wert setzen, gilt der Trap als bestätigt.

Aktionsknöpfe:

Bei Betätigen dieses Buttons wird die ID des Traps angezeigt, der auf eine Bestätigung wartet. Diesen Wert können Sie ändern (reduzieren).

Durch Betätigen dieses Buttons bestätigen Sie den Trap mit der im Dialogfeld spezifizierten ID.

Traps in der Warteschlange

Im Dialogfeld *Traps in der Warteschlange* wird die Anzahl der Traps angezeigt, die sich in der Warteschlange befinden, weil ein zu bestätigender Trap noch nicht bestätigt wurde. Wenn Sie einen kleineren Wert als den angezeigten setzen, wird die Anzahl der Traps in der Warteschlange auf den spezifizierten Wert reduziert.

Aktionsknöpfe:

Bei Betätigen dieses Buttons wird die Anzahl der Traps in der Warteschlange angezeigt.

Durch Betätigen dieses Buttons setzen Sie die im Dialogfeld spezifizierte Länge der Warteschlange.

9.2.1.6 Reaktionen-Dialogbox

Die Dialogbox *Reaktionen* wird angezeigt bei Aufruf der Menüleiste *Optionen* → *Reaktionen* und ermöglicht das Festlegen von Reaktionen auf eintreffende Meldungen.

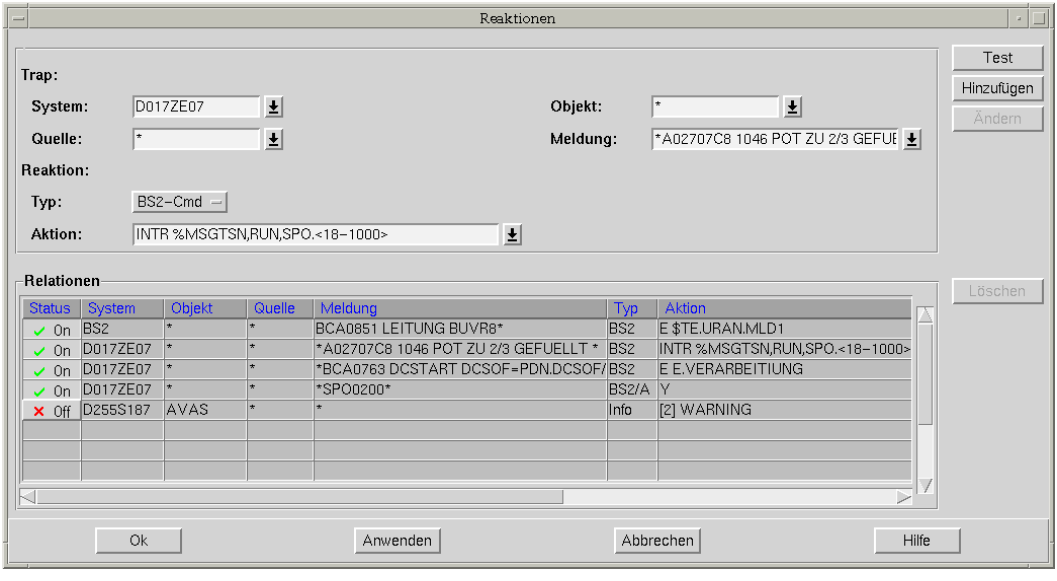


Bild 52: Reaktionen-Dialogbox

Das Fenster gliedert sich in vier Bereiche:

– Bereich für die Definition eines Ereignisses
– Bereich für die Definition der zugehörigen Reaktion
– Tabelle für die Auflistung aller definierten Relationen
– Aktionsbereich (Aktionsknöpfe) zur Bestätigung der Definitionen und Modifikationen

Definitionsbereich / Trap

Im Bereich für die Ereignisdefinition spezifizieren Sie die Ereignisse, bei denen die Reaktion ausgelöst wird. Dabei können Sie als Wildcard folgende Zeichen angeben:

– "*" für eine beliebige Zeichenkette
– "?" für ein beliebiges Zeichen

Zusätzliche Möglichkeiten sind für das Feld *Meldung* vorgesehen. Dabei wird der Filter aus der logischen UND-Verknüpfung der folgenden, in den vier Comboboxen des Fensters spezifizierten Parameter gebildet:

- Combobox *System*

  Durch die Angabe eines Systems oder einer Systemgruppe schränken Sie die Reaktion auf Traps ein, die von einem bestimmten System oder einer Gruppe von Systemen gesendet werden. Systemgruppen sind in der Form "[gruppenname]" zu spezifizieren. Bei der Eingabe von Gruppennamen müssen Sie die eckigen Klammern nicht angeben. Systemgruppen können Sie bearbeiten in der Menüleiste *Optionen* → *Einstellungen* → *Gruppen*. Die Angabe von "*" als Wildcard ist nicht erlaubt. Vorbelegt ist die Liste der Combobox durch die Systemliste und die bereits definierten Systemgruppen.

- Combobox *Quelle*

  Den Quellen-Filter können Sie direkt in das Textfeld eintragen. Die Reaktion beschränkt sich dann auf die entsprechenden Quellen. Die Angabe von "*" schränkt die Reaktionen nicht auf eine bestimmtes Quelle ein. Vorbelegt ist die Liste der Combobox mit den Filtereinträgen, die in der Menüleiste *Optionen* → *Einstellungen* → *Meldungen* unter "Quellen-Filter bearbeiten" definiert sind.

- Combobox *Objekt*

  Den Objekt-Filter können Sie direkt in das Textfeld eintragen. Die Reaktion beschränkt sich dann auf die spezifizierten Objekte. Vorbelegt ist die Liste der Combobox mit den Filtereinträgen, die in der Menüleiste *Optionen* → *Einstellungen* → *Meldungen* unter "Objekt-Filter bearbeiten" definiert sind.

- Combobox *Meldung*

  Den Meldungsfilter können Sie direkt in das Textfeld eintragen. Ausgewertet wird dieser Filter durch Vergleich des spezifizierten Strings mit der Nettonachricht nach den "global style"-Regeln. Insbesondere ist damit auch die Einschränkung auf das Gewicht einer Meldung möglich. Vorbelegt ist die Liste der Combobox mit den Filtereinträgen, die in der Menüleiste *Optionen* → *Einstellungen* → *Meldungen* unter "Meldungs-Filter bearbeiten" definiert sind.

Beginnt die Definition des Meldungsfilters mit "[RE]", so wird der nachfolgende Ausdruck mit der Meldung als regulärer Ausdruck verglichen. Dies bietet mehr Möglichkeiten als ein Vergleich nach "global-style"-Regeln. Außerdem lassen sich so nahezu beliebige Teilausdrücke für die Übernahme ins Kommando definieren.

Definitionsbereich / Reaktion

Im Definitionsbereich legen Sie außerdem die Reaktionen auf die definierten Ereignisse fest. Eine Reaktion wird in zwei Schritten definiert:

1. Reaktionstyp spezifizieren
2. Reaktion festlegen

Den Typ einer Reaktion spezifizieren Sie mit dem Optionenmenü *Typ*, in dem folgende Reaktionstypen zur Auswahl stehen:

Reaktionstyp	**Beschreibung**	**Anzeige in der Tabelle „Reaktionen“**
BS2-Cmd	BS2000-Konsol-Kommando ohne Ergebnisanzeige	BS2
BS2-Cmd/out	BS2000-Konsol-Kommando mit Ergebnisanzeige	BS2/O
BS2-Antwort	BS2000-Antwort auf eine Frage	BS2/A
Shell-Cmd	lokales Kommando ohne Ergebnisanzeige	Shell
Inform	farbige Markierung der Meldung	Info
Löschen	Löschen der Meldung	Del
Bell	Tonsignal	Bell

Je nachdem, welchen Reaktionstyp Sie im Optionenmenü *Typ* spezifizieren, werden Ihnen unterschiedliche Eingabefelder angeboten, in denen Sie die gewünschte Reaktion festlegen können.

- Reaktionstyp *BS2-Cmd* oder *BS2-Cmd/out*

  Angeboten wird die Combobox *Aktion*. Sie können die BS2000-Konsol-Kommandos ohne/mit Ergeebnisanzeige wahlweise

  – direkt in das Textfeld der Combobox eintragen oder
  – Combobox-Liste übernehmen.

  Die Combobox-Liste ist vorbelegt mit den Standard-Kommandos, die in der Menüleiste *Optionen →Einstellungen →Kommandos* bereits definiert wurden.

- Reaktionstyp *BS2-Antwort*

  Zur Eingabe der Antwort wird ein Eingabefeld *Aktion* angeboten. Die TSN wird dabei der Antwort automatisch vorangestellt.

- Reaktionstyp *Shell-Cmd*

  Zur Eingabe des lokalen Kommandos wird ein Eingabefeld *Aktion* angeboten.

- Reaktionstyp *Information*

  Angeboten wird ein Eingabefeld *Aktion*. Um die Meldung farbig zu markieren, spezifizieren Sie im Eingabefeld eines der Schlüsselwörter ERROR, WARNING oder MESSAGE.

- Reaktionstyp *Löschen*
- Reaktionstyp *Bell*

Bei Eingabe eines Kommandos bestehen folgende Möglichkeiten, Teile der Meldung in das Kommando zu übernehmen:

1. Schlüsselwörter:

Schlüsselwort	**Bedeutung**
%ALL	bezeichnet die gesamte Meldung.
%DEVICE	bezeichnet das Objekt.
%SYSTEM	bezeichnet das Absendersystem.
%SOURCE	bezeichnet die Quelle.
%MSGTXT	bezeichnet den Meldungstext.
%MSGWEIGHT	bezeichnet das Gewicht.
%MSGNUMBER	bezeichnet die Meldungsnummer.
%MSGTSN	bezeichnet die TSN.
%MSGSEQNR	bezeichnet die Sequenznummer.

2. feste Position der Meldung:

<a-b>	bezeichnet die Zeichen zwischen den Positionen a und b (inklusive a und b); maximal können 10 Bereiche ausgewählt werden.

3. reguläre Teilausdrücke:

   %i bezeichnet den i-ten regulären Teilausdruck der Meldung.
   Voraussetzung: Der Meldungsfilter muss als regulärer Ausdruck definiert sein.

4. Meldungsinserts:

   &i bezeichnet den i-ten Insert der Meldung.
   Voraussetzung: Der Meldungstyp muss in der Datei *bs2msge.dat* hinterlegt sein.

Optional können Sie durch ein der Aktion vorangestelltes "[<time>]" eine Verzögerung der Reaktionsausführung von <time> Minuten festgelegt werden. In diesem Fall die Reaktion nur dann ausgelöst, wenn zum Zeitpunks des Starts die Meldung noch nicht gelöscht ist.

Tabelle der Relationen

In diesem Bereich werden die Relationen zwischen den eintreffenden Meldungen und den generierten Reaktionen tabellarisch dargestellt. Die Tabellenzeilen sind lexikografisch nach den Systemnamen geordnet. In den Tabellenspalten werden die folgenden Informationen angezeigt:

Status (act) Angabe, ob die Reaktion aktiviert ist (*On*) oder nicht (*Off*). Durch Anklicken dieses Feldes mit der linken Maustaste kann der Status geändert werden.

System Dieser Parameter entspricht dem Parameter *System* im Definitionsbereich / Trap (siehe Seite 376).

Objekt Dieser Parameter entspricht dem Parameter *Objekt* im Definitionsbereich / Trap.

Quelle Dieser Parameter entspricht dem Parameter *Quelle* im Definitionsbereich /Trap.

Meldung Dieser Parameter entspricht dem Parameter *Meldung* im Definitionsbereich /Trap.

Typ Dieser Parameter entspricht dem Parameter *Typ* im Definitionsbereich / Reaktion (siehe Seite 377).

Aktion (Kommando) Dieser Parameter entspricht dem Parameter *Aktion* im Definitionsbereich / Reaktion.

Die Reaktionentabelle unterliegt den Standardregeln für eine erweiterte Selektion.

Aktionsknöpfe im Aktionsbereich

Test Dieser Aktionsknopf ist nur dann aktiv, wenn mindestens ein Eintrag in der Tabelle *Traps* des Hauptfensters selektiert ist. Es wird geprüft, ob die Angaben im *Definitionsbereich* / *Reaktionen* beim Eintrffen eines solchen Traps zu einer Reaktion führen würden. Das Ergebnis wird in einem Meldungsfenster angezeigt.

Hinzufügen Die Angaben im *Definitionsbereich* / *Trap* und im *Definitionsbereich* / *Reaktionen* werden in die Tabelle lexikografisch eingefügt.

Ändern Dieser Aktionsknopf ist nur dann aktiv, wenn genau ein Eintrag in der Tabelle selektiert ist. Die Angaben im *Definitionsbereich / Trap* und im *Definitionsbereich / Reaktion* ersetzen den selektiven Eintrag.

Löschen Dieser Aktionsknopf ist nur dann aktiv, wenn mindestens ein Eintrag in der Tabelle selektiert ist. Die selektierten Einträge werden gelöscht.

Ok Die Einstellungen werden übernommen, die Dialogbox wird geschlossen. Gültig sind nur die Definitionen, die in der Tabelle vermerkt sind, nicht jedoch die Definitionen im Definitionsbereich.

Anwenden Die Einstellungen werden übernommen, die Dialogbox bleibt geöffnet. Gültig sind nur die Definitionen, die in der Tabelle vermerkt sind, nicht jedoch die Definitionen im Definitionsbereich.

Abbrechen Die Einstellungen werden verworfen, die Dialogbox wird geschlossen.

Hilfe Der spezifizierte Hilfetext wird angezeigt.

Beispiele zu den Reaktionen

Beispiel 1:

Bei Eintreffen der Meldung

```
%BCAM-000.060653 %BCA0763 /DCSTART DCSOF=PDN.DCSOF/ACK>
```

soll folgender Enter-Job ausgeführt werden:

```
/E E.VERARBEITUNG
```

Meldung: *BCA0763 DCSTART DCSOF=PDN.DCSOF/ACK*
Typ: BS2-Cmd
Aktion: E E.VERARBEITUNG

Beispiel 2a:

Jede Frage mit der Meldungsnummer SPS0200, z.B.

```
?SPAA-000.060653 % SPS0200 TSN '7163':FORM 'FTPR' MOUNTED ON PRINTER 'L0'
REPLY (...)
```

soll mit "Y" beantwortet werden:

```
/SPAA.Y
```

Meldung: *SPS0200*
Typ: BS2-Antwort
Aktion: Y

Beispiel 2b:

Jede Frage mit der Meldungsnummer SPS0200 vom Drucker "L0", z.B.

```
?SPAA-000.060653 % SPS0200 TSN '7163':FORM 'FTPR' MOUNTED ON PRINTER 'L0'
REPLY (...)
```

soll mit "Y" beantwortet werden:

```
/SPAA.Y
```

Meldung: *SPS0200* MOUNTED ON PRINTER 'L0'*
Typ: BS2-Antwort
Aktion: Y

Beispiel 3:

Bei Eintreffen der Meldung

```
%1848-000.060653 BINDEX A02707C8 1046 POT zu 2/3 gefuellt
```

soll folgendes Kommando abgesetzt werden:

```
/INTR 1848,RUN,SPO,BINDEX
```

Dabei sind TSN und Programmname "BINDEX" zu übernehmen.

Meldung: *A02707C8 1046 POT zu 2/3 gefuellt*
Typ: BS2-Cmd
Aktion: /INTR %MSGTSN,RUN,SPO,<18-1000>

Beispiel 4:

Alle Meldungen der Quelle "Hardware" sollen in der Datei *./trace* auf dem lokalen System protokolliert werden.

Quelle: *Hardware*
Meldung: *
Typ: Shell-Cmd
Aktion: cmd.exe /C "echo { %ALL} >>./trace"

Beispiel 5:

Fragen, die länger als zwei Minuten unbeantwortet bleiben, werden als Warnung markiert.

Quelle: *
Meldung: <*> \?*
Typ: Information
Aktion: [2] WARNING

9.2.1.7 Trap-Filter

Für Traps im allgemeinen Format bietet der Trap-Filter die Möglichkeit, die Traps mit Werten für "Source" und "Device" zu versorgen. Außerdem lassen sich mit dem Trap-Filter Traps völlig unterbinden. (Für Application Monitor-spezifische Traps bestehen die genannten Möglichkeiten nicht.)

Dateien und Verzeichnisse

Durch die Umsetzung wird eine Datei *trap.cnf* ausgewertet. Die Datei *trap.cnf* muss unter *<CMONBASE>/config* liegen.

Einträge in der Datei *trap.cnf*

Ein Eintrag in der Datei *trap.cnf* hat die folgende Sysntax:

```
<filter> <aktion>

<filter> ::= <IP-Adresse>:<community>:<trapoid>
```

<IP-Adresse>
IP-Adresse oder * (beliebige IP-Adresse)

<community>
Community-String oder * (beliebige Community)

<trapoid>
OID des Trap oder * (beliebige Trap-OID)

```
<aktion> ::= ignore | <host>:<source>:<device>:<text>
```

ignore
Trap soll ignoriert werden

<host>
IP-Adreese des Host oder * (unverändert übernehmen)

<source>
Sourcename oder * (unverändert übernehmen)

<device>
Gerätename oder * (unverändert übernehmen)

<text>
Text oder * (unverändert übernehmen)

Bei <source>, <device> und <text> bestehen folgende Möglichkeiten, Teile der Variablenbindung des Trap zu übernehmen:

– `%V(<oid>)` wird ersetzt durch den Wert der Variablenbindung.

– `%I(<oid>)` wird ersetzt durch die Instanz der Variablenbindung.

i Voraussetzung ist, dass dem Console Monitor Subagenten die MIB bekannt ist.

Beispiele:

```
*:*:1.3.6.1.4.1.231.99.0.333   ignore
*:*:1.3.6.1.4.1.231.99.0.444   *:TestSource:TestDevc::Das ist ein Text
*:*:1.3.6.1.4.1.231.99.0.555   ignore
*:*:1.3.6.1.4.1.231.99.0.666   139.25.105.176:TestSource:TestDevc:*
139.25.22.22:*:1.3.6.1.4.1.231.2.34.2.0.301   *:supervisor:%V(1.3.6.1.4.1.231.2.34.1.2.2.1.1):Gestartet
```

9.2.1.8 Einstellungen der Optionen-Dialogbox

Die Dialogbox *Optionen* entsteht bei Aufruf der Funktion *Optionen* → *Einstellungen* und dient der Einstellung von Parametern für die laufende Sitzung. Bei Bedarf können die Einstellungen bei Beendigung der Management-Anwendung gesichert werden

Die Beschreibung zur Dialogbox *Optionen* entnehmen Sie bitte der Seite 396 ff.

9.2.2 Anwendung PMBS2 für den Performance-Monitor

PMBS2 unterstützt die Ausgabe der vom Performance-Monitor SSA-SM2-BS2 gelieferten SM2-Daten auf die Management-Station und bietet eine grafische Übersicht über die Performance-Daten aller BS2000/OSD-Systeme in einem Netz.

Funktionalität

Der Performance-Monitor liefert zum einen Informationen zum SM2 selbst:

– Status des SM2,
– Version,
– Größe des Messintervalls,
– Stichprobenzyklus.

Die eigentlichen Messwerte lassen sich entsprechend der Reportgruppen des SM2 im Wesentlichen in sieben Objektgruppen einteilen:

Objektgruppe	**Messwerte**
BASIC	Basisgruppe
TIMEIO	CPU Auslastung und I/O-Aktivität
MEMORY	Auslastung des Hauptspeichers und des virtuellen Adressraumes
CATEGORY	Belegung des Hauptspeichers durch die vier Standardkategorien von Tasks
DEVICES	Ein- und Ausgabeoperationen auf periphere Geräte während eines Messintervalls
UTM	applikationsspezifische Daten von UTM-Anwendungen
PERTASK	Verbrauchswerte einzelner Tasks

Hinsichtlich der Darstellung der Werte werden zwei Typen von Objekten unterschieden:

Skalare Objekte: verfügen über nur eine Instanz. Zu diesen zählen die Objektgruppen BASIC, MEMORY und CATEGORY.

Tabellenobjekte: sind Objekte, die über mehrere Instanzen verfügen können. So können z.B. die Informationen zur CPU-Auslastung und die Messwerte zum IO-Report separat für die generierten logischen Maschinen, wie auch für das gesamte System angezeigt werden. Ebenso werden die Werte für DEVICES, UTM und PERTASK tabellarisch aufgelistet. Eine konkrete Instanz eines Tabellenobjektes kann man als skalares Objekt auffassen.

Starten und Beenden von PMBS2

PMBS2 wird auf UNIX-Systemen aus der Shell-Ebene durch Aufruf der Prozedur *PerfMon* gestartet. Es erscheint das Hauptfenster der Anwendung.

Auf Windows NT wird die Anwendung aus der Programmgruppe *SNMP Management Applications* heraus gestartet. Alternativ kann sie durch Doppelklick auf den Eintrag *PerformancMonitor* im Verzeichnis *<tcldir>\appl\ pmbs2* aufgerufen werden.

PMBS2 kann aus jedem Fenster heraus beendet werden, indem im Menü *PerfMon* die Funktion *PerfMon Beenden* ausgewählt wird. Unbeabsichtigtes Beenden wird durch eine Sicherheitsabfrage vermieden. Je nach Einstellung der Parameter für *Sichern* werden Veränderungen der Parameter gesichert, verworfen oder abgefragt.

9.2.2.1 Hauptfenster

Das Hauptfenster entsteht bei Aufruf von PMBS2. Von ihm ausgehend können Fenster für Diagramme geöffnet werden. Wird dieses Fenster geschlossen, so wird PMBS2 beendet.

Das Fenster gliedert sich in vier Bereiche:

1. Menüleiste
2. Toolbar
3. Arbeitsbereich
4. Hilfezeile.

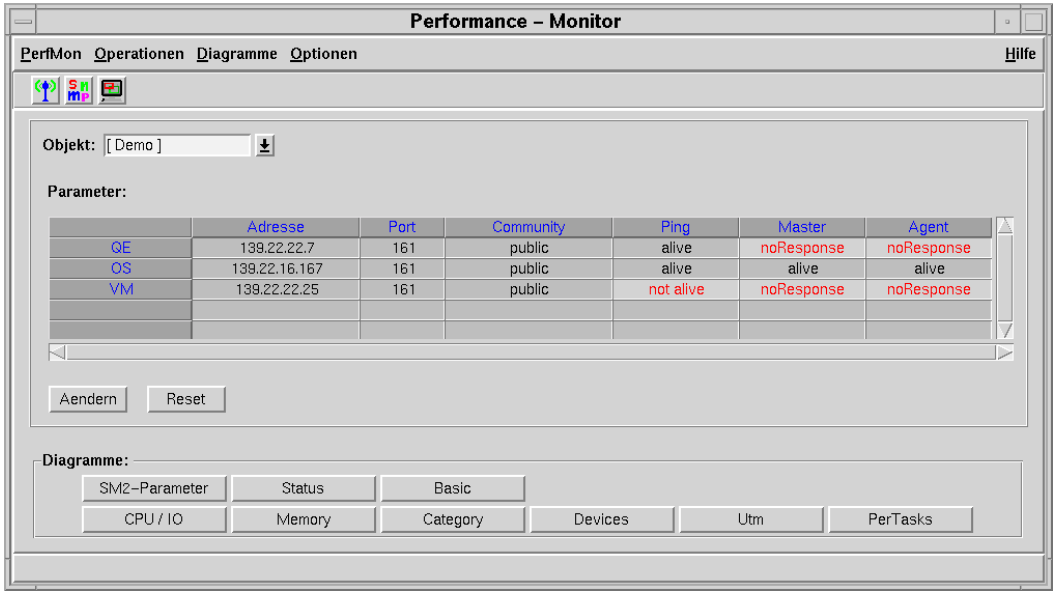


Bild 53: Hauptfenster des Performance-Monitors

Menüleiste

Die Menüleiste umfasst die Menüs *PerfMon*, *Operationen*, *Diagramme*, *Optionen* und *Hilfe*.

Das Menü *PerfMon* enthält den Eintrag *PerfMon Beenden*.

Das Menü *Operationen* enthält:

- die Funktion *Ping Test*, mit der die Erreichbarkeit des angegebenen Systems via ICMP geprüft werden kann. Ist das angegebene System erreichbar, wird für das System in der Spalte *Ping* der im Arbeitsbereich liegenden Tabelle das Wort *alive* eingetragen, andernfalls *not alive*. Diese Funktion ist nur für UNIX-Systeme aktiv. In der Dialogbox *Optionen* → *Einstellungen* → *Ping* können Parameter für die Ping-Funktion eingestellt werden.
- die Funktion *SNMP Test*, mit der der Status des SNMP-Masteragenten durch Abruf der *SysUpTime* kontrolliert werden kann. Ist der Masteragent des angegebenen Systems erreichbar, wird für das System in der Spalte *Master* der Tabelle *Parameter* das Wort *alive* eingetragen, andernfalls erscheint die Fehlermeldung von SNMP.
- die Funktion *Pmon Test*, mit der der Status des Performance-Monitor durch Abfrage der Version angezeigt werden kann. Ist der Subagent des angegebenen Systems erreichbar, wird für das System in der Spalte *Agent* der Tabelle das Wort *alive* eingetragen, andernfalls erscheint die Fehlermeldung von SNMP.

Die drei genannten Tests sind Kontrollmöglichkeiten in aufsteigender Folge.

Das Menü *Diagramme* enthält die Einträge zum Aufruf der Diagrammfenster für die verschiedenen vordefinierten Diagrammgruppen. Jede Diagrammgruppe entspricht einer vom Performance-Monitor kontrollierten Messwertgruppe des SM2. Das spezielle Aussehen der Diagramme und die anzuzeigenden Werte hängen neben der Diagrammgruppe auch davon ab, ob ein oder mehrere Systeme überwacht werden.

Optionen enthält die folgenden Einträge:

– *Einstellungen*. *Einstellung* öffnet eine Optionen-Dialogbox, in der Einstellungswerte editiert werden können.

– *Sichern* → *Einstellungen* speichert alle Werte der Einstellungsbereiche sofort in der Konfigurationsdatei. Der Menüeintrag *Sichern* ist nur aktiv, wenn alle Dialogboxen geschlossen sind.

Im Menü *Hilfe* gibt es Informationen zur Version, zum *Sichern*, zum aktiven Fenster, zu den Objekten der MIB und zum Index (Übersicht).

Toolbar

Die Toolbar enthält eine Auswahl der im Menü angebotenen Funktionen. Sie soll einen schnellen Zugriff auf häufig benötigte Operationen erlauben. Ein Stichwort zu der hinter dem jeweiligen Icon verborgenen Funktionalität erhält man, wenn der Mauszeiger länger als eine Sekunde auf dem Icon verweilt. Über eine Toolbar verfügen Hauptfenster und Diagrammfenster.

Die Toolbar umfasst folgende Funktionen:

– Mit der Funktion *Ping Test* kann die Erreichbarkeit des angegebenen Systems via ICMP geprüft werden. *Ping Test* ist nur für UNIX-Systeme aktiv.

– Mit der Funktion *SNMP Test* kann der Status des SNMP-Masteragenten durch Abruf der *SysUpTime* kontrolliert werden.

– Mit der Funktion *Pmon Test* kann der Status des Performance-Monitor durch Abfrage der Version angezeigt werden.

Arbeitsbereich

Der Arbeitsbereich des Hauptfensters besteht aus zwei Teilen:

1. dem Bereich für die Einstellung des zu überwachenden Systems bzw. der Systemgruppe und seiner Parameter, sowie deren Tests und
2. Aktionsknöpfen zum Aufruf der Fenster für die vordefinierten Diagrammklassen.

Einstellungen und Tests

Um eine Nachricht via SNMP korrekt an ein System senden zu können, ist die Angabe der IP-Adresse des Zielsystems, eines Ports und eines Community-Strings nötig. Der Community-String bestimmt die Zugangsberechtigung und den Berechtigungsumfang. In diesem Bereich können diese Einstellungen vorgenommen werden.

- Combobox *Objekt*

  Durch die Angabe eines Objektes werden die Zeilen der nachstehenden Tabelle und die Systemnamen für die weiteren Fenster vorbelegt. Gruppen werden durch [gruppenname] dargestellt. Bei der Eingabe von Gruppennamen müssen die eckigen Klammern nicht angegeben werden. Die Bearbeitung von Gruppen erfolgt in der Menüleiste *Optionen →Einstellungen → Gruppen*. Die Liste der Combobox ist vorbelegt durch die Systemliste und die bereits definierten Systemgruppen.

- Tabelle *Parameter*

  In der Tabelle werden für jedes System die SNMP-Transportparameter sowie die Erreichbarkeit von System, Masteragent und Performance-Subagent angezeigt. Adresse, Port und Community können direkt in der Tabelle editiert werden. Eine Änderung muss mit dem Aktionsknopf *Ändern* bestätigt werden. Bis zur Bestätigung ist ein Rücksetzen der Werte durch *Reset* möglich.

  In der Spalte *Ping* wird bei Aufruf der Funktion *Operationen → Ping Test* die Erreichbarkeit des angegebenen Systems via ICMP angezeigt.

  In der Spalte *Master* wird bei Aufruf der Funktion *Operationen → SNMP Test* die Erreichbarkeit des Masteragenten dokumentiert.

  In der Spalte *Agent* wird bei Aufruf der Funktion *Operationen → Pmon Test* die Erreichbarkeit des Performance Subagenten angezeigt.

Aktionsknöpfe

Ändern	Die Änderungen der SNMP-Parameter werden wirksam. Die Veränderungen betreffen allerdings nicht bereits geöffnete Diagrammfenster.
Reset	Noch nicht bestätigte Änderungen werden zurückgesetzt.

Diagramme

Dieser Bereich enthält die Aktionsknöpfe zum Aufruf der Fenster für die vordefinierten Diagrammklassen. Jede Diagrammklasse entspricht einer vom Agenten kontrollierten Messwertgruppe des SM2. Alternativ können die Fenster auch über das Menü *Diagramme* geöffnet werden.

9.2.2.2 Diagrammfenster

Ein Diagrammfenster wird aus dem Hauptfenster heraus aufgerufen. Dabei übernimmt es die Angabe des Systems oder der Systemgruppe und somit auch die SNMP-Transportparameter.

Das Fenster gliedert sich wie das Hauptfenster in vier Bereiche:

1. die Menüleiste
2. die Parameterleiste
3. den Arbeitsbereich
4. die Hilfezeile.

Menüleiste

Die Menüleiste umfasst die Menüs *PerfMon*, *Operationen*, *Schwellwerte* und *Hilfe*.

Das Menü *PerfMon* enthält den Eintrag *PerfMon Beenden*.

Das Menü *Operationen* enthält den Eintrag *Schließen*, mit dem das Diagrammfenster wieder geschlossen werden.

Das Menü *Schwellwert* ist nur für Kurvendiagramme aktiv. Der Checkbutton *Aktiv* aktiviert bzw. deaktiviert die Schwellwertüberwachung. Über den Menüeintrag *Einstellung* wird die Dialogbox zum Einstellen der Schwellwertparameter geöffnet.

Aktiv	aktiviert bzw. deaktiviert die Schwellwertüberwachung.
Einstellung	Öffnen einer Dialogbox zum Einstellen der Schwellwertparameter.

Das Hilfemenü ist identisch mit dem des Hauptfensters und liefert Informationen zur Version, zum aktiven Fenster, zu den Objekten der MIB und eine Übersicht mit Index.

9.2.2.3 Parameterleiste

In der Parameterleiste können Einstellungen vorgenommen werden, die die Anzeige in den Diagrammen beeinflussen.

Combobox *System*

System oder Systemgruppe, von denen die Performancewerte angezeigt werden sollen. Das Eingabefeld ist vorbelegt durch die Auswahl des Systems bzw. der Systemgruppe im Hauptfenster. Während die Angabe eines Einzelsystems auch im Diagrammfenster geändert werden kann, ist dies für Systemgruppen nicht möglich. Die Liste der Combobox ist vorbelegt durch die Einträge in der Systemliste.

Skala *Pollintervall*

Zeitabstand, in dem PMBS2 die Werte vom Subagenten abgefragt. Da SM2 seine Werte nur in einem bestimmten Zyklus - Default 120 Sekunden - aktualisiert (*SM2Parameter → Intervall*), sind Pollzeiten kleiner diesem Intervall nicht sinnvoll.

Aktionsknöpfe:

– *Start*

  Mit diesem Aktionsknopf wird der Poll gestartet und gestoppt. Ist das Pollintervall auf "0" eingestellt, wird ein einzelner Request gesendet.

– *Grid*

  Mit diesem Aktionsknopf kann in Kurven- und Balkendiagrammen ein Koordinatennetz eingeblendet werden.

– *Stack*

  Dieser Aktionsknopf bewirkt in Balkendiagrammen das Umschalten der Anzeige zwischen Parallel- und Stackmodus.

Arbeitsbereich

Der Arbeitsbereich des Diagrammfensters ist als "Notebook" gebildet. Auf jeder Seite werden ein oder mehrere Diagramme dargestellt. Die Art des Diagramms ist abhängig vom Typ des darzustellenden MIB-Objektes und von der Anzahl der überwachten Systeme.

Folgende Diagrammtypen sind möglich:

Formular

Formulare werden verwendet für die Anzeige der aktuellen Werte skalarer MIB-Objekte eines Systems. Die Werte werden in einfachen Ausgabefeldern angezeigt.

Tabelle

Tabellen werden verwendet für die Anzeige der aktuellen Werte skalarer MIB-Objekte mehrerer Systeme. Sie finden auch Anwendung bei der Darstellung der zeitlichen Änderung von Werten eines Systems. Die Werte werden tabellarisch aufgelistet.

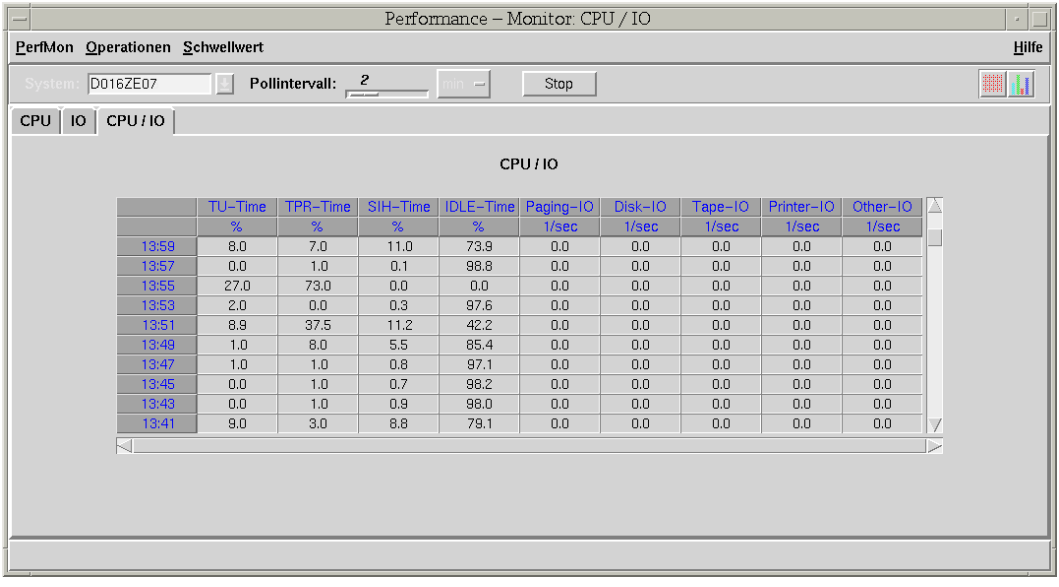


Bild 54: Anzeige von Werten skalarer MIB-Objekte in einer Tabelle

Kurvendiagramme

Kurvendiagramme dokumentieren die zeitliche Veränderung von Werten eines Systems oder mehrerer Systeme.

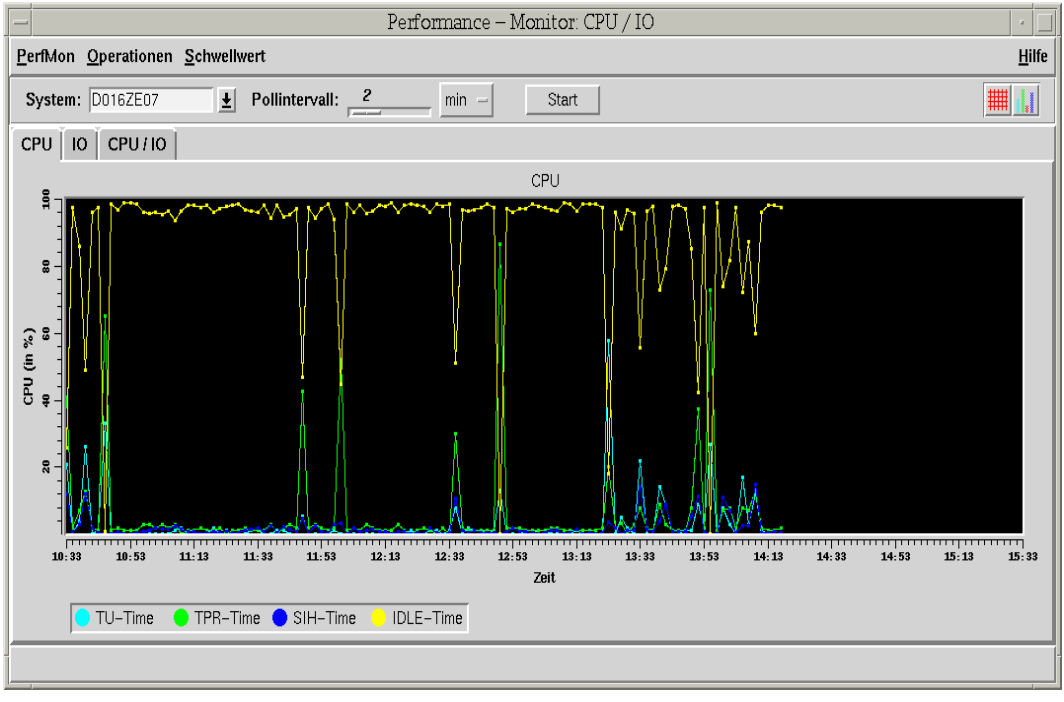


Bild 55: Kurvendiagramm

Durch Überstreichen eines Kurvenbereichs (klicken - ziehen - klicken) kann der markierte Bereich gezoomt werden. Durch einen Klick mit der rechten Maustaste kann in die Ausgangsposition zurückgesetzt werden.

Wenn der Mauszeiger auf einem Element der Legende positioniert ist, wird die zugehörige Kurve optisch hervorgehoben.

Balkendiagramme

Balkendiagramme zeigen die aktuellen Werte mehrerer Objekte von mehreren Systemen.

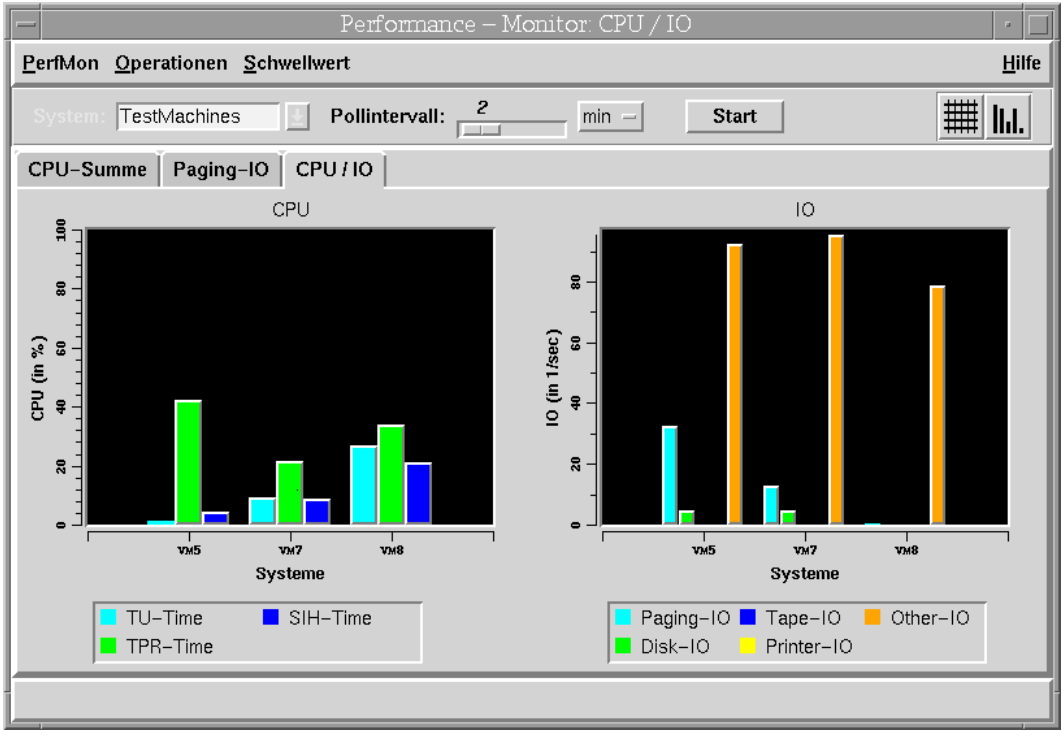


Bild 56: Anzeige der aktuellen Werte mehrerer Systeme in einem Balkendiagramm

Hilfezeile

Ein Doppelklick auf einen Gruppennamen im Eingabefeld System zeigt in der Hilfezeile die Konfiguration der Gruppe. Ist unter *System* ein Einzelsystem eingetragen, so werden in der Hilfezeile die SNMP-Transportparameter angezeigt. Darüber hinaus erscheinen in der Hilfezeile Fehlermeldungen von SNMP.

9.2.2.4 Generierung der Diagramme

Für jede Messwertgruppe sind eine Reihe von Diagrammen sowohl für die Überwachung eines Systems, als auch einer Gruppe von Systemen generiert. Die Beschreibungsdateien mit Namen *gen....tcl* sollen nach Möglichkeit nicht verändert werden. Die Parameter sind aber größtenteils selbsterklärend oder in den Dateien kommentiert. Bei guter Kenntnis der Performance-MIB können Sie kleine Veränderungen und Anpassungen ohne Schwierigkeiten selbst versuchen.

Eine besondere Rolle spielt das Statusdiagramm. Es zeigt, auf welche Messbereiche des SM2 der Subagent derzeit überhaupt Zugriffsmöglichkeit hat und gegebenenfalls warum nicht.

9.2.2.5 Einstellungen der Schwellwert-Dialogbox

Die Dialogbox *Schwellwerte* entsteht bei Aufruf der Funktion *Schwellwerte* → *Einstellung* und dient der Einstellung von Schwellwertparametern für die laufende Sitzung. Die Einstellung von Schwellwerten ist nur für Kurvendiagramme möglich.

Die Dialogbox ist als "Notebook" dargestellt und gliedert sich entsprechend der im zugehörigen Diagrammfenster definierten Kurvendiagramme.

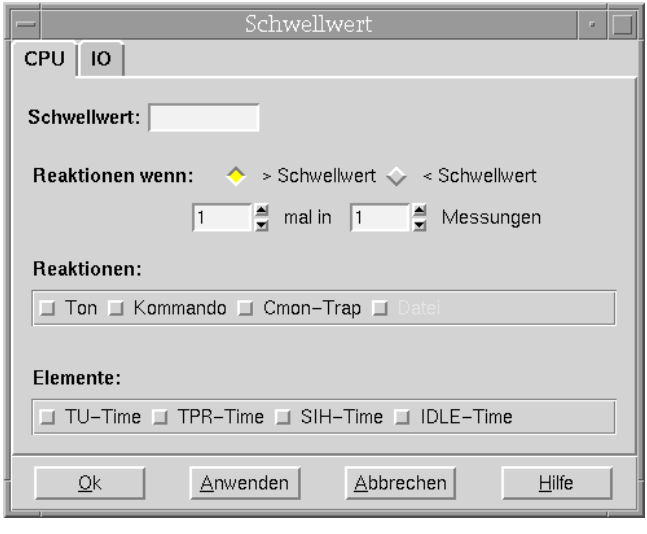


Bild 57: Dialogbox „Schwellwerte“

Feld	Bedeutung
Eingabefeld *Schwellwert*	Angabe des Schwellwertes. Erfolgt keine Angabe, wird kein Schwellwert ausgewertet.
Radiobutton *Reaktion bei*	Angabe, ob die Reaktion bei einer Unter- oder Überschreitung des Schwellwertes erfolgen soll.
Eingabefelder *x* 'mal in' *y* 'Messungen'	Eine Reaktion erfolgt nur, wenn die Anzahl der Überschreitungen unter den letzten *y* Messungen mindestens *x* beträgt **und** der Wert der aktuellen Messung den angegebenen Schwellwert überschreitet.
Checkbutton *Reaktion*	Angabe, welche Reaktion bei Überschreitung des Schwellwertes erfolgen soll. Die Angabe des Shell-Kommandos und der Datei erfolgt in der Parameterdatei.
Checkbutton *Elemente*	Angabe, für welche Elemente des Diagramms die Schwellwert-Überwachung gelten soll.
OK	Die Einstellungen werden übernommen, die Dialogbox geschlossen.
Anwenden	Die Einstellungen werden übernommen, die Dialogbox bleibt geöffnet.
Abbrechen	Die Einstellungen werden verworfen, die Dialogbox geschlossen.
Hilfe	Der Hilfetext zur Schwellwert-Dialogbox wird angezeigt.

Wenn ein Schwellen-Wert eingestellt ist, kann er vom Diagramm-Fenster mit der mittleren Maustaste verschoben werden.

9.2.2.6 Einstellungen der Optionen-Dialogbox

Die Dialogbox *Optionen* entsteht bei Aufruf der Funktion *Optionen* → *Einstellungen* und dient der Einstellung von Parametern für die laufende Sitzung. Beispielsweise kann für die Oberfläche die Landessprache (deutsch/englisch) eingestellt werden. Bei Bedarf können die Einstellungen bei Beendigung der entsprechenden Management-Anwendung gesichert werden. Die folgende Beschreibung gilt sowohl für CMBS2 als auch für PMBS2.

Die Dialogbox erscheint als "Notebook". Die folgende Tabelle zeigt die vorhandenen Bereiche bezogen auf die entsprechende Management-Anwendung:

Bereich	CMBS2	PMBS2
Systeme	X	X
Gruppen	X	X
Ping	X	X
SNMP	X	X
Meldungen	X	
Kommandos	X	
Reaktionen		X
Protokoll	X	
Sichern	X	X

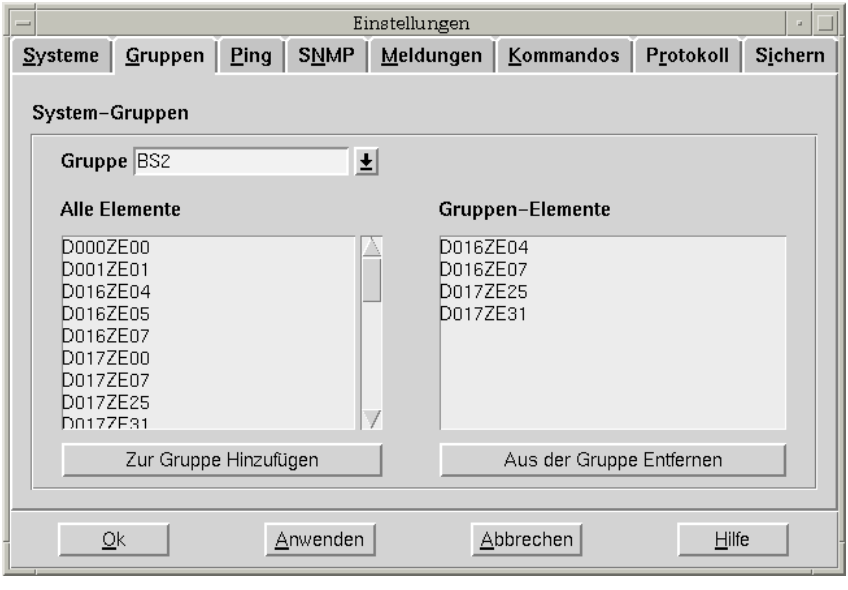


Bild 58: Optionen-Dialogbox des Console Monitors

Systeme

Systeme gilt sowohl für CMBS2 als auch für PMBS2.

Die Management-Anwendung erzeugt beim Start die Systemliste. Jedes in der Liste enthaltene Zielsystem wird durch den Systemnamen und die SNMP-Parameter (IP-Adresse, Port und Community) definiert.

Die Erzeugung der Systemliste erfolgt in drei Schritten:

1. Die Systemliste entsteht durch das Einlesen von Systembeschreibungen aus der Konfigurationsdatei, die Systeme aus den vorausgegangenen Sitzungen in diesem Einstellungsbereich enthält.
2. Systeme, die in der */etc/hosts* aufgeführt sind und noch nicht in die Systemliste aufgenommen wurden, werden der Systemliste zugefügt, wobei die Ports auf den Default-Port 161 und die Communities auf den Default *public* gesetzt werden (nur UNIX).
3. Die Systemliste wird alphanumerisch sortiert. Durch den Einstellungsbreich *Systeme* wird die Systemliste bearbeitet:
   - SNMP-Parameter einzelner Systeme können verändert werden,
   - neue Systeme können in die Systemliste aufgenommen werden.

Feld	**Bedeutung**
Combobox *Name*	Aktuelle Systemliste mit eindeutigen Systemnamen. Belegung des Eingabefeldes: leer kein System selektiert, die SNMP-Parameter *Adresse*, *Port* und *Community* bleiben ebenfalls leer. vorhandener Systemname die SNMP-Parameter werden entsprechend gesetzt. neuer Systemname bereits gesetzte SNMP-Parameter bleiben erhalten, unbesetzte Parameter erhalten Defaultwerte. *OK* oder *Anwenden* im Aktionsbereich erweitern die Systemliste um den neuen Systemnamen mit den entsprechenden SNMP-Parametern für die aktuelle Sitzung. Unter *Optionen* → *Sichern* kann die neue Systemliste in der Konfigurationsdatei gesichert werden.
Adresse	IP-Adresse des Zielsystems in vier byte langer, dezimaler Punkt-Notation. Default: 127.0.0.1.
Port	Numerischer Port des SNMP-Dienstes am Zielsystem. Defaultwert: 161

Feld	Bedeutung
Community	String, der Zugangsberechtigung und Berechtigungsumfang für das SNMP-Management am Zielsystem festlegt. Default-Community: *public*

Gruppen

Gruppen gilt sowohl für CMBS2 als auch für PMBS2.

Systeme können zu Gruppen zusammengefasst werden. Die Gruppennamen werden im Unterschied zu Systemnamen in Klammern *[gruppenname]* ausgegeben.

Feld	Bedeutung
Combobox *Gruppe*	Aktuelle Gruppenliste mit eindeutigen Gruppennamen. Belegung des Eingabefeldes: leer — keine Gruppe selektiert, die Listbox *Gruppen-Elemente* bleibt ebenfalls leer vorhandener Gruppenname — die Listbox *Gruppen-Elemente* enhält die die Systemnamen der Gruppe neuer Gruppenname — bereits vorhandene Systemnamen in der Listbox *Gruppen-Elemente* bleiben erhalten *OK* oder *Anwenden* im Aktionsbereich erzeugen die neue Gruppe und machen sie im Console Monitor für die aktuelle Sitzung verfügbar. Unter *Optionen* → *Sichern* kann die neue Gruppe in der Konfigurationsdatei gesichert werden.
Combobox *Alle Elemente*	Alle Systemnamen aus der aktuellen Systemliste.
Combobox *Gruppen-Elemente*	Systemnamen der in der Combobox *Gruppe* eingetragenen Gruppe.
Aktionsknopf *Zur Gruppe Hinzufügen*	Die in der Listbox *Alle Elemente* selektierten Systemnamen werden in die Listbox *Gruppen-Elemente* übernommen.

Feld	Bedeutung
Aktionsknopf *Aus der Gruppe Entfernen*	Die in der Listbox *Gruppen-Elemente* selektierten Systemnamen werden aus dieser Listbox entfernt. Eine vorhandene Gruppe kann vollständig gelöscht werden, indem alle ihre Elemente entfernt werden und im Aktionsbereich *OK* oder *Anwenden* ausgeführt wird.

Ping

Ping gilt sowohl für CMBS2 als auch für PMBS2.

Feld	Bedeutung
TimeOut	Festlegung, nach welcher Zeit (Sekunden) ein Ping-Request als unbeantwortet gilt
Wiederholungen	Anzahl der Ping-Versuche
Verzögerung	Zeit (Sekunden) zwischen den einzelnen Versuchen
Radiobutton Separates Fenster	Mögliche Werte: Ja Resultate von Ping-Requests werden in einem eigenen Fenster angezeigt. Nein Resultate von Ping-Requests erhalten kein eigenes Fenster.

SNMP

SNMP gilt sowohl für CMBS2 als auch für PMBS2.

Globaler Defaultwert für das System, der beim Öffnen des Hauptfensters eingetragen wird. Die Liste der Combobox ist vorbelegt durch die in der Systemliste eingetragenen Rechner.

Feld	Bedeutung
Version	Aktuell verwendete SNMP-Version. *Version* ist ein Ausgabefeld.
TimeOut	legt fest, nach welcher Zeit (Angabe in Sekunden) ein SNMP-Request als unbeantwortet verworfen wird.
Wiederholungen	steht für die Anzahl Versuche, mit denen festgestellt werden soll, ob eine Antwort auf ein abgesetztes BS2000-Kommando vorliegt. Der Wert 0 bedeutet, dass ohne Begrenzung gearbeitet wird.

Feld	Bedeutung
Eingabefeld *Port* (nur CMBS2)	Port für den Trap-Empfang (162 oder 1024)
Verzögerung	enthält die Zeit (Sekunden) zwischen den Versuchen um festzustellen, ob eine Antwort auf ein abgesetztes BS2000-Kommando vorliegt.

Meldungen

Meldungen gilt nur für CMBS2.

Im Einstellungsbereich *Meldungen* können Parameter für das Trap-Fenster festgelegt werden.

Feld	Bedeutung
Eingabefeld *Max. Anzahl*	Maximale Anzahl der Meldungen, die im Trap-Fenster angezeigt werden können. Bei Überschreiten dieser Anzahl wird die älteste Meldung gelöscht.
Radiobutton *Beantwortete Fragen löschen*	Ja Beantwortete Fragen werden im Trap-Fenster gelöscht. Nein Beantwortete Fragen werden im Trap-Fenster nicht gelöscht.
Folder *Objekt-Filter Bearbeiten* *Quellen-Filter Bearbeiten* *Meldungs-Filter Bearbeiten*	Das Filter-Eingabefeld ist mit dem entsprechenden Wert des Trap-Fensters vorbelegt.Durch den Aktionsknopf *Hinzufügen* kann die Vorbelegung in die Listbox der Filter aufgenommen werden. Das Eingabefeld ermöglicht so auch die Aufnahme hier neu eingegebener Filter. Wurde ein Filter in der Listbox selektiert, so erscheint dieser im Eingabefeld. Mit dem Aktionsknopf *Ändern* bietet sich so eine komfortable Änderungsmöglichkeit des in der Listbox selektierten Eintrags.
Aktionsknopf *Hinzufügen*	Gültige Einträge werden als Filter in die Listbox aufgenommen, sofern sie dort noch nicht existieren.
Aktionsknopf *Ändern*	Wurde ein Filter in der Listbox selektiert, erscheint er im Eingabefeld. Bei Betätigung des Aktionsknopfs *Ändern* ersetzt der im Eingabefeld geänderte Filter den in der Listbox selektierten.
Listbox	Listet alle aktuellen Filter auf.
Aktionsknopf *Löschen*	Durch Betätigen des Aktionsknopfs *Löschen* wird ein in der Listbox selektierter Filter aus dieser entfernt.

Kommandos

Kommandos gilt nur für CMBS2.

Beim Starten des Console Monitor werden aus der Konfigurationsdatei *Standard Kommandos* gelesen.Durch die Eingabe neuer Kommandos im Kommando-Fenster oder hier in diesem Einstellungsbereich können *Temporäre Kommandos* erstellt werden. Der Einstellungsbereich Kommandos ermöglicht das Bearbeiten von *Temporären* und *Standard Kommandos*, sowie ihre Konvertierung untereinander.

Feld	**Bedeutung**
Eingabefeld	Das Kommando-Eingabefeld dient der Eingabe neuer *Temporärer Kommandos* oder der Änderung existierender Kommandos in den Listboxen der *Temporären* oder *Standard Kommandos*. Durch den Aktionsknopf *Hinzufügen* kann ein neues Kommando in die Listbox *Temporäre Kommandos* aufgenommen werden. Zum Ändern muss in der entsprechenden Listbox ein Kommando selektiert sein. Anschließend wird mit dem Aktionsknopf *Ändern* das geänderte Kommando im Eingabefeld an die Stelle des selektierten gesetzt, vorausgesetzt das geänderte Kommando existiert noch in keiner Listbox.
Listbox Temporäre Kommandos	Listet die temporären Kommandos auf. Zu Beginn einer Sitzung ist diese Liste leer. Diese Kommandos werden nach der aktuellen Sitzung nicht gesichert, sind also in der nächsten Sitzung nicht mehr greifbar.
Listbox *Standard Kommandos*	Listet die Standard Kommandos auf. Die Liste enthält die Standard Kommandos der vorhergehenden Sitzung. Werden Standard Kommandos geändert und sollen auch für künftige Sitzungen zugreifbar bleiben, müssen sie gesichert werden: *Optionen* → *Sichern*
Aktionsknopf *Hinzufügen*	Gültige Einträge im Eingabefeld werden als neue Kommandos der Listbox *Temporäre Kommandos* hinzugefügt, sofern sie in den beiden Listboxen noch nicht existieren.
Aktionsknopf *Ändern*	Ein in einer Listbox selektiertes Kommando erscheint im Eingabefeld. Das im Eingabefeld geänderte Kommando ersetzt bei Betätigung des Aktionsknopfs *Ändern* das in der Listbox selektierte Kommando.
Aktionsknopf →	Die selektierten Einträge aus der Listbox *Temporäre Kommandos* werden in die Listbox *Standard Kommandos* verschoben. Das erweitert den Umfang der *Standard Kommandos*.

Feld	Bedeutung
Aktionsknopf ◄—	Die selektierten Einträge aus der Listbox *Standard Kommandos* werden in die Listbox *Temporäre Kommandos* verschoben. Das reduziert den Umfang der *Standard Kommandos*.
Aktionsknopf *Löschen*	Die selektierten Einträge aus der Listbox *Temporäre Kommando* werden gelöscht. *Standard Kommandos* können nur über die Listbox *Temporäre Kommandos* vollständig entfernt werden.

Protokoll

In diesem Bereich kann die Protokollierung von Reaktionen eingestellt werden.

Feld	Bedeutung
Radiobutton *Protokollieren*	Mögliche Werte: Ja Reaktionen werden protokolliert. Nein Reaktionen werden nicht protokolliert.
Eingabefeld *Datei*	Name der Datei, in die protokolliert wird. Derzeit kann der Name nicht geändert werden.
Radiobutton *Start-Modus*	Mögliche Werte: – Überschreiben: Die Datei wird bei jedem Neustart überschrieben. – Hinzufügen: Die Datei wird beim Neustart fortgeschrieben. – Sichern und Neu: Die existierende Datei wird gesichert, eine neue Datei wird angelegt.
Radiobutton *OnLine*	Mögliche Werte: Ja Das Ergebnis des *SetRequests* eines BS2000/OSD-Konsol-Kommandos wird in der Tabelle *Traps* des Hauptfensters angezeigt. Voraussetzung hierfür ist, dass der Radiobutton *Protokollieren* aktiv ist. Nein Das Ergebnis wird nicht angezeigt.

Reaktionen (nur für PMBS2)

Der Einstellungsbereich *Reaktionen* definiert allgemeine Parameter für Reaktionen bei der Überschreitung von Schwellwerten. Voraussetzung für die Ausführung von Reaktionen ist, dass in der Dialogbox *Schwellwerte* ein Schwellwert definiert und im Menü *Schwellwert* der Button *Aktiv* betätigt ist.

Feld	**Bedeutung**
Eingabefeld *Datei*	Angabe der Datei, in der die Schwellwert-Überschreitungen protokolliert werden.
Eingabefeld *Kommando*	Angabe eines Kommandos, das bei Schwellwert-Überschreitung ausgeführt wird. Dabei können folgende Schlüsselwörter verwendet werden.
Eingabefeld *Trap:Manager*	Angabe des Systems, an das der Trap gesendet werden soll.
Eingabefeld *Trap:Port*	Angabe des Ports, an den der Trap auf dem Zielsystem gesendet werden soll.
Eingabefeld *Trap:Objekt*	Kennzeichnung des Objektes im Trap. Das Objekt wird in der Tabelle der Console Monitor-Anwendung in der Spalte "Objekt" angezeigt
Eingabefeld *Trap:Quelle*	Kennzeichnung der Quelle im Trap. Die Quelle wird in der Tabelle der Console Monitor-Anwendung in der Spalte "Quelle" angezeigt.
Eingabefeld *Trap:Meldung*	Meldungstext des Traps. Der Meldungstext wird in der Tabelle der Console Monitor-Anwendung in der Spalte "Meldung" angezeigt.

Sichern

Sichern gilt sowohl für CMBS2 als auch für PMBS2. Hiermit werden die Einstellungen zum Sichern festgelegt.

Feld	**Bedeutung**	
Radiobutton *Beim Beenden Sichern*	Ja	Beim ordnungsgemäßen Beenden der Anwendung werden die Werte der Einstellungsbereiche ohne Abfrage automatisch in der Konfigurationsdatei gesichert.
	Nein	Änderungen von Werten der Einstellungsbereiche werden beim Beenden der Anwendung nicht gesichert.
	Abfrage	Beim ordnungsgemäßen Beenden der Anwendung wird eine Frage-Dialogbox geöffnet. Mit der Beantwortung der Abfrage können Änderungen in den Einstellungsbereichen in der Konfigurationsdatei gesichert werden.
Radiobutton *Sprache*	Auswahl der Sprache für den Neustart	

10 Web-Zugriff auf Management-Informationen

Neben der Verarbeitung von SNMP-Requests ermöglicht der Masteragent den Zugriff auf Management-Informationen über das World Wide Web (WWW). Somit lassen sich die von beliebigen EMANATE-Subagenten bereitgestellten Informationen sowohl über traditionelle SNMP-Managementanwendungen als auch via Web-Browser abfragen und ändern.

10.1 Überblick

Der Masteragent hört das Netz auf zwei verschiedene Arten von Requests ab:

– Auf dem SNMP-Port (normalerweise UDP 161) erwartet der Masteragent die SNMP-Set- und GetRequests.

  Als Antwort auf die SNMP-Requests sendet der Masteragent SNMP-GetResponse-Nachrichten.

– Auf dem Web-basierten Management-Port (normalerweise TCP 280) erwartet der Masteragent HTTP-Verbindungsanforderungen.

  Als Antwort auf eine HTTP-Nachricht sendet der Masteragent eine HTML-Seite an den Browser zurück. Diese HTML-Seite kann eine vordefinierte, benutzerspezifische Web-Seite (Custom Page) sein oder eine automatisch generierte Web-Seite (Subtree Page), die Werte von MIB-Variablen enthält, die beim Durchlaufen des MIB-Baums gelesen wurden.

  Der Teil des Masteragenten, der für die Verarbeitung von HTTP-Nachrichten zuständig ist, heißt HTTP-Engine.

HTTP-Requests werden in gleicher Weise verarbeitet wie SNMP-Requests. Nach Auswertung eines SNMP- oder HTTP-Requests legt der Masteragent die relevanten Bestandteile des Requests im EMANATE Event Queueing Subsystem ab, einer internen Warteschlange des Masteragenten. Von dort aus beschafft sich der Masteragent die Information auf dem üblichen Weg über die EMANATE-Subagenten.

Sobald der Masteragent die Informationen erhalten hat, generiert er, je nach Typ des bearbeiteten Requests, eine SNMP-GetResponse-Nachricht oder eine HTML-Seite und sendet diese mit den gewünschten Informationen an den Sender der ursprünglichen Nachricht zurück.

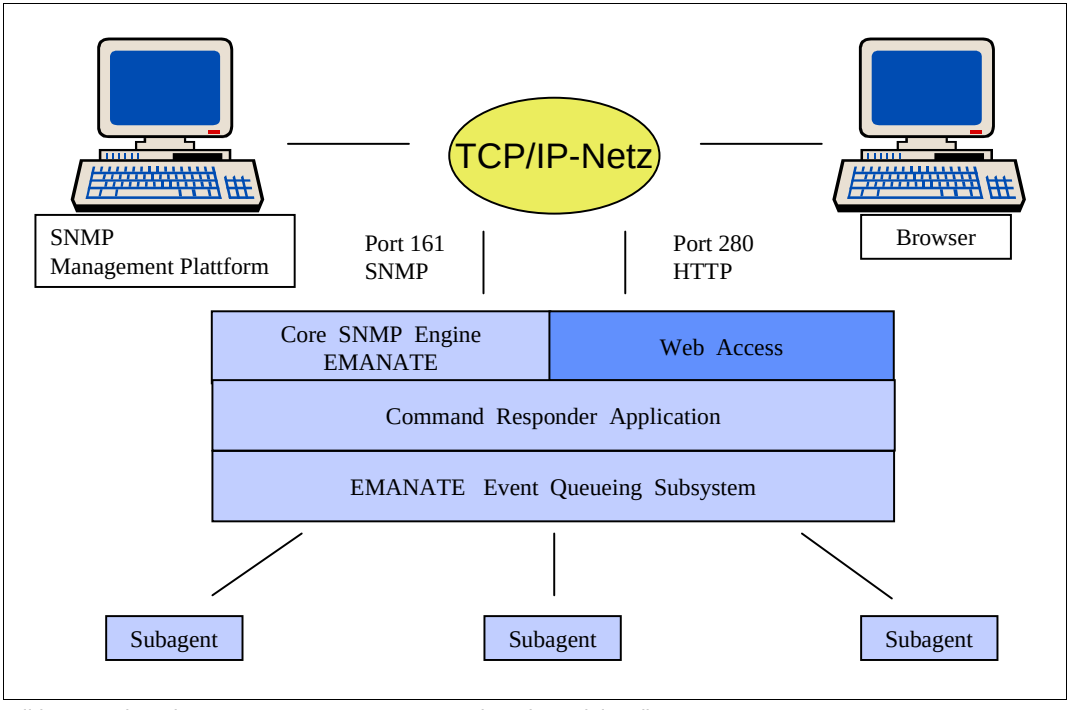


Bild 59: Struktur des EMANATE-Masteragenten mit Web-Funktionalität

10.2 Schnittstelle des BS2000/OSD-Web-Agenten (Web Interface)

Dieser Abschnitt informiert über folgende Themen:

– Verbindungsaufbau zum BS2000/OSD-Web-Agenten

– automatisch generierte Web-Seiten (Subtree-Funktionalität)

– kundenspezifische Web-Seiten (Custom-Page-Funktionalität)

10.2.1 Verbindungsaufbau zum BS2000/OSD-Web-Agenten aufbauen

Für den Verbindungsaufbau zum BS2000/OSD-Web-Agenten (DR-Web-Entity) geben Sie an Ihrem Web-Browser Netzadresse und Portnummer wie folgt ein:

http://*netzadresse***:***portnummer*

Beispielsweise ist http://D016ZE07:280 die Adresse des Web-Agenten auf dem System D016ZE07.

Benutzername und Kennwort eingeben

Nach dem Verbindungsaufbau werden Sie aufgefordert, am Browser Benutzername und Kennwort einzugeben. Die Dialogbox könnte wie folgt aussehen:

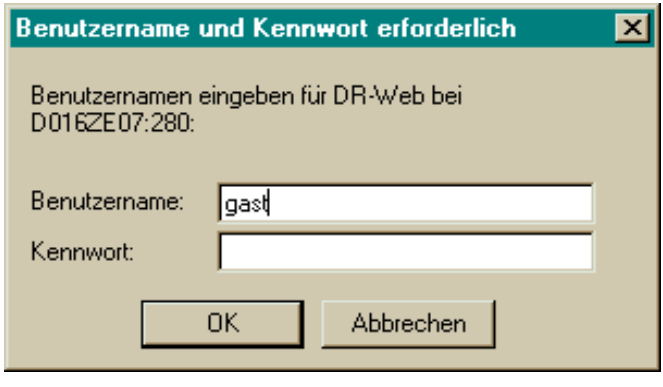


Bild 60: Eingabe von Benutzername und Kennwort

Benutzername und Kennwort müssen am Agenten konfiguriert sein (siehe Abschnitt „Security-Konfiguration“ auf Seite 30). Die Konfiguration ist bei Auslieferung so voreingestellt, dass als gültige Eingabe der Benutzername *gast* und als Kennwort der leere String akzeptiert wird (d.h. Sie geben unter „Kennwort“ nichts an).

Bei erfolgreicher Anmeldung präsentiert der Web-Agent am Browser den Begrüßungsbildschirm.

Begrüßungsbildschirm des BS2000/OSD-Web-Agenten

Die folgende Abbildung zeigt den Standard-Begrüßungsbildschirm mit Hyperlinks auf die Subtree- und Custom-Page-Funktionalität.

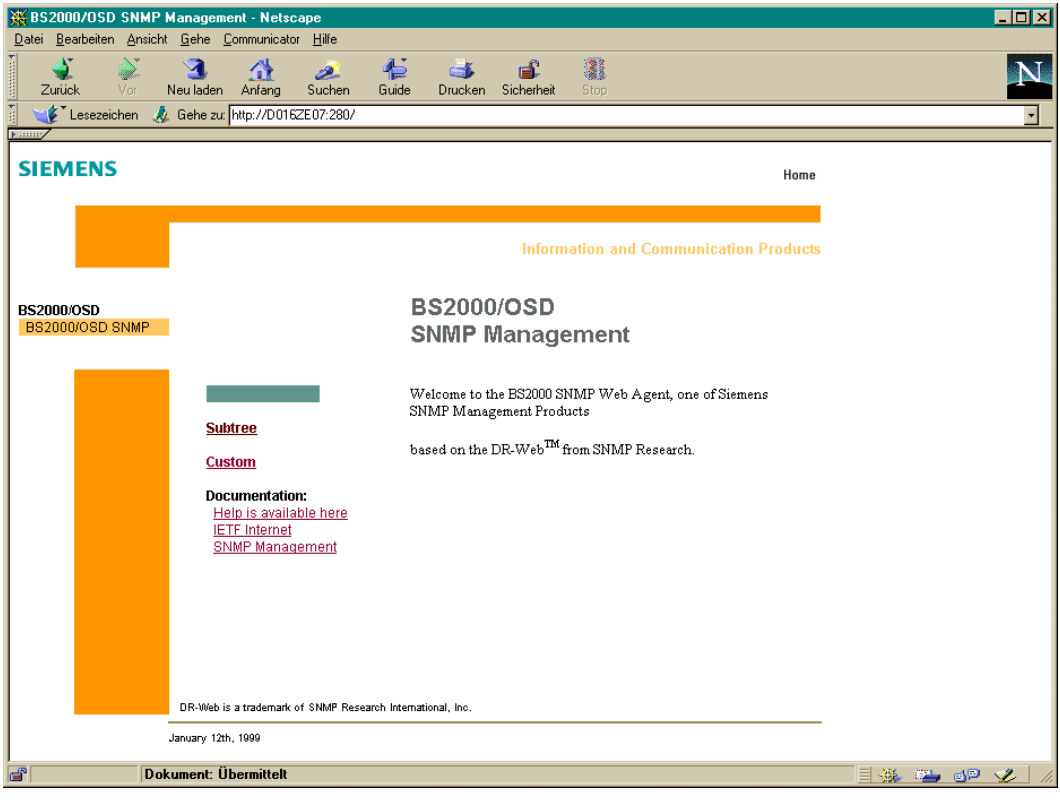


Bild 61: Begrüßungsbildschirm des Web-Agenten

10.2.2 Subtree-Funktionalität

Mit dem Klick auf den Hyperlink *subtree* im DR-Web-Begrüßungsbildschirm steht Ihnen die Subtree-Funktionalität zur Verfügung, die ein einfaches MIB-Browsen ermöglicht.

10.2.2.1 Subtree-Page des Web-Agenten (DR-Web-Subtree-Page)

Die Subtree-Funktionalität wird über die Subtree-Page des Web-Agenten angeboten. Sie können sich die Subtree-Page am Browser anzeigen lassen, indem Sie auf den Subtree-Hyperlink im Begrüßungsbildschirm klicken oder die URL „http://*ip_adresse*:280/subtree/“ im Adressfeld Ihres Browsers eingeben.

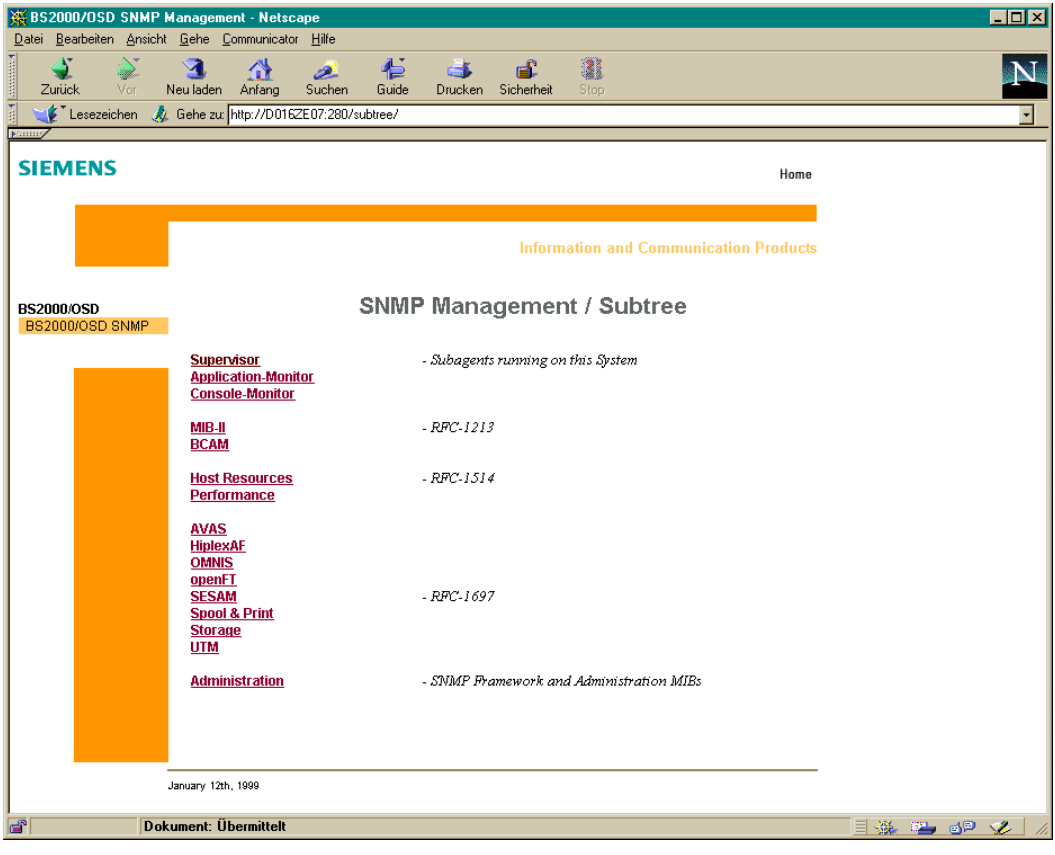


Bild 62: DR-Web-Subtree-Page

Die Subtree-Page enthält Hyperlinks auf Subtree-URLs, mit denen die über den Web-Agenten zugänglichen Management-Informationen angezeigt werden können. Diese Seite ist so vorkonfiguriert, dass ein schneller Zugang zu allen vom SNMP-Management in BS2000/OSD unterstützten MIBs gewährleistet ist. Beispielsweise lässt sich durch Anklikken des MIB-II-Hyperlinks der gesamte MIB-II-Baum darstellen.

Wenn Sie sich lediglich die System-Gruppe der MIB-II anschauen wollen, geben Sie die URL „http://*ip_adresse*:280/subtree/system/“ im Adressfeld Ihres Browsers ein.

10.2.2.2 Subtree-URL - GetRequest-Funktionalität

Durch Angabe eines OBJECT-IDENTIFIER (OID) in der URL können Sie den Web-Agenten direkt veranlassen, einen bestimmten MIB-Zweig anzuzeigen. Da der Web-Agent die Umsetzung von Namen in OIDs beherrscht, können Sie wahlweise den OID-Namen oder die numerische Form des OID angeben.

Beispiel: Supervisor-MIB

Der Supervisor Subagent überwacht alle an den Masteragenten angeschlossenen Subagenten. Wenn der Supervisor Subagent im Zielsystem abläuft, sind die durch die Supervisor-MIB beschriebenen MIB-Objekte über die DR-Web-Schnittstelle verfügbar.

Den gesamten Supervisor-Subtree können Sie sich anzeigen lassen, indem Sie wahlweise

– „subtree/sniSupervisor“ im Adressfeld des Browsers angeben oder
– „subtree/1.3.6.1.4.1231.34“ im Adressfeld des Browsers angeben oder
– *Supervisor*-Hyperlink in der DR-Web-Subtree-Seite anklicken.

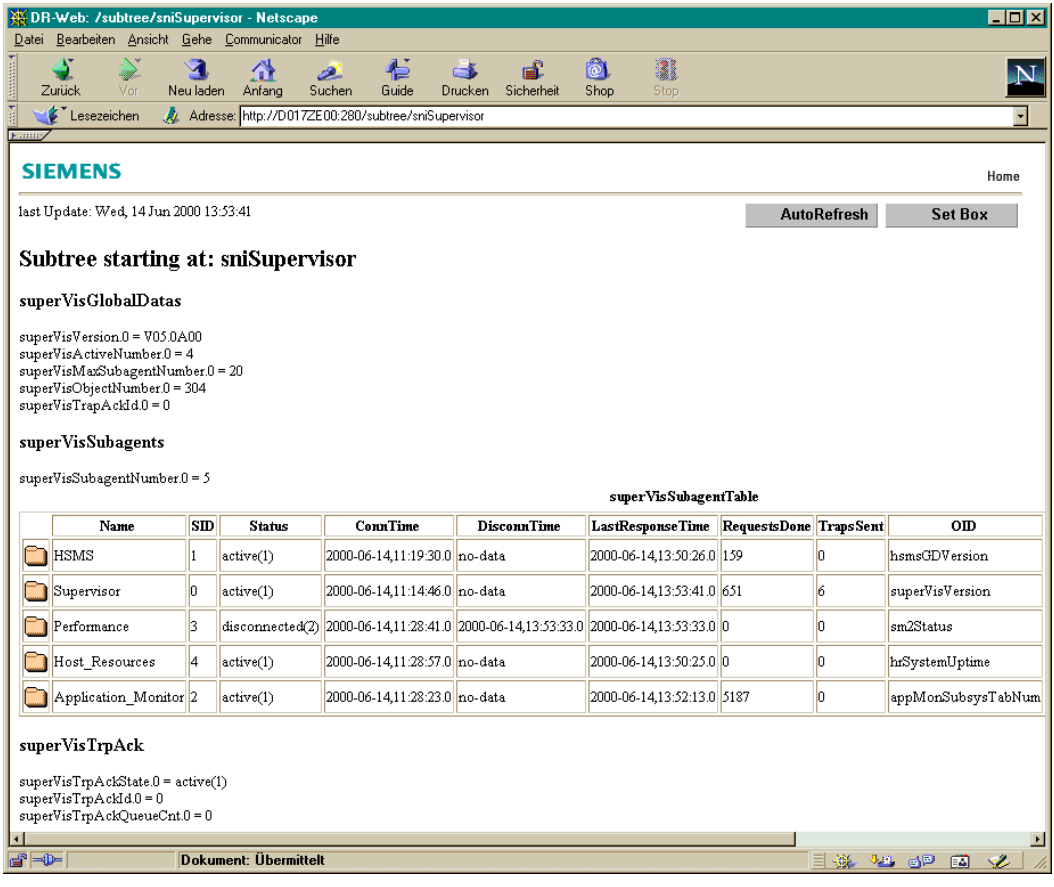


Bild 63: *subtree/sniSupervisor*-Seite

Wenn Sie sich nur die GlobalDatas aus der MIB anzeigen lassen wollen, geben Sie „subtree/superVisGlobalDatas“ in der URL im Adressfeld des Browsers ein.

Wenn Sie nur die Variablen aus der *superVisSubagentTable* extrahieren wollen, geben Sie „subtree/superVisSubagentTable“ oder „subtree/superVisSubagentEntry“ in der URL im Adressfeld des Browsers ein.

10.2.2.3 Row-URL - einzelne Tabellenzeilen auswählen

Für die Auswahl einer einzelnen Zeile aus der *superVisSubagentTable* spezifizieren Sie „row/superVisSubagentName“, gefolgt von einer Instanz. Um beispielsweise Informationen über die Instanz MIB-II (77.73.66.95.73.73 in ASCII und der Länge 6) zu erhalten, spezifizieren Sie „row/superVisSubagentName.6.77.73.66.95.73.73“. Normalerweise werden Sie

die URL nicht explizit eintippen, sondern das Ordner-Symbol der betreffenden Tabellenzeile anklicken. Die gewünschte Information wird dann in einem Lay-out ähnlich wie bei skalaren Objekten präsentiert.

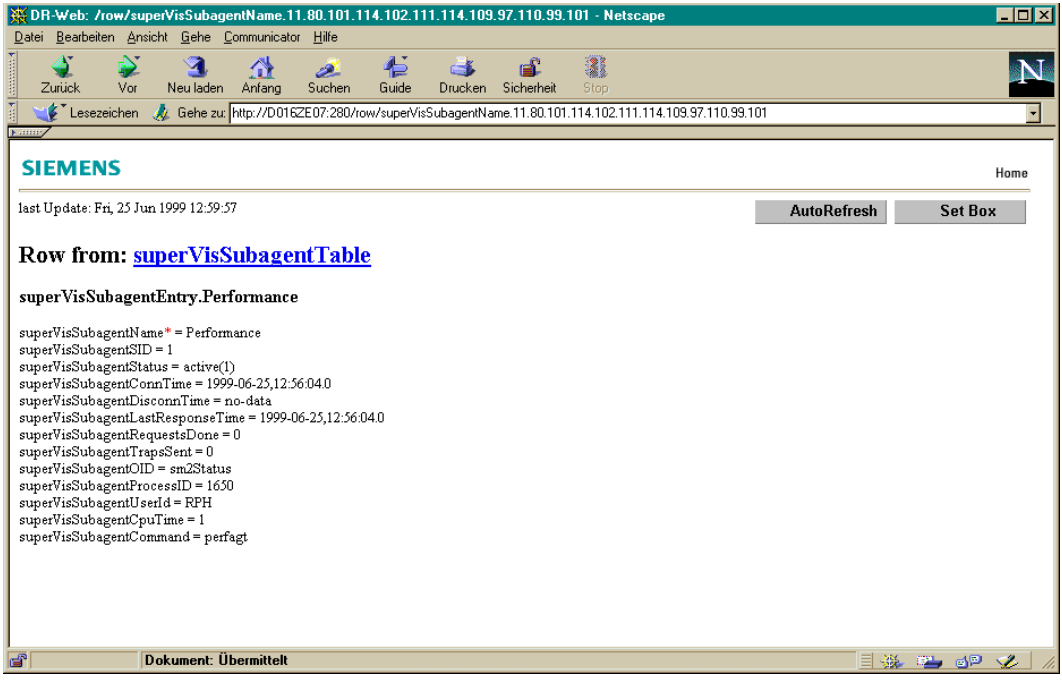


Bild 64: Die Seite row/superVisSubagentName.6.77.73.6.73.73

10.2.2.4 Raw-URL - Darstellung von MIB-Informationen im „raw data“-Format

Die DR-Web-Schnittstelle ermöglicht den Zugang zu Management-Informationen im „raw data“-Format. Dieses Leistungsmerkmal wird im Hinblick auf Java-Applets für die einfache Analyse von Informationen über MIB-Objekte angeboten. Einen MIB-Zweig im „raw data“-Format erhalten Sie, wenn Sie in der URL *subtree* durch *subtree+raw* ersetzen. Beispielsweise erhalten Sie den MIB-II-Zweig im „raw data“-Format, wenn Sie am Browser „subtree+raw/mib_2“ spezifizieren.

10.2.2.5 Refresh-URL - Automatische Aktualisierung von Management-Informationen

Die DR-Web-Schnittststelle unterstützt die automatische, periodische Aktualisierung (AutoRefresh) von Management-Informationen. Zu diesem Zweck muss der Web-Agent eine HTML-Seite an den Browser schicken, die den Meta-Tag <meta http-equiv="Refresh" content=60> enthält.

Den AutoRefresh können Sie aktivieren, indem Sie wahlweise

– in der URL den String „subtree“ durch „subtree+refresh“ ersetzen oder

– den *AutoRefresh*-Button anklicken, der sich rechts oben in den meisten DR-Web-Seiten befindet.

Der Standardwert für das AutoRefresh-Intervall beträgt 60 Sekunden. Für DR-Web-Custom-Pages kann der AutoRefresh-Wert durch Angabe von „RefreshTime = *value*“ innerhalb der Attribute des <body>-Tags individuell angepasst werden.

10.2.2.6 Set-URL - SetRequest-Funktionalität

Neben der Abfrage von MIB-Werten (GetRequests) können Sie an der DR-Web-Schnittstelle auch SetRequests absetzen und somit Werte von MIB-Variablen (MIB-Objekten) ändern, die am Browser angezeigt werden.

Eine DR-Web-Seite mit Feldern zum Ändern von MIB-Variablen können Sie sich am Browser anzeigen lassen, indem Sie wahlweise

– in der URL den String „subtree“ durch „subtree+set“ ersetzen oder

– den *Set Box*-Button anklicken, der sich rechts oben in den meisten DR-Web-Seiten befindet.

Bei einer änderbaren Variablen wird der momentane Wert in einem Eingabefeld angezeigt. In der Check-Box rechts neben dem Eingabefeld spezifizieren Sie, ob der Wert geändert werden soll. Alternativ kann änderbaren MIB-Variablen auch ein Button oder ein Pull-down-Menü zugeordnet sein, jeweils gefolgt von einer Check-Box.

Folgende Voraussetzungen müssen erfüllt sein, damit Sie den Wert einer MIB-Variablen ändern können:

– Das MIB-Objekt ist in der MIB als *read-write* oder *read-create* definiert und im Agenten als *read-write* oder *read-create* implementiert.

– Für das MIB-Objekt sind Sie schreibberechtigt.

Die aktuelle Security-Konfiguration (siehe Seite 30) wird bei der Generierung der Web-Seite berücksichtigt.

Für jedes an Ihrem Browser angezeigte MIB-Objekt, das Sie ändern wollen, verfahren Sie wie folgt:

1. Tragen Sie den gewünschten Wert ein.
2. Klicken Sie die zugehörige Check-Box an.

Nachdem Sie diese Schritte für alle MIB-Objekte durchgeführt haben, klicken Sie abschließend den Set-Button an, der unterhalb der MIB-Variablen positioniert ist.

Wert einer skalaren Variablen ändern

Mit der nachfolgend dargestellten DR-Web-Seite können Sie einige Objekte der System-Gruppe der MIB-II ändern:

– Die MIB-Objekte *sysContact.0*, *sysName.0* und *sys.Location.0* haben *read-write*-Status. Die zugehörigen Werte sind in Eingabefeldern dargestellt. (*sysName* hat als MIB-Objekt zwar den Status *read-write*, in der vorliegenden Implementierung wurde der Schreibzugriff jedoch untersagt.)

– Fünf Objekte haben den Status *read-only* und können demzufolge nicht verändert werden.

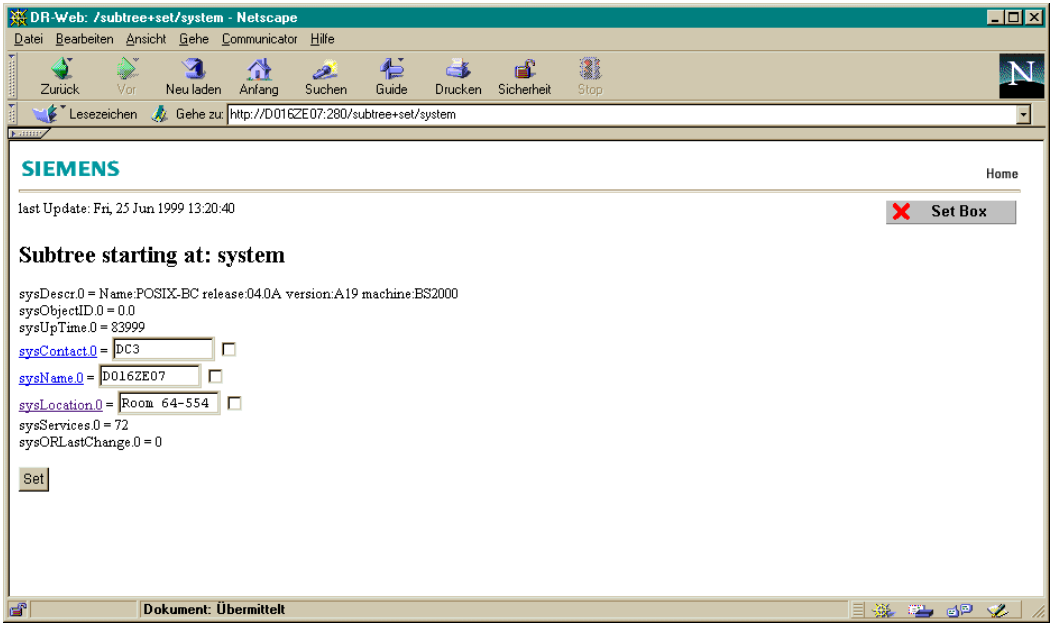


Bild 65: Subtree+set/system-Seite

Wert von Variablen in einer Tabellenzeile ändern

Wenn Sie in einer Tabellenzeile einen Wert ändern wollen, können Sie wahlweise

– das Ordner-Symbol der betreffenden Seite anklicken oder

– eine URL eingeben, die den folgenden String „row+set/*tabellenindex*“, gefolgt von einem Instanznamen, enthält.

Wie bei den änderbaren skalaren Variablen wird jeder Wert innerhalb eines Eingabefeldes angezeigt. Ebenso kann änderbaren MIB-Variablen auch ein Button oder ein Pull-down-Menü zugeordnet sein, jeweils gefolgt von einer Check-Box.

Beim Ändern eines MIB-Objekts gehen Sie wie bei skalaren Objekten vor:

1. Tragen Sie den gewünschten Wert ein.
2. Klicken Sie die zugehörige Check-Box an.

Nach dem Sie diese Schritte für alle MIB-Objekte, die Sie ändern wollen, durchgeführt haben, klicken Sie abschließend den Set-Button an, der sich unten auf der Seite befindet.

Tabelleninstanz erzeugen

Wenn Sie die *subtree+set*-URL im Zusammenhang mit einer Tabelle verwenden, unterscheidet sich die so erzeugte DR-Web-Seite nur dann von der Subtree-Page, wenn für die Tabelle in der MIB die Instanzengenerierung via TEXTUAL-CONVENTIONS RowStatus unterstützt wird.

Beim Generieren einer neuen Tabellenzeile gehen Sie wie folgt vor:

1. Klicken Sie wahlweise auf das Ordner-Symbol neben dem Text *New Row* oder geben Sie eine URL ein, die den String „row+set/*tabelle*“ enthält. Dabei ist zu beachten, dass auf die URL keinerlei Informationen über eine Instanz folgen sollte.
2. Für jedes zu ändernde MIB-Objekt, das auf der Web-Seite angezeigt wird, führen Sie die folgenden Schritte durch:
   – Initialisieren Sie die zugehörige MIB-Variable, oder ändern Sie ihren Default-Wert.
   – Aktivieren Sie die zugehörige Check-Box.
3. Klicken Sie auf einen der beiden Buttons *Create and Go* oder *Create and Wait*.

10.2.3 Custom-Page-Funktionalität

Wenn Sie auf Ihrem System den HTML-Subagenten einsetzen, steht Ihnen mit einem Klick auf den Hyperlink *Custom* des DR-Web-Begrüßungsbildschirms (siehe Seite 410) die Custom-Page-Funktionalität zur Verfügung. Damit können Sie die vorkonfigurierten Web-Seiten nutzen oder eigene Web-Seiten (Custom-Pages) erstellen, die neben allen Bestandteilen (Text, Grafik etc.) zusätzlich Makros für den Zugriff auf einzelne MIB-Objekte enthalten. Darüber hinaus können Sie Informationen nach individuellen Gesichtspunkten gruppieren. Wie Custom-Pages generiert werden, ist im Abschnitt „Konfiguration einer Custom-Page“ auf Seite 427 beschrieben.

Für den Zugriff auf eine Custom-Page geben Sie in der URL hinter der Netzadresse das Schlüsselwort „custom“ ein.

10.2.3.1 Vorkonfigurierte Custom-Pages

Für folgende Aufgabenbereiche werden vorkonfigurierte Custom-Pages angeboten:

– SNMP-Management
– Netzmanagement
– Systemmanagement
– Anwendungsmanagement

Die vorkonfigurierten Custom-Pages können als Arbeitsbeispiele verwendet werden. Jede Seite enthält einen Zeitstempel, die wichtigsten Informationen aus der Systemgruppe der MIB-II sowie die folgenden aufgabenspezifischen Informationen:

- SNMP-Management
  - SNMP-Parameter
  - SNMP-Security-Informationen
  - SNMP-Web-Konfiguration
- Netzmanagement
  - ICMP-Statistikwerte
  - Interface-Tabellen
  - Routing-Tabellen und Routing-Informationen
- Systemmanagement
  - Systemressourcen
  - grafische Anzeige von CPU-Werten
- Anwendungsmanagement
  - Subsysteme
  - Benutzer- und BCAM-Anwendungen

Zu jedem Aufgabenbereich ist eine Benutzerkennung definiert, die lesenden und schreibenden Zugriff ausschließlich auf die zum Aufgabenbereich gehörenden MIB-Variablen hat.

Aufgabenbereich	**Kennung**	**Passwort**
SNMP-Management	snmpAdmin	admin
Netzmanagement	netAdmin	admin
Systemmanagement	systemAdmin	admin
Anwendungsmanagement	applicationAdmin	admin

10.2.3.2 DR-Web-Menü-Seite

Zur Menü-Seite des Web-Agenten gelangen Sie, indem Sie wahlweise

– den *Custom*-Hyperlink im Begrüßungsbildschirm des Web-Agenten anklicken oder

– die URL „http://*netzadresse*:280/custom“ (z.B. http://D016ZE07:280/custom) im Adressfeld des Begrüßungsbildschirms eingeben.

Bild 66 auf der nächsten Seite zeigt ein Beispiel für eine Menü-Seite.

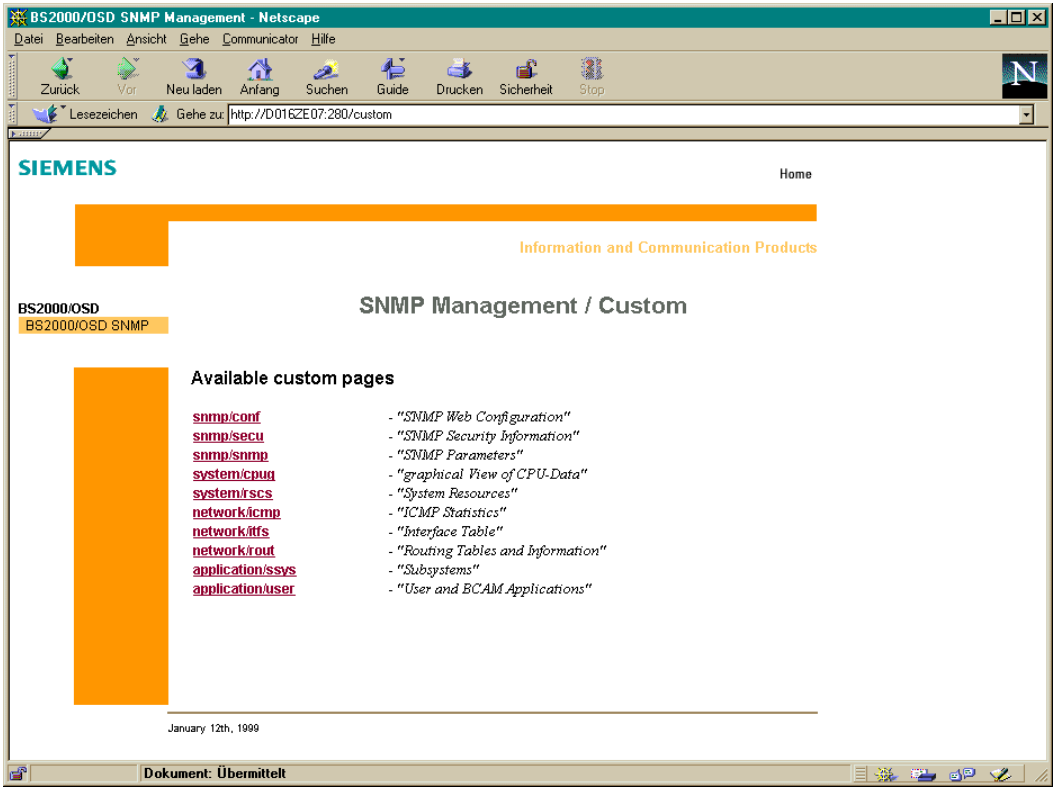


Bild 66: Menü-Seite des Web-Agenten

Durch Anklicken der einzelnen Hyperlinks können Sie sich die vom Web-Agenten unterstützten Custom-Pages an Ihrem Browser anzeigen lassen. Wenn Sie sich z.B. die Seite *SNMP-Parameters* ansehen wollen, klicken Sie auf den Hyperlink *snmp/snmp*. Dasselbe Ergebnis erzielen Sie, wenn Sie im Adressfeld Ihres Browsers eine passende, auf „custom/snmp/snmp“ endende URL eingeben. Die Custom-Page *SNMP-Parameters* ist in Bild 67 dargestellt.

Falls Sie eigene Web-Seiten erstellen, werden diese automatisch in die Liste der Custom-Pages aufgenommen. Beachten Sie, dass Sie eigene Web-Seiten nur dann erstellen können, wenn der HTML-Agent eingesetzt wird.

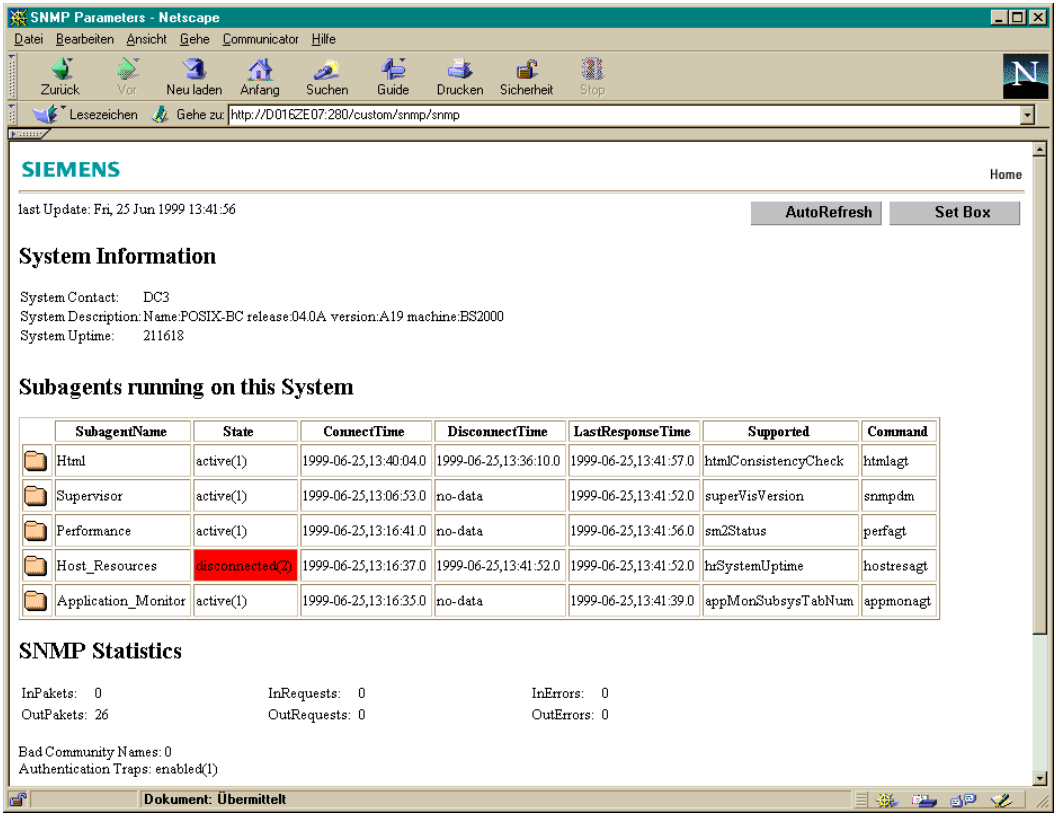


Bild 67: Custom-Page *SNMP-Parameters*

10.2.3.3 Parametrisierung der Custom-Page

Custom-Pages können so konfiguriert sein, dass Benutzereingaben erforderlich sind. In diesem Fall werden Sie zur Eingabe von Parametern aufgefordert. Dies ist z.B. bei der *Interface Overview*-Seite der Fall. Zu dieser Custom-Page gelangen Sie, wenn Sie die zugehörige, auf „custom/interface/overview“ endende URL an Ihrem Browser eintippen. Für die Anzeige der Informationen über ein bestimmtes Interface muss der Web-Agent wissen, über welches Interface Sie sich informieren wollen. Zu diesem Zweck sendet der Web-Agent eine Seite an den Browser, um Eingabeparameter und Interface-Nummer abzufragen. Nachfolgend ist eine solche „Parameter-Seite“ dargestellt.

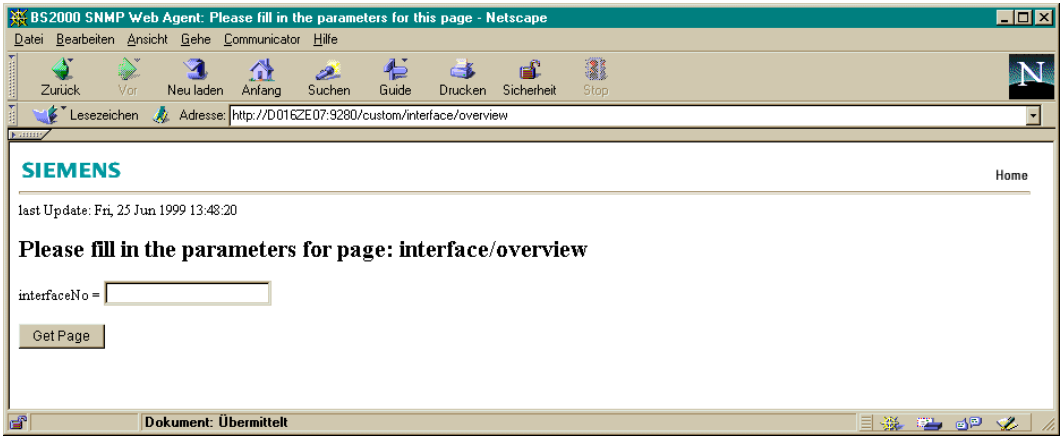


Bild 68: Parameterabfrage für die *interface/overview*-Custom-Page

Tippen Sie die benötigten Informationen in das Eingabe-Feld und klicken Sie anschließend auf den *Get Page*-Button. Wenn Sie auf einem bestimmten System als Interface-Nummer den Wert „1“ eingeben, wird z.B. die auf der nächsten Seite dargestellte Custom-Page auf Ihrem Browser angezeigt.

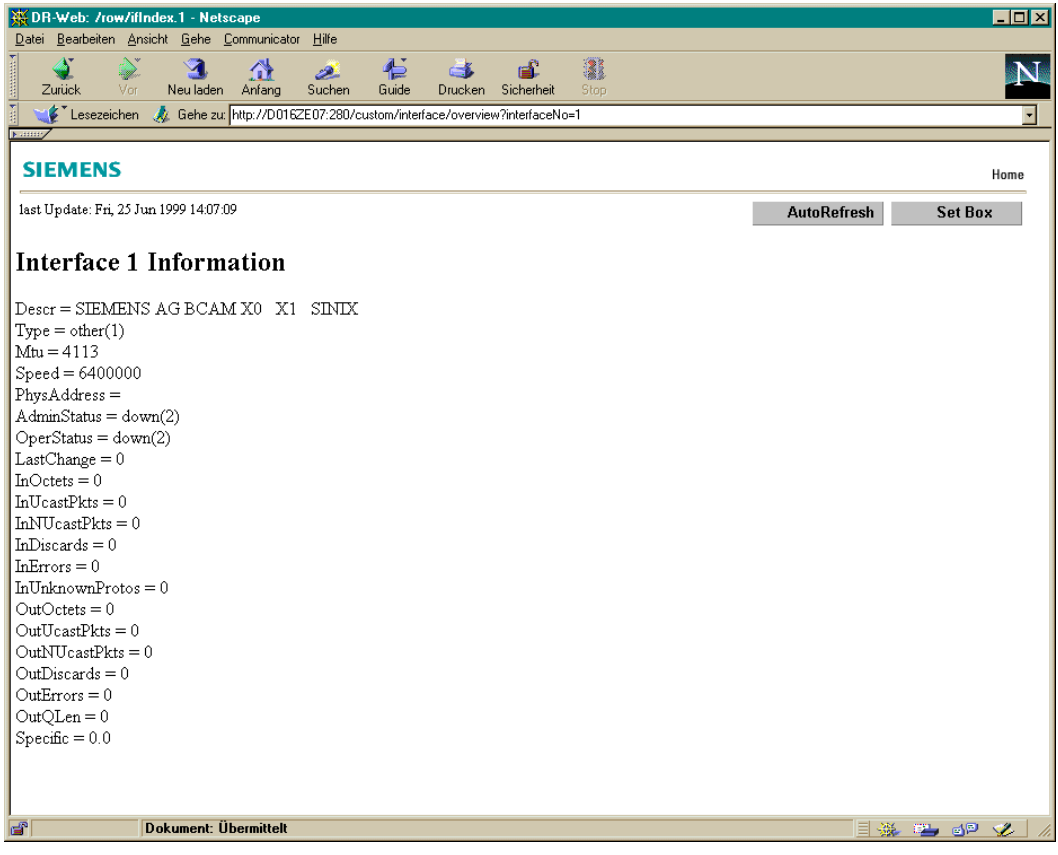


Bild 69: Die *interface/overview*-Custom-Page: interfaceNo = 1

10.2.4 Trap-Anzeige im Web-Browser

Über die DR-Web-Schnittstelle können Sie eine Web-Seite aufrufen, die eingehende Traps in einer Tabelle anzeigt. Diese Tabelle ist als Java-Applet realisiert. Aufgrund der Zugriffbeschränkungen, die für die Sicherheit von Java-Applets gefordert werden, können nur Traps empfangen werden, die von dem System stammen, von dem aus die Web-Seite geladen wurde.

Voraussetzungen an der Management-Station

An der Management-Station muss folgende Software verfügbar sein:

– Java-Plug-in-fähiger Browser, z.B. Netscape Communicator ≥ V4.7

– Java-Plug-in x-java-applet ≥ V1.2.2

  Falls dieses Plug-in auf der Management-Station nicht vorhanden ist, wird eine WWW-Adresse angezeigt, unter der es verfügbar ist.

Voraussetzung am SNMP-Agenten

Am SNMP-Agenten, dessen Traps im Web-Browser angezeigt werden sollen, müssen die IP-Adressen der einzelnen Management-Stationen als Trap-Ziele mit dem Port 9162 konfiguriert sein. Der Port kann geändert werden, muss aber nicht-privilegiert (d.h. > 1024) sein und dem Parameter PORT in der Datei *trap.html* entsprechen.

Für die Trap-Anzeige im Browser werden vom SNMP-Agenten folgende Dateien und Verzeichnisse geladen:

/etc/snmp/dr-web/doc/root-a.htm	HTML-Seite, die den Link zu *trap.html* enthält
/etc/snmp/dr-web/doc/trap.html	HTML-Seite, die das Java-Applet enthält
/etc/snmp/dr-web/doc/img/Snmp.jar	Bibliothek der benötigten Java-Klassen

Applet-Parameter

Die folgende Übersicht zeigt die Parameter, mit denen Sie in *trap.html* das Applet konfigurieren können.

Name	Wert	Erläuterung
PORT	> 1014	Trap-Empfänger (siehe Dateien und Verzeichnisse am Agenten) Default: 9162
MAXMESS	_	Maximale Anzahl angezeigter Traps Default: 100
SHOWMESS	_	Anzahl der angezeigten Traps (bestimmt die Größe der Tabelle)
WIDTH / HEIGHT		Breite und Höhe des Applets
TRACE	true / false	Trace-Anzeige ein- bzw. ausgeschaltet
DEBUG	true / false	Debug-Anzeige ein- bzw. ausgeschaltet

Trap-Tabelle bearbeiten

Für die Bearbeitung der Trap-Tabelle stehen Ihnen folgende Möglichkeiten zur Verfügung:

– Mit einem Doppel-Klick auf eine selektierte Tabellenzeile können Sie sich diese Zeile vollständig in einem separaten Fenster anzeigen lassen.

– Mit der DELETE-Taste können Sie selektierte Tabellenzeilen löschen.

– Ferner können Sie Spalten umsortieren, die Spaltenbreite verändern sowie in der Tabelle scrollen.

Fehlermeldungen

Folgende Java-Exceptions können auftreten:

SnmpException	Port möglicherweise belegt
IllegalArgumentException	ungültiger Port (z.B. Portnummer < 0)
SecurityException	Port im privilegierten Bereich (Portnummer < 1024)

10.2.5 Verwendung des Web-Agenten als Web-Server

Der Web-Agent kann allgemein als Web-Server eingesetzt werden (General Web Server-Facility). In diesem Fall spezifizieren Sie für den Zugriff auf ein einfaches HTML-Dokument eine URL, die nach der Netzadresse das Schlüsselwort „doc“ enthält, gefolgt von einem „/“ und dem Dokumentnamen. So können Sie beispielsweise mit der URL „doc/custom.html“ auf die Seite *custom.html* zugreifen, in der die Online-Dokumentation über Custom-Pages abgelegt ist. Der Hyperlink *Help_is_available_here* im Begrüßungsbildschirm des Web-Agenten ist ein Verweis auf die URL „doc/custom.html“.

Falls der Name eines einfachen HTML-Dokuments nicht in der URL spezifiziert ist, sucht der Web-Agent nach der Datei *index.html*.

10.2.6 Customizing der DR-Web-Schnittstelle

Der Begrüßungsbildschirm des Web-Agenten, die Subtree-Page sowie die Custlists-Page sind lediglich Beispiele für Web-Seiten und können bequem individuell angepasst werden.

Die HTTP-Engine führt eine spezielle Abbildung von Root-URL, Subtree-URL und Custom-Page-URL durch:

– Die Angabe der Root-URL („/“) ist gleichbedeutend mit der Angabe der URL „doc/root-a.html“.

– Die Angabe der Subtree-URL ist gleichbedeutend mit der Angabe der URL „doc/subtree.html“ .

– Die Angabe der Custom-URL ist gleichbedeutend mit der Angabe der URL „doc/custlist.html“.

Somit können Begrüßungsbildschirm und Subtree-Page einfach durch Modifikation der zugehörigen HTML-Datei geändert werden. Die Custlists-Page muss den String ****CUSTOMTABLE**** enthalten, der durch die Liste der Custom-Pages ersetzt wird.

10.3 Konfiguration einer Custom-Page

Dieser Abschnitt beschreibt,

– wie Sie ausgehend von einem gewöhnlichen HTML-Dokument durch Einsetzen von MIB-Objekten und Parametern eine Custom-Page erstellen,

– wie Sie die Custom-Page in der HTML-MIB konfigurieren, indem Sie Meta-Informationen zur Custom-Page in die Tabellen der HTML-MIB einbringen.

10.3.1 Erstellen der Custom-Page

Im Folgenden werden die Schritte, die für das Erzeugen einer Custom-Page erforderlich sind, anhand eines Beispiels erläutert. Mit Custom-Pages lassen sich z.B. ausgewählte Werte von MIB-Objekten in einem übersichtlichen Lay-out darstellen. Für die Erstellung einer Custom-Page sollte der Entwickler auf einem Web-Dokument aufsetzen können, das ggf. bereits das gewünschte Lay-out enthält, einschließlich Grafiken, Text, Java-Applets, Java-Skripts usw. Dieses Ausgangsdokument kann von Hand oder mit einem beliebigen HTML-Editor erstellt werden.

HTML-Ausgangsdokument

Bild 70 auf der nächsten Seite zeigt das Lay-out, das von einem HTML-Ausgangsdokument erzeugt wird. In diesem Lay-out sind die Labels für die gewünschte MIB-Information bereits enthalten, die Werte selbst werden jedoch nicht angezeigt.

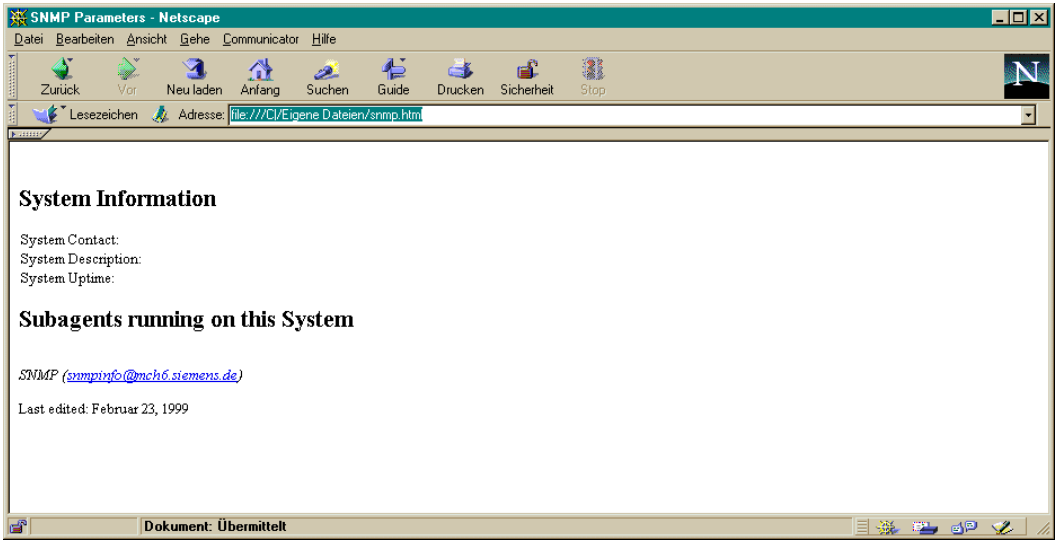


Bild 70: Lay-out eine Ausgangsdokuments ohne MIB-Werte

Das in Bild 70 gezeigte Lay-out enthält lediglich einfache Textpassagen ohne Grafiken. Das zugehörige HTML-Ausgangsdokument sieht wie folgt aus:

```
<html>
<head>
       <title> SNMP Parameters </title>
</head>
<body>
       <h2> System Information </h2>
            System Contact:<br>
            System Description:<br>
            System Uptime:<br><p>
       <h2>Subagents running on this System</h2>
       <address>
            SNMP(<a href=mailto:snmpinfo@mch6.siemens.de>
                              snmpinfo@mch6.siemens.de</a>)
       </address><p>
       Last edited: February 23rd, 1999
</body>
</html>
```

MIB-Objekte in das HTML-Ausgangsdokument einfügen

Die in Bild 70 dargestellte Custom-Page erfordert die Anzeige von drei Werten der System-Gruppe der MIB-II sowie der Subagent-Tabelle der Supervisor-MIB. Für die Konvertierung einer normalen Web-Seite in eine Custom-Page fügen Sie ein `<mibobj> ... </mibobj>`-Tag überall dort in das HTML-Dokument ein, wo Name und Wert eines MIB-Objekts angezeigt werden sollen. Soll lediglich der Wert des MIB-Ojekts (ohne den Namen der MIB-Variablen) angezeigt werden, dann fügen Sie das Attribut „value“ in den Tag ein.

Um beispielsweise den String „sysContact.0“, gefolgt vom aktuellen Wert von sysContact.0 angezeigt zu bekommen, fügen Sie `<mibobj>sysContact.0</mibobj>` in die Custom-Page ein. Wenn Sie dagegen nur den aktuellen Wert von sysContact.0 sehen wollen, fügen Sie `<mibobj value> sysContact.0</mibobj>` in die HTML-Seite ein.

MIB-Tabellen lassen sich ebenfalls in die Custom-Page einbringen. Eine MIB-Tabelle als Ganzes fügen Sie, analog einer skalaren Variablen, als `<mibobj> ... </mibobj>` in die HTML-Seite ein. Mithilfe des *columns*-Attributs können einzelne Spalten einer MIB-Tabelle in der Web-Seite angezeigt werden.

Betrachten Sie z.B. die *superVisSubagentTable* in der Supervisor-MIB. Der Entwickler der Custom-Page kann die gesamte MIB-Tabelle mit `<mibobj> superVisSubagentTable </mibobj>` in die Web-Seite einfügen. Wenn aus dieser Tabelle nur die Objekte *superVisSubagentName*, *superVisSubagentStatus*, *superVisSubagentConnTime* und *superVisSubagentLastResponseTime* angezeigt werden sollen, fügt der Entwickler der Custom-Page folgenden Tag in die HTML-Seite ein:

```
<mibobj coumns='superVisSubagentName, superVisSubagentStatus,
superVisSubagentConnTime, superVisSubagentResponseTime'</mibobj>
```

Das vollständige Beispiel ist auf Seite 431 dargestellt.

Tag-Attribute im HTML-Dokument verwenden

- **name-value**

  name-value ist der Default-Wert und zeigt *name* = *value*-Paare an.

  Beispiel:

  `<mibobj name-value>sysContact.0</mibobj>` zeigt „sysContact.0 = HelpDesk“ an, wobei „HelpDesc“ hier der aktuelle Wert des MIB-Objekts *sysContact.0* ist.

- **value**

  value zeigt ausschließlich Werte an

  Beispiel:

  `<mibobj value>sysContact.0</mibobj>` zeigt „HelpDesk“ an.

- **columns = '<column> [,<column>] ...'**

  In einer Tabelle werden nur die in *list-of-columns* angegebenen Spalten angezeigt.

  Beispiel

  Der folgende Tag zeigt in der in der Tabelle *SuperVisSubagentTable* alle Zeilen an, jedoch nur die Spalten *superVisSubagentName* und *superVisSubagentStatus*:

  ```
  <mibobj columns= 'superVisSubagentName,superVisSubagentStatus'>
  superVisSubagentTable</mibobj>
  ```

- **columns = <column:title> [,<column:title>] ...**

  In einer Tabelle werden nur die angegebenen Spalten mit den spezifizierten Titeln angezeigt.

  Beispiel:

  Um in der Tabelle *SuperVisSubagentTable* alle Zeilen, jedoch nur die Spalten *superVisSubagentName* und *superVisSubagentStatus* mit den Titeln *SubagentName* bzw. *Status* anzeigen zu lassen, ist in der HTML-Seite zu spezifizieren:

  ```
  <mibobj columns= 'superVisSubagentName:SubagentName,
  superVisSubagentStatus:Status'>superVisSubagentTable</mibobj>.
  ```

- **rowselect=<column>,<color>:<value> [,<color>:<value>] ...**
  mit den Werten: **a | a-b | a- | -b**

  In einer Tabelle wird die Farbe der in <column> spezifizierten Spalte (Attribut) in die Farbe *color* geändert, wenn der Attributwert „value“ ist.

  Beispiele

  1. ```
     <mibobj rowselect='superVisSubagentStatus,#FFFF00:3,#FF0000:2'>
     superVisSubagentTable</mibobj>
     ```

     liefert folgendes Ergebnis für das Attribut *superVisSubagentStatus*:

     – ein gelbes Feld bei dem Wert 3 (undefiniert)
     – ein rotes Feld bei dem Wert 2 (Verbindung abgebrochen)

  2. ```
     <mibobj rowselect='sm2TimeIOMachTabIdleTime,#FFFF00:200-500,
     #FF0000:-200'>sm2TimeIOMachTab</mibobj>
     ```

     liefert folgendes Ergebnis für das Attribut *sm2TimeIOMachTabIdleTime*:

     – ein gelbes Feld, falls 200 < *idletime* < 500
     – ein rotes Feld, falls *idletime* < 200

Parameter im HTML-Dokument verwenden

Einige HTML-Dokumente benötigen Eingabe-Parameter. Entsprechend konfiguriert, sucht der Web-Agent nach Parameterwerten in der URL und leiten diese Parameterwerte an die Custom-Page weiter. Einen Parameterwert können Sie ansprechen, indem Sie den Parameternamen *parametername* wie folgt spezifizieren:

```
&$parametername;
```

Beispiel

Um den Wert des Parameters *interfaceNo* an die Custom-Page zu übergeben, fügen Sie „&$interfaceNo;“ in den HTML-Text der Custom-Page ein.

Konfigurationsfertige Custom-Page

Mit den oben beschriebenen Ergänzungen haben Sie aus der HTML-Ausgangsseite eine Custum-Page erzeugt, die für die Konfiguration des Web-Agenten verwendet werden kann.

Der vollständige HTML-Code der Custom-Page sieht wie folgt aus:

```
<html>
<head>
        <title> SNMP Parameters </title>
</head>
<body>
        <h2>System Information </h2>
              System Contact: <mibobj value>sysContact.0</mibobj><br>
              System Description: <mibobj value>sysDescr.0</mibobj><br>
              System Uptime: <mibobj value>sysUpTime.0</mibobj><br><p>
        <h2>Subagents running on this System</h2>
              <mibobj rowselect='superVisSubagentStatus,#FFFF00:3,#FF0000:2'
              columns='superVisSubagentName,superVisSubagentStatus,
              superVisSubagentConnTime,superVisSubagentDisconnTime,
              superVisSubagentLastResponseTime,superVisSubagentCommand
              superVisSubagentOID'>
              superVisSubagentTable</mibobj><p>
        <address>
              SNMP (<a href=mailto:snmpinfo@mch6.siemens.de>
                        snmpinfo@mch6.siemens.de</a>)
        </address><p>
        Last edited: Februar23, 1999
</body>
</html>
```

Beachten Sie, dass ein Web-Browser, der nicht über DR-Web-Erweiterungen verfügt, die <mibobj>-Tags ignoriert. Der Web-Agent hingegen ersetzt diese Tags durch MIB-Werte und setzt und sendet die so modifizierte Seite an den Browser.

10.3.2 Konfiguration der Custom-Page mithilfe der HTML-MIB

Nach der Fertigstellung der Custom-Page können Sie die Custom-Page in der HTML-MIB konfigurieren. Der vorliegende Abschnitt gibt zunächst einen Überblick über die Konfiguration der Custom-Page. Danach werden drei verschiedene Möglichkeiten vorgestellt, wie die Konfiguration durchgeführt werden kann.

10.3.2.1 Konfiguration der HTML-MIB-Tabellen

Folgende Tabellen der HTML-MIB müssen mit Informationen über die Custom-Page versorgt werden:

– htmlPageTable
– htmlPageParameterTable
– htmlPageContentTable

Konfiguration der *htmlPageTable*

Die *htmlPageTable* der HTML-MIB enthält Informationen über die Eigenschaften der Custom-Page, wie z.B. Name und Titel. Ein Eintrag in der *htmlPageTable* bedeutet, dass die Custom-Page existiert. Außerdem enthält die *htmlPageTable* Informationen aus dem Header der Custom-Page, beginnend beim Anfang der Custom-Page bis zum <body>-Tag, einschließlich eventueller <body>-Tag-Attribute:

```
<html>
       <head>
              <title> SNMP Parameters </title>
       </head>
<body>
```

Die *htmlPageTable* enthält ferner die Informationen, die normalerweise aus dem unteren Teil der der Custom-Page zu finden sind: Die Kontaktadresse innerhalb von <address> ... </address> sowie das Datum der letzten Änderung.

```
       <address>
          SNMP (<a href=mailto:snmpinfo@mch6.siemens.de>
                                              snmpinfo@mch6.siemens.de</a>)
       </address><p>
       Last edited: Februar23, 1999
</body>
</html>
```

Bei der Konfiguration des Web-Agenten ist zubeachten, dass der HTML-Generator des Web-Agenten die Objektwerte in der *htmlPageTable* für die Generierung des HTML-Codes für den Browser verwendet. Da viele Tags generiert werden, sollten die Tags nicht im Wert der MIB-Objekte enthalten sein. Beispielsweise sollte der Wert von *htmlPageTitle* nicht die Strings <title> und </title> enthalten. Ebenso sollte *htmlPageBodyArgs* zwar die Attribute des <body>-Tags enthalten, nicht jedoch den String <body> selbst.

Konfiguration der *htmlPageParameterTable*

Falls es Parameter gibt, die von der Custom-Page referenziert werden, enthält die *htmlPageParameterTable* Informationen über diese Parameter. Typischerweise werden die Parameterwerte erst dann benötigt, wenn der Benutzer am Web-Browser auf die Custom-Page zugreift. Falls in der *htmlPageParameterTable* für einen Parameter kein Default-Wert definiert ist, wird der Benutzer am Browser zur Eingabe eines Wertes aufgefordert. Zu diesem Zweck wird der Parametername sowie ein durch Delimiterzeichen begrenztes Eingabefeld am Browser angezeigt.

Konfiguration der *htmlPageContentTable*

Die *htmlPageContentTable* enthält Informationen über den <body>-Bereich der Custom-Page, und zwar sämtliche Information zwischen <body> und </body>, mit Ausnahme der Kontaktadresse (<address>...</address>) und dem Datum der letzten Änderung. Auch hier ist zu beachten, dass keine Zeile der *htmlPageContentTable* die Strings „<body>“ oder „</body>“ enthalten darf.

```
<h2> System Information </h2>
       System Contact: <mibobj value>sysContact.0</mibobj><br>
       System Description: <mibobj value>sysDescr.0</mibobj><br>
       System Uptime: <mibobj value>sysUpTime.0</mibobj><br><p>
<h2>Subagents running on this System</h2>
       <mibobj rowselect='superVisSubagentStatus,#FFFF00:3,#FF0000:2'
       columns='superVisSubagentName,superVisSubagentStatus,
       superVisSubagentConnTime,superVisSubagentDisconnTime,
       superVisSubagentLastResponseTime,superVisSubagentCommand
       superVisSubagentOID'>
        superVisSubagentTable</mibobj><p>
```

10.3.2.2 Konfiguration der Custom-Page mithilfe einer Konfigurationsdatei

Das mit Abstand einfachste Verfahren zur Konfiguration von Custom-Pages ist das manuelle Editieren der HTML-Dateien, die den DR-Web-Seiten zu Grunde liegen.

Wenn Sie eine neue Custom-Page mit dem Namen *custompage* direkt in der Konfigurationdatei des Web-Agenten konfigurieren wollen, gehen Sie wie folgt vor:

1. Fügen Sie die folgenden Zeilen in diese Konfigurationsdatei ein:
   - eine *htmlPageEntry*-Zeile
   - je nach Zielsetzung keine, eine oder mehrere *htmlPageParameterEntry*-Zeilen
   - eine oder mehrere *htmlPageContentEntry*-Zeilen

   Einträge in der DR-Web-Konfigurationsdatei entsprechen den in der HTML-MIB definierten MIB-Objekten (siehe Seite 203).
2. Erstellen Sie im Verzeichnis */etc/snmp/dr-web/pages/snmp* eine Datei mit dem Namen der Custom-Page, ergänzt um das Suffix „.cnf“ (in den Beispielen: *snmp.cnf*).
3. Machen Sie dem Web-Agenten die neue Konfigurationsdatei bekannt, indem Sie den Namen der Custom-Page in die Datei */etc/snmp/dr-web/pages/pagelist* aufnehmen.

Im Folgenden werden werden Aufbau und Bedeutung der einzelnen Einträge näher beschrieben.

htmlPageEntry - Eigenschaften der Custom-Page festlegen

Zur Festlegung der Eigenschaften einer Custom-Page fügen Sie mit dem Tag <htmlPageEntry> eine Zeile in die DR-Web-Konfigurationsdatei ein.

Die VALUE-Klausel hat folgendes Format:

```
htmlPageName htmlPageTitle htmlPageAddressInfo htmlPageLastUpdated
htmlPageBodyArgs
```

Bedeutung:

- *htmlPageName* spezifiziert den Namen der Custom-Page
- *htmlPageTitle* spezifiziert den Titel, der oben in der Custom-Page angezeigt wird (z.B. SNMP-Parameter).
- *htmlPageAddressInfo* enthält Kontaktinformationen, die auf der Custom-Page angezeigt werden. Dieser Eintrag kann HTML-Text enthalten, z.B. einen Hyperlink für das Versenden von e-mail:

  ```
  "SNMP(<ahref=mailto:snmpinfo@mch6.siemens.de>snmpinfo@mch6.siemens.de
  </a>)"
  ```
- *htmlPageLastUpdated* ist ein Character-String der das Datum angibt, an dem die Custom-Page zuletzt geändert wurde (z.B. `"Last edited: Februar23, 1999"`)

– *htmlPageBodyArgs* ist eine Liste von Attributen, die im <body>-Tag verwendet werden (z.B. "#bgcolor=’EFEFEF’").

Beachten Sie, dass mit Ausnahme von *htmlPageName* alle Felder der VALUE-Klausel einen Oktet-String der Länge null als Wert enthalten können. In der Konfigurationsdatei wird ein Oktet-String der Länge 0 durch einen waagrechten Srich (-) dargestellt.

Beispiel

Der folgende Eintrag in einer Custom-Page-Konfigurationsdatei zeigt, wie die Eigenschaften der in Bild 63 auf Seite 413 dargestellten Web-Seite zu konfigurieren sind:

```
htmlPageEntry  \
snmp/snmp \
"SNMP Parameters" \
"SNMP
   (<ahref=mailto:snmpinfo@mch6.siemens.de>snmpinfo@mch6.siemens.de</a>)"\
"Last edited: Februar23, 1999" – –
```

htmlPageParameterEntry - Parameter der Custom-Page festlegen

Zur Festlegung der Parameter einer Custom-Page fügen Sie mit dem Tag <htmlPageParameterEntry> eine Zeile in die Konfigurationsdatei des Web-Agenten ein.

Die VALUE-Klausel hat folgendes Format:

```
htmlPageParameterName htmlPageParameterDefault htmlPageName
```

Bedeutung:

– *htmlPageParameterName* spezifiziert den Namen des Parameters, der innerhalb des HTML-Textes der Custom-Page referenziert wird.

– *htmlPageParameterDefault* ist der Wert, der bei einem Aufruf des Parameters zurückgeliefert wird. Wenn der Parameter keinen Default-Wert hat (z.B. Octet-String der Länge 0), wird der Benutzer am Web-Browser beim Zugriff auf die Web-Seite aufgefordert, den Parameterwert einzugeben. Ein Oktet-String der Länge 0 wird in der Konfigurationsdatei durch einen waagrechten Strich (-) dargestellt.

– *htmlPageName* ist der Name eines *htmlPageEntry*, der die Custom-Page identifiziert, auf die sich der Parameter bezieht.

htmlPageContentEntry - Inhalt der Custom-Page festlegen

Zur Festlegung des Inhalts einer Custom-Page fügen Sie mit dem Tag <htmlPageParameterEntry> eine Zeile in die DR-Web-Konfigurationsdatei ein.

Die VALUE-Klausel hat folgendes Format:

```
htmlPageContentIndex htmlPageContentText htmlPageName
```

Bedeutung:

– *htmlPageContentIndex* ist eine beliebige ganzzahlige Nummer für die Zeile mit HTML-Text.

– *htmlPageContentText* ist eine Textzeile, die den Inhalt der Custom-Page umfasst. Der *htmlPageContentText*-Eintrag kann gültigen HTML-Text, Verweise auf Parameter sowie <mibobj> ... </mibobj>-Elemente enthalten.

– *htmlPageName* ist der Name eines *htmlPageEntry*, der die Custom-Page identifiziert, auf die sich der HTML-Text bezieht.

Beispiel

Die folgenden Zeilen einer Custom-Page-Konfigurationsdatei zeigen, wie die Inhalte für die Beispiel-Web-Seite in Bild 63 auf Seite 413 zu konfigurieren sind. Beachten Sie, dass bei den hier gezeigten VALUE-Klauseln kein Zeilenumbruch in der Mitte der in Hochkommas (") eingeschlossenen Strings erfolgt: Die Zeilen sind lediglich aus Platzgründen unterbrochen.

```
htmlPageContentEntry \
1 " <h2> System Information </h2>" snmp/snmp
htmlPageContentEntry \
2 " System Contact: <mibobj value>sysContact.0</mibobj><br>" snmp/snmp
htmlPageContentEntry \
3 " System Description: <mibobj value>sysDescr.0</mibobj><br>" snmp/snmp
htmlPageContentEntry \
4 " System Uptime: <mibobj value>sysUpTime.0</mibobj><br><p>" snmp/snmp
htmlPageContentEntry \
10 " <h2> Subagents running on this System </h2>" snmp/snmp
htmlPageContentEntry \
11 " <mibobj rowselect='superVisSubagentStatus #FFFF00:3,#FF0000:2'
columns='superVisSubagentName,superVisSubagentStatus,superVisSubagentConnTime
,
superVisSubagentDisconnTime,superVisSubagentLastResponseTime,superVisSubagent
Command
superVisSubagentOID'>
superVisSubagentTable</mibobj><p>" snmp/snmp
```

10.3.2.3 Konfiguration der Custom-Page mithilfe von SNMP-Requests

Da in der HTML-MIB alle Informationen über die Custom-Page-Konfigurationsparameter abgelegt sind, können Sie Custom-Pages mithilfe von SetRequest-Anweisungen erstellen oder modifizieren. Die HTML-MIB ist beschrieben ab Seite 203.

10.3.2.4 Konfiguration der Custom-Page über die DR-Web-Schnittstelle

Custom-Pages können Sie auch über die DR-Web-Schnittstelle konfigurieren. Dabei gehen Sie wie folgt vor:

1. Eigenschaften der Custom-Page festlegen:

   Seite mit der URL „subtree+set/htmlPages“ aufrufen und eine neue Zeile in der *htmlPageTable* der HTML-MIB erzeugen

2. Parameter der Custom-Page festlegen:

   Seite mit der URL „subtree+set/htmlPageParameterTable“ aufrufen und je nach Zielsetzung keine, eine oder mehrere Zeilen in der *htmlPageParameterTable* der HTML-MIB erzeugen

3. Inhalt der Custom-Page festlegen:

   Seite mit der URL „subtree+set/htmlPageContentTable“ aufrufen und eine oder mehrere Zeilen in der *htmlPageContentTable* der HTML-MIB erzeugen

Einträge in der DR-Web-Konfigurationsdatei entsprechen den in der HTML-MIB definierten MIB-Objekten (siehe Seite 203).

10.4 DR-Web-Benutzerkonfiguration

Für den Zugriff auf die vom Web-Agenten gelieferte Information muss der Benutzer am Web-Browser Namen und Kennwort eingeben (siehe Seite 409). Diese Informationen werden für die Implementierung einer Benutzerkonfiguration verwendet, die festlegt,

– auf welche Informationen der Benutzer lesend zugreifen darf,
– auf welche Informationen der Benutzer schreibend zugreifen darf.

Die DR-Web-Benutzerkonfiguration ist beschrieben ab Seite 30 im Abschnitt „Security-Konfiguration“.

11 Trap-Server für Solaris und Reliant UNIX

Der Trap-Server ist ein einfacher Dämon-Prozess in Solaris und Reliant UNIX, der Traps empfängt und an konfigurierte Ports am eigenen oder an fernen Rechnern weiterleitet.

Damit erfüllt der Trap-Server folgende Aufgaben:

– Er vervielfacht und verteilt Traps.

– Er ermöglicht es Programmen ohne Root-Berechtigung, Traps zu empfangen.

Mit dem Kommando-Programm *trpcmd* können Sie den Trap-Server lokal oder remote steuern (siehe Seite 443).

Der Trap-Server wird gemäß dem Package-Verfahren mit *pkgadd* installiert. Er ist Bestandteil der Produkte BS2-SNMP-SO bzw. BS2-SNMP-SX, die Sie auf der mitgelieferten CD finden.

Im Einzelnen sind auf der CD enthalten:

Paket	**Erläuterung**
trpsrv aus BS2-SNMP-SX	Trap-Server für Reliant UNIX
SMAWtrpsv aus BS2-SNMP-SO	Trap-Server für Solaris

11.1 Dateien und Verzeichnisse

Durch die Installation des Trap-Servers wird unter */opt/lib/emanate* ein Verzeichnis *trpsrv* angelegt, das folgende Programme enthält:

- *trpsrv* (Server-Programm)
- *trpcmd* (Kommando-Programm)
- *trpsnd* (Trap-Sende-Programm)
- *trpmsg* (Trap-Sende-Programm für das spezielle BS2-Console-Format)
- *trprcv* (Trap-Empfangs-Programm)

Die Start-/Stop-Prozedur *ptrpsrv* für den Server-Prozezess ist im Verzeichnis */etc/init.d* abgelegt. Die *rc*-Prozeduren *S90trpsrv* (*rc2.d*) und *K10trpsrv* (*rc0.d* und *rcS.d*) sind lediglich Links auf die Datei *ptrprsv.*

11.2 Umgebungsvariablen

Der Trap-Server und die zugehörigen Programme verwenden die nachfolgend beschriebenen Umgebungsvariablen.

Umgebungsvariablen von *trpsrv* und *trpcmd*

TRPSRVPORT	Empfänger-Port
TRPSRVCNFDAT	Target-Konfigurationsdatei (vollständiger Pfadname)
TRPSRVCOMPORT	Kommunikationsport zwischen Server und Komandoprogramm
TRPSRVTGSPORT	Start-Port für die dynamische Vergabe des Ports
TRPSRVTGRANGE	Bereich für die dynamische Vergabe des Ports

Umgebungsvariablen von *trpsnd* und *trpmsg*

TRPSNDPORT	Sender-Port
TRPSNDADDR	Sendeadresse
TRPSRCADDR	Absenderadresse

Umgebungsvariable von *trprcv*

TRPSRVPORT	Empfänger-Port

11.3 Trap-Server-Prozess *trpsrv* (Dämon-Prozess)

Die Installation des Trap-Servers ist so ausgelegt, dass der Server-Prozess nach der Installation und bei jedem System-Start gestartet wird.

Server-Programm starten

Das Kommando zum Starten des Server-Programms lautet:

```
trpsrv [-p <port>][-l][-t {c|e}]
```

-p <*port*>
spezifiziert den Trap-Eingangs-Port.

-l
Es werden nur lokale Verbindungen eines Kommandoprogramms zugelassen.

-t
spezifiziert die Trace-Stufe.

Es gibt folgende Trace-Stufen:

– c
Von Trap-Empfang und Trap-Verteilung kann ein Trace erstellt werden.

– e
Meldungen der Klasse ERROR werden ausgegeben.

Trap-Eingangs-Port

Der Trap-Server-Prozess nimmt die von den SNMP-Agenten gesendeten Traps am Trap-Eingangs-Port entgegen. Den Trap-Eingangs-Port bestimmt der Trap-Server wie folgt:

1. Falls ein Port über den Schalter *-p* spezifiziert wurde, wird dieser Port als Trap-Eingangs-Port verwendet. Andernfalls wird mit 2) fortgesetzt.
2. Falls die Umgebungsvariable TRPSRVPORT gesetzt ist, wird TRPSRVPORT ausgewertet und der dort vermerkte Port als Trap-Eingangs-Port verwendet. Andernfalls wird mit 3) fortgesetzt.
3. Der Service *snmp-trap* in der Datei */etc/services* wird ausgewertet und der Trap-Eingangs-Port entsprechend gewählt. Falls dies nicht möglich ist, wird Port 162 als Trap-Eingangs-Port verwendet.

Verteilung der Traps

Der Trap-Server-Prozess verteilt die empfangenen Traps unverändert an die konfigurierten Empfänger-Ports.

Die Empfänger-Ports können wie folgt festgelegt werden:

– mit einem Eintrag in einer Target-Konfigurationsdatei

– mit dem Kommandoprogramm *trpcmd* (siehe Seite 443)

Empfänger-Ports in der Target-Konfigurationsdatei festlegen

Standardmäßig wird die Datei *trpsrvtargets*, die im Verzeichnis */opt/lib/emanate/trpsrv* liegt, als Target-Konfigurationsdatei verwendet. Wenn Sie eine andere Datei als Target-Konfigurationsdatei verwenden wollen, teilen Sie dies dem Trap-Server über die Umgebungsvariable TRPSRVCNFDAT mit, indem Sie dort die Target-Konfigurationsdatei mit ihrem vollständigen Pfadnamen spezifzieren.

Die Einträge in der Target-Konfigurationsdatei, mit denen Sie Trap-Ziele (Empfänger-Ports) spezifizieren, sind wie folgt aufgebaut:

<*port*> [<*system*>]

port
: Nummer des Ports auf dem spezifizierten System <*system*>, an den die Traps gesendet werden sollen

system
: IP-Adresse des Systems, auf dem der Empfänger-Port *port* liegt
Default: IP-Adresse des lokalen Systems

Empfänger-Ports, die über die Datei *trpsrvtargets* oder eine andere Target-Konfigurationsdatei konfiguriert sind, können nicht mit dem Kommandoprogramm *trpcmd* gelöscht werden.

11.4 Kommandoprogramm *trpcmd*

Mit dem Kommando-Programm *trpcmd* können Sie den Trap-Server konfigurieren.

Kommunikation mit dem Trap-Server-Prozess

Das Kommandoprogramm *trpcmd* kommuniziert über eine TCP-Verbindung mit demTrap-Server, wobei standardmäßig der Port 5410 verwendet wird. Mithilfe der Umgebungsvariablen TRPSRVCOMPORT können Sie einen anderen Port einstellen. In diesem Fall müssen Sie Kommandoprogramm und Trap-Server in der geänderten Umgebung neu starten.

Bei entsprechender Parametrisierung kann mit dem Kommandoprogramm auch remote auf den Server-Prozess zugegriffen werden, sofern der Trap-Server nicht Remote-Steuerungen abweist (siehe „Server-Programm starten, Schalter -l, auf Seite 441).

Das Kommando zur Konfiguration des Trap-Servers ist wie folgt aufgebaut:

```
trpcmd [-s <server>] {-a <port>[/<system>] | -n | -r | -d <port>[/<system>] | i } [-t {c | e}]
```

-s <*server*>
: Das Kommandoprogramm wendet sich an den Trap-Server auf dem System <*server*>. Für <*server*> geben Sie eine IP-Adresse an.

-a <*port*>[/<*system*>]
: fügt ein neues Trap-Ziel hinzu. Für <*port*> spezifizieren Sie die Portnummer, für <*system*> spezifizieren Sie die IP-Adresse des neuen Trap-Ziels. Wenn Sie für <*system*> nichts angeben, wird das lokale System angenommen.

-n
: fügt ein neues Trap-Ziel hinzu, wobei das System die zugehörige Portnummer dynamisch vergibt. Standardmäßig beginnt die Vergabe bei Port 16000 und umfasst einen Bereich von 50 Ports. Diese Werte können Sie über die Umgebungsvariablen TRPSRVTGSPORT und TRPSRVTGRANGE ändern.

  Eine dynamische Vergabe von Ports ist nur auf dem lokalen System möglich. Die Nummer des vom System ausgewählten Ports wird vom Kommandoprogramm auf *stdout* ausgegeben.

Beispiel

```
% trpcmd –n
16001
```

-d <*port*>[/<*system*>]
löscht das angegebene Trap-Ziel aus der Verteilung. Das Löschen von Trap-Zielen ist nur möglich, wenn der betreffende Port über das Kommandoprogramm mit den Schaltern *-a* oder *-n* in die Verteilung aufgenommen wurde.

-r
löscht alle Trap-Ziele. Die Datei *trpsrvtargets* mit den konfigurierten Empfänger-Ports (Trap-Zielen) wird neu eingelesen.

-i
gibt Informationen über die Trapverteilung auf die Standardausgabe aus.

Beispiel

```
% trpcmd –i
Empfangsport: 9999
_____________________________________

Nr.     Type     Port     Adresse

_____________________________________
000     PERM     08822    127.0.0.1
001     PERM     05566    139.25.105.176
002     PERM     00162    139.25.104.105
```

-t
stellt die Trace-Stufe am Server ein.

Es gibt folgende Trace-Stufen:

– c
Trap-Empfang und Verteilung können getraced werden.

– e
Meldungen der Klasse ERROR werden ausgegeben.

Ergebnisse des Kommandoprogramms

Das Kommandoprogramm liefert folgende Return-Codes:

0	o.k.
1	allgemeiner Fehler
2	nicht gefunden
3	existiert schon
4	Socket-create fehlgeschlagen
5	Check fehlgeschlagen
6	maxclient erreicht
7	maxrange erreicht

11.5 Trap-Sende-Programm *trpsnd*

Mit dem Trap-Sende-Programm *trpsnd* können Sie einen Trap im allgemeinen Format senden.

***trpsnd* aufrufen:**

`trpsnd <schalter> ...`

<schalter>	Bedeutung	Default-Wert
-d	Zieladresse	Pflicht-Paramerter, kein Default!
-p	Ziel-Port	162
-a	Absenderadresse	Lokale Adresse
-c	Community	public
-g	Generische Trap-Nummer	0
-s	Spezifische Trap-Nummer	-
-u	Time-Ticks	-
-o	Objekt-Liste	-

11.6 Trap-Sende-Programm *trpmsg*

Mit dem Trap-Sende-Programm *trpmsg* können Sie einen Trap im Application Monitor-spezifischen Format senden.

***trpmsg* aufrufen:**

```
trpmsg <schalter> ...
```

<schalter>	Bedeutung	Default-Wert
-d	Zieladresse	Pflicht-Parameter, kein Default!
-p <*port*>	Ziel-Port	162
-a	Absenderadresse	Lokale Adresse
-s	Quelle => BS2-<*Quelle*>	BS2Console
-o	Objekt	-
-w	Gewicht	0
-m	Meldung	noMessage

11.7 Trap-Empfangs-Programm *trprcv*

Mit dem Trap-Empfangs-Programm *trprcv* kann ein Trap empfangen werden.

***trprcv* aufrufen:**

```
trprcv [-p <port>] [-t]
```

-p <*port*>
Trap-Eingangs-Port
Default: 162

-t
schaltet den Trace ein.

12 Konfigurationsbeispiele

Eine Management-Station bietet dem Administrator drei Informationsebenen:

- Monitoring zur zentralen Überwachung aller Komponenten im Netz auf ihre Funktionsfähigkeit,
- gezielte Informationsbeschaffung durch Parameter, Auslastungsdaten, Statistikwerte,
- Steuerung durch manuelle oder automatische Eingriffe in die Systeme auf Grund der erhaltenen Informationen.

Die BS2000/OSD-Systeme können damit in die umfangreichen Möglichkeiten des Informations- und Alarmmanagements moderner Management-Stationen integriert werden.

Im Mittelpunkt dieses Kapitels steht die Erläuterung von vier zentralen Beispielen für ein Monitoring:

1. Basisüberwachung
2. Überwachung der Konsole
3. Überwachung unternehmenskritischer Anwendungen
4. Überwachung der Systemperformance

Die Beispiele bauen aufeinander auf, müssen aber nicht in einem Zug konfiguriert werden. Eine Basisüberwachung Ihres Systems ist bereits nach wenigen Installationsschritten möglich.

Zur Überwachung zentraler Komponenten auf ihre Funktionsfähigkeit und ihren Zustand existieren zwei Verfahren:

– das Polling und
– der Trap.

Im Polling-Modus fragt die Management-Station in regelmäßigen Abständen den Zustand der zu überwachenden Systeme ab. Der aktive Teil der Kommunikation liegt in diesem Fall beim Manager, der die Aktivitäten steuert. Der Vorteil dieses Verfahrens liegt in seiner Sicherheit, da zeitweilige Ausfälle des Agenten, des Managers oder des Netzes nach Wiederherstellung der Kommunikation keinen Einfluss auf das Ergebnis haben. Aufmerksamkeit muss der Polling-Rate gelten, denn sie ist ein Kompromiss zwischen Netzbelastung und Verzögerung der Information.

Ein Trap ist die asynchrone Meldung des Agenten über einen Problemzustand. Der aktive Teil ist in diesem Fall ist der Agent. Bei diesem Verfahren steht die Performance im Vordergrund; die Netzbelastung ist auf das Minimum reduziert, die Meldung erfolgt unmittelbar.

Oft wird die Kombination beider Verfahren genutzt. Ein Trap an die Management-Station schaltet das Polling ein oder setzt eine hochgehaltene Polling-Rate herunter.

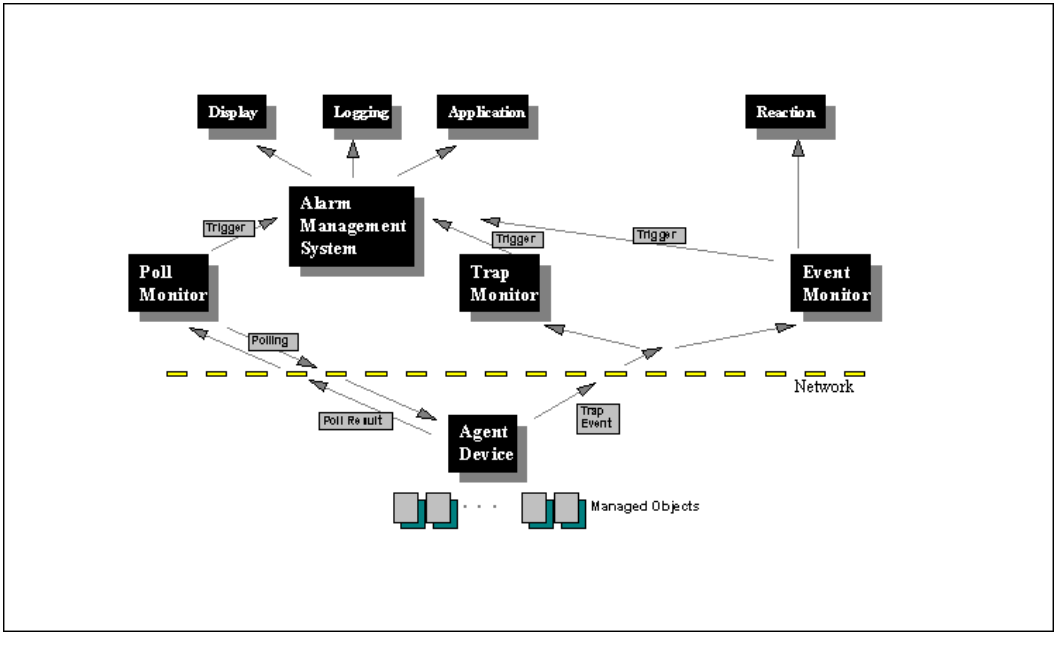


Bild 71: Überwachung mit Polling und Traps

12.1 Basisüberwachung

Aufgabenstellung

Sie wollen ständig informiert sein, ob der SNMP-Agent auf Ihrem System korrekt arbeitet. Dazu müssen Sie Ihre Management-Station so konfigurieren, dass regelmäßig ein Objekt der zentralen System-Gruppe (z.B. wie oben *SysDescr.0*) abgefragt wird. Erhalten Sie keine Anwort, dann können Sie sich entsprechend der Möglichkeiten Ihres Management-Systems den Fehler optisch oder akustisch anzeigen lassen.

Konfiguration

Führen Sie die folgenden Konfigurationsschritte an der Management-Station durch.

1. Konfiguration des Netzbildes (TransView):

Im Netzbild richten Sie eine Ikone für das BS2000/OSD-System ein. Geben Sie dazu in der Geräteübersicht den Namen, die IP-Adresse des Systems und den Community entsprechend der Konfigurationsdatei des Agenten *snmpd.cnf* an. Setzen Sie das Gerät auf *verwaltet*.

TransView Geräteübersicht:

1.	Name:	<systemname>
2.	Adressse:	<ip-adresse des BS2000/OSD-Systems>
3.	Community:	master
4.	verwaltet:	verwaltet

2. Definition eines Alarms (TransView)

In TransView ist bereits ein Alarm *Status* definiert. Stellen Sie sicher, dass dieser Alarm eingeschaltet ist.

Alarm:

Alarmname	Status	check	ON

3. Definition eines Polls (TransView)

Nutzen Sie den vorhandenen Poll *Sys_poll*. Dieser erfragt beim Agenten im Abstand von 3 Minuten (Standardeinstellung) ein Objekt der System-Gruppe. Erhält er keine Antwort, wird der Alarm ausgelöst. Überzeugen Sie sich, dass der Poll eingeschaltet ist.

Poll:

Poll-Name Sys_poll check ON

Ändern Sie die Eigenschaft des Polls von *system* auf *system-mib-II*.

Ergebnis

Stoppen Sie jetzt den Masteragenten im BS2000/OSD mit dem Kommando:

```
/STOP-SNMP-MASTER
```

Innerhalb der nächsten drei Minuten (Polling-Rate) wird TransView einen Request an den Agenten senden und keine Antwort erhalten. Diese *NoResponse*-Information wird die Ikone Ihres BS2000/OSD-Systems im Netzbild gelb färben und damit auf den Fehlerzustand hinweisen.

Starten Sie jetzt den Masteragenten erneut mit dem Kommando:

```
/START-SNMP-MASTER
```

Nach spätestens drei Minuten wird der Alarm zurückgesetzt werden.

Ist Ihnen die Zeitspanne von 3 Minuten zu hoch, so können Sie die Polling-Rate im Poll *Sys_poll* herabsetzen, was aber eine höhere Netzbelastung zur Folge hat.

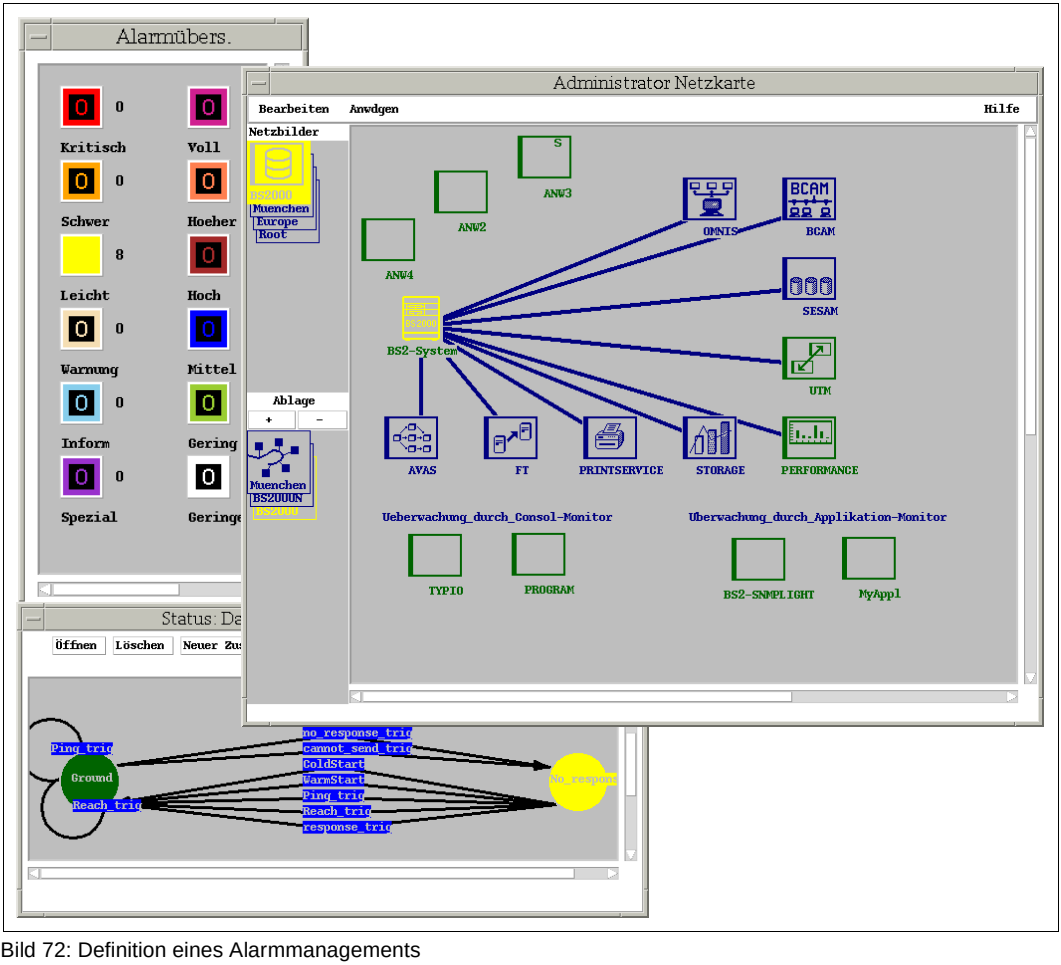


Bild 72: Definition eines Alarmmanagements

12.2 Überwachung von Meldungen durch den Console Monitor Subagenten

Aufgabenstellung

Sie wollen, dass die drei folgenden *open*UTM-Ereignisse an die Management-Station gemeldet werden:

– Beendigung einer Anwendung
– Verbindungsverlust
– Sicherheitsschutzverletzung

*open*UTM ist im Netzbild von TransView als Ikone dargestellt. Die verschiedenen Ereignisklassen sollen sich in unterschiedlicher Verfärbung dieser *open*UTM-Ikone zeigen.

Konfiguration

Führen Sie die Konfigurationsschritte 1 und 2 in BS2000/OSD und die Schritte 3 bis 6 an der Management-Station durch.

1. *open*UTM-Anwendungen:

Im *open*UTM-Meldungsmodul werden die Meldungsziele festgelegt und können mit dem Dienstprogramm *KDCMOD* verändert werden. Der geänderte Meldungsmodul muss mit den Teilprogrammen einer Anwendung zusammengebunden werden. (Genaue Informationen finden Sie in den Manualen zu *open*UTM).

Auf diese Weise sichern Sie, dass die folgenden *open*UTM-Meldungen auf Konsole ausgeben werden:

Ereignis	**Meldung**
Anwendungsende/ Taskende	K056, K058, K059, K060
Verbindungsverlust	K032, K036, K069
Sicherheitsschutzverletzung	K004, K005, K006, K031

Die Auswahl der Meldungen kann variiert werden.

2. Console Monitor Subagent

Die Filterdatei des Console Monitors muss um den folgenden Eintrag erweitert werden:

```
< UTM0100 [weight] SOURCE=UTM DEVICE=UTM >
```

Wird von *open*UTM eine der oben genannten Meldungen auf Konsole ausgegeben, so wird vom Console Monitor Subagenten ein Trap erzeugt, in dem Quelle mit *BS2-UTM* und Objekt sowie Community mit *UTM* versorgt sind.

3. Konfiguration des Netzbildes (TransView)

Nehmen Sie in das Netzbild eine Ikone mit dem Namen *UTM*, der IP-Adresse Ihres BS2000/OSD-Systems und dem Community *UTM* auf. Da *Gerätename* und *Community* gleich sind, wird die Anwendung von TV-CC als "Objekt ohne eigene IP-Adresse" erkannt. Nehmen Sie das Objekt *UTM* in die Liste der *Systeme der Domäne* auf und aktualisieren Sie das TransView Control Center.

TransView Geräteübersicht:

1.	Name:	UTM
2.	Adressse:	<ip-adresse des BS2000/OSD-Systems>
3.	Community:	UTM
4.	verwaltet:	verwaltet

Anschließend müssen Sie noch TV-CC aktualisieren

4. Definition einer Anwendung (TransView)

Im Fenster *Integrierte Anwendungen* ist eine Anwendung mit dem Namen *BS2-UTM* zu definieren. An diese Anwendung wird keine Aktion gebunden.

5. Definition eines Ereignisses (TransView)

Es sind drei Ereignisse zu definieren. Die Ereignisse entsprechen den gewünschten Meldungsgruppen und zeichnen sich durch unterschiedliche Alarmstufen aus.

Ereignis	**Name**	**Alarmstufe**	**Musterliste**
Anwendungsende / Taskende	utmTermEv	Schwer	.*K056.*, .*K058.*, .*K059.*, .*K060.*
Verbindungsverlust	utmConnEv	Inform	.*K032.*, .*K036.*, .*K069.*

Ereignis	Name	Alarmstufe	Musterliste
Sicherheitsschutzverletzung	utmAccEv	Special	.*K004.*, .*K005.*, .*K006.*, .*K031.*

6. Definition der Verknüpfungen (TransView)

Über das Menü des Fensters *Integrierte Anwendungen → Ereignisse und Reaktionen aktivieren* sind Knoten, Anwendung, Ereignisse und ggf. Reaktion zu verbinden. Als Knoten ist das Objekt *UTM* anzugeben, als Anwendung *BS2-UTM* und als Ereignisse - die im Punkt 5 festgelegten.

Knoten:	UTM
Anwendung:	BS2-UTM
Ereignis:	utmTermEv
Ereignis:	utmConnEv
Ereignis:	utmAccEv

Ergebnis

Der Subagent leitet alle Meldungen, die mit der Meldungsnummer *UTM0100* auf die Konsole geschrieben werden, an die Management-Station weiter. In dieser Trap-Information ist als Objekt *UTM* und als Quelle *BS2-UTM* vermerkt. TransView hat mit dieser Quelle und diesem Objekt drei Ereignisse verbunden. Welches dieser Ereignisse ausgelöst wird, hängt letztlich von der in der eigentlichen Meldung enthaltenen UTM-Fehlernummer Kxxx ab. Auf diese Weise wird der definierte Alarm ausgelöst. Die *open*UTM-Ikone verfärbt sich dem Alarmniveau entsprechend.

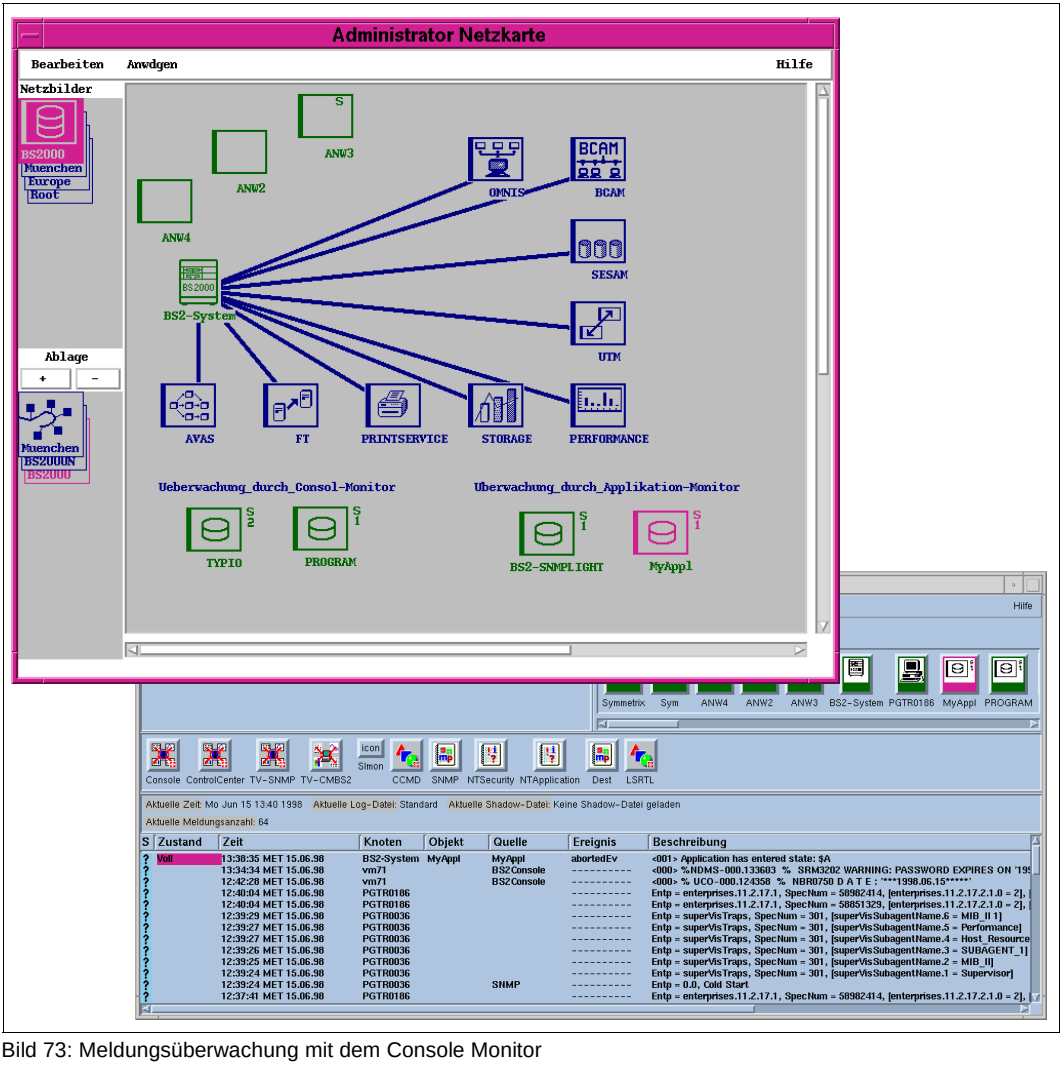


Bild 73: Meldungsüberwachung mit dem Console Monitor

12.3 Überwachung von Anwendungen durch den Application Monitor Subagenten

Aufgabenstellung

Sie wollen ausgewählte, für Sie besonders wichtige Anwendungen überwachen, um schnell über mögliche Ausfälle informiert zu sein. Dazu nehmen Sie die Anwendungen als Ikonen ins Netzbild von TransView SNMP auf. Beendet sich eine dieser Anwendungen abnormal, soll sich die entsprechende Ikone verfärben. Das ermöglicht ein schnelles und differenziertes Erfassen der problematischen Anwendungen. Darüber hinaus erscheint im Ereignismanager eine Meldung, die Sie über den Anwendungsnamen und das System, auf dem sie läuft, informiert. Das Alarmniveau können Sie entsprechend der Bedeutung der Anwendung wählen. Wird die Anwendung erneut gestartet, wird der Alarm zurückgesetzt.

Konfiguration

Führen Sie den ersten Konfigurationsschritt in BS2000/OSD und die Schritte 2 bis 5 an der Management-Station durch.

1. Application Monitor Subagent

Nehmen Sie in der Konfigurationsdatei des Application Monitor Subagenten einen Eintrag mit der Anweisung ADD-APPLICATION-RECORD vor.

a) Setzen Sie für den APPLICATION-NAME den Namen Ihrer Anwendung ein. Die Angabe TYPE=*USER kennzeichnet die Anwendung als Benutzer-Anwendung.

b) Geben Sie für JV-NAME den Namen der Monitor-Jobvariablen an, mit der Sie Ihre Anwendung starten.

c) Die Angabe der Trap-Bedingungen *A* und *R* führt dazu, dass vom Subagenten Änderungen der MONJV in die Zustände $A (aborted) und $R (running) gemeldet werden.

d) ICON = *YES bedeutet, dass für diese Anwendung ein eigenes Objekt mit dem Namen der Applikation im Netzbild der Management-Station erwartet wird.

```
//ADD-APPLICATION-RECORD  -
APPLICATION-NAME = <anwendung>, -
TYPE = *USER, -
JV-NAME = <jv-name>, -
TRAP-CONDITION=(A,R), -
ICON = *YES
```

Starten Sie den Agenten mit der neuen Konfigurationsdatei.

Der Subagent abonniert dadurch jede Änderung der angegebenen MONJV in die angegebenen Zustände und leitet Statusänderungen als Trap an die Management-Station weiter, vorausgesetzt die Anwendung wurde mit MONJV gestartet.

2. Konfiguration des Netzbildes (TransView)

Nehmen Sie in das Netzbild eine Ikone mit dem Namen der zu überwachenden Anwendung auf. Im Übersichtsfenster dieses "Gerätes" wird als Adresse die Adresse des BS2000/OSD-Systems, auf dem die Anwendung läuft, eingetragen. *Gerätename* und *Community* müssen gleich dem Anwendungsnamen sein. Dadurch wird die Anwendung von TV-CC als "Objekt ohne eigene IP-Adresse" erkannt. Aktualisieren Sie TransView Control Center wie im vorigen Beispiel.

TransView Geräteübersicht:

1.	Name:	<anwendung>
2.	Adressse:	<ip-adresse des BS2000/OSD-Systems>
3.	Community:	<anwendung>
4.	Gruppe:	tcc
5.	verwaltet:	verwaltet

Anschließend müssen Sie noch TV-CC aktualisieren

3. Definition einer Anwendung (TransView)

Im Fenster *Integrierte Anwendungen* ist eine Anwendung mit dem Namen des zu überwachenden Objektes zu definieren. An diese Anwendung wird keine Aktion gebunden.

4. Definition eines Ereignisses (TransView)

Es sind zwei Ereignisse zu definieren. Das Erste wird ausgelöst wird, wenn eine Zustandsänderung der MONJV auf ‘$A’ (aborted) gemeldet wird, das Zweite bei einer Zustandsänderung auf ‘$R’ (running). Das zweite Ereignis setzt das Erste zurück.

Ereignis	**Name**	**Alarmstufe**	**Musterliste**
Benutzer-Anwendung läuft (running)	runningEv	Normal	R$
Benutzer-Anwendung abnormal beendet (aborted)	abortedEv	Voll	A$

5. Definition der Verknüpfungen (TransView)

Über das Menü des Fensters *Integrierte Anwendungen → Ereignisse und Reaktionen aktivieren* sind Knoten, Anwendung und Ereignisse zu verbinden. Als Knoten ist jetzt das unter 2 definierte Objekt im Netzbild anzugeben, als Anwendung - die unter 3 definierte und als Ereignisse - die im Punkt 4 festgelegten.

Knoten:	<anwendung>
Anwendung:	<anwendung>
Ereignis:	runningEv
Ereignis:	abortedEv

Ergebnis

Der Subagent gibt alle Änderungen Ihrer MONJV an die Management-Station weiter. In dieser Trap-Information ist als Quelle der Name Ihrer Anwendung vermerkt. Sie haben mit der Anwendungsikone und dieser Quelle zwei Ereignisse verbunden. Das Ereignis *abortedEv* wird ausgelöst, wenn die Änderung der MONJV auf $A gemeldet wird. Die dazu festgelegte Alarmstufe *Hoch* wird durch die Verfärbung der Anwendungsikone angezeigt. Das Ereignis *runningEv* tritt ein, wenn die MONJV den Wert $R annimmt und setzt das vorherige Ereignis zurück. Durch die Angabe ICON=*YES wird der Parameter *Objekt* mit dem Anwendungsnamen versorgt. TransView leitet den Alarm nun an dieses Objekt (ohne eigene IP-Adresse) im Netzbild weiter.

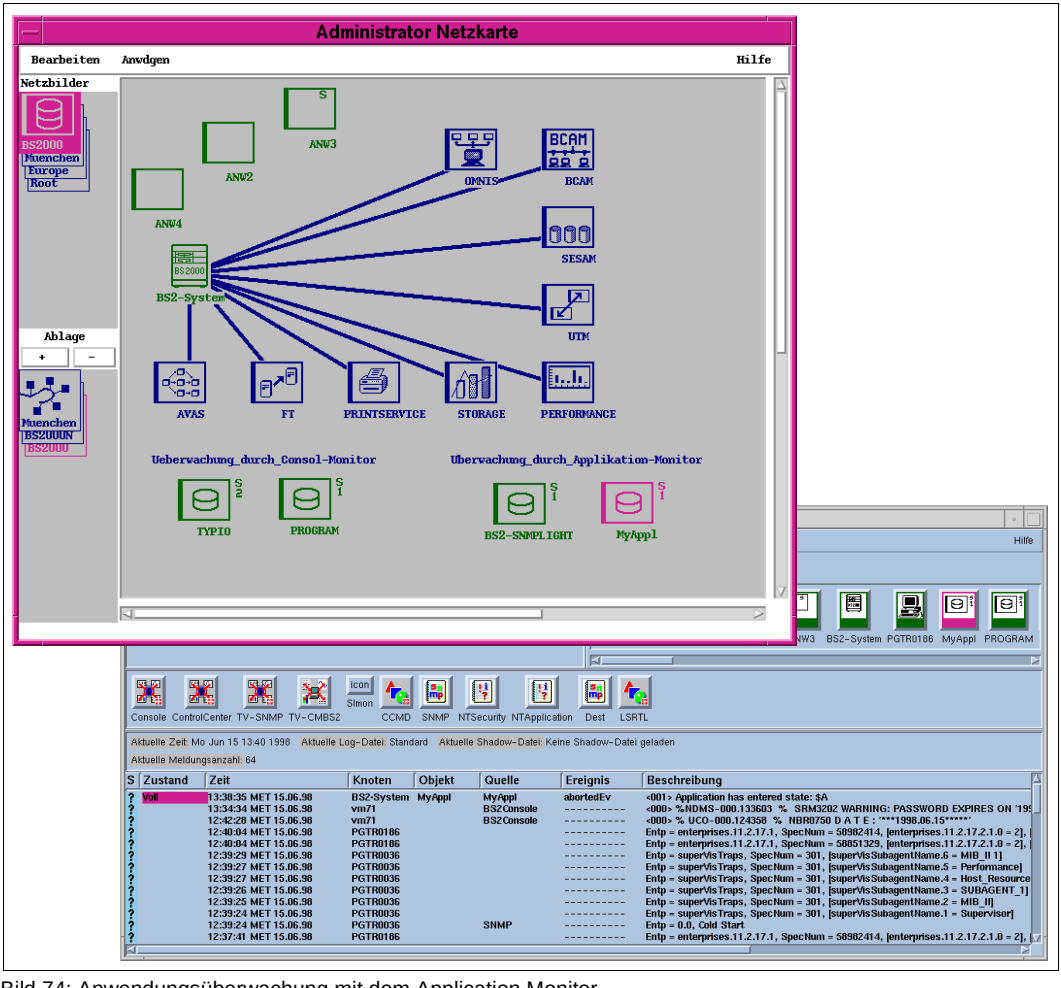


Bild 74: Anwendungsüberwachung mit dem Application Monitor

12.4 Überwachung des Systems durch den Performance Monitor Subagenten

Aufgabenstellung

Sie wollen sich die Auslastung der CPU in unterschiedlicher Färbung der Performance-Ikone im Netzbild von TransView anzeigen lassen. Hellgrün bedeutet dabei eine geringe Auslastung, blau eine mittlere und braun eine hohe. Diese Farben entsprechen den Alarmniveaus in TransView SNMP.

Konfiguration

Im Performance-Monitor Subagent ist keine spezielle Konfiguration nötig, führen Sie daher bitte alle folgenden Schritte an der Management-Station durch.

1. Konfiguration des Netzbildes (TransView)

Im Netzbild haben Sie bereits eine Ikone für das BS2000/OSD-System oder nutzen Sie die PERFORMANCE-Ikone aus der Installation von SMBS2. Setzen Sie das Gerät auf *verwaltet*.

TransView Geräteübersicht:

1.	Name:	<system-name> (PERFORMANCE)
2.	Adressse:	<ip-adresse des BS2000/OSD-Systems>
3.	Community:	master (PERFORMANCE)
4.	verwaltet:	verwaltet

2. Definition der Polls (TransView)

Definieren Sie die folgenden vier Polls.

Poll-Name / Trigger	**Zyklus**	**Bedingung**	**Eigenschaft**
PerfStart	10 min	*sm2TimeIOMachTabEntry.* *sm2TimeIOMachTabIdleTime* vorhanden	*sm2TimeIOMachTabEntry*
PerfGe-ring	2 min	*sm2TimeIOMachTabEntry.* *sm2TimeIOMachTabIdleTime* ≥ 700	*sm2TimeIOMachTabEntry*
PerfMittel	2 min	*sm2TimeIOMachTabEntry.* *sm2TimeIOMachTabIdleTime* < 700 **und** *sm2TimeIOMachTabEntry.* *sm2TimeIOMachTabIdleTime* ≥ 200	*sm2TimeIOMachTabEntry*
PerfHoch	2 min	*sm2TimeIOMachTabEntry.* *sm2TimeIOMachTabIdleTime* < 200	*sm2TimeIOMachTabEntry*

Der erste Poll dient lediglich der Initialisierung der Instanzen und wurde deshalb mit einer hohen Polling-Rate definiert. Die anderen Polls entsprechen in ihrer Polling-Rate dem Standardzyklus von SM2.

3. Definition eines Alarms (TransView)

Definieren Sie das folgende Alarmdiagramm:

Alarm

Alarmname:	Performance
Zustände:	Gering, Mittel, Hoch
Eigenschaft:	NO_PROP
Trigger:	entsprechend der folgenden Abbildung

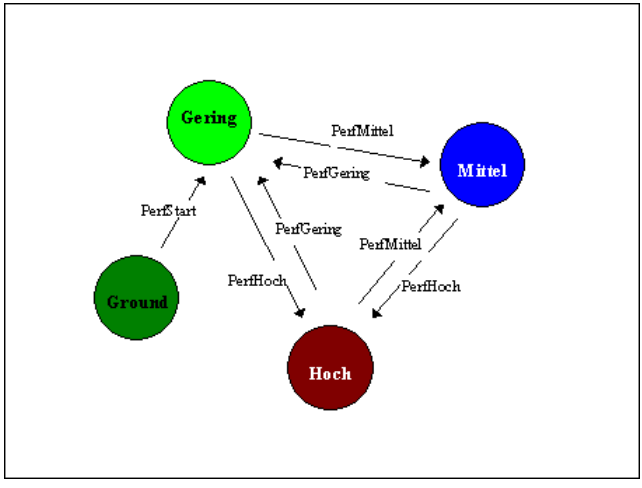


Bild 75: Alarm-Diagramm für ein Performance-Monitoring

Ergebnis

TransView fragt im Abstand der angegebenen Polling-Rate den Wert *IdleTime* des Systems ab. Erhält TransView z.B. einen Wert kleiner 200 (die Zeit ist in Promille angegeben), so wird durch den Trigger *PerfHoch* das Alarmdiagramm des Systems in den Zustand *Hoch* versetzt.

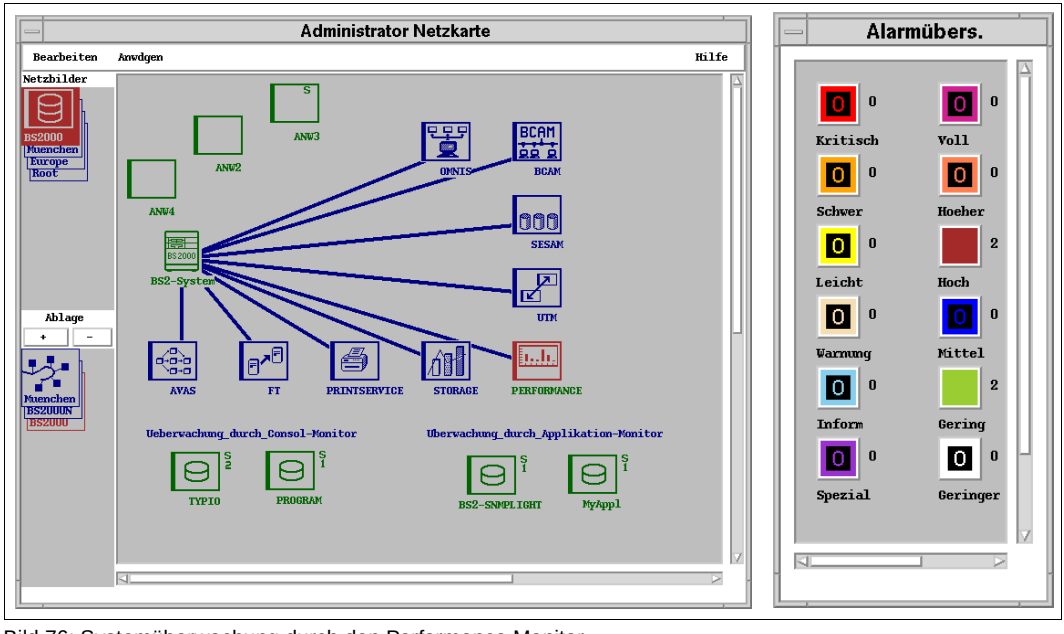


Bild 76: Systemüberwachung durch den Performance Monitor

13 Anhang: DCAM-Returncodes

Wird der YOPNCON-Aufruf sofort mit einem negativen Returncode abgewiesen, wird der Zustand auf ’unknown’ gesetzt.

Ausnahmen:

Code	Bedeutung	Zustand
0C 08	Der Partner ist bereits mit der DCAM-Anwendung verbunden.	running
0C 4C	Der Partner ist nicht erreichbar; falls DCAM-Anwendung, dann ist diese nicht eröffnet.	terminated

DCAM-Returncodes und daraus abgeleitete Zustände:

Makroaufruf erfolgreich ausgeführt (Code: 00)

Code	Bedeutung	Zustand
00	Makroaufruf erfolgreich ausgeführt	running

Makroaufruf mit Warnung beendet (Code: 04)

Code	Bedeutung	Zustand
04 0C	Keine Aufforderung oder keine Aufforderung mit passender EDIT-Option zum Verbindungsaufbau in der Warteschlange	running
04 10	Makroaufruf beendet wegen Zeitablauf (TOVAL)	running
04 18	In einer Warteschlange stehende Aufforderung zum Verbindungsaufbau annulliert wegen (System-)Zeitablauf	running
04 20	Verbindungsnachricht abgeschnitten	running
04 44	Kein Drucker für Datenausgabe betriebsbereit	running

Makroaufruf zurückgewiesen wegen des aktuellen Zustands der DCAM-Anwendung (Code: 08)

Code	Bedeutung	Zustand
08 04	Die DCAM-Anwendung ist von der aufrufenden Task nicht eröffnet (ungültiges AID)	unknown
08 20	Warnung: Erzwungene Beendigung der DCAM-Anwendung	unknown
08 24	Erzwungene Beendigung der DCAM-Anwendung	unknown
08 28	Erzwungene Beendigung der DCAM-Anwendung wegen eines DCAM-Fehlers	unknown
08 2C	Erzwungene Beendigung der DCAM-Anwendung wegen der Angabe eines ungültigen Contingency/Ereigniskennzeichens durch die Primärtask	unknown
08 38	Beendigung der DCAM-Anwendung durch eine Anforderung der Primärtask	unknown
08 40	Für diese Task wurden zu viele Aufrufe gleichen Typs gleichzeitig gegeben (max. 8, bei YOPNCON ACQUIRE 128 erlaubt).	running
08 60	Zu viele Verbindungen für die nicht vordefinierte Anwendung	running

Makroaufruf zurückgewiesen wegen des aktuellen Zustands des Partners (Code: 0C)

Code	Bedeutung	Zustand
0C 08	Der Partner ist bereits mit der DCAM-Anwendung verbunden.	running
0C 0C	Von diesem Partner wurde bereits eine Aufforderung in die Warteschlange eingereiht (kein ACQUIRE möglich).	running
0C 10	Der DIP-Steuerblock ist nicht aktiv (ungültiges DID).	running
0C 18	Die Verbindung ist durch eine Anforderung des Benutzers abgebaut worden, oder durch einen YCLSCON.	running
0C 34	Die Lage des Verteilcodes überschreitet die maximale Länge der Nachricht.	running
0C 40	Das Partnersystem hat die Verbindung ohne Angabe eines Grundes zurückgewiesen.	unknown
0C 44	Partner fordert falsches Protokoll.	running
0C 48	Systemzeitablauf für die Verbindungsanforderung	running
0C 4C	Der Partner ist nicht erreichbar; falls DCAM-Anwendung, dann ist diese nicht eröffnet.	terminated

Code	Bedeutung	Zustand
0C 50	Der Partner bearbeitet keine Aufforderungen zum Verbindungsaufbau. (Die DCAM-Anwendung befindet sich im STOP-Zustand.)	terminated
0C 54	Der Partner will keine Aufforderungen zum Verbindungsaufbau annehmen. (Die DCAM-Anwendung hat die Eigenschaften ATTR=NLOGON.)	running
0C 58	ungültiges Kennwort (LOGPW)	running
0C 5C	Die Verbindungsaufforderung ist vom Partner zurückgewiesen worden (z.B. REJLOG-Makroaufruf). Nur für DCAM(NEA)-Transport-Service-Anwendungen.	running
0C 60	Die Partnercharakteristika wurden vom Partner nicht angenommen.	running
0C 64	Fehler im Stationsdienstprotokoll	running
0C 68	Der Partner bearbeitet keine Aufforderungen zum Verbindungsaufbau; eine Aufforderung zum Verbindungsaufbau durch den Partner folgt.	running
0C 6C	Fehler in der Aktivierung der VTSU-Unterstützung des Partners	running
0C 70	Der Partner ist einer anderen DCAM-Anwendung zugehörig.	running
0C 74	Der DIP-Steuerblock adressiert keinen DCG-Steuerblock	running
0C 78	Die Verbindung wurde unmittelbar nach dem Verbindungsaufbau vom Partner oder vom System abgebaut.	running
0C 90	Die vorgeschlagene Transport-Serviceklasse wurde vom Partner nicht angenommen.	running
0C 94	Die vorgeschlagene Datennetz-Priorität wurde vom Partner nicht angenommen.	running
0C 98	Fehler bei der Verarbeitung (z.B. Störung bei X.25)	running
0C 9C	Die Aufforderung zum Verbindungsaufbau wurde von der Verwaltung zurückgewiesen. In diesem Fall mit dem Systemverwalter Verbindung aufnehmen.	running

Der Makroaufruf ist wegen des aktuellen Zustands des Kommunikationszugriff-Systems (DCM) zurückgewiesen worden (Code: 10).

Code	Bedeutung	Zustand
10 04	DCAM: Mangel an Speicherplatz	terminated
10 08	Warnung: Beendigung des DCM	terminated
10 0C	Beendigung des DCM	terminated
10 10	DCM ist nicht aktiv	terminated
10 14	DCM-Fehler	terminated

Unzulässiger Gebrauch des Makroaufrufs (Code: 14)

Code	Bedeutung	Zustand
14 04	Der Makroaufruf kann nicht von einer Sekundärtask ausgegeben werden.	unknown
14 0C	Der Makroaufruf ist nicht anwendbar im Zusammenhang mit DCAM-Anwendungen, die die Eigenschaft ATTR=NLOGON haben.	unknown
14 10	Gleichwertige Makroaufrufe stehen bereits zur Bearbeitung an (OPTCD=(ACQUIRE,ASY) oder OPTCD=(ACCEPT,SPEC,ASY))	unknown
14 14	Die DCAM-Anwendung ist nicht berechtigt, diesen Makroaufruf zu geben.	unknown
14 18	Ein synchroner Aufruf ist bereits in der Warteschlange für diese Tasks eingetragen OPTCD=(SYN,Q).	unknown

Der Makroaufruf wurde wegen falscher Operanden zurückgewiesen (Code: 18).

Code	Bedeutung	Zustand
18 04	ungültige ACB-Steuerblockadresse	unknown
18 08	ungültige CCB-Steuerblockadresse	unknown
18 0C	ungültige DCG-Steuerblockadresse	unknown
18 10	ungültige DIP-Steuerblockadresse	unknown
18 20	ungültige PTNNAME-Adresse	unknown
18 28	ungültige Adresse des Ereigniskennzeichens	unknown
18 2C	ungültige AREA-Adresse	unknown

Code	Bedeutung	Zustand
18 3C	ungültiger Partnername	unknown
18 40	Prozessor nicht aktiviert (kein /BCACT) oder nicht generiert etc.	unknown
18 44	Der CCB-Steuerblock ist für einen asynchron ablaufenden Makroaufruf belegt (aktiver CCB)	unknown
18 54	ungültige PRONAME-Adresse	unknown
18 58	negative AREALN	unknown
18 5C	nicht behebbarer Fehler, die Nachrichtenaufbereitung betreffend	unknown
18 60	ungültige Verteilcodelänge (CODELN)	unknown
18 7C	Inkonsistenz zwischen ROUTL und ROUTN	unknown
18 80	ungültige ROUTL-Adresse	unknown

Der Makroaufruf wurde zurückgewiesen wegen falscher Adressierung oder Registerangabe (Code: 20).

Code	Bedeutung	Zustand
20	Der Makroaufruf wurde zurückgewiesen wegen falscher Adressierung oder Registerangabe.	unknown

Der Aufruf wurde nicht ausgeführt, da das DCAM-Subsystem entweder nicht geladen wurde oder sich im HOLD/DELETE-Status befindet und die betroffene Task noch keine DCAM-Aufrufe absetzte (Code: 24).

Code	Bedeutung	Zustand
24	Der Aufruf wurde nicht ausgeführt, da das DCAM-Subsystem entweder nicht geladen wurde oder sich im HOLD/DELETE-Status befindet und die betroffene Task noch keine DCAM-Aufrufe absetzte.	unknown

Fachwörter

Agent

Der Agent wird auch als Management-Agent bezeichnet. Dabei handelt es sich um die Implementierung eines Management-Protokolls, die mit einer Management-Station Management-Informationen austauscht. Ein Agent ist also eine Software, die auf einem Gerät abläuft und die aktuelle Informationen über das Gerät an einen Manager oder eine entsprechende Manager-Anwendung meldet.

Alarm

Eine Gruppe von Zuständen und Zustandsübergängen. Die Zustände entsprechen Instanzen eines Objekttyps mit Attributwerten, die vom Netzverwalter angegeben werden. Immer wenn der überwachte Objekttyp eines Geräts oder einer Leitung in einen Zustand übergeht, der vom Verwalter als Alarmzustand gekennzeichnet wurde, meldet TransView SNMP das Ereignis durch Anzeigen eines entsprechenden Icons und durch eine Farbänderung für die Alarm- und Geräte-Icons.

Alarm-Aktion

Wenn ein Alarm ein Trigger-Signal empfängt, findet ein Zustandsübergang statt. Der Netzverwalter kann den Alarm so konfigurieren, dass eine Aktion ausgelöst wird, wenn ein bestimmter Zustandsübergang stattfindet. Dabei kann es sich zum Beispiel um eine der folgenden Aktionen handeln: das Protokollieren der Übergangsinformationen, das Versenden der Aktionen *Mail* oder *Beep*, das Signal eines Paging-Geräts, das Versenden eines Traps, das Absetzen eines Shell-Kommandos oder um eine Anwendung, die aufgerufen wird.

Alarm-Instanz

Eine Alarm-Instanz ist einem Management-Gerät oder den Instanzen des Objekttyps eines Management-Geräts zugeordnet.

Attribut

Ein Attribut ist Teil einer Objekttypdefinition in einem MIB-Modul. Es bezeichnet eine Eigenschaft in einem Objekttyp. Enthält der Objekttyp mehr als eine Instanz, so definieren die Attribute die Spalten und die Instanzen die Zeilen in einer Tabelle für den Objekttyp. Die Tabelleneinträge sind die Instanzwerte für die Attribute.
Siehe auch *Objekttyp* und *Objektinstanz*.

Bilddatei (Pict-Datei)

Eine bestimmte Art einer Datei von TransView SNMP, die durch die Erweiterung *.pict* gekennzeichnet ist. Diese Datei enthält Informationen über die Hintergrundbilder von Netzbildern und die Objektinstanz-Diagramme der Bedienoberfläche.

Community-String

Ein einfaches Passwort, das bei Hinzufügen eines Geräte-Icons im Netzbild angegeben wird. Der Agent, der auf dem Gerät läuft, benötigt dieses Passwort vom Manager, bevor Informationen über das Gerät zur Verfügung gestellt werden.

Eigenschaft

Dabei handelt es sich entweder um einen Objekttyp oder einen Eigenschaften-String. Beide können einer Eigenschaftsgruppe angehören. Ein Eigenschaften-String ist eine Eigenschaft (aber kein Objekttyp), die vom Hersteller oder dem Netzverwalter zur Begrenzung des Gültigkeitsbereichs von Polls und Alarmen einer Eigenschaftsgruppe hinzugefügt wird. Ein Eigenschaften-String definiert das Menü und die Untermenüs, die unter dem Aktionsknopf *Objekte* in der Geräteübersicht zur Verfügung stehen. Außerdem definiert ein Eigenschaften-String die Anwendungen, die unter dem Aktionsknopf *Anwdgen* in der Geräteübersicht zur Verfügung stehen.

Ereignismeldung

Ereignismeldungen zeigen Fehler, Zustandsänderungen und ähnliche wichtige Ereignisse im System an. Sie entstehen asynchron ("spontan"), sind kommandounabhängig, objektorientiert und werden einer beliebigen Netzmanagement-Station im Netz nach dem Bestellerprinzip zugestellt.

Gateway

Ein Gateway verknüpft heterogene Netze.

Gerät

Ein Netzsystem, Router, Hub oder eine andere adressierbare Einrichtung im Netz. Nicht: eine Leitung, ein Tap oder ein Netzbild-Icon.

Geräte-Icon

Ein Icon von TransView SNMP, das ein System, einen Router, eine Bridge, einen Hub oder eine andere verwaltbare Einrichtung im Netz (Poll möglich) darstellt. TransView SNMP enthält ein Reihe von Icons, die unterschiedliche Arten von Geräten darstellen. Geräte-Icons können auch benutzerspezifisch definiert werden.

Herstellerspezifische Erweiterungen

Zusätzliche Management-Objekte für ein Gerät, die von einem Hersteller für den Agenten dieses Geräts und für TransView SNMP zur Verfügung gestellt werden. Sie werden häufig auch als Hersteller-MIB bezeichnet.

HTML

HTML (HyperText Markup Language) ist eine genormte Auszeichnungssprache und stellt eine Teilmenge des SGML-Standards (Standard Generalized Markup Langunage) dar. HTML-Dokumente können über das genormte Kommunikationsprotokoll HTTP zwischen beliebigen Rechnersystemen ausgetauscht werden.

HTTP

HTTP (HyperText Transfer Protocol) ist das Kommunikationsprotokoll zwischen den Systemen im World Wide Web (WWW). Mit HTTP lassen sich HTML-Dokumente zwischen beliebigen Rechnersystemen und Anwendungen austauschen.

Internet

Der Name für eine Vielzahl miteinander verbundener Netze, die die Internet-Protokolle verwenden.

IP-Adresse

Darstellung eines Anschlusspunkts im Internet (32 Bit).

Leitung

Bei TransView SNMP hat eine Leitung zwei Aspekte. Zum einen stellt sie ein grafisches Icon zur Darstellung der Netztopologie dar. Zum anderen handelt es sich dabei um ein Paar von Geräte-Objektinstanzen (eine Instanz für jedes Ende der Leitung). Es wird davon ausgegangen, dass die Enden an Netzmanagement-Geräte angeschlossen sind.

Major-Trap-Nummer

Der SNMP-Standard (RFC 1157) definiert sieben Trap-Kategorien mit den Nummern 0 bis 6. Diese Nummern werden als Major-Trap-Nummern bezeichnet.

MIB

MIB steht für "Management Information Base". Der Begriff MIB bezeichnet ein Datenmodell, das die mithilfe von Netzmanagement zu verwaltenden Netzelemente (Managed Nodes) in einer abstrakten Form beschreibt. Dieses Datenmodell besteht aus den formalen Beschreibungen von Objekttypen (Objektklassen), die nach Konventionen aus dem RFC1157 aufgebaut sind.

MIB-II

Die MIB-II ist eine Standard-MIB, deren Verwendung im Internet verbindlich ist. Sie bietet für die Verwaltung von Geräten ein ausreichendes Datenmodell. Die MIB-II ist genormt und im RFC1213 definiert. Sie ist eine Erweiterung der MIB-I (RFC1156).

Netzbild

Eine Ansammlung von Leitungen und Icons, die in einer Gruppe von verschachtelten Netzbildern angeordnet werden. Optional sind entsprechende Hintergrundbilder für die Netzbilder, die ein Netz und dessen Teilnetze darstellen.

Netzbilddatei

Eine Textdatei, die die Konfigurationsinformationen zu Ihrem Netz enthält: die Dateinamen der Hintergrundbilder für Netz- und Teilnetzbilder; die Dateinamen und Positionen der Icons für Systeme, Router, Hubs und Leitungen; Konfigurationsinformationen zu Polls, Masken und Alarmen; Eigenschaftsgruppen. Diese Datei wird auch "Map Database"-Datei oder "Map_db"-Datei genannt.

Netzbild-Icon

Ein Icon von TransView SNMP, das ein Netzbild in einer Gruppe verschachtelter Netzbilder darstellt. Das Icon wird im nächsthöheren Netzbild angezeigt. Netzbild-Icons können auch benutzerspezifisch definiert werden.

Netzmanagement-Protokoll

Das Protokoll für den Austausch von Management-Informationen.

Netzmanagement-Station

Ein System im Netz, auf dem TransView SNMP oder eine entsprechende Management-Anwendung abläuft.

News

Asynchrone („spontane“) Ereignismeldungen des TRANSDATA-Netzmanagements, die von SINIX-Systemen mit ACX, BS2000- und PDN-Systemen erzeugt werden.

Objekt

In einer MIB: ein Objekttyp oder Attribut.
Auf der grafischen Bedienoberfläche: Gerät, Leitung, Tap, Poll, Maske oder Alarm - bzw. eine bestimmte Instanz davon.

Objektbezeichner (object identifier)

Eine Notation, die die Position eines Objekts in einem MIB-Baum angibt. So gibt 1.3.6.1.4.1.231.1.3.2 (iso.org.dod.internet.private.enterprise.sni.1.3.2) zum Beispiel ein RM600-System an. Es gibt auch MIB-Namen für den Objektbezeichner (z. B. *cisco* für einen Cisco-Router).

Objektinstanz

Repräsentant für Eigenschaften (Attributwerte) eines Geräts. Die Instanzen werden von dem Agenten des Geräts verwaltet.
Die Objektinstanz wird durch den Instanz-Bezeichner oder Index angegeben.

Objekttyp

Eine Klasse gleichartiger Objektinstanzen, die durch eine formale Beschreibung festgelegt ist. Zu einem Objekttyp kann es auf einem Gerät genau eine oder mehrere Instanzen geben. Wenn es mehrere Instanzen zu einem Objekttyp auf einem Gerät geben kann, ist der Objekttyp als Tabelle konstruiert. Die Zeilen dieser Tabelle repräsentieren jeweils eine Objektinstanz, die Spalten die Attribute des Objekttyps.
Ein anderer Name für Objekttyp ist Objektklasse.

Ping

Ein Protokoll, mit dem die IP-Ebenen-Konnektivität von einer IP-Adresse zu einer anderen geprüft wird.

Poll

Zyklische Anforderung von Informationen über MIB-Objekttypen. Die Konfiguration kann vom Netzverwalter vorgenommen werden.

Pollzyklus

Der Pollzyklus ist der Parameter, der bestimmt, wie oft TransView SNMP Kontakt mit einem Agenten auf einem Gerät aufnimmt, um Informationen von der MIB dieses Geräts abzurufen.

Protokoll

Eine Menge an Regeln, mit deren Hilfe Systeme miteinander kommunizieren. Siehe auch *SNMP* und *Ping*.

RFC

Request for Comments. Die Dokumentreihe, die die Internet-Protokolle und verwandte Standards beschreibt.

SNMP

SNMP steht für "Simple Network Management Protocol". SNMP ist ein Standardprotokoll für das Netzmanagement in TCP/IP-Netzen.

Tap

Ein Tap stellt in einem Netzbild den Anschlusspunkt zwischen einem Gerät und dem Netz dar. Ein Tap kann erzeugt, konfiguriert und gelöscht werden, aber er kann nicht verwaltet werden.

TCP/IP

TCP/IP steht für "Transmission Control Protocol/Internet Protocol", d.h. die Internet-Protokolle. Eine Regelmenge, die definiert, wie Systeme in einer offenen (nicht herstellergebundenen) Umgebung miteinander kommunizieren. Dabei handelt es sich normalerweise um eine große Kommunikationsinfrastruktur (Internet).

Teilnetz

Ein physikalisches Netz innerhalb eines IP-Netzes.

Teilnetzbild-Icon

Ein Icon in einem Root-Netzbild oder Teilnetzbild, das ein verschachteltes Teilnetzbild eine Ebene unter dem aktuellen Netzbild oder Teilnetzbild darstellt.

Trap

Unter SNMP sind Traps Problemmeldungen, die automatisch von einem Geräteagenten gesendet werden.

Trigger

Ein Trigger ist eine Meldung, die vom Poll- oder Maskensystem an das Alarmsystem gesendet wird. Ein Alarm führt einen Zustandsübergang durch, wenn ein bestimmter Trigger empfangen wird.

Übersicht

Ein Fenster mit Informationen, die von einem Gerät oder einer Leitung eingeholt wurden.

URL

URL (Uniform Resource Locator) ist eine Zeichenfolge, die der Benutzer am Web-Browser eingibt, um ein WWW-Dokument anzuwählen.
Die URL für das WWW enthält die Adresse der gewünschten Web-Seite und besteht aus den Komponenten Protokoll, Rechneradresse (Hostdomain-Name bzw. IP-Adresse), evtl. Portnummer, evtl. Pfad- und Dateiname sowie (optional) der Angabe einer Textstelle im Dokument.

Variable

Unter SNMP ist eine Variable das Ergebnis der Verknüpfung eines Objektinstanz-Namens mit einem zugeordneten Wert.

Verbindung

Die Objektinstanz, die eine (Leitungs-) Verbindung zu einem Netzmanagement-Gerät beschreibt.

Verbindungsinstanz

Eine Objektinstanz einer Verbindung zu einem Gerät. Siehe *Objektinstanz*.
Einem Gerät können beide Enden eines Leitungs-Icons von TransView SNMP zugeordnet werden. Diese Verbindung hat zwei Aspekte. Zum einen ist sie eine grafische Darstellung eines Teils des physikalischen Netzes; zum anderen ist sie ein Objekttyp des Geräts (z.B. ein Objekttyp für Anschluss- oder Verbindungsinformationen).

Zustand

Alarmzustand: Ein Element in einer Alarmdefinition. (Siehe *Alarm*.)
MDC-Zustand: Das Fenster *Domain Table View* führt unter dem Eintrag *State* einen Code an. Dieser Code beschreibt, ob ein lokaler oder ferner Client Manager eine Domäne überträgt oder zurückholt.

World Wide Web (WWW)

Das World Wide Web, kurz Web genannt, ist ein Internet-Dienst, der den Benutzern den Abruf und die Veröffentlichung von multimedialen Inhalten (Text, Grafik, Vides, Animation und Audio) ermöglicht. Die Dokumente im World Wide Web müssen im HTML-Format vorliegen.

Zustandsübergang

Änderung des Zustands für einen Alarm, die durch einen Trigger ausgelöst wird.

Literatur

TransView Control Center (UNIX)
Enterprise Management für Client/Server-Umgebungen
Manager (UNIX) und Agenten (UNIX, Windows NT)

Benutzerhandbuch

Zielgruppe
Administratoren und Operatoren von Management-Anwendungen
Inhalt
Mit dem TransView Control Center integrieren Sie die unterschiedlichsten Anwendungen für das System-, Anwendungs- und Netzmanagement. Das Handbuch beschreibt alle Funktionen des Control Center Managers auf UNIX und der Agenten auf UNIX und Windows NT.

TransView SNMP (UNIX)
Konfigurieren
Benutzerhandbuch

Zielgruppe
Netzadministratoren, Programmierer von Netzmanagement-Anwendungen
Inhalt
Das Handbuch beschreibt die Vorbereitung und Konfigurierung von TransView SNMP für das Management von TCP/IP-Netzen mit der grafischen Bedienoberfläche. Insbesondere werden das Erstellen von Netzbildern und die Funktionen des Alarmmanagements dargestellt.

TransView SNMP (UNIX)
Programmschnittstellen
Zielgruppe
Programmierer von Netzmanagement-Anwendungen
Inhalt
Für Programmierer mit Kenntnissen in C und Motif beschreibt das Handbuch die Elemente der Programmschnittstellen des Netzmanagementproduktes TransView SNMP. Anhand einer ablauffähigen Alarmanwendung wird das Programmierverfahren erläutert.

TRANSVIEW Extensible Agent
(SINIX V5.41)
Benutzerhandbuch

Zielgruppe
Netzverwalter lokaler Netze auf Basis von TCP/IP, SINIX-Systemverwalter und Anwendungsprogrammierer
Inhalt
Das Handbuch beschreibt, wie Sie mit Hilfe des Extensible Agent eigene MIBs implementieren, MIB-Konfigurationsdateien entfernt verändern, über SNMP spontan entfernte Operationen ausführen lassen und SNMP-Traps versenden.

TransView SNMP-Proxy BS2000/PDN (SINIX)
TRANSDATA-Netzmanagement über SNMP-Manager
Benutzerhandbuch

Zielgruppe
Das Handbuch richtet sich an Netzverwalter, die TRANSDATA-Netzmanagement über SNMP-Manager betreiben wollen.
Inhalt
Das Handbuch beschreibt die Installation/Konfiguration des Produkts Proxy BS2000/PDN, sowie dessen Bedienung über den SNMP-Manager oder die grafische Bedienoberfläche. Zudem wird die Vorgehensweise für eine Erweiterung des Funktionsumfangs (Erstellen neuer MIB-Objekte) erklärt.

TRANSVIEW NMC/NMA/NMAE
TRANSVIEW AutoOperator
(TRANSDATA, SINIX)
Allgemeine Funktionen
Benutzerhandbuch
Zielgruppe
Bediener von TRANSVIEW NMC und TRANSVIEW NMA (SINIX)

Inhalt
TRANSVIEW NMC und -NMA (SINIX) realisieren den Manager und den Agent für das Netzmanagement in TRANSDATA-Netzen. Das Handbuch beschreibt die grundlegenden Basisfunktionen und den automatischen Operator zur Reaktion auf Ereignismeldungen.

TransView NMC/NMA/NMAE
TransView NMC Developer's Tools
TransView NTAC2/NTAC2E
TransView PerfMonitor
DCAM
(TRANSDATA, SINIX, BS2000, PDN)

Meldungen und Haltkennungen
Benutzerhandbuch
Zielgruppe
Agent-Bediener, Bediener von TransView NMC und DCAM.
Inhalt
Dieses Handbuch enthält alle Meldungen des Netzmanagements in den Betriebssystemen BS2000, PDN und SINIX sowie nähere Erklärungen zu den ausgegebenen Meldungen. Die Haltkennungen erläutern den Softwarehalt bei PDN-Systemen.

TransView-NMA/-NMAE V1.2A, TransView-NTAC2 V7.1A, NTAC2E V5.1A (TRANSDATA, BS2000)
Netzmanagement im BS2000
Handbuchtyp

Zielgruppe
Das Handbuch wendet sich an den Netzplaner, Netzverwalter, Netzoperator sowie an Diagnose- und Wartungstechniker.
Inhalt
Es behandelt das Netzmanagement von BS2000-Systemen aus. Einsatz, Funktionsweise und Zusammenwirken mit anderen Produkten werden beschrieben. Das Handbuch ist aufgabenbezogen orientiert; die vollständige Referenz aller Netzmanagement-Kommandos ist nicht mehr hier, sondern im Handbuch „Netzmanagement-Kommandos“ enthalten.

TransView NMA/NMAE
(TRANSDATA, PDN)
Netzmanagement im PDN
Benutzerhandbuch
Zielgruppe
Bediener des PDN-Agent
Inhalt
TransView NMA (PDN) und TransView NMAE (PDN) realisieren gemäß dem TransView-Konzept die Agent-Funktionalität.

BS2000/OSD-Handbücher

BCAM (BS2000/OSD)
BCAM V15.0A Band 1
Benutzerhandbuch

Zielgruppe
Das Handbuch richtet sich an Netzplaner, -generierer und -verwalter, die in BS2000-Systemen BCAM betreiben.
Inhalt
BCAM Band 1 beschreibt BCAM selbst, seine Einbettung in TRANSDATA und TCP/IP- und ISO-Netze, sowie Generierungs- und Administrationstätigkeiten. Generierungsbeispiele verdeutlichen die Beschreibung. Es werden BCAM-Tools zur Generierung und Diagnose beschrieben.

BCAM (BS2000/OSD)
BCAM V15.0A Band 2
Referenzhandbuch

Zielgruppe
Das Handbuch richtet sich an Netzoperateure, -generierer und -verwalter, die in BS2000-Systemen BCAM betreiben.
Inhalt
BCAM Band 2 baut auf Band 1 auf und beschreibt ausführlich die zur Generierung und zum Betrieb nötigen BCAM-Kommandos. Es werden die zur statischen Generierung nötigen KOGS-Makros vorgestellt und die BCAM-Fehlermeldungen aufgelistet.

***open*Net Server V1.0**
SNMP-Management für *open*Net Server
Benutzerhandbuch

Zielgruppe
Das Handbuch richtet sich an Netz- und Systemverantwortliche, die ein SNMP-basiertes Netz- und Systemmanagement nutzen möchten.
Inhalt
Das Handbuch beschreibt detailliert die mit *open*Net Server ausgelieferten MIBs, die Installation und den Betrieb der Subagenten. Ein eigenes Kapitel behandelt ausführlich die Bedienung des BCAM Managers.

***inter*Net Services V1.0** (BS2000/OSD)
Administratorhandbuch

Zielgruppe
Das Handbuch richtet sich an Netzplaner, -generierer und -verwalter, die in BS2000/OSD Internet Services betreiben wollen.
Inhalt
*inter*Net Services ersetzt die Liefereinheiten TCP-IP-AP und TCP-IP-SV.
Das Handbuch beschreibt die Funktionalität der Internet Services BOOTP/DHCP, TFTP, DNS, FTP, LDAP und NTP in BS2000/OSD, außerdem wird die Nutzung der FTAC-Schnittstelle für FTP vorgestellt. Installation, Administration, Betrieb, Logging- und Diagnose-Möglichkeiten der einzelnen Komponenten sind weitere Themen dieses Handbuchs.

***inter*Net Services V1.0** (BS2000/OSD)
Benutzerhandbuch

Zielgruppe
Das Handbuch richtet sich an Netzplaner, -generierer und -verwalter sowie Nutzer, die die Internet Services in Verbindung mit BS2000/OSD nutzen wollen.
Inhalt
*inter*Net Services ersetzt die Liefereinheiten TCP-IP-AP und TCP-IP-SV.
Das Handbuch stellt die Komponenten von *inter*Net Services vor. Ausführlich werden die Nutzung von FTP, der FTAC-Schnittstelle für FTP und TELNET beschrieben. Netzverwalter benötigen dieses Handbuch zusätzlich zum Administratorhandbuch.

BS2000/OSD-BC
Verwaltung von Subsystemen (DSSM/SSCM)
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an die Systembetreuung und die Softwareberatung des BS2000.
Inhalt
Es werden das Subsystemkonzept des BS2000, die Dynamische Subsystemverwaltung DSSM und die Subsystemkatalog-Verwaltung SSCM mit den dazugehörigen Kommandos und Anweisungen beschrieben.

SPOOL V4.1A (BS2000/OSD)
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an nichtprivilegierte Anwender,
den Spool & Print - Verwalter, den RSO-Geräteverwalter und die Systembetreuung.
Inhalt
Es wird der Betrieb von SPOOL beschrieben.

RSO V3.1A(BS2000/OSD)
Remote SPOOL Output
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an nichtprivilegierte Benutzer, RSO-Geräteverwalter, SPOOL-Verwalter und Systembetreuer des BS2000/OSD.
Inhalt
Für die einzelnen Anwendergruppen werden die Aufgaben und Möglichkeiten zur Nutzung und Steuerung von dezentralen Druckern (RSO-Drucker) beschrieben. Das Handbuch enthält die Druckermerkmale aller RSO-Drucker.

AVAS (BS2000/OSD)
Auftragsverwaltung
Benutzerhandbuch

Zielgruppe
AVAS-Benutzer
Inhalt
Beschreibung der Menüs und Anweisungen zur Auftragsverwaltung; Erstellen von Jobs/S-Prozeduren und Netzen, Bedingungseinträgen und Kalendern; Kopplung von AVAS mit MAREN; Dienstprogramm AVAS-QUER.

AVAS (BS2000/OSD)
für den Administrator
Systemverwalterhandbuch

Zielgruppe
AVAS-Administratoren
Inhalt
Das Handbuch beschreibt das Einrichten des AVAS-Systems, die regelmäßig wiederkehrenden Aufgaben der Administration, die externe Erstellung von AVAS-Elementen, die AVAS-Programmschnittstelle und die AVAS Server-Schnittstelle. Es weist hin auf die Möglichkeiten, den BS2000 Mehrrechnerbetrieb zu nutzen.

AVAS (BS2000/OSD)
Auftragsverwaltungs- und Abwicklungssystem
Einführung

Zielgruppe
Alle, die das AVAS-System kennenlernen wollen.
Inhalt
Einführung in das AVAS-System. Das Handbuch zeigt den Kundennutzen von AVAS auf, stellt die wesentlichen Funktionen vor, empfielt eine Vorgehensweise bei der AVAS-Einführung und stellt Produkte im AVAS-Umfeld vor. Als Nachschlagewerk dienen die AVAS-Benutzerhandbücher.

***open*FT für BS2000 V7.0**
Enterprise File Transfer in der offenen Welt
Benutzerhandbuch

Zielgruppe
Das Handbuch richtet sich an Benutzer, die mit *open*FT Dateien übertragen oder Dateimanagement betreiben möchten.
Inhalt
Das Benutzerhandbuch stellt die Leistungen von *open*FT vor. Die Beschreibung beinhaltet auch die optionalen Komponenten *open*FT-AC für den Zugangs- und Zugriffsschutz und *open*FT-OS zur Unterstützung der FTAM-Funktionalität. Die Kommandoschnittstelle und Meldungen werden ausführlich dargestellt.

***open*FT für BS2000 V7.0**
Enterprise File Transfer
Installation und Administration
Systemverwalterhandbuch

Zielgruppe
Das Handbuch richtet sich an Verwalter, die auf ihren BS2000-Rechnern *open*FT, *open*FT-OS und *open*FT-AC betreiben möchten.
Inhalt
Das Systemverwalterhandbuch beschreibt Installation und Inbetriebnahme von *open*FT und den optionalen Komponenten *open*FT-AC und *open*FT-OS. Betrieb und Steuerung des *open*FT-Systems werden eingehend vorgestellt. Die Kommandoschnittstelle enthält die Beschreibung aller Administratorkommandos.

OMNIS/OMNIS-MENU (TRANSDATA, BS2000)
Administration und Programmierung
Benutzerhandbuch

Zielgruppe
– OMNIS-Administrator
– Programmierer
Inhalt
– Grundlagen der Administration von OMNIS und OMNIS-MENU
– OMNIS-Dienstprogramme
– Anwenderschnittstelle zur Erweiterung des Funktionsumfangs von OMNIS
– Meldungen

SESAM/SQL-Server (BS2000/OSD)
Datenbankbetrieb
Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an den SESAM/SQL-Systemverwalter.
Inhalt
Das Handbuch beschreibt, welche Möglichkeiten der Systemverwalter hat, den Datenbankbetrieb zu steuern und zu überwachen.

SM2 (BS2000/OSD)
Software Monitor
Band 1: Verwaltung und Bedienung

Zielgruppe
Anwender und Systembetreuung
Inhalt
Das Meßsystem SM2 liefert dem Benutzer statistische Daten über die Leistung des DV-Systems und die Auslastung der Betriebsmittel. Im Band 1 werden die Bedienung des Meßmonitors SM2, die SM2-Meßprogramme und die SM2-Bildschirmreports beschrieben. Zur Auswertung und Darstellung der SM2-Meßwerte siehe Band 2 des Handbuchs.

openUTM (BS2000/OSD)
Anwendungen generieren und betreiben
Benutzerhandbuch

Zielgruppe
Das Handbuch richtet sich an Anwendungsplaner, Fachprogrammierer, Administratoren und Anwender von UTM-Anwendungen.
Inhalt
Das Handbuch beschreibt die Generierung von UTM-Anwendungen mit verteilter Verarbeitung, die Tools, die *open*UTM dazu zur Verfügung stellt und die UTM-Objekte, die bei der Generierung erzeugt werden. Außerdem enthält das Handbuch alle Informationen, die für die Strukturierung, den Betrieb und die Kontrolle einer UTM-Produktivanwendung benötigt werden.

Literatur zu Unicenter TNG

Zu Unicenter TNG der Firma COMPUTER ASSOCIATES werden folgende Handbücher angeboten:

- Unicenter TNG *Getting Started*
- Unicenter TNG *Concepts Guide*
- Unicenter TNG *Administrator Guide*
- Unicenter TNG *Release Summary*
- Unicenter TNG *Managing NetWare with Unicenter TNG*

Sonstige Literatur

Douglas Steedman
Abstract Syntax Notation One (ASN.1): The Tutorial and Reference
Isleworth, 1990
(ISBN 1-871802-06-7)

Marshall T. Rose
The Simple Book: An Introduction to Management of TCP/IP-based Internets
Prentice-Hall
(ISBN 0-13-812611-9)

Bestellen von RFCs

Die im Text zitierten Request for Comments (RFCs) sind, soweit sie nicht mitausgeliefert wurden, als gedruckte Ausgaben gegen eine Kopiergebühr oder als Datei über "anonymous Internet FTP" bzw. E-Mail erhältlich.

Anonymous Internet FTP: Um einen RFC über Internet vom System *nic.ddn.mil* (IP-Adresse 192.67.67.20) zu erhalten, gehen Sie wie folgt vor:

– Erzeugen Sie eine FTP-Verbindung zum System: *ftp nic.ddn.mil*.
– Sie können nun aus dem Verzeichnis *rfc* die gewünschten Dokumente laden. Eine Liste aller verfügbaren Dokumente finden Sie in der Datei *rfc-index.txt*.

E-Mail:

Wenn Sie keinen Internet-Anschluss haben, aber Zugang zu Electronic Mail, können Sie einen RFC auch über E-Mail anfordern. Das Dokument wird Ihnen als Antwort auf Ihre Anfrage *Mail* zurückgesandt.

Senden Sie hierzu eine Mail an den Benutzer *service* auf dem System *nic.ddn.mil*: `mail service@nic.ddn.mil`
Geben Sie im Feld *Subject* die Nummer des gewünschten RFCs ein, z.B.:
`Subject: RFC 1155`

Schriftliche Anfragen zu RFCs richten Sie an:

DDN Network Information Center
SRI International
333 Ravenswood Ave.
Menlo Park, CA 94025, U.S.A.
Telefon: 415-859-3695

E-Mail: nic@nic.ddn.mil

Wenden Sie sich zum Bestellen von Handbüchern bitte an Ihre zuständige Geschäftsstelle.

Stichwörter

Inhalt

SNMP Management V5.0
SNMP Management für BS2000/OSD

Benutzerhandbuch

Zielgruppe
Das Handbuch wendet sich an Netzverwalter, -operateure und Systemverwalter, die BS2000-Systeme in ein SNMP-basiertes Management integrieren bzw. ein solches System bedienen wollen.

Inhalt
Dieses Handbuch beschreibt einerseits die Einbettung von SBA-BS2, SSC-BS2, SSA-SM2-BS2 und SSA-OUTM-BS2 in BS2000/OSD und die zum Betrieb notwendigen Installations- und Konfigurationsschritte sowie den Betrieb selbst. Die zur Überwachung notwendigen Agenten und ihre MIBs werden detailliert vorgestellt. Andererseits wird die Installation und Konfiguration der entsprechenden Management-Anwendungen auf den Management-Plattformen Unicenter TNG, TransView SNMP und HP OpenView beschrieben.
Weitere zentrale Themen des Handbuchs sind der Zugriff auf Management-Informationen über das World Wide Web sowie der Trap-Server für Solaris und Reliant UNIX.

Ausgabe: Juli 2000

Datei: snmp.pdf

Fujitsu Siemens Computers GmbH
Handbuchredaktion
81730 München

Kritik
Anregungen
Korrekturen

Fax: 0 700 / 372 00000

e-mail: DOCetc@mchp.siemens.de
http://manuals.mchp.siemens.de

Absender

Kommentar zu SNMP Management V5.0
SNMP Management für BS2000/OSD

Information on this document

On April 1, 2009, Fujitsu became the sole owner of Fujitsu Siemens Computers. This new subsidiary of Fujitsu has been renamed Fujitsu Technology Solutions.

This document from the document archive refers to a product version which was released a considerable time ago or which is no longer marketed.

Please note that all company references and copyrights in this document have been legally transferred to Fujitsu Technology Solutions.

Contact and support addresses will now be offered by Fujitsu Technology Solutions and have the format *...@ts.fujitsu.com*.

The Internet pages of Fujitsu Technology Solutions are available at *http://ts.fujitsu.com/*...
and the user documentation at *http://manuals.ts.fujitsu.com*.

Hinweise zum vorliegenden Dokument

Zum 1. April 2009 ist Fujitsu Siemens Computers in den alleinigen Besitz von Fujitsu übergegangen. Diese neue Tochtergesellschaft von Fujitsu trägt seitdem den Namen Fujitsu Technology Solutions.

Das vorliegende Dokument aus dem Dokumentenarchiv bezieht sich auf eine bereits vor längerer Zeit freigegebene oder nicht mehr im Vertrieb befindliche Produktversion.

Bitte beachten Sie, dass alle Firmenbezüge und Copyrights im vorliegenden Dokument rechtlich auf Fujitsu Technology Solutions übergegangen sind.

Kontakt- und Supportadressen werden nun von Fujitsu Technology Solutions angeboten und haben die Form *...@ts.fujitsu.com*.

Die Internetseiten von Fujitsu Technology Solutions finden Sie unter *http://de.ts.fujitsu.com/*..., und unter *http://manuals.ts.fujitsu.com* finden Sie die Benutzerdokumentation.