Novell® Sentinel™

5.1.3

www.novell.com

Band III – SENTINEL WIZARD-BENUTZERHANDBUCH

7. Juli 2006

Novell®

Rechtliche Hinweise

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online-Dokumentation: Zugriff auf die Online-Dokumentation für dieses und andere Novell-Produkte sowie auf Aktualisierungen erhalten Sie unter www.novell.com/documentation.

Novell-Marken

Informationen zu Novell-Marken finden Sie in der Liste der Marken und Dienstleistungsmarken von Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Alle Marken von Drittanbietern sind Eigentum der jeweiligen Inhaber.

Rechltliche Hinweise zu Drittanbieterprodukten

Sentinel 5 enthält möglicherweise folgende Drittanbietertechnologien:

- Apache Axis und Apache Tomcat, Copyright © 1999 bis 2005, Apache Software Foundation. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.apache.org/licenses/
- ANTLR. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.antlr.org
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000–2004, the Legion of Bouncy Castle. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.bouncycastle.org.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, Dienstprogrammpaket. Copyright © Doug Lea. Wird ohne die Klassen CopyOnWriteArrayList und ConcurrentReaderHashMap verwendet.
- Crypto++ Compilation. Copyright © 1995–2003, Wei Dai, beinhaltet folgende durch Copyright geschützte Werke: mars.cpp von Brian Gladman und Sean Woods. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.eskimo.com/~weidai/License.txt.
- Crystal Reports Developer und Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991–2003.
- edpFTPj, lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, lizenziert unter der Lesser General Public License, verfügbar unter: http://shark.objectweb.org/license.html.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003–2004.
- ILOG, Inc. Copyright © 1999–2004.
- Installshield Universal. Copyright © 1996–2005, Macrovision Corporation und/oder Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

  Java 2 Platform kann außerdem folgende Drittanbieterprodukte enthalten:

  - CoolServlets © 1999
  - DES and 3xDES © 2000, Jef Poskanzer
  - Crimson © 1999–2000, The Apache Software Foundation
  - Xalan J2 © 1999–2000, The Apache Software Foundation
  - NSIS 1.0j © 1999–2000, Nullsoft, Inc.

- Eastman Kodak Company © 1992
- Lucinda, eine eingetragene Marke oder Marke von Bigelow and Holmes
- Taligent, Inc.
- IBM, einige Teile verfügbar unter: http://oss.software.ibm.com/icu4j/

Weitere Informationen zu diesen Drittanbietertechnologien und den zugehörigen Haftungssauschlüssen und Einschränkungen finden Sie unter: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.java.sun.com/products/javabeans/glasgow/jaf.html, klicken Sie auf „Download“ > „License“.
- JavaMail. Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.java.sun.com/products/javamail/downloads/index.html, klicken Sie auf „Download“ > „License“.
- Java Ace von Douglas C. Schmidt und seiner Forschungsgruppe an der Washington University und Tao (mit ACE-Wrappers) von Douglas C. Schmidt und seiner Forschungsgruppe an der Washington University, University of California, Irvine, und Vanderbilt University. Copyright © 1993–2005. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.cs.wustl.edu/~schmidt/ACE-copying.html und http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Java Authentication and Authorization Service Modules, lizenziert unter: Lesser General Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://free.tagish.net/jaas/index.jsp.
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.java.sun.com/products/javawebstart/download-jnlp.html, klicken Sie auf „Download“ > „License“.
- Java Service Wrapper. Teile wie folgt durch Copyright geschützt: Copyright © 1999, 2004 Tanuki Software und Copyright © 2001 Silver Egg Technology. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE. Copyright © 2002 bis 2005, JIDE Software, Inc.
- jTDS ist lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, lizenziert unter: Lesser General Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://web.ukonline.co.uk/mseries
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Teile des Codes unterliegen dem Copyright verschiedener juristischer Personen, die sich alle Rechte vorbehalten. Copyright © 1989, 1991, 1992 by Carnegie Mellon University; Copyright © 1996, 1998 bis 2000, the Regents of the University of California; Copyright © 2001 bis 2003 Networks Associates Technology, Inc.; Copyright © 2001 bis 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc., und Copyright © 2003 bis 2004, Sparta, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://net-snmp.sourceforge.net.
- The OpenSSL Project. Copyright © 1998–2004, The Open SSL Project. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.openssl.org.
- Oracle Help für Java. Copyright © 1994–2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, vormals Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000–2006 L2FProd.com. Lizenziert unter der Apache-Softwarelizenz. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter https://skinlf.dev.java.net/.
- Sonic Software Corporation. Copyright © 2003–2004. Die SSC-Software enthält Sicherheitssoftware, die von RSA Security, Inc., lizenziert wurde.

- Tinyxml. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://grinninglizard.com/tinyxmldocs/index.html.
- SecurityNexus. Copyright © 2003 bis 2006. SecurityNexus, LLC. Alle Rechte vorbehalten.
- Xalan und Xerces, jeweils von der Apache Software Foundation lizenziert, Copyright © 1999–2004. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://xml.apache.org/dist/LICENSE.txt.
- yWorks. Copyright © 2003 bis 2006, yWorks.

HINWEIS: Zum Zeitpunkt der Veröffentlichung dieser Dokumentation waren die oben stehenden Links aktiv. Sollten Sie feststellen, dass einer der oben angegebenen Links unterbrochen oder die verlinkten Webseiten inaktiv sind, wenden Sie sich an Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Inhalt

Vorwort

Bei der technischen Dokumentation von Sentinel handelt es sich um allgemeine, zweckorientierte Handbücher für den Betrieb und zur Referenz. Diese Dokumentation ist für Mitarbeiter des Bereichs Informationssicherheit konzipiert. Der Text in dieser Dokumentation gilt als Referenzquelle zum Enterprise Security Management System von Sentinel. Im Sentinel-Webportal steht weitere Dokumentation zur Verfügung.

Die Technische Dokumentation von Sentinel umfasst fünf einzelne Ausgaben. Dazu gehören:

- Band I – Sentinel™ 5-Installationshandbuch
- Band II – Sentinel™ 5-Benutzerhandbuch
- Band III – Sentinel™ 5 Wizard-Benutzerhandbuch
- Band IV – Sentinel™ 5-Referenzhandbuch für Benutzer
- Band V – Sentinel™-Handbuch für Drittanbieter-Integration

Band I – Sentinel Installationshandbuch

In diesem Handbuch wird die Installation folgender Komponenten erläutert:

- Sentinel Server
- Sentinel Console
- Sentinel Correlation Engine
- Sentinel Crystal Reports
- Wizard Collector Builder
- Wizard Collector Manager
- Advisor

Band II – Sentinel Benutzerhandbuch

In diesem Handbuch werden die folgenden Themen behandelt:

- Verwendung der Sentinel Console
- Sentinel-Funktionen
- Sentinel-Architektur
- Sentinel-Kommunikation
- Herunterfahren/Starten von Sentinel
- Anfälligkeitsbewertung
- Ereignisüberwachung
- Ereignisfilterung
- Ereigniskorrelation
- Sentinel Data Manager
- Ereigniskonfiguration für Unternehmensrelevanz
- Zuordnungsservice
- Verlaufsberichte
- Wizard-Host-Verwaltung
- Vorfälle
- Szenarios
- Benutzerverwaltung
- Workflow

Band III – Wizard-Benutzerhandbuch

In diesem Handbuch werden die folgenden Themen behandelt:

- Wizard Collector Builder-Operation
- Wizard Collector Manager
- Collectors
- Wizard-Host-Verwaltung
- Erstellen und Verwalten von Collectors

Band IV – Sentinel Referenzhandbuch für Benutzer

In diesem Handbuch werden die folgenden Themen behandelt:

- Wizard-Skriptsprache
- Wizard-Parsing-Befehle
- Wizard-Administratorfunktionen
- META-Tags für Wizard und Sentinel
- Sentinel Correlation Engine
- Benutzerberechtigungen
- Korrelations-Befehlszeilenoptionen
- Sentinel Datenbankschema

Band V – Sentinel Handbuch für Drittanbieter-Integration

- Remedy
- HP OpenView Operations
- HP Service Desk

1 Einführung in Wizard

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Das Wizard-Benutzerhandbuch dient der Einführung in die Arbeit mit Novell Wizard. In diesem Handbuch werden die einzelnen Komponenten sowie deren Funktionsweise erläutert.

In diesem Handbuch wird davon ausgegangen, dass Sie mit den Aspekten der Netzwerksicherheit, der Datenbankverwaltung sowie den Windows- und UNIX-Betriebssystemen vertraut sind.

Inhalt

Dieses Handbuch enthält folgende Kapitel:

- Kapitel 1 – Einführung in Wizard
- Kapitel 2 – Verwalten von Wizard-Hosts
- Kapitel 3 – Erstellen und Warten von Collectors
- Anhang A – Syslog-Connector
- Anhang B – Socket-Server
- Anhang C – Copyright-Informationen

Verwendete Konventionen

Hinweise und Warnhinweise

HINWEIS: Hinweise stellen zusätzliche Informationen bereit, die sich als hilfreich erweisen können.

ACHTUNG: Warnhinweise stellen zusätzliche Informationen bereit, mit denen sich Beschädigungen des Systems bzw. Datenverluste u. U. vermeiden lassen.

Befehle

Befehle sind in Courier-Schriftart angegeben. Beispiel:

```
useradd –g dba –d /export/home/oracle –m –s /bin/csh
   oracle
```

Wizard

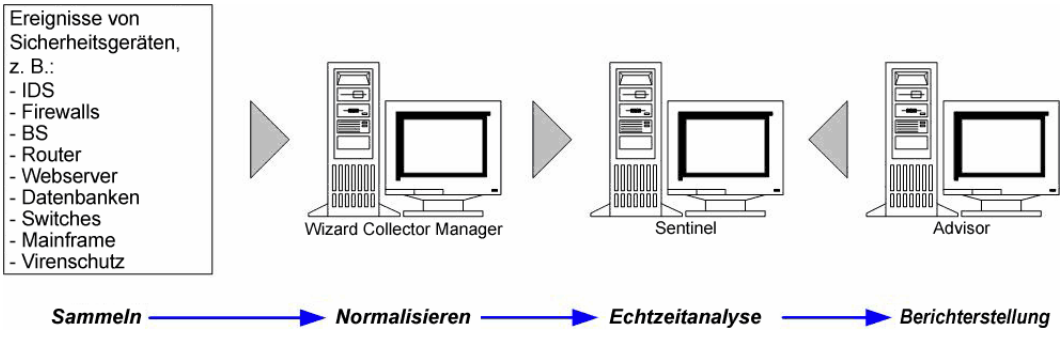
Mit Wizard können Collectors erstellt, konfiguriert und gesteuert werden. Collectors werden für die Sammlung und Normalisierung von Ereignissen von Sicherheitsgeräten und -programmen verwendet. Diese normalisierten Ereignisse werden dann für Echtzeitanalyse, Korrelation, Berichterstellung und Vorfallsreaktion an Sentinel gesendet.

HINWEIS: Es ist zwar keine Voraussetzung, jedoch empfehlenswert, dass bei einer Wizard-Konfiguration mit mehreren Collector Builder-Instanzen ein Collector Builder als primärer Collector Builder bestimmt wird. Auf diesem Computer werden Collectors gespeichert, entwickelt oder geändert sowie Ports konfiguriert.

Wizard umfasst folgende Komponenten:

- Collector Builder ist die Wizard-Benutzeroberfläche, über die Sie Collectors erstellen, konfigurieren, bereitstellen und steuern können. Collector Builder ermöglicht neben der lokalen Ausführung von Collectors zudem das Heraufladen, das Herunterladen sowie das Steuern von Collectors auf Remote-Systemen.
- Collector Manager ist die Wizard-Back-End-Komponente, die Collectors und Meldungen zum Systemstatus verwaltet und eine globale Filterung von Ereignissen durchführt.

Als Collector wird ein Rezeptor bezeichnet, der unverarbeitete (rohe) Ereignisse aus Sicherheitsgeräten und Programmen sammelt und normalisiert. Diese Ereignisse können korreliert, gemeldet und für Antworten auf Vorfälle verwendet werden. Die Sentinel-Software stellt Tier 1-Collectors bereit. Über das Sentinel-Kundenporal unter http://www.esecurityinc.com/ können zusätzliche Collectors heruntergeladen werden.



Collectors

Collectors werden zum Filtern und Standardisieren kritischer Ereignisdaten in ein normalisiertes Format sowie zum Bereitstellen dieser Daten für den Sentinel-Vorgang verwendet. Es gibt drei Collector-Stufen:

- Unterstützte Collectors (T1) – Für diese Collectors gilt Folgendes:
  - sie sind dokumentiert
  - sie weisen Metadaten auf
  - sie sind für alle Kunden verfügbar
  - für sie wird technischer Support angeboten
- Dokumentierte Collectors (T2) – Für diese Collectors gilt Folgendes:
  - sie sind für die Collector-Bibliothek bestimmt
  - sie sind dokumentiert
  - sie weisen Metadaten auf
  - sie basieren auf den standardmäßigen Sentinel-Schablonen
  - für sie wird eingeschränkter technischer Support angeboten

- Beispiel-Collectors (T3) – Für diese Collectors gilt Folgendes:
  - sie weisen ein bewährtes Konzept auf
  - sie wurden für einen bestimmten Kunden entwickelt
  - weisen u. U. keine Metadaten bzw. unterstützte Dokumentation auf
  - für sie wird eingeschränkter technischer Support angeboten

Über Collectors können Sie auf Ereignisdaten zahlreicher Quellen zugegriffen werden. Hierzu zählen:

- Intrusion Detection-Systeme (Host)
- Intrusion Detection-Systeme (Netzwerk)
- Firewalls
- Betriebssysteme
- Richtlinienüberwachung
- Authentifizierung
- Router & Switches
- VPN
- Virenschutz
- Webserver
- Datenbanken
- Mainframe
- Anfälligkeitsbewertung
- Directory Services
- Netzwerk-Management
- Proprietäre Systeme

Collectors bestehen aus:

- Schablonendateien
- Parameterdateien
- Suchdateien
- Zuordnungsdateien
- Beschreibungsdatei für Parameter sowie Manifest-Dateien

Die Schablonendatei und die zugehörige Parameterdatei werden bei der Erstellung des Collector-Skripts in unterschiedliche Skriptdateien zusammengeführt.

Die einzelnen Skriptdateien werden anhand des Spaltennamens der Wertegruppe in der Parameterdatei benannt. Skriptdateien werden der Reihenfolge nach in Start- und Zurücksetzungssequenzen unterteilt.

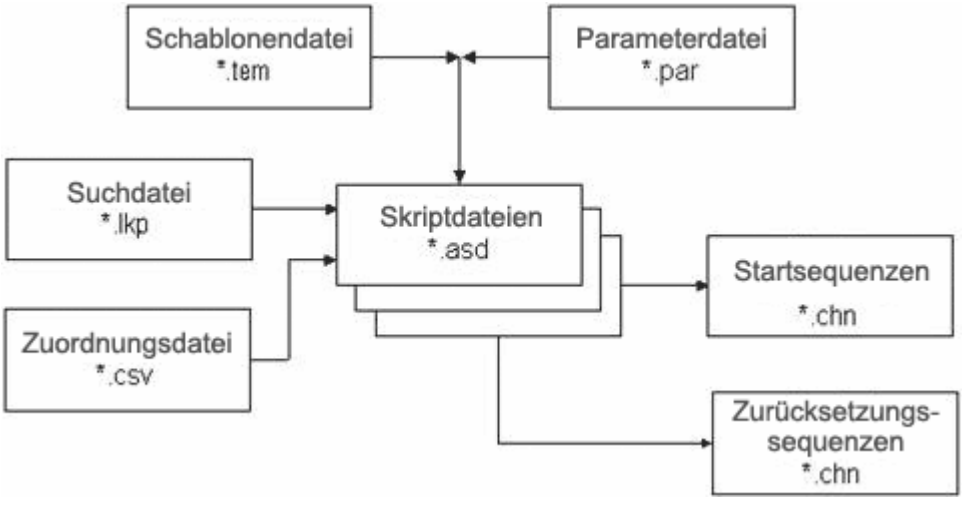
Start- und Zurücksetzungssequenzen werden einem Port zugewiesen, der eine Reihe von Skripts ausführt, die verfügbar sind, wenn der Port gestartet oder angehalten wird. Ein Skript muss in eine Start- oder Zurücksetzungssequenz eingebunden sein, damit es vom Port verwendet werden kann. Über Ports kann ein Collector im Netzwerk nach Wizard-Hosts suchen; hierzu werden die IP-Adresse bzw. der Dateiname des Host angegeben. Ports stellen für Sentinel außerdem Informationen zum Speicherort der Sensoren und des Collector bereit, der zum Verwalten der Daten für diese Sensoren verwendet wird. Folgende Optionen können für Ports konfiguriert werden:

- Verbindungstyp
  - Seriell – Daten werden von einem seriellen RS-232C Anschluss gelesen
  - Socket – eine TCP-Socket-Verbindung
  - Datei neu – liest nur Sicherheitsereignisdaten, die einer Datei hinzugefügt werden, nachdem das Skript gestartet wurde (liest vom Ende der Datei)
  - Datei alle – liest sämtliche Sicherheitsereignisdaten in einer Datei
  - Permanenter Vorgang - startet einen permanenten Vorgang, wenn der Anschluss aktiviert wird, sorgt durch Empfangs- und Übertragungsstatusangaben für die Kommunikation zwischen dem diesem Anschluss zugewiesenen Collector und einer externen Anwendung und wird für die aktive Dauer des Anschlusses fortgesetzt.

    - Temporärer Vorgang – sorgt durch Empfangs- und Übertragungsstatusangaben für die Kommunikation zwischen dem diesem Anschluss zugewiesenen Collector und einer externen Anwendung. Temporäre Vorgänge können mehrmals gestartet werden.
    - SNMP – empfängt SNMP v1-, v2- und v3-Traps
    - Keine
- Collectorname – Collectors können umbenannt, kopiert und hinzugefügt werden

Wenn eine Schablone den LOOKUP()-Parsing-Befehl verwendet, wird die entsprechende Suchdatei nach einem bestimmten Block mit Parsing-Befehlen zur Ausführung durchsucht.

Wenn eine Schablone den TRANSLATE-Parsing-Befehl verwendet, lädt der Befehl eine Zuordnungsdatei, um die schnelle Suche nach Schlüsseleinträgen zu ermöglichen.



Schablonendateien

Schablonen können erstellt, um Zustände ergänzt, bearbeitet und gelöscht werden. Mit Schablonen wird die Verarbeitung der Datensätze bestimmt. Die Entscheidungen beziehen sich mehrheitlich darauf, mit welchen Datensatztypen Sie arbeiten sowie auf deren Format. Es gibt eine äquivalente Schablonendatei mit der Erweiterung .tem. Ihr Speicherort: %WORKBENCH_HOME%\elements\<collector-name>.

Schablonendateien basieren auf dem jeweiligen Zustand. Ein Zustand ist ein Entscheidungspunkt im logischen Fluss oder Pfad einer Schablone. Jeder Punkt (Zustand) enthält Informationen, die Aufschluss über den durchzuführenden Vorgang geben. Zustände schließen Verweise auf Parameter ein; wenn die Schablone mit einer Parameterdatei zusammengeführt wird, werden die Parameter durch spezifische Werte ersetzt. Wenn die Parameter durch spezifische Werte ersetzt werden, werden eine oder mehrere Skriptdateien erstellt.

Wenn ein Status in eine Schablone eingefügt wird, wird dem Status eine Zahl zugewiesen, die nicht geändert wird, unabhängig davon, an welche Position innerhalb der Schablone der Status verschoben wird. Es gibt drei Statusgruppierungen.

- Die Zustände „Übertragen“, „Empfangen“, „Entscheiden“ und „Analysieren“ werden in der Reihenfolge nummeriert, in der Sie in die Schablone eingefügt werden.
  - Status „Übertragen“ (Tx) – überträgt eine Zeichenkette an einen definierten Port
  - Status „Empfangen“ (Rx) – definiert, ob Wizard Informationen von einer Sicherheitsmeldung in einem Puffer empfängt. Informationen werden der Portdefinition entnommen.
  - Status „Entscheiden – verwendet eine Zeichenkette oder Variable, um zu bestimmen, in welchen Status als Nächstes gewechselt werden soll
  - Status „Analysieren“ – verwendet die Parsing-Befehle, um Schablonen für die Verarbeitung der im Empfangspuffer gesammelten Informationen zu erstellen
- Die Statusangaben „Weiter“ und „Gehe zu“ werden durch die Nummer des Status identifiziert, auf den sie verweisen.
  - Status „Weiter“ – gibt an, zu welchem Status im nächsten Skript gewechselt werden soll
  - Status „Gehe zu“ – wird verwendet, um zu einem anderen Status im aktuellen Skript zurückzukehren
- Status „Stoppen“ ist stets 0. Gibt an, wann die Verarbeitung an einem Port gestoppt werden soll.

Status „Übertragen“

Vom Status „Übertragen“ wird entweder eine Zeichenkette oder Variable (je nachdem, welche Art von Daten ausgewählt wurden) an den für diesen Collector konfigurierten Verbindungstyp gesendet. Wenn beim Wechsel in den Status „Übertragen“ die Verbindung getrennt wurde und im Bereich mit den Portinformationen ein Wert in das Feld für den Empfangs-/Übertragungswert (Rx/Tx) eingegeben wird, tritt das nachfolgend angegebenen Ereignis ein. Es wird so lange versucht, die Verbindung wiederherzustellen, bis dies der Fall ist.

Es kommt zu einer Verzögerung zwischen Zeichen, aus der die Anzahl der Millisekunden (ms) zwischen dem Senden der einzelnen Datenbyte hervorgeht.

Status „Empfangen“

Der Status „Empfangen“ gibt Aufschluss über die Methode, mit der Wizard ermittelt, wann Daten vom Collector empfangen wurden. Im Status „Empfangen“ machen Sie folgende Angaben:

- Empfangstyp
- Minimale Byte
- decide-Zeichenkette für Begrenzungszeichen

Wenn beim Wechsel in den Status „Übertragen“ die Verbindung getrennt wurde und im Bereich mit den Portinformationen ein Wert in das Feld für den Empfangs-/Übertragungswert (Rx/Tx) eingegeben wird, tritt das nachfolgend angegebenen Ereignis ein. Es wird so lange versucht, die Verbindung wiederherzustellen, bis dies der Fall ist.

Nach dem Status „Empfangen“ des Empfangspuffers (RxBuffer) werden zwei Variablen automatisch mit dem Ergebnis des Status „Empfangen“ gefüllt:

- s_RXBufferString enthält den vom RxBuffer empfangenen Text
- i_RXBufferLength enthält die Länge von s_RXBufferString

Dies entspricht der Ausführung folgenden Skriptcodes im Anschluss an den Status „Empfangen“:

- COPY(s_RXBufferString:)
- LENGTH(i_RXBufferLength,s_RXBufferString)

Diese automatisch gefüllten Variablen ermöglichen im Status „Entscheiden“ den einfachen Vergleich, um zu ermitteln, ob eine Zeitüberschreitung des Status „Empfangen“ aufgetreten ist (i_RXBufferLength = 0). Sie ermöglichen zudem die direkte Verwendung des Empfangspuffers (RXbuffer) über die s_RXBufferString-Variable.

Empfangstypen – Im Schabloneneditor stehen vier Emfpangstypen zur Verfügung. Hierbei handelt es sich um:

- Zeitüberschreitung – Hiermit kann ein Skript die Verarbeitung auch dann fortsetzen, wenn die Daten nicht innerhalb des angegebenen Zeitaums eingehen. Wenn Sie „Zeitüberschreitung“ aktivieren, kann Wizard Daten empfangen, bis der Zeitüberschreitungszeitraum (wird durch die Variable RX_TIMEOUT_DELAY definiert) erreicht ist.
- Warten – Kommt hauptsächlich beim Eingang nicht angeforderter Ereignismeldungen zum Einsatz. Wizard wartet mit dem Datenempfang so lange wie unter „Zeitüberschreitung“ angegeben.

  HINWEIS: Bei den Empfangstypen „Zeitüberschreitung“ und „Warten“ wird das Skript erst fortgesetzt, wenn die minimale Anzahl an Byte eingegangen ist bzw. wenn bei der Zeitüberschreitungsoption die Zeitüberschreitung eintritt.

- Zeitüberschreitung (Begrenzungszeichen) – Verwendet eine vordefinierte Zeichenkette, um Wizard darüber zu informieren, dass Daten eingegangen sind. Die Daten im Feld „decide-Zeichenkette für Begrenzungszeichen“ werden beim Eingang der einzelnen Byte anhand der Daten im Empfangspuffer überprüft.
- Warten (Begrenzungszeichen) – Wird beim Warten auf nicht angeforderte Meldungen verwendet. Eine benutzerdefinierte Zeichenkette informiert Wizard darüber, dass Daten eingegangen sind. Wizard verwendet die Daten im Feld „decide-Zeichenkette für Begrenzungszeichen“ zur Überprüfung der Empfangsdaten beim Eingang der einzelnen Byte. Wenn die Option „Warten (Begrenzungszeichen)“ verwendet wird, hat der Parameter RX_TIMEOUT_DELAY keine Auswirkung.

  HINWEIS: Bei den Empfangstypen „Zeitüberschreitung (Begrenzungszeichen)“ und „Warten (Begrenzungszeichen)“ wird das Skript erst fortgesetzt, wenn die decide-Zeichenkette für Begrenzungszeichen als „true“ ausgewertet wird und die minimale Anzahl an Byte eingegangen ist bzw. wenn bei der Option „Zeitüberschreitung (Begrenzungszeichen)“ die Zeitüberschreitung eintritt.

Minimale Byte – Bei der minimalen Anzahl an Byte handelt es sich um die Anzahl an Byte, die eingehen müssen, bevor Wizard entweder den standardmäßigen Zeitüberschreitungszeitraum verwendet oder mit der Verarbeitung fortfährt. Die Verarbeitung im Skript wird erst fortgesetzt, wenn die minimale Anzahl an Byte eingegangen ist.

decide-Zeichenkette für Begrenzungszeichen – Die decide-Zeichenkette für Begrenzungszeichen wird vervollständigt, wenn „Zeitüberschreitung (Begrenzungszeichen)“ bzw. „Warten (Begrenzungszeichen)“ der Empfangstyp ist. Die Collector-Verarbeitung wechselt erst dann zum nächsten Status, wenn die decide-Zeichenkette für Begrenzungszeichen mit den eingelesenen Daten übereinstimmt und die minimale Anzahl an Byte eingegangen ist.

Bei der decide-Zeichenkette für Begrenzungszeichen handelt es sich um einen mit POSIX 1003.2 konformen regulären Ausdruck.

Empfangstyp-Szenarien – Es gibt vier Empfangstyp-Szenarien:

- Szenario „Zeitüberschreitung“ – Nachdem der Wechsel in den Status „Empfangen“ erfolgt ist, wird die Verarbeitung gestoppt, bis die minimale Anzahl an Byte gelesen wurde bzw. die RX_TIMEOUT_DELAY-Sekunden verstrichen sind. Nachdem bei Wizard mehr als die angegebene minimale Anzahl an Byte eingegangen ist bzw. nachdem der Zeitüberschreitungswert überschritten wurde, wird die Collector-Port-Verarbeitung fortgesetzt und wechselt zum nächsten Status des Skripts.
- Szenario „Warten“ – Beim Empfangstyp „Warten“ wird gewartet, bis die im Feld „Minimale Byte“ angegebene Mindestzahl an Byte bei Wizard Collector eingeht. Nachdem bei Wizard mehr als die im Feld „Minimale Byte“ angegebene minimale Anzahl an Byte eingegangen ist, wird die Collector-Port-Verarbeitung fortgesetzt und wechselt zum nächsten Status des Skripts. Wenn die minimale Anzahl an Byte nicht eingeht, kommt es nie zur Zeitüberschreitung der Collector-Port-Verarbeitung.
- Szenario „Zeitüberschreitung (Begrenzungszeichen)“ – Wenn die decide-Zeichenkette für Begrenzungszeichen gefunden wird, nachdem die im Feld „Minimale Byte“ angegebene Zahl an Byte eingegangen ist, werden die Daten bis zum und einschließlich des Begrenzungszeichens im Empfangspuffer (Rx Buffer) gespeichert. Wenn die decide-Zeichenkette für Begrenzungszeichen nicht gefunden wird, werden keine Daten in den Empfangspuffer übertragen und die Zeitüberschreitung der Collector-Port-Verarbeitung tritt innerhalb des standardmäßigen Zeitüberschreitungszeitraums ein.
- Szenario „Warten (Begrenzungszeichen)“ – Wenn die decide-Zeichenkette für Begrenzungszeichen gefunden wird, nachdem die im Feld „Minimale Byte“ angegebene minimale Anzahl an Byte eingegangen ist, wird die Collector-Port-Verarbeitung fortgesetzt und die Daten werden verarbeitet. Wenn die decide-Zeichenkette für Begrenzungszeichen nicht gefunden wird, werden keine Daten in den Empfangspuffer übertragen und es kommt zu keiner Port-Zeitüberschreitung. Wenn die decide-Zeichenkette für Begrenzungszeichen in keinem Fall gefunden wird, kommt es in keinem Fall zur Zeitüberschreitung der Collector-Port-Verarbeitung. Zudem gilt Folgendes: Wenn die decide-Zeichenkette für Begrenzungszeichen gefunden wird, die minimale Anzahl an Byte jedoch nicht eingegangen ist, kommt es in keinem Fall zur Zeitüberschreitung der Collector-Port-Verarbeitung.

Status „Entscheiden“

Im Status „Entscheiden“ wird der Inhalt des Empfangspuffers bzw. der Variable ausgewertet, um zu ermitteln, welche Maßnahme ergriffen werden soll. Wenn die Informationen im Empfangspuffer den ausgewählten decide-Typ enthalten, verarbeitet Collector Manager den Befehl als „true“ und die „Yes“-Route wird verfolgt. Wenn der Empfangspuffer den ausgewählten decide-Typ nicht enthält, verarbeitet Collector Manager die Entscheidung als „false“ und die „No“-Route wird verfolgt.

Beim Empfangspuffer (size Rxbuffer) handelt es sich um einen Parameter, der bearbeitet werden kann und sich in folgendem Verzeichnis befindet:

```
$WORKBENCH_HOME/config/wizard.properties/
   system.max_receive_buffer_size
```

Mit diesem Parameter können Sie den Empfangspuffer (Rx buffer) von Collector Manager konfigurieren. 50.000 Ereignisse ist der Standardwert. Das Minimum beträgt 5.000 Ereignisse. Wenn der Empfangspuffer (Rx buffer) die maximale Größe erreicht, werden neue Ereignisse abgelegt, da sie gedrosselt werden.

Es gibt vier decide-Typen:

- Zeichenkette – Vergleicht eine benutzerdefinierte decide-Zeichenkette mit dem Inhalt des Empfangspuffers. Der Inhalt der decide-Zeichenkette wird anhand des Inhalts des Empfangspuffers bzw. anhand einer Variable verglichen, um zu ermitteln, welche Entscheidungsroute verarbeitet werden soll. Bei der decide-Zeichenkette handelt es sich um einen mit POSIX 1003.2 konformen regulären Ausdruck. Eine Variable unterstützt Zeichenketten, Ganzzahlen und Float-Variablen.
- True – Erzwingt die Auswertung in „true“; Collector-Manager folgt der „Yes“-Route.
- False – Erzwingt die Auswertung in „false“; Collector-Manager folgt der „No“-Route.
- Data – Vergleicht eine benutzerdefinierte decide-Zeichenkette mit einer anderen Zeichenkette bzw. dem Wert einer Variablen.

Status „Analysieren“

Der Status „Analysieren“ wird für die Entwicklung von Skripts verwendet, die an den Ports ausgeführt werden sollen. Die Parsing-Befehle (also die Befehle für den Analysevorgang) können Parameter enthalten, die mit der Schablone zusammengeführt werden, wenn die Skripts erstellt werden. Für die Definition von Parsing-Befehlen stehen ein visueller Editor und ein Texteditor zur Verfügung.

Der Status „Analysieren“ dient zudem dem Einfügen von Parsing-Befehlen in eine Schablone. Die Parsing-Befehle können Parameter enthalten, die durch bestimmte Werte ersetzt werden, wenn die Schablone im Rahmen der Skripterstellung mit einer Parameterdatei zusammengeführt wird. Das Zusammenführen einer Schablone und einer Parameterdatei resultiert möglicherweise in mehreren Skripts zur Ausführung an den Ports.

Parameterdateien

Parameter bilden das Äquivalent zu Variablen. Parameterdateien (.par-Dateien) sind Tabellen, mit deren Hilfe Variablennamen für die verknüpften Ausführungsskriptdateien definiert werden. Sie werden verwendet, wenn eine Referenz im Analysecode vorliegt. Parameter werden als Zeichenketten gespeichert. Zur Bearbeitung muss ein numerischer Wert in eine Zeichenkette konvertiert werden. Werden neue Werte für Parameter eingegeben, werden diese wirksam, nachdem Sie Ihr Skript erstellt haben. Beim Erstellen eines Skripts werden sie mit der Schablonendatei zusammengeführt.

Die Dateinamen der Ausführungsskriptdateien werden in der ersten Zeile der Tabelle angezeigt, die Parameternamen oder Labels werden in der ersten Spalte der Tabelle angezeigt. In der zweiten Zeile der Tabelle werden die Symbole definiert, die im Collector-Baum angezeigt werden. In den restlichen Zeilen werden die Variablen oder die Parameterwerte definiert, die für die Parameter verwendet werden, da diese zu einem bestimmten Skript gehören.

Werte innerhalb der Parameterdatei sind:

- META-Tags, Informationen und Kommentare – es sind mehr als 200 META-Tags verfügbar; 100 können vom Benutzer konfiguriert werden, die restlichen sind reserviert.
- Regel – Dateinamen werden in der Kopfzeile der Tabelle angezeigt, die Parameter selbst werden in der ersten Spalte der Tabelle angezeigt.
- Bitmap – zweite Zeile in der Tabelle. Es wird die Bitmap definiert, die für diese Datei verwendet wird. Die Bitmap wird in der Collectors-Liste angezeigt.

Suchdateien

Suchdateien sind optionale Tabellen (.lkp-Dateien), die zum Vergleich empfangener Werte verwendet werden können, um zu ermitteln, welche Maßnahmen ggf. als Reaktion auf Sicherheitsereignisse ergriffen werden müssen. In den Suchdateien sind Abgleichsklauseln enthalten, die zum Vergleich der einzelnen Zeichenketten verwendet werden. Auf der Grundlage der Abgleichsklauseln in einer spezifischen Suchdatei und den von den Quellgeräten empfangenen Daten wird mit dem LOOKUP-Befehl bestimmt, ob die gesuchte Zeichenkette gefunden wird oder nicht.

Optional können der Abgleichzeichenkette Parsing-Befehle zugeordnet werden. Die Parsing-Befehle werden ausgeführt, wenn eine Übereinstimmung gefunden wird.

Zuordnungsdateien

Zuordnungsdateien sind optionale Dateien (.csv), mit denen die schnelle Suche nach Schlüsseleinträgen möglich ist. Die CSV-Datei stellt einen relativen Pfad von einem Skriptverzeichnis des Collector dar. Zurzeit können diese Dateien in Collector Builder nicht bearbeitet werden. Die Bearbeitung in Excel ist jedoch möglich.

Hier ein Beispiel einer Zuordnungsdatei:

```
~Month~   ~Number~
Jan              1
Feb              2
Mar              3
Apr              4
May              5
Jun              6
Jul              7
Aug              8
Sep              9
Oct             10
Nov             11
Dec             12
```

Bei den Einträgen kann es sich um eine variable Anzahl an Skriptvariablen (Zeichenkette, Variable oder Float-Wert) handeln, mit denen die Variablen zum Speichern der Daten angegeben werden. Im vorliegenden Beispiel wird „Month“ in eine „Number“ übersetzt (ihr also zugeordnet), beispielsweise „Jan“ mit „1“.

Manifest-Dateien

Manifest-Dateien machen den Unterschied zwischen Collectors mit Version 5.* und bisherigen Collectors aus. Manifest-Dateien unterstützen die Entwicklung von Collectors über Sentinel Console; zudem wird die Collector-Versionsermittlung unterstützt. Collector-Parsing wird in der Datei agent.lkp definiert. Es gibt folgende Suchfälle:

- Setup – Einmalige Einrichtung von Variablen und Parametern
- Check_Setup – Einmalige Prüfung dieser Variablen und Parameter
- Initialize_Vars – Der Anfang der einzelnen Schleifen; Variablen werden hierbei einmal pro Analysevorgang (Parse) initialisiert
- Parse – Der Ort, an der der Analysevorgang durchgeführt wird

Auf diese Weise können neue Collectors als Plugins in bestehende Schablonen eingefügt werden. Zudem ist der Overlay-Vorgang für neue Versionen des Collector-Analysevorgangs und somit die Aktualisierung des Codes möglich. Nachfolgend sind die Manifest-Dateien und ihr Inhalt für V5.0 aufgeführt:

- agent.nfo
  - product,Snort
  - product.vendor,GNU
  - product.version,2.0
  - product.security.type,IDS
  - product.sensor.type,N
  - product.name,IDSx_GNUx_SNRT
  - file.version,1

Weitere Sentinel-Referenzen

Folgende Handbücher sind auf den Sentinel-Installations-CDs enthalten:

- Sentinel™-Installationshandbuch
- Sentinel™-Benutzerhandbuch
- Sentinel™ 5 Wizard-Benutzerhandbuch
- Sentinel™-Referenzhandbuch für Benutzer
- Sentinel™-Handbuch für Drittanbieter-Integration
- Versionshinweise

Kontaktaufnahme mit Novell

- Website: http://www.novell.com
- Technischer Support von Novell: http://www.novell.com/support/index.html
- Internationaler technischer Support von Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Self-Support: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Für Support rund um die Uhr: +1 800-858-4000

2 Verwalten von Wizard-Hosts

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Wizard-Hosts sind Computer, auf denen Collector Manager installiert ist. Host interagieren über das Netzwerk mit Collector Builder-Computern und Sentinel. Collectors empfangen und analysieren Daten. Basierend auf diesen Daten senden Hosts Warnmeldungen an Sentinel.

Wizard erkennt Hosts im Netzwerk automatisch und fügt sie der Liste auf der Registerkarte mit den Wizard-Hosts hinzu. Hosts können nicht manuell hinzugefügt werden. Sie können vorhandene Hosts umbenennen und Hosts löschen, die im Netzwerk physisch nicht mehr vorhanden sind und nicht mehr kommunizieren.

Collector Builder sammelt Zustandsmeldungen für Hosts. Wenn ein Host nicht mit einer Zustandsmeldung reagiert, wird er im Baum mit den Wizard-Hosts mit einem roten X versehen. Ein Host mit einem roten X kann entfernt werden, wenn Collector Builder erkennt, dass der Host kommuniziert, wird der Host wieder im Baum mit den Wizard-Hosts angezeigt. Ebenso gilt: Wenn Sie einen Host entfernen, der bereits kommuniziert, gelangt er durch die Zustandsmeldung wieder in den Baum mit den Wizard-Hosts.

Wenn ein Host erkannt wird, wird ihm eine Kennnummer zugewiesen.

Aktuelle Collectors finden Sie auf der Service Pack-CD. Weitere Informationen finden Sie in den Service Pack-Versionshinweisen.

HINWEIS: Weitere Informationen zur Konfiguration der Demo-Collectors finden Sie im Sentinel-Installationshandbuch unter „Testen der Installation“.

So ruft ein Wizard-Host Collector-Daten ab

Um einem Wizard-Host (einem Computer, auf dem Collector Manager installiert ist) den Empfang von Daten von einem Collector zu ermöglichen, laden Sie den Collector von einem Collector Builder-Computer über einen in Collector Builder konfigurierten Port auf den Wizard-Host herauf. Nachdem ein Collector auf einen Host heraufgeladen wurde, kann der Host Daten von diesem Collector empfangen.

Jeder Wizard-Host kann mit mehreren Ports verbunden sein und kann Daten von mehreren Collectors überwachen. Ein Wizard-Host kann über Ports mit Collectors verfügen, die Verbindungen zu vielen unterschiedlichen Datenquellen herstellen. Einzelne Collectors auf einem Wizard-Port-Host müssen zum Ausführen heraufgeladen werden. Zudem stellen Ports Informationen zu Datenquellenstandorten für Collector Manager bereit.

Wizard-Host-Berechtigungen

Die Wizard-Host-Berechtigungen werden über die Admin-Registerkarte von Sentinel Control Center verwaltet. Es gibt folgende Wizard-Host-Benutzerberechtigungen:

Berechtigungsname	Beschreibung
Collectors anzeigen	▪ Collector-Registerkarte in Sentinel Control Center anzeigen ▪ Registerkarte mit Wizard-Hosts in Collector Builder anzeigen
Collectors steuern	▪ Umfasst dieselben Fähigkeiten wie die Berechtigung „Collectors anzeigen“ ▪ Ermöglicht die Steuerung von Collectors über Sentinel Control Center ▪ Ermöglicht die Steuerung von Collectors über Wizard Collector Builder
Collector-Administration	▪ Umfasst dieselben Fähigkeiten wie die Berechtigung „Collectors steuern“ ▪ In Collector Builder: Bearbeiten und Bereitstellen von Collectors ▪ In Collector Builder: Erstellen, Bearbeiten und Kompilieren von Collectors sowie Durchführen der Fehlersuche für Collectors ▪ In Collector Builder: Herauf- und Herunterladen von Collectors ▪ In Collector Builder: Exportieren von Wizard-Hosts ▪ In Collector Builder: Hinzufügen, Bearbeiten und Löschen von Ports ▪ In Collector Builder: Festlegen von Portoptionen

Die Steuerung umfasst folgende Schritte:

- Einzelne Ports starten/stoppen
- Alle Ports starten/stoppen
- Hosts neu starten
- Hosts umbenennen

Wizard-Host-Verwaltung

In diesem Kapitel werden folgende Themen erläutert:

- Starten von Collector Manager
- Stoppen von Collector Manager
- Collector Manager-Administration
- Umbenennen eines Host
- Löschen eines Host
- Neustarten eines Host
- Exportieren eines Host
- Anzeigen von Host-Eigenschaften
- Bearbeiten einer Schablonendatei
- Löschen einer Schablonendatei
- Umbenennen einer Suchdatei
- Löschen einer Suchdatei
- Löschen einer Startsequenz
- Starten und Stoppen von Wizard-Ports
- Bearbeiten eines Wizard-Ports
- Löschen eines Wizard-Ports
- Herauf- und Herunterladen eines Collectors
- Durchführen der Fehlersuche bei einem Wizard-Port

Starten und Stoppen von Collector Manager

HINWEIS: Bei der ersten Ausführung von Wizard Collector Builder wird unter Umständen eine Meldung mit etwa folgendem Wortlaut ausgegeben: „Verzeichnis ‘Collectors’ ist nicht vorhanden.“ Es wird automatisch erstellt. Einige Informationen sind möglicherweise nicht mehr verfügbar. Wenn Sie auf „OK“ klicken, wird das Verzeichnis erstellt und Wizard Collector Builder wird gestartet. Wenn diese Meldung nach der erstmaligen Ausführung von Collector Builder angezeigt wird, wurde das Collector-Verzeichnis möglicherweise versehentlich gelöscht und Sie müssen überprüfen, ob Informationen nicht mehr verfügbar sind.

Starten oder Stoppen des Collector Manager-Services unter Windows

Starten oder Stoppen von Collector Manager-Services unter Windows

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*.
2. Doppelklicken Sie in der *Systemsteuerung* auf *Verwaltung* und klicken Sie dann auf *Dienste.*
3. Klicken Sie im Dialogfeld „Dienste“ mit der rechten Maustaste auf *Collector Manager* und klicken Sie dann entweder auf *Starten* oder *Stoppen*.

Starten von Collector Manager-Services unter Windows (Befehlszeile)

1. Begeben Sie sich zu %WORKBENCH_HOME%
2. So starten Sie Collector Manager:
   - ./agent-manager start
   - ./agent-manager restart – Startet das Collector Manager-Skript im Hintergrund und startet den Collector Manager-Vorgang automatisch, wenn er gestoppt wurde. Wenn der agentmanager-Vorgang bereits ausgeführt wird, wird er gestoppt und neu gestartet.
   - ./agent-manager.sh console – Startet den Collector Manager-Vorgang im Vordergrund.

HINWEIS: Wenn Sie sich im Konsolenmodus befinden, vergewissern Sie sich, dass nur eine Instanz von Collector Manager auf dem Computer ausgeführt wird.

Stoppen von Collector Manager-Services unter Windows (Befehlszeile)

1. Begeben Sie sich zu %WORKBENCH_HOME%
2. So stoppen Sie Collector Manager:

```
./agent-manager stop
```

Starten von Collector Manager unter UNIX (Normal- und Konsolenbetrieb)

Starten von Collector Manager unter UNIX

1. Wechseln Sie als Benutzer „esecadm“ zu folgendem Verzeichnis:

```
$WORKBENCH_HOME
```

2. Geben Sie den folgenden Befehl ein:

```
./agent-manager.sh start
```

   - ./agent-manager.sh restart – Startet das Collector Manager-Skript im Hintergrund und startet den Collector Manager-Vorgang automatisch, wenn er gestoppt wurde. Wenn der Collector Manager-Vorgang bereits ausgeführt wird, wird er gestoppt und neu gestartet.
   - ./agent-manager.sh console – Startet den Collector Manager-Vorgang im Vordergrund.

Stoppen von Collector Manager unter UNIX

Stoppen von Collector Manager unter UNIX

1. Wechseln Sie als Benutzer „esecadm“ zu folgendem Verzeichnis:

```
$WORKBENCH_HOME
```

2. Geben Sie den folgenden Befehl ein:

```
./agent-manager.sh stop
```

Collector Manager-Administration

Es gibt eine ausführbare Datei (Windows) bzw. ein Skript (UNIX), mit dem Sie folgende Schritte ausführen können:

- Collector Manager-Service für Windows installieren (nur unter Windows)
- Collector Manager-Service für Windows entfernen (nur unter Windows)
- Collector Manager-Service festlegen
- Ausführliche Informationen zur Fehlersuche drucken
- Build-Version anzeigen
- Hilfe anzeigen

Installieren des Collector Manager-Services für Windows (nur unter Windows)

Installieren des Collector Manager-Services für Windows (nur unter Windows)

1. Begeben Sie sich an der Eingabeaufforderung zu „%workbench_home%“.
2. Geben Sie den folgenden Befehl ein:

```
agent-manager.bat -install
```

3. Führen Sie einen der folgenden Schritte durch, um den Service zu starten:
   - Geben Sie an der Eingabeaufforderung Folgendes ein:

```
net start “agent manager”
```

   - Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*. Doppelklicken Sie auf *Dienste*, wählen Sie *Collector Manager*. Starten Sie den *Collector Manager*-Service.

HINWEIS: Wenn das Fenster „Dienste“ bereits geöffnet ist, klicken Sie auf *Aktion* > *Aktualisieren* und starten Sie dann den *Collector Manager*-Service.

Entfernen des Collector Manager-Services für Windows (Windows)

Entfernen des Collector Manager-Services für Windows (Windows)

1. Führen Sie einen der nachfolgenden Schritte aus, um den Collector Manager-Service zu stoppen:
   - Geben Sie an der Eingabeaufforderung Folgendes ein:

     ```
     net stop “agent manager”
     ```

   - Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*. Doppelklicken Sie auf *Dienste*, wählen Sie *Collector Manager*. Stoppen Sie den *Collector Manager*-Service. Schließen Sie das Fenster „Dienste“.
2. Begeben Sie sich an der Eingabeaufforderung zu „%workbench_home%“.
3. Geben Sie den folgenden Befehl ein:

   ```
   agent-manager.bat -remove
   ```

Ändern des Collector Manager-Passworts unter Windows

HINWEIS: Um die strengen Sicherheitskonfigurationen zu erfüllen, die von Common Criteria Certification gefordert werden, wird die Verwendung eines starken (also komplexen) Passworts mit folgenden Eigenschaften dringend empfohlen:

1. Wählen Sie Passwörter aus, die mindestens 8 Zeichen umfassen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen (!@#$%^&*()_+) und eine Zahl (0-9) enthalten.

2. Das Passwort darf nicht Ihren Email-Namen oder einen Teil Ihres vollständigen Namens enthalten.

3. Bei Ihrem Passwort sollte es sich nicht um ein „übliches“ Wort handeln (z. B. kein Wort, das im Wörterbuch steht oder ein allgemein gebräuchliches, umgangssprachliches Wort).

4. Ihr Passwort sollte keine Wörter aus irgendeiner Sprache enthalten, da es zahlreiche Programme zum Knacken von Passwörtern gibt, die in wenigen Sekunden Millionen möglicher Wortkombinationen durchgehen können.

5. Sie sollten ein Passwort wählen, das Sie sich merken können und das dennoch komplex ist. Beispiel: mSi5!JalT (Mein Sohn ist 5 Jahre alt) oder iLs5#JiK (Ich lebe seit 5 Jahren in Köln).

Ändern des Collector Manager-Passworts unter Windows

1. Begeben Sie sich an der Eingabeaufforderung zu „%workbench_home%“.
2. Geben Sie den folgenden Befehl ein:

   ACHTUNG: Sie werden nicht zur Bestätigung des Passworts aufgefordert bzw. Sie werden zur Eingabe des alten Passworts aufgefordert.

   ```
   agent-manager.bat –password <neues Passwort>
   ```

3. Führen Sie einen der folgenden Schritte durch, damit das Passwort in Kraft tritt:
   - Geben Sie an der Eingabeaufforderung Folgendes ein:

     ```
     net stop “agent manager”
     net start “agent manager”
     ```

- Klicken Sie in Collector Builder mit der rechten Maustaste auf Ihren Host-Computer und wählen Sie die Option für den Host-Neustart.
- Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*. Doppelklicken Sie auf *Dienste*, wählen Sie *Agenten-Manager*. Stoppen und starten Sie den Service für den *Agenten-Manager*.

Ändern des Collector Manager-Passworts unter UNIX

HINWEIS: Um die strengen Sicherheitskonfigurationen zu erfüllen, die von Common Criteria Certification gefordert werden, wird die Verwendung eines starken (also komplexen) Passworts mit folgenden Eigenschaften dringend empfohlen:

1. Wählen Sie Passwörter aus, die mindestens 8 Zeichen umfassen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen (!@#$%^&*()_+) und eine Zahl (0-9) enthalten.

2. Das Passwort darf nicht Ihren Email-Namen oder einen Teil Ihres vollständigen Namens enthalten.

3. Bei Ihrem Passwort sollte es sich nicht um ein „übliches“ Wort handeln (z. B. kein Wort, das im Wörterbuch steht oder ein allgemein gebräuchliches, umgangssprachliches Wort).

4. Ihr Passwort sollte keine Wörter aus irgendeiner Sprache enthalten, da es zahlreiche Programme zum Knacken von Passwörtern gibt, die in wenigen Sekunden Millionen möglicher Wortkombinationen durchgehen können.

5. Sie sollten ein Passwort wählen, das Sie sich merken können und das dennoch komplex ist. Beispiel: mSi5!JalT (Mein Sohn ist 5 Jahre alt) oder iLs5#JiK (Ich lebe seit 5 Jahren in Köln).

Ändern des Collector Manager-Passworts unter UNIX

1. Begeben Sie sich als Benutzer „esecadm“ zum Verzeichnis „$WORKBENCH_HOME“.
2. Geben Sie den folgenden Befehl ein:

   ACHTUNG: Sie werden nicht zur Bestätigung des Passworts aufgefordert bzw. Sie werden zur Eingabe des alten Passworts aufgefordert.

   ```
   ./agent-manager.sh –password <neues Passwort>
   ```

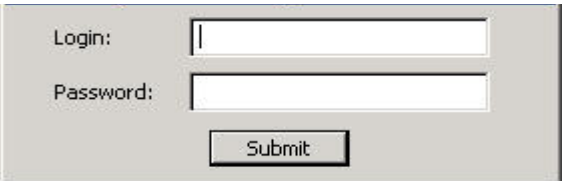
3. Gehen Sie wie folgt vor, damit das Passwort in Kraft tritt: Begeben Sie sich zu „/usr/local/bin“ und geben Sie folgenden Befehl ein:

   ```
   ./agent-manager.sh -restart
   ```

Starten von Collector Builder

Starten von Collector Builder

1. Wählen Sie die Optionsfolge *Start* > *Programme* > *Sentinel* > *Collector Builder* oder doppelklicken Sie auf Ihrem Desktop auf das Symbol für *Collector Builder*.
2. Melden Sie sich abhängig von Ihrer Installation entweder als „esecadm“ oder mit Ihrem Benutzernamen für die Windows-Authentifizierung an.



Umbenennen eines Wizard-Host

Umbenennen eines Wizard-Host

1. Aktivieren Sie in Collector Builder (Wizard) die Registerkarte „Wizard-Hosts“, um den Baumbereich mit den Wizard-Hosts zu öffnen.
2. Klicken Sie im Baum mit den Wizard-Hosts mit der rechten Maustaste auf den Host, der umbenannt werden soll, und wählen Sie *Host umbenennen*. Nur aktive Hosts können umbenannt werden.
3. Geben Sie den neuen Namen des Host ein und drücken Sie die Eingabetaste.

HINWEIS: Beim Umbenennen eines Host bleibt die ID-Nummer, die einem Wizard-Host bei der Installation zugewiesen wird, unverändert. Diese Angabe wird in %WORKBENCH_HOME%\wizard\agents\names.dat gespeichert.

Löschen eines Wizard-Host

Um einen Host löschen zu können, muss er zunächst aus dem Netzwerk entfernt werden. Hosts, die über das Netzwerk kommunizieren, können nicht entfernt werden. Wenn ein Host im Netzwerk vorhanden ist, jedoch nicht kommuniziert, ist das Host-Symbol im Baum mit den Wizard-Hosts mit einem roten X versehen.

Löschen eines Wizard-Host

1. Aktivieren Sie die Registerkarte *Wizard-Hosts*, um den Baumbereich mit den Wizard-Hosts zu öffnen.
2. Klicken Sie im Baum mit den Wizard-Hosts mit der rechten Maustaste auf den Host.
3. Klicken Sie auf *Host löschen*.

Neustarten eines Wizard-Host

Neustarten eines Wizard-Host

1. Aktivieren Sie die Registerkarte *Wizard-Hosts*, um den Baumbereich mit den Wizard-Hosts zu öffnen und einen Host auszuwählen.
2. Klicken Sie mit der rechten Maustaste auf einen Host und wählen Sie *Port starten*. Nur aktive Wizard-Hosts können neu gestartet werden.

Exportieren eines Wizard-Host

Exportieren eines Wizard-Host

1. Aktivieren Sie die Registerkarte „Wizard-Hosts“, um den Baumbereich mit den Wizard-Hosts zu öffnen. Wählen Sie einen Host aus.
2. Wählen Sie die Optionsfolge *Datei* > *Host exportieren.* Daraufhin wird folgendes Unterverzeichnis erstellt:

   ```
   %WORKBENCH_HOME%\upload_<Hostname>
   ```

   Dieses Unterverzeichnis kann mithilfe von Secure Shell (SSH) bzw. mithilfe eines Datenträgers auf einen Remote-Computer übertragen werden. Nachdem das Unterverzeichnis auf den Remote-Computer übertragen wurde, führen Sie den uploadhost-Befehl aus. Hiermit werden die erforderlichen Dateien in die entsprechenden Verzeichnisse kopiert.

HINWEIS: Wenn die SNMP-(Simple Network Management Protocol-)Einstellungen geändert werden, kann Collector Builder ab dem Zeitpunkt, ab dem die Schaltfläche „Exportieren“ aktiviert wird, so lange nicht mit dem Remote-Computer kommunizieren, bis die exportieren Collector-Dateien heraufgeladen werden.

Anzeigen von Wizard-Host-Eigenschaften

Anzeigen von Wizard-Host-Eigenschaften

1. Aktivieren Sie die Registerkarte *Wizard-Hosts*, um den Baumbereich mit den Wizard-Hosts zu öffnen.
2. Klicken Sie im Baum mit den Wizard-Hosts mit der rechten Maustaste auf den Host und wählen Sie *Eigenschaften*. Im Fenster mit den Wizard-Eigenschaften werden folgende Informationen angezeigt:
   - Name
   - ID
   - Hostname
   - IP-Adresse
   - Version
   - Aktivzeit
3. Mit *OK* wird das Fenster mit den Eigenschaften geschlossen.

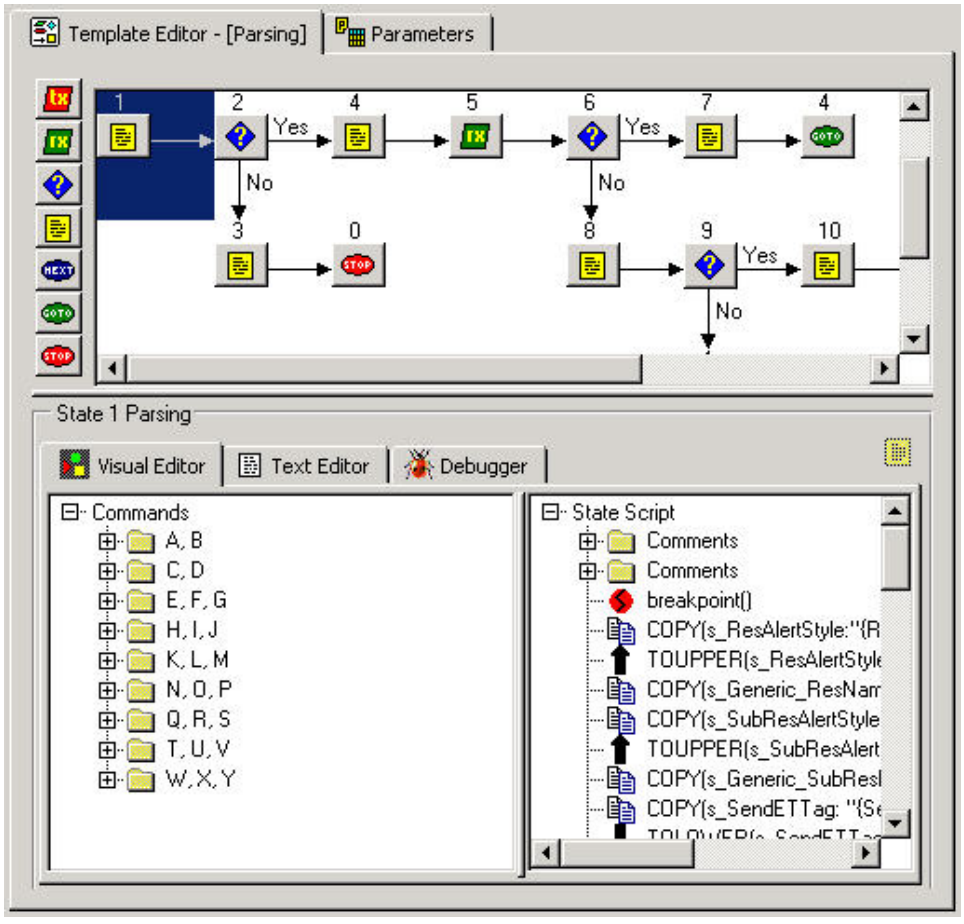
HINWEIS: Wenn der Host nicht ausgeführt wird, wird beim Klicken auf „Eigenschaften“ ein Fenster angezeigt, aus dem hervorgeht, dass der Host nicht reagiert.

Bearbeiten einer Schablonendatei

Bearbeiten einer Schablonendatei

1. Klicken Sie auf die Registerkarte *Collectors*, um den Bereich mit dem Collector-Baum zu öffnen.
2. Klicken Sie im Collector-Baum auf die Schablone und dann auf die Registerkarte „Schabloneneditor“.

3. Klicken Sie im Schabloneneditor auf den zu bearbeitenden Status und nehmen Sie die gewünschten Änderungen vor. Ein Status kann mithilfe des visuellen Editors oder des Texteditors bearbeitet werden. Informationen zu Parsing-Befehlen (Befehlen für Analysevorgänge) finden Sie im Sentinel-Referenzhandbuch für Benutzer.



Löschen einer Schablonendatei

Löschen einer Schablonendatei

1. Klicken Sie auf die Registerkarte *Collectors*, um den Bereich mit dem Collector-Baum zu öffnen.
2. Klicken Sie im Collector-Baum mit der rechten Maustaste auf eine Schablone und wählen Sie dann *Schablone löschen*.

Umbenennen einer Suchdatei

Umbenennen einer Suchdatei

1. Klicken Sie auf die Registerkarte *Collectors*, um den Bereich mit dem Collector-Baum zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf die Suchdatei und wählen Sie dann *Suchdatei umbenennen*.
3. Geben Sie den neuen Namen ein und drücken Sie die *Eingabetaste*.

Löschen einer Suchdatei

Löschen einer Suchdatei

1. Klicken Sie auf die Registerkarte *Collectors*, um den Bereich mit dem Collector-Baum zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf die Suchdatei und wählen Sie dann *Suchdatei löschen*.

Löschen eines Skripts

Löschen eines Skripts

1. Ein Skript kann auf zweierlei Art gelöscht werden.
   - Klicken Sie im Collector-Baum mit der rechten Maustaste auf ein Skript und wählen Sie dann *Löschen*.
   - Klicken Sie in der Spalte „Startskripts“ bzw. „Zurücksetzungsskripts“ mit der rechten Maustaste auf das Skript und wählen Sie „Skript löschen“.

Löschen einer Startsequenz

Löschen einer Startsequenz

1. Wählen Sie im Bereich mit den Startskripts die Startsequenz im Dropdown-Menü aus, damit der Sequenzname im Feld „Startskripts“ angezeigt wird.
2. Klicken Sie im Collector-Baum mit der rechten Maustaste auf das Skript und wählen Sie „Aktuelle Startsequenz löschen“. Daraufhin wird die Startsequenz aus der Liste „Startskripts“ entfernt.

HINWEIS: Wenn Sie die standardmäßige Startsequenz löschen, werden sämtliche, der standardmäßigen Startsequenz zugewiesene Skripts aus der Spalte „Startskripts“ entfernt, der Standard wird im Menü mit den Startsequenzen jedoch weiterhin angezeigt.

Wizard-Ports

In diesem Abschnitt wird das Stoppen, Starten, Bearbeiten und Löschen von Wizard-Ports sowie die Fehlersuche bei Wizard-Ports erläutert.

Starten und Stoppen eines Wizard-Ports – GUI

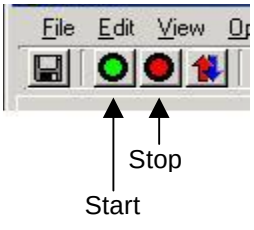
Wenn ein Collector gestartet oder gestoppt wird, verändert sich die Schaltfläche „Starten“ bzw. „Stoppen“ unterhalb der Starten-/Stoppen-Spalte, sobald der Collector tatsächlich startet bzw. stoppt. Bei der Arbeit mit einem Remote-Collector wird diese Änderung möglicherweise mit Verzögerung übermittelt, da auf Informationen zum Collector-Status gewartet wird.

Durch das Starten bzw. Stoppen eines Ports werden das ausgewählte Startskript und das ausgewählte Zurücksetzungsskript ausgeführt.

Wenn sämtliche Ports gestartet werden, wird ein Port nur gestartet, wenn im Menü „Optionen“ unter „Andere Portoptionen“ das Kontrollkästchen „Port beim Start ausführen“ aktiviert ist.

Starten und Stoppen aller Wizard-Ports

1. Gehen Sie zur Durchführung folgender Schritte im Wizard-Fenster wie folgt vor:
   - Wenn Sie alle Ports stoppen möchten, klicken Sie in der Symbolleiste auf die Schaltfläche „Stoppen“.
   - Wenn Sie alle Ports starten möchten, klicken Sie in der Symbolleiste auf die Schaltfläche „Starten“.



Starten und Stoppen eines einzelnen Wizard-Ports

1. Gehen Sie zur Durchführung folgender Schritte im Wizard-Fenster wie folgt vor:
   - Wenn Sie einen Port stoppen möchten, klicken Sie in der entsprechenden Starten-/Stoppen-Spalte auf die Schaltfläche „Stoppen“.
   - Wenn Sie einen Port starten möchten, klicken Sie in der entsprechenden Starten-/Stoppen-Spalte auf die Schaltfläche „Starten“.

Bearbeiten eines Wizard-Ports

Wenn Sie die Konfiguration eines Ports bearbeiten, während dieser aktiv ist (also ausgeführt wird), wird der Port gestoppt. Um Datenverluste zu vermeiden, stoppen Sie den Port manuell, bevor Sie seine Konfiguration bearbeiten.

Bearbeiten eines Wizard-Ports

1. Stoppen Sie den Port für den entsprechenden Host.
2. Befolgen Sie die Schritte zum Erstellen eines Wizard-Ports in Kapitel 3. Wenn Sie den Port speichern oder heraufladen, wird die vorhandene Konfiguration mit der neuen Konfiguration überschrieben.

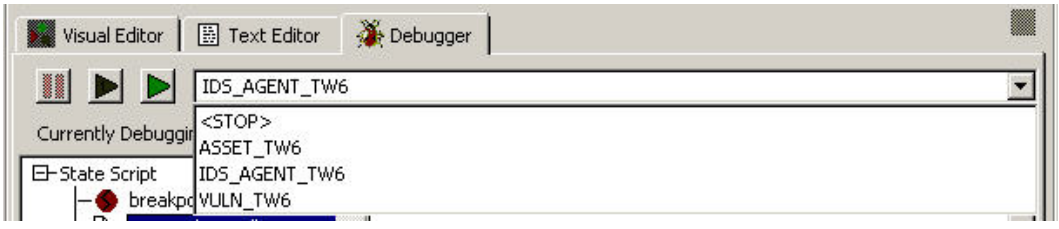
Löschen eines Wizard-Ports

Löschen eines Wizard-Ports

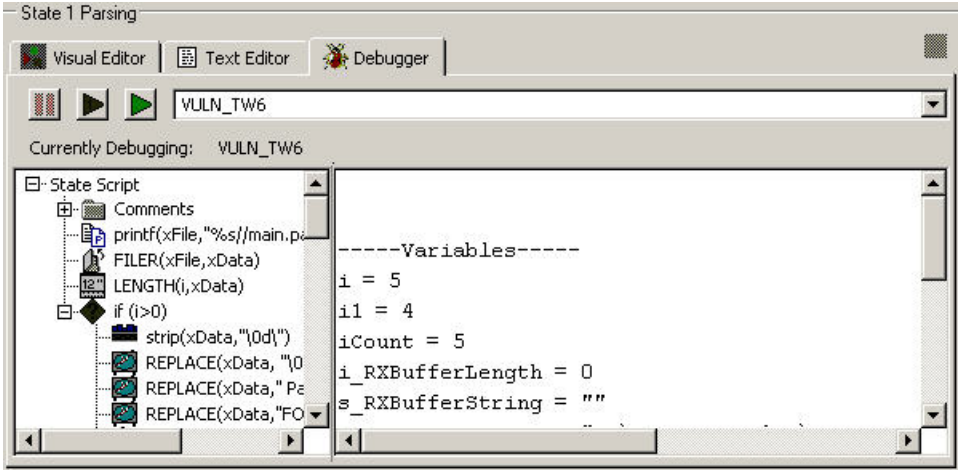
1. Stoppen Sie den Port.
2. Klicken Sie im Collector Builder-Bereich mit den Portinformationen mit der rechten Maustaste auf den Portnamen und wählen Sie dann „Port löschen“. Alle Ports unterhalb des gelöschten Ports werden automatisch gelöscht.
3. Gehen Sie beim Löschen von folgendem Standort wie folgt vor:
   - Lokaler Host – Wählen Sie die Optionsfolge *Datei* > *Speichern* und dann „Portinformationen“
   - Remote-Host – Wählen Sie die Optionsfolge *Datei* > *Heraufladen/ Herunterladen*.

Durchführen der Fehlersuche bei einem Wizard-Port

Das Fehlersuchprogramm (Debugger) ermöglicht Ihnen die Fehlersuche hinsichtlich des an einem Port ausgeführten Collector-Codes. Auf der linken Seite des Bereichs mit dem Fehlersuchprogramm wird das Statusskript angezeigt. Auf der rechten Seite des Bereichs werden Skripts und RX_Buffer-Variablen angezeigt, die Namen bis zu 32 Zeichen umfassen können.



Damit das Fehlersuchprogramm effektiv arbeiten kann, muss es sich beim ersten Status um einen Analysestatus handeln und es müssen Breakpoint()-Befehle vorhanden sein.



Warten Sie beim Durchführen der Fehlersuche, bis der Empfangspuffer (Rx Buffer) aktualisiert wird, bevor Sie die nächste Funktion ausführen.

HINWEIS: Wenn die Konnektivität des Collector Manager-Host nicht mehr gegeben ist (), ist das Durchführen der Fehlersuche für einen Port dieses Collector Manager-Host nicht möglich.

Durchführen der Fehlersuche bei einem Wizard-Port

1. Aktivieren Sie im Schabloneneditor im Bearbeitungsbereich die Registerkarte „Fehlersuchprogramm“, um auf das Fehlersuchprogramm zuzugreifen. Daraufhin wird ein leerer Bereich angezeigt und Sie können in einer Dropdown-Liste den Wizard-Port auswählen, für den Sie die Fehlersuche durchführen möchten.

   Wenn Sie auf die Registerkarte mit den Wizard-Hosts klicken, wird für den Port, für den zurzeit die Fehlersuche durchgeführt wird, angegeben, dass er sich im Fehlersuchmodus befindet.

VULN_TW6	File All	C:\workarea\vuln_inf	DemoVulnerabilityUploa	Stop	Debug
ASSET_TW6	File All	c:\workarea\asset_o	T1_GNUx_NMAP_035	Start	Off

2. Wählen Sie in der Dropdown-Liste einen Port aus, um den Fehlersuchvorgang zu starten. Führen Sie zur Fehlersuche hinsichtlich des Ports einen der folgenden Schritte durch:

   - Drücken Sie F6, um die Befehle einzeln zu durchlaufen, bzw. klicken Sie auf die Schaltfläche für die Ausführung eines einzelnen Befehls.

     Klicken Sie erneut auf die Schaltfläche bzw. drücken Sie F6, um die Skriptausführung fortzusetzen.
   - Drücken Sie F7, um die Befehle automatisch zu durchlaufen, oder klicken Sie auf die Schaltfläche für die Wiederaufnahme der Befehlsausführung.

     Drücken Sie F5, um den Vorgang vorübergehend anzuhalten; Sie können auch auf die Schaltfläche zum vorübergehenden Anhalten der Befehlsausführung klicken.

     Der Vorgang wird so lange angehalten, bis Sie F7 drücken bzw. auf die Schaltfläche für die Wiederaufnahme der Befehlsausführung klicken.

   Das Fehlersuchprogramm stoppt bei allen Haltepunkten, seine Ausführung wird jedoch fortgesetzt. Der Port weist den Status „Ein“ auf.

   Bei Pausen im Fehlersuchmodus werden keine Ereignisse gesendet.

   Wenn der Parser (das Analyseprogramm) beendet wird, werden die Schaltflächen abgeblendet und in der Auswahlliste wird angegeben, dass zurzeit keine Fehlersuche für einen Port durchgeführt wird.

   Das Fehlersuchprogramm unterbricht eine Pause nicht eigenständig: Wenn Sie also die Fehlersuche für einen Parser durchführen, der auf einen Befehl zum vorübergehenden Anhalten (Pause) gestoßen ist, wird die Schaltfläche für das Stoppen bzw. für den Schritt erst aktiv, wenn die Pause verstrichen ist.

Herauf- und Herunterladen von Collectors und Hosts

Das Fenster Heraufladen/Herunterladen enthält die folgenden drei Registerkarten:

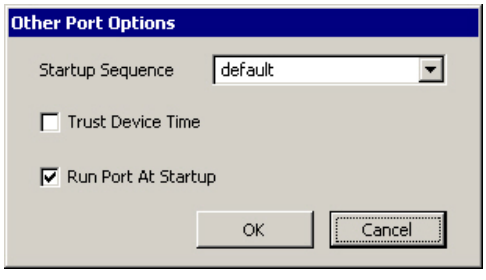
- Hosts – Hiermit werden die einzelnen Portkonfigurationen sowie die einzelnen Collector-Erfassungen auf jeden der angegebenen Hosts heraufgeladen. Jeder Host verfügt weiterhin über seine eigene Portkonfiguration und Collector-Erfassung.
- Collectors – Für das Heraufladen einzelner Collectors
- Netzwerk auffüllen – Hiermit werden die Portkonfigurationen/Agenten eines einzelnen angegebenen Host auf alle ausgewählten Hosts heraufgeladen. Alle ausgewählten Hosts erhalten dieselbe Portkonfiguration und Collector-Erfassung wie der Quell-Host.

Beim Herunterladen wird die Portkonfiguration für einen Remote-Collector auf dem für das Herunterladen ausgewählten Host angezeigt und sämtliche Collectors auf dem Remote-Host mit demselben Namen wie auf dem lokalen Host werden überschrieben.

Heraufladen eines Collector auf einen einzelnen Host

Heraufladen eines Collector auf einen einzelnen Host

1. Wenn Ihr Collector bereits vorschriftsmäßig konfiguriert ist und Sie Ihr Skript erstellt haben, können Sie Schritt 2 bis 11 überspringen.
2. Klicken Sie auf die Registerkarte „Wizard-Hosts“ und wählen Sie einen Host aus.
3. Doppelklicken Sie unterhalb der Spalte mit dem Portnamen auf *neu.*…. Geben Sie einen Namen Ihrer Wahl ein.
4. Wählen Sie unter der Collector-Spalte einen Collector aus.
5. Konfigurieren Sie den Collector gemäß den Angaben in der Collector-Dokumentation (`%WORKBENCH_HOME%\Elements\<Collector-Name>\docs\<Dateiname>.pdf`).
6. Aktivieren Sie die Registerkarte *Collectors*, erweitern Sie den jeweiligen Collector-Eintrag und markieren Sie die Schablonendatei.
7. Klicken Sie rechts auf die Registerkarte *Parameter*.
8. Legen Sie die Parameterwerte gemäß den Angaben in der Collector-Dokumentation fest.
9. (Optional) Wenn dieser Collector beim Systemstart nicht gestartet werden soll bzw. die vom Gerät angegebene Uhrzeit verwenden soll, aktivieren Sie die Registerkarte *Wizard-Hosts*, klicken Sie mit der rechten Maustaste auf den Namen des *Wizard-Ports*, wählen Sie *Andere Portoptionen…* und deaktivieren Sie *Port beim Start ausführen* bzw. aktivieren Sie *Uhrzeit des Geräts verwenden*. Klicken Sie auf *OK*.



10. Klicken Sie auf *Speichern*.
11. Aktivieren Sie die Registerkarte *Collectors*, klicken Sie mit der rechten Maustaste auf die Schablonendatei und wählen Sie dann *Skripts erstellen*.

12. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie die Optionsfolge *Datei* > *Heraufladen/Herunterladen*
    - Klicken Sie mit der rechten Maustaste auf den *Collector* und wählen Sie dann *Collector heraufladen*
    - Klicken Sie auf die Schaltfläche *Heraufladen/Herunterladen* 

    Daraufhin wird das Fenster *Heraufladen/Herunterladen* geöffnet.
13. Klicken Sie im Fenster *Heraufladen/Herunterladen* auf die Registerkarte *Collectors*.
14. Wählen Sie in der Dropdown-Liste den *Collector* aus, der heraufgeladen werden soll.
15. Klicken Sie auf *Heraufladen*. Wenn Sie diesen Schritt zum ersten Mal durchführen, werden Sie zur Eingabe eines *Collector Manager*-Passworts aufgefordert, auch bei einem lokalen Wizard-Host. Das Fenster mit dem Übertragungsfortschritt wird geöffnet, aus dem der Fortschritt des Heraufladevorgangs hervorgeht.

HINWEIS: Über das Fenster mit dem Übertragungsfortschritt können Hosts im Anschluss an eine Übertragung neu gestartet werden.

Heraufladen eines Collector auf mehrere Hosts

Heraufladen eines Collector auf mehrere Hosts

ACHTUNG: Wenn Sie einen Host heraufladen, auf dem sich ein Collector mit demselben Namen wie auf dem lokalen Host befindet, wird der Collector auf dem Remote-Host ohne Benachrichtigung überschrieben.

1. Wenn Ihr Collector bereits vorschriftsmäßig konfiguriert ist und Sie Ihr Skript erstellt haben, können Sie Schritt 2 bis 11 überspringen.
2. Klicken Sie auf die Registerkarte *Wizard-Hosts* und wählen Sie einen Host aus.
3. Doppelklicken Sie unterhalb der Spalte mit dem Portnamen auf *neu.*…. Geben Sie einen Namen Ihrer Wahl ein.
4. Wählen Sie unter der Collector-Spalte einen Collector aus.
5. Konfigurieren Sie den Collector gemäß den Angaben in der Collector-Dokumentation (`%WORKBENCH_HOME%\Elements\<Collector-Name>\docs\<Dateiname>.pdf`).
6. Aktivieren Sie die Registerkarte *Collectors*, erweitern Sie den jeweiligen Collector-Eintrag und markieren Sie die Schablonendatei.
7. Klicken Sie rechts auf die Registerkarte *Parameter*.
8. Legen Sie die Parameterwerte gemäß den Angaben in der Collector-Dokumentation fest.
9. (Optional) Wenn dieser Collector beim Systemstart nicht gestartet werden soll bzw. die vom Gerät angegebene Uhrzeit verwenden soll, aktivieren Sie die Registerkarte *Wizard-Hosts*, klicken Sie mit der rechten Maustaste auf den Namen des Wizard-Ports, wählen Sie „Andere Portoptionen…“ und deaktivieren Sie „Port beim Start ausführen“ bzw. aktivieren Sie „Uhrzeit des Geräts verwenden“. Klicken Sie auf „OK“.
10. Klicken Sie auf „Speichern“.
11. Klicken Sie auf die Registerkarte „Collectors“, um den Bereich mit dem Collector-Baum zu öffnen.

12. Klicken Sie auf einen Collector.
13. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie die Optionsfolge *Datei > Heraufladen/Herunterladen*
    - Klicken Sie mit der rechten Maustaste auf den Collector und wählen Sie dann „Collector heraufladen“
    - Klicken Sie auf die Schaltfläche „Heraufladen/Herunterladen“ 

    Daraufhin wird das Fenster „Heraufladen/Herunterladen“ geöffnet.
14. Aktivieren Sie im Fenster „Heraufladen/Herunterladen“ die Registerkarte „Hosts“ und aktivieren bzw. deaktivieren Sie das Kontrollkästchen „Collectors beim Heraufladen heraufladen“.

    Wenn dieses Kontrollkästchen aktiviert ist, werden auf der Registerkarte „Collectors“ ausgewählte Collectors heraufgeladen. Dieses Kontrollkästchen ist standardmäßig aktiviert. Diese Option hat keinerlei Auswirkung auf das Herunterladen von Collectors von einem Host.
15. Wählen Sie in der Liste die Wizard-Hosts aus, auf die Collectors heraufgeladen werden sollen.

    Alle Wizard-Hosts im Netzwerk werden automatisch in die Liste aufgenommen. Die Schaltflächen geben Aufschluss darüber, ob der Hostcomputer online ist oder nicht.

    Klicken Sie auf „Alle auswählen“, um alle Wizard-Hosts in der Liste auszuwählen. Klicken Sie auf „Keine Auswahl“, um die Auswahl aller Wizard-Hosts in der Liste aufzuheben.
16. Klicken Sie auf „Heraufladen“, um ausgewählte Collectors auf die ausgewählten Hosts heraufzuladen. Wenn Sie diesen Schritt zum ersten Mal durchführen, werden Sie zur Eingabe eines Collector Manager-Passworts aufgefordert, auch bei einem lokalen Wizard-Host.

Herunterladen eines Host

Herunterladen eines Host

ACHTUNG: Wenn Sie einen Host herunterladen, auf dem sich ein Collector mit demselben Namen wie auf dem lokalen Host befindet, wird der Collector auf dem lokalen Host ohne Benachrichtigung überschrieben.

1. Klicken Sie auf die Registerkarte „Wizard-Hosts“, um den Bereich mit dem Host-Baum zu öffnen.
2. Klicken Sie im Baum mit den Wizard-Hosts auf den Host, den Sie herunterladen möchten.
3. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie die Optionsfolge *Datei > Heraufladen/Herunterladen*
    - Klicken Sie mit der rechten Maustaste auf den Collector und wählen Sie dann „Collector heraufladen“
    - Klicken Sie auf die Schaltfläche „Heraufladen/Herunterladen“ 

    Daraufhin wird das Fenster „Heraufladen/Herunterladen“ geöffnet. Der von Ihnen ausgewählte Collector ist standardmäßig aktiviert.

4. Klicken Sie auf „Herunterladen“. Wenn Sie diesen Schritt zum ersten Mal durchführen, werden Sie zur Eingabe eines Collector Manager-Passworts aufgefordert, auch bei einem lokalen Wizard-Host. Der Host wird heruntergeladen und dem Baum mit den Wizard-Hosts hinzugefügt. Das Fenster mit dem Übertragungsfortschritt wird geöffnet, aus dem der Fortschritt des Herunterladevorgangs hervorgeht.

HINWEIS: Über das Fenster mit dem Übertragungsfortschritt können Hosts im Anschluss an eine Übertragung neu gestartet werden.

HINWEIS: Es kann nur jeweils ein Host heruntergeladen werden. Wenn mehrere Hosts aktiviert werden, wird kein Herunterladevorgang durchgeführt.

Herunterladen von Collectors von einem einzelnen Host

Herunterladen von Collectors von einem einzelnen Host

1. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie die Optionsfolge *Datei > Heraufladen/Herunterladen*
   - Klicken Sie auf die Schaltfläche „Heraufladen/Herunterladen“ 

   Daraufhin wird das Fenster „Heraufladen/Herunterladen“ geöffnet.
2. Wählen Sie in der Liste den Wizard-Host aus, von dem Collectors heruntergeladen werden sollen.

   Alle Wizard-Hosts im Netzwerk werden automatisch in die Liste aufgenommen. Die Schaltflächen geben Aufschluss darüber, ob der Hostcomputer online ist oder nicht.

   Klicken Sie auf „Alle auswählen“, um alle Wizard-Hosts in der Liste auszuwählen. Klicken Sie auf „Keine Auswahl“, um die Auswahl aller Wizard-Hosts in der Liste aufzuheben.
3. Klicken Sie auf „Herunterladen“, um Collectors vom ausgewählten Host herunterzuladen.

Heraufladen von Ports auf mehrere Hosts

Heraufladen von Ports auf mehrere Hosts

1. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie die Optionsfolge *Datei > Heraufladen/Herunterladen*
   - Klicken Sie auf die Schaltfläche „Heraufladen/Herunterladen“ 
2. Daraufhin wird das Fenster „Heraufladen/Herunterladen“ geöffnet.
3. Aktivieren Sie im Fenster „Heraufladen/Herunterladen“ die Registerkarte „Netzwerk auffüllen“.
4. Wählen Sie in der Liste zur Auswahl des Host, dessen Portkonfiguration und Collectors heraufgeladen werden sollen, den Host aus, dessen Portkonfigurationseinstellungen und Collectors heraufgeladen werden sollen.

5. Wählen Sie in der Liste zur Auswahl der Hosts, auf die diese Konfiguration heraufgeladen werden soll, den Host aus, auf den die ausgewählten Einstellungen heraufgeladen werden sollen.

   Alle Wizard-Hosts im Netzwerk werden automatisch in die Liste aufgenommen. Die Schaltflächen geben Aufschluss darüber, ob der Hostcomputer online ist oder nicht.

   Klicken Sie auf „Alle auswählen“, um alle Wizard-Hosts in der Liste auszuwählen. Klicken Sie auf „Keine Auswahl“, um die Auswahl aller Wizard-Hosts in der Liste aufzuheben.

Heraufladen mehrerer Collectors in ein Netzwerk

Heraufladen mehrerer Collectors in ein Netzwerk

1. Wählen Sie im Wizard-Hauptfenster einen Collector im Collector-Baum aus.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie die Optionsfolge *Datei > Heraufladen/Herunterladen*
   - Klicken Sie mit der rechten Maustaste auf den Collector und wählen Sie dann „Collector heraufladen“
   - Klicken Sie auf die Schaltfläche „Heraufladen/Herunterladen“ 
3. Aktivieren Sie die Registerkarte „Netzwerk auffüllen“.
4. Geben Sie im ersten Auswahlfeld mithilfe des Dropdown-Menüs an, welche Portkonfiguration und Collectors eines Host heraufgeladen werden sollen.
5. Geben Sie im zweiten Auswahlfeld mithilfe des Dropdown-Menüs an, auf welche Hosts die Konfiguration heraufgeladen werden soll.

   HINWEIS: Sie müssen mindestens eine Auswahl in mindestens einem der Auswahlfelder treffen, damit die zugehörige Konfiguration heraufgeladen werden kann.

   Sie können für jedes Dropdown-Feld einen anderen Collector auswählen. Jeder in der Hauptliste markierte Collector erhält die Portkonfiguration und Collectors des Host, der im Feld zur Auswahl des Host, dessen Portkonfiguration und Collectors heraufgeladen werden soll, ausgewählt ist, es sei denn, „Keine“ ist ausgewählt.
6. Wenn Sie die Einrichtung der Netzwerkkonfiguration abgeschlossen haben, klicken Sie auf die Schaltfläche „Heraufladen“, um mit dem Heraufladen zu beginnen.

Aufrüsten von Collectors

Aufrüsten von Collectors

1. Ziehen Sie die Dokumentation, die im Lieferumfang des neuen Collector enthalten ist, hinsichtlich sämtlicher vorgenommenen Änderungen zurate.
2. Speichern Sie die neue Version des Collector im Verzeichnis „%workbench_home%/Elements“ auf dem PC, der als Master für den Collector fungiert.
3. Öffnen Sie die Parameterdatei des Collector, der ersetzt wird, und übertragen Sie die entsprechenden Parameter durch Ausschneiden und Einfügen in den neuen Collector.

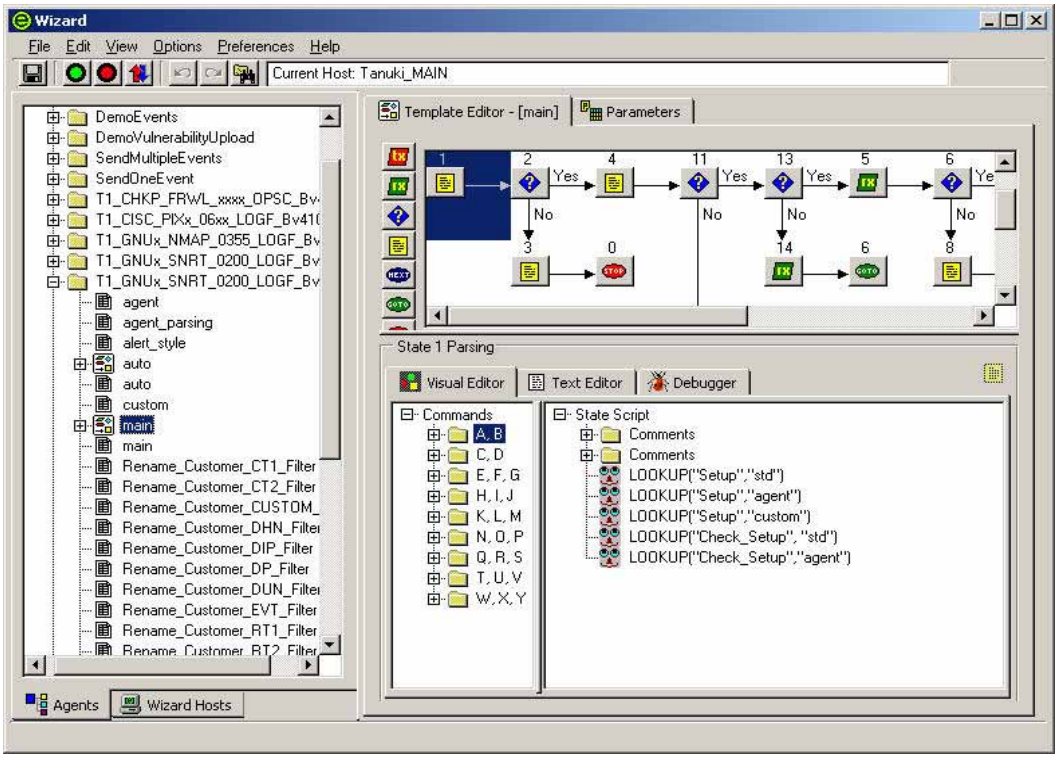
4. Wenn gemäß der Dokumentation für den neuen Collector Parametervariablen entfernt bzw. neue Parametervariablen hinzugefügt werden müssen, führen Sie diese Schritte durch. Wenn Sie neue Parametervariablen hinzufügen, füllen Sie die Variable auf.
5. Speichern Sie die Parameterdatei im neuen Collector.
6. Erstellen Sie den neuen Collector.
7. Bearbeiten Sie die Portkonfigurationsinformationen zur Verwendung des neuen Collector.
8. Speichern Sie die Portkonfigurationsinformationen.
9. Laden Sie den neuen Collector sowie die Portkonfiguration herauf.
10. Starten Sie den Port neu.

3 Erstellen und Warten von Collectors

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

HINWEIS: Bei MS SQL 2000 darf die Ereignisgröße 8 KB nicht überschreiten.

Ein Collector ist verantwortlich für die Analyse der Daten aus einer Sicherheitsereignisquelle und für das Senden von Ereignissen aus Sentinel. Collectors werden mithilfe von Wizard Collector Builder erstellt, aktiviert und gewartet. Klicken Sie auf die Registerkarte *Collectors*, um den Collectors-Baum und somit alle Collector-Komponenten Ihres Sentinel-Systems anzuzeigen.



Collector Manager bietet Ihnen folgende Möglichkeiten:

- Erstellen eines Collector
  - Erstellen und Konfigurieren von Schablonendateien
  - Erstellen und Konfigurieren von Parameterdateien
  - Erstellen und Konfigurieren von Suchdateien
  - Erstellen von Skripts
  - Erstellen eines Wizard-Ports

Grundlagen zur Collector-Erstellung

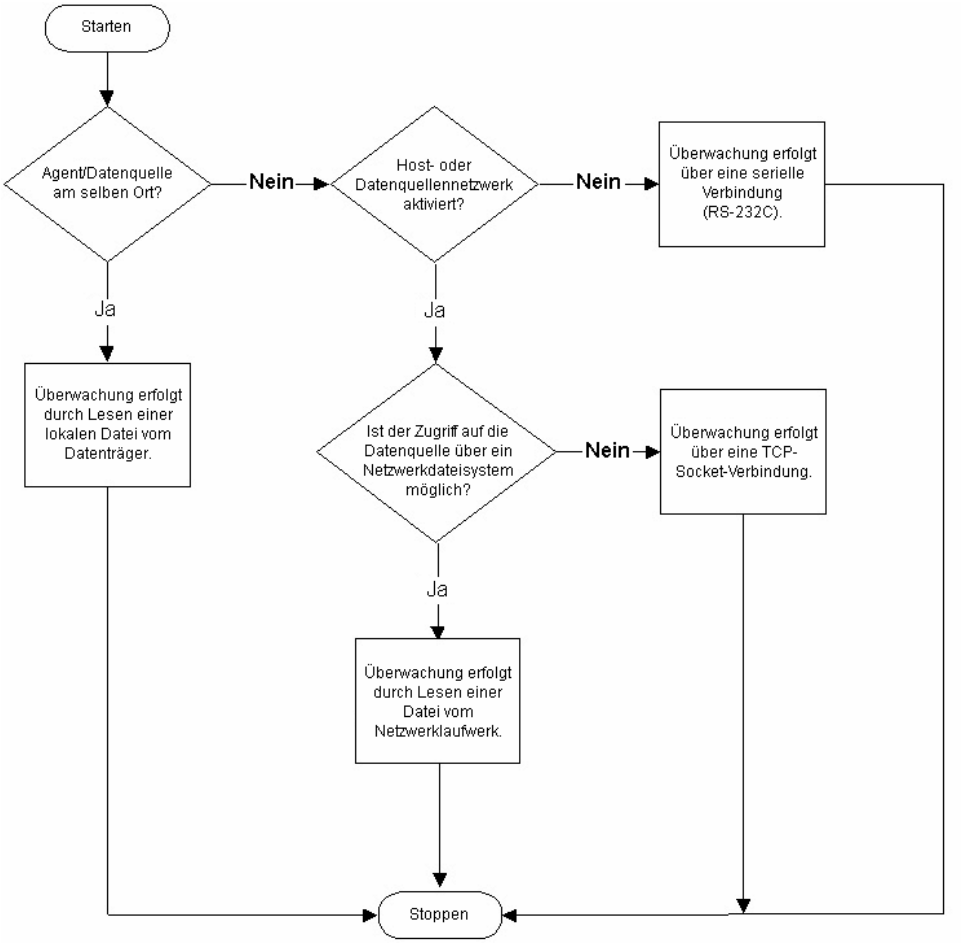
Die grundlegenden Schritte zum Erstellen von Collectors sind folgende:

- Erstellen und Konfigurieren von Schablonendateien, einschließlich Entscheidungspunkten auf der Grundlage der Anwendung von Statuswerten
- Erstellen und Konfigurieren von Parameterdateien
- Erstellen und Konfigurieren von Suchdateien (optional)
- Erstellen von Skripts
- Zuweisen einer Startsequenz zu einem Skript
- Erstellen, Zuweisen, Starten und Stoppen eines Wizard-Ports

Grundlegende Schritte für die Implementierung von Collectors

Das Implementieren eines Collector gliedert sich in folgende grundlegende Schritte.

- Bestimmen der zu überwachenden Elemente
- Festlegen der Art und Weise der Datenüberwachung
- Ermitteln des Betriebssystems des Produkts
  - Wenn sich Host und Produkt auf demselben Computer befinden, besteht die naheliegendste Methode zur Gewinnung der Daten darin, sie aus der Protokolldatei des Produkts auszulesen.
  - Wenn sich Host und Produkt nicht auf demselben Computer befinden, können die benötigten Daten durch die Einrichtung eines Netzwerkdateisystems (wie NFS-, Samba- oder SMB-Freigabe), einer TCP/IP-Socket-Verbindung oder einer seriellen Verbindung gewonnen werden.
- Erstellen Sie die Collectors und starten Sie die Ports.
- Bei Verwendung von Remote-Hosts müssen Sie die Collector-Dateien auf diese Remote-Hosts heraufladen. Starten Sie den Port zur Ausführung der Start-Skripts; die gesammelten Informationen werden über das Sentinel-System gemeldet.



Erstellen eines Collector

Wie bereits erörtert, müssen Sie zur Erstellung eines Collector folgende Elemente erstellen:

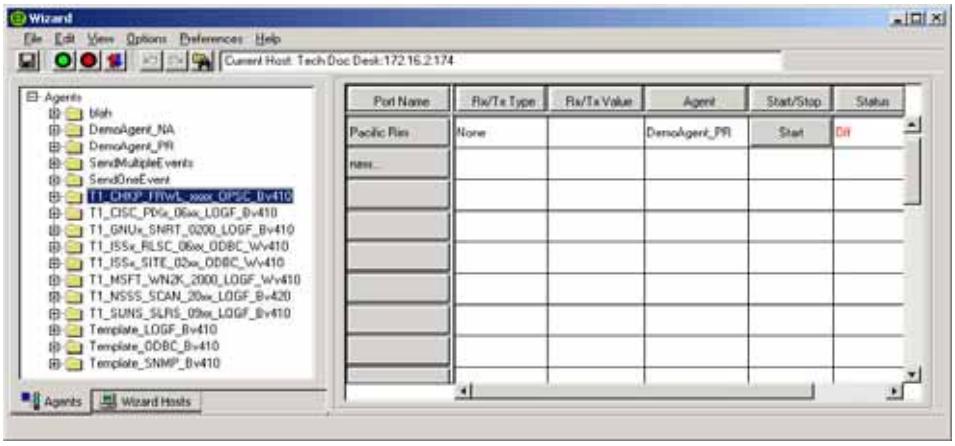
- Schablonendateien
- Parameterdateien
- Suchdateien (optional)
- Skripts
- Zuweisen eines Wizard-Portnamens für einen Collector

Erstellen und Konfigurieren von Schablonendateien

Erstellen und Konfigurieren von Schablonendateien

1. Starten Sie Collector Builder.
2. Klicken Sie auf die Registerkarte *Collectors*, um das Feld mit dem Collector-Baum zu öffnen.
3. Klicken Sie im Collector-Baum mit der rechten Maustaste auf *Collectors* und klicken Sie dann auf *Neuer Collector*.
4. Geben Sie den Namen des neuen Collector in das vorgesehene Feld ein und drücken Sie die Eingabetaste.

5. Klicken Sie mit der rechten Maustaste auf den neuen *Collector* und klicken Sie anschließend auf *Neue Schablone*.



6. Geben Sie in das Feld „Neue Schablone“ im Collector-Baum einen neuen Schablonennamen ein und drücken Sie die Eingabetaste.
7. Wählen Sie die neue Schablone aus und klicken Sie auf die Registerkarte *Schabloneneditor*.
8. Ziehen Sie im Feld *Schabloneneditor* die Statuswerte in den Bearbeitungsbereich und legen Sie sie dort ab. Verwenden Sie hierfür die Statusschaltflächen im linken Fensterbereich. Informationen zum Hinzufügen von Statuswerten zu einer Schablone finden Sie unter Hinzufügen eines Status zu einer Schablonendatei.
9. Klicken Sie auf *Speichern*.

Hinzufügen eines Status zu einer Schablonendatei

Alle Collectors beginnen die Verarbeitung bei Status 1, unabhängig davon, wo Status 1 in der Schablone vorkommt. Angenommen, Status 1 ist ein Verarbeitungsstatus, fügen Sie den neuen Status nach Status 1 ein.

Collector Builder weist automatisch dem ersten Status den Statuswert 1 zu. Dieser erste Status sollte nur einen Parsing-Befehl vom Typ BREAKPOINT() enthalten. Wenn nur ein Haltepunkt nach Status 1 gesetzt wird, wird die Fehlersuche einfacher. Bei der Fehlersuche stoppt der Parser automatisch beim nächsten Status.

Beginnen Sie beim Erstellen einer Schablone mit dem Analysestatus „nur Haltepunkt“. Fügen Sie den Arbeitsstatus (Status „Empfangen“, Status „Analysieren“ usw.) bei Status 2 ein. Wenn Sie einen Status am Anfang der Schablone einfügen müssen, fügen Sie ihn lediglich nach dem BREAKPOINT (Haltepunkt) ein.

Löschen Sie den Analysestatus „nur BREAKPOINT“ nur, wenn ein weiterer Status am Anfang der Schablone eingefügt werden muss. Optional können Sie bei diesem Analysestatus „nur BREAKPOINT“ Kommentare zur Funktionsweise der Schablone eingeben.

So fügen Sie einen Status zu einer Schablone hinzu

1. Klicken Sie auf die Registerkarte *Collectors*, um das Feld mit dem Collector-Baum zu öffnen.
2. Wählen Sie im Collector-Baum eine Schablone, die im Schabloneneditor im rechten Fenster angezeigt werden soll.

3. Klicken Sie auf *Optionen* > *Status hinzufügen* > *Übertragen, Empfangen, Entscheiden, Analysieren, Weiter, Gehe zu* oder *Stoppen* (je nach Bedarf) oder klicken Sie auf die entsprechenden Schaltflächen.
   -  Übertragen
   -  Empfangen
   -  Entscheiden
   -  Analysieren
   -  Weiter
   -  Gehe zu
   -  Stoppen
4. Fügen Sie mithilfe des Bearbeitungsbereichs unten im Fenster „Schabloneneditor“ den neuen Code in die einzelnen Status ein, während Sie sie hinzufügen.

   Eine weitere Möglichkeit besteht darin, eine Analysestatus-Schaltfläche von der linken Seite des Schabloneneditors in den Bearbeitungsbereich zu ziehen und dort abzulegen.

HINWEIS: Verwenden Sie in der decide-Zeichenkette keine doppelten Anführungszeichen, weder im Status „Empfangen“ (um beispielsweise das Begrenzungszeichen in einer Protokolldatei abzugleichen) noch im Status „Entscheiden“; Sie erhalten folgende Fehlermeldung:

```
***ERROR: Reading Template File..."
```

Wenn ein oder mehrere Anführungszeichen in die decide- bzw. delimiter-Zeichenkette eingefügt werden, tritt ein Fehler der folgenden Art auf:

```
StateDecideString: "test"123"
```

Sie können das Problem umgehen, indem Sie anstelle von Anführungszeichen (") die Zeichenkette \22\ verwenden.

HINWEIS: Wenn Sie ein weiteres Element auf der Registerkarte „Collectors“ auswählen (auch wenn es sich dabei um denselben Collector handelt) und anschließend zu der problematischen Schablone zurückkehren, gibt Collector Builder diese Fehlermeldung aus und zeigt keinen Teil oder Status der Schablone an. Dieser Fehler tritt auf, weil das Anführungszeichen (") zur Begrenzung der Feldwerte in .tem-Dateien verwendet wird Beispiel:

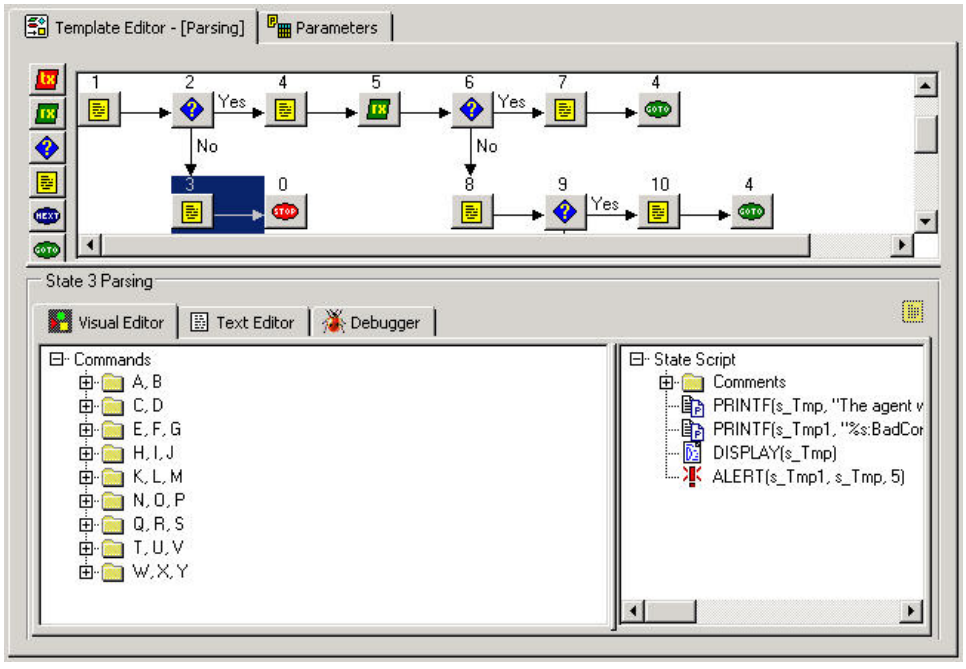
```
StateDecideString: "test"
StateDelimiterString: "123"
```

Eingabe eines Parsing-Befehls über den visuellen Editor

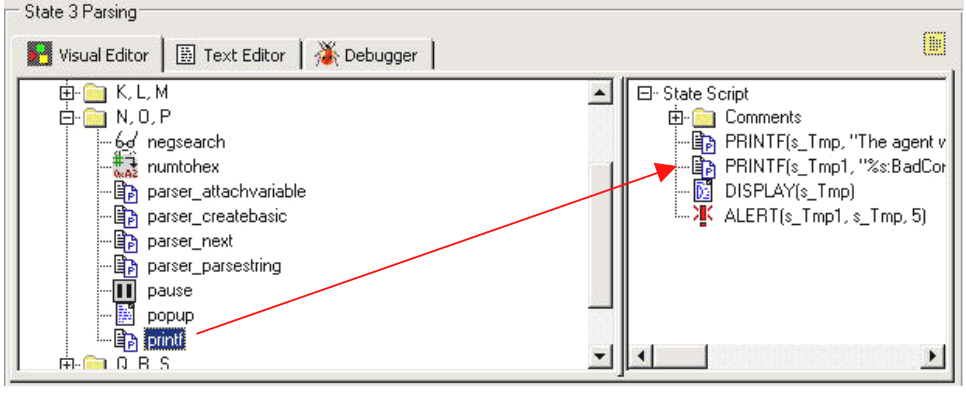
Es gibt zwei Methoden zur Eingabe eines Parsing-Befehls: über den visuellen Editor und über den Texteditor. Verwenden Sie nicht mehr als 4096 Befehle.

Eingabe eines Parsing-Befehls über den visuellen Editor

1. Wählen Sie im Schabloneneditor einen Analysestatus aus. Die Registerkarte „Visueller Editor“ ist standardmäßig geöffnet, wenn Sie auf eine zu öffnende Schablone klicken.



2. Ziehen Sie im visuellen Editor die Parsing-Befehle auf die rechte Seite des Fensters.



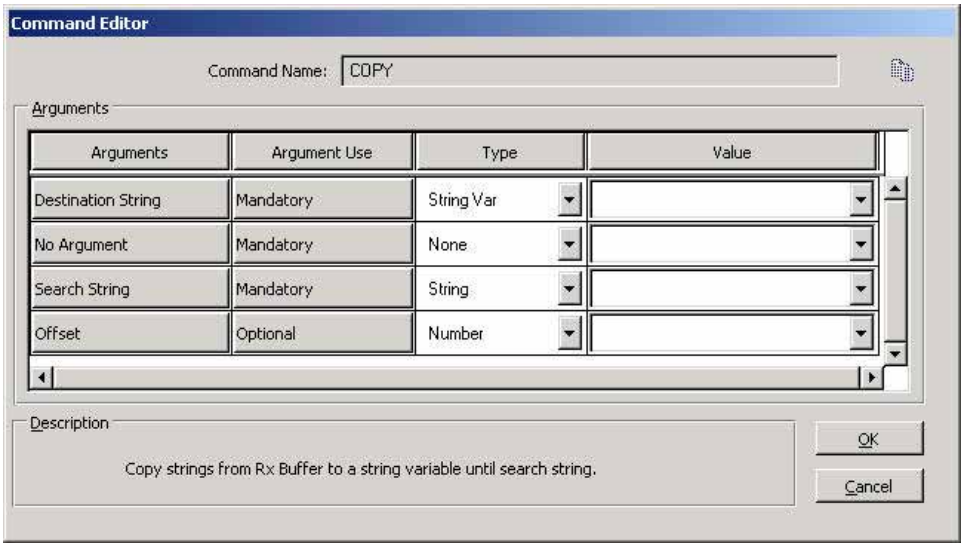
3. Geben Sie die Argumentwerte im Popup-Fenster„Befehlseditor“ ein.
   - Wählen Sie einen Typ aus – Die Typen für die einzelnen Parsing-Befehle sind im Sentinel-Referenzhandbuch für Benutzer beschrieben.
   - Geben Sie einen Wert an – Werte werden für eine bestimmte Anwendung definiert. Beispiele für die Werte der einzelnen Parsing-Befehle finden Sie im Sentinel-Referenzhandbuch für Benutzer.

Eingabe eines Parsing-Befehls über den Texteditor

1. Klicken Sie im Schabloneneditor auf die Registerkarte *Texteditor*.
2. Geben Sie die gewünschten Parsing-Befehle manuell ein.

   Mit der Tabulatortaste können Sie bei Verwendung einer nichtproportionalen Schriftart den Text ausrichten. Die Optionen zum Kopieren, Ausschneiden und Einfügen funktionieren wie bei jedem Standard-Texteditor.

Bearbeiten von Parsing-Befehlen



- Argumente – Enthält alle möglichen Argumente für den im visuellen Editor ausgewählten Parsing-Befehl.
- Argumentenverwendung – Legt fest, ob das Argument obligatorisch oder optional ist.
- Typ – Legt den Variablentyp fest; beispielsweise Zeichenketten, Zeichenkettenvariablen, Zahlen, Zahlenvariablen, Gleitkommazahlen, Gleitkommavariablen oder vordefinierte Variablen
- Wert – Der Wert, den Sie für die in der Spalte „Typ“ genannte Variable festlegen

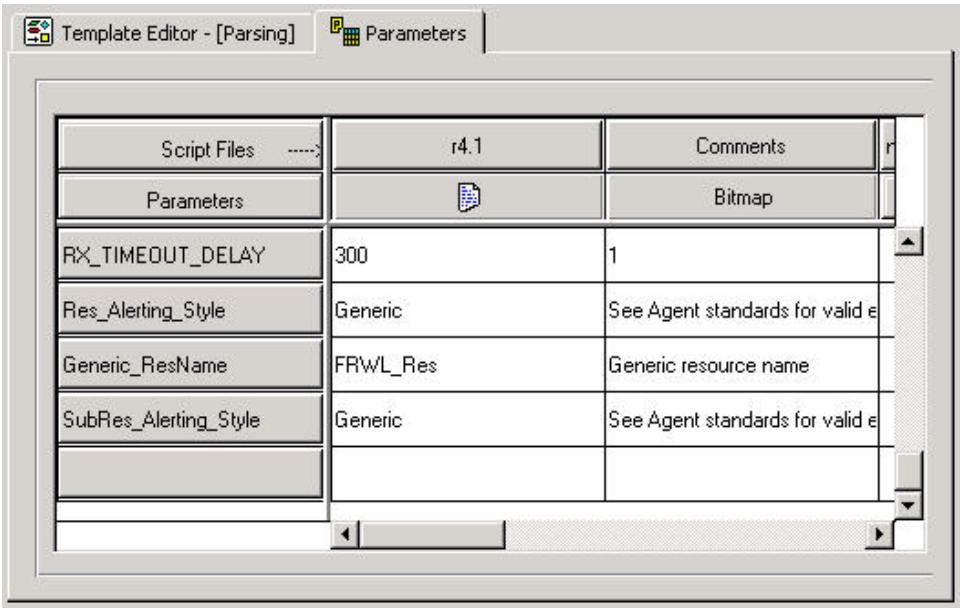
Bearbeiten von Parsing-Befehlen

1. Verwenden Sie im visuellen Editor eine der folgenden Vorgehensweisen:
   - Klicken Sie mit der rechten Maustaste auf einen Parsing-Befehl und wählen Sie die Option *Zu Statusanalyseliste hinzufügen*.
   - Doppelklicken Sie auf einen Parsing-Befehl. Der Befehlseditor wird geöffnet.
2. Füllen Sie die Felder „Typ“ und „Wert“ aus, um die Bearbeitung abzuschließen. Weitere Informationen zu den Beschreibungen der Parsing-Befehle finden Sie im Sentinel-Referenzhandbuch für Benutzer.

Erstellen und Konfigurieren von Parameterdateien

Erstellen und Konfigurieren von Parameterdateien

1. Klicken Sie auf die Registerkarte *Collectors*.
2. Wählen Sie eine Schablone aus und klicken Sie auf die Registerkarte *Parameter* im rechten Fensterbereich.



3. Doppelklicken Sie in der ersten Spalte der Parametertabelle auf *Neu...*.
4. Geben Sie den neuen Parameternamen ein (dies ist der Name Ihres Skripts, beispielsweise r4.1) und drücken Sie die Eingabetaste.
5. (Optional) Klicken Sie mit der rechten Maustaste auf die Schaltfläche *Bitmap* (zweite Spalte/zweite Zeile) und klicken Sie auf *Bitmap zuweisen*. Wählen Sie im Dialogfeld „Bitmap-Zuweisung“ eine *Bitmap*-Schaltfläche aus.
6. Doppelklicken Sie auf die einzelnen neuen Parameterfelder und geben Sie die entsprechenden Werte ein.
7. Wenn alle Werte definiert sind, müssen die Parameter- und die Schablonendatei kompiliert werden, um ein Skript zu erstellen. Gehen Sie zum Abschnitt Erstellen von Skripts.

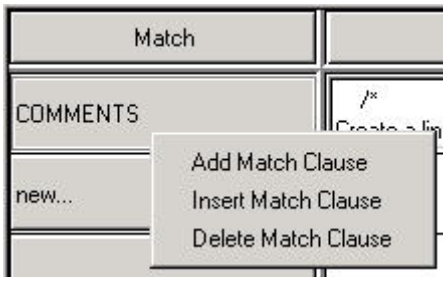
Erstellen und Konfigurieren von Suchdateien

Dieses Verfahren ist optional.

Erstellen und Konfigurieren von Suchdateien

1. Klicken Sie auf die Registerkarte *Collectors*, um das Feld mit dem Collector-Baum zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf einen Collector und klicken Sie auf *Neue Suchdatei*.
3. Geben Sie im Feld „Neue Suchdatei“ einen neuen Suchdateinamen ein und drücken Sie die Eingabetaste.

4. Doppelklicken Sie in der Spalte „Abgleichen“ auf *Neu...*, geben Sie die abzugleichende Zeichenkette ein und drücken Sie die Eingabetaste. Abgleichsklauseln können hinzugefügt, eingefügt und gelöscht werden.
   - Hinzufügen – Klicken Sie in der Spalte „Abgleichen“ mit der rechten Maustaste auf eine Klausel und klicken Sie dann auf *Abgleichsklausel hinzufügen*.
   - Einfügen – Klicken Sie in der Spalte „Abgleichen“ mit der rechten Maustaste auf eine Klausel und klicken Sie dann auf *Abgleichsklausel einfügen*.
   - Löschen – Klicken Sie in der Spalte „Abgleichen“ mit der rechten Maustaste auf eine Klausel und klicken Sie dann auf *Abgleichsklausel löschen*.



5. (Optional) Klicken Sie zur Eingabe von Parsing-Befehlen mit der rechten Maustaste auf die Analysespalte, um den visuellen Editor zu öffnen. Informationen zur Verwendung des visuellen Editors finden Sie unter Eingabe eines Parsing-Befehls über den visuellen Editor.
6. Wählen Sie die gewünschten Parsing-Befehle aus und stellen Sie sie im Fenster „Befehlseditor“ fertig. Die Befehle werden in der Analysespalte angezeigt.
7. Wenn alle Werte definiert wurden, muss durch Kompilieren ein Skript erstellt werden. Gehen Sie zu Abschnitt Erstellen von Skripts.

Skripts

Skripts werden aus Schablonen generiert. Aus einer Schablone können mehrere Skripts erstellt werden. Collector Manager bietet Ihnen folgende Möglichkeiten:

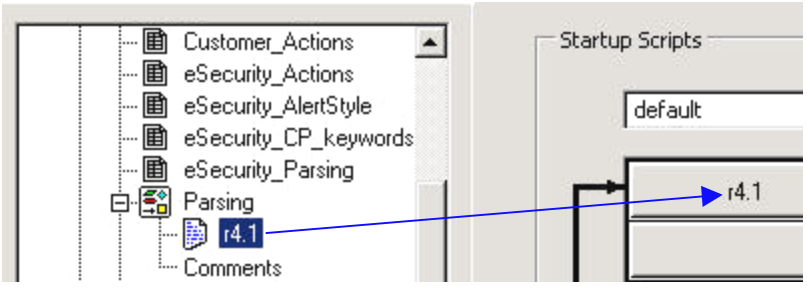
- Erstellen von Skripts
- Fehlersuche bei einem Skript
- Zuweisen einer Startsequenz zu einem Skript

Erstellen von Skripts

Erstellen von Skripts

1. Klicken Sie auf die Registerkarte *Collectors*, um das Feld mit dem Collector-Baum zu öffnen.
2. Wählen Sie im linken Fensterbereich die Schablone aus, von der aus Sie die Skripts erstellen.
3. Wählen Sie die Optionsfolge *Datei > Skripts erstellen*.

4. Ziehen Sie auf der Registerkarte „Schabloneneditor“ ein Skript von der Schablone in die Spalte „Startskripts“ bzw. „Zurücksetzungsskripts“ im rechten Fensterbereich.



Die Skripts werden in der Reihenfolge ausgeführt, in der sie in den Spalten „Startskripts“ und „Zurücksetzungsskripts“ angezeigt werden. Sie können die Skriptreihenfolge ändern, indem Sie die Skripts in den Spalten nach oben bzw. unten verschieben.

HINWEIS: Das Endskript in einer Zurücksetzungssequenz muss mit dem Verarbeitungsstatus „Stoppen“ enden.

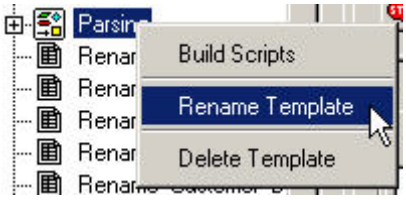
5. (Optional) Führen Sie mit dem Fehlersuchprogramm eine Fehlersuche durch.
6. Klicken Sie auf *Datei* > *Speichern*.
7. Damit die Änderungen wirksam werden, müssen Sie den Port mithilfe der Schaltflächen „Stoppen“ und „Starten“ in der Symbolleiste stoppen und erneut starten.

Aktivieren von AutoBuild für Collectors vor Version 5.0

Durch Aktivieren der AutoBuild-Funktion können Sie den Schritt der Skripterstellung bei der Konfiguration und Bereitstellung von Collectors überspringen.

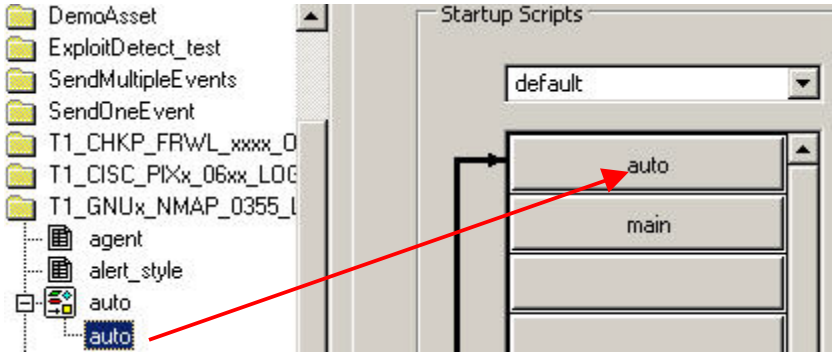
So aktivieren Sie AutoBuild für Collectors vor Version 5.0:

1. Kopieren Sie folgende Dateien aus einem bestehenden v5.* Collector und kopieren Sie sie in den Collector, für den Sie AutoBuilding aktivieren möchten.
   - auto.tem
   - auto.asd
   - auto.lkp
   - auto.par
2. Benennen Sie die Schablonendatei in main.tem um. Dies kann in Collector Builder vorgenommen werden.



3. Markieren Sie die umbenannte Schablonendatei und klicken Sie auf die Registerkarte *Parameter*. Ändern Sie den Namen des Spaltenheaders, der den Namen Ihrer Skriptdatei aufweist (z. B. r4.1) in „main“ und drücken Sie die Eingabetaste.

4. Klicken Sie auf „Speichern“.
5. Klicken Sie in der Startkette mit der rechten Maustaste auf auto.asd und ziehen Sie die Datei vor „main“.



Fehlersuche bei einem Skript

Wenn Sie mit der Fehlersuche beginnen, wird der Status des Ports im Fensterbereich „Portinformationen“ auf „Fehlersuche“ gesetzt. Informationen zur Fehlersuche in Skripts finden Sie unter „Durchführen der Fehlersuche bei einem Wizard-Port“ in Kapitel 2.

Zuweisen einer Startsequenz zu einem Skript

Wenn ein Port beim Start ausgeführt werden soll, können Sie eine Startsequenz zuweisen, die beim Start eine angegebene Menge von Skripts ausführt. Eine Startsequenz ist eine Datei, die die Namen der beim Start auszuführenden Skripts enthält.

Zuweisen einer Startsequenz zu einem Skript

1. Klicken Sie mit der rechten Maustaste auf einen Skriptnamen im Collector-Baum und wählen Sie „Neue Startsequenz“. Das Dialogfeld „Neue Startsequenz“ wird angezeigt.
2. Geben Sie im Dialogfeld „Neue Startsequenz“ den Sequenznamen ein und klicken Sie auf *OK*. Der neue Startsequenzname wird zu dem Menü oben im Feld „Startskripts“ hinzugefügt. Für Sequenznamen gelten folgende Einschränkungen:
   - Die Wörter „startup“ und „backout“ dürfen nicht als Sequenznamen verwendet werden.
   - Verwenden Sie keine Sequenznamen im selben Collector doppelt.
3. Ziehen Sie Skriptdateinamen aus dem Collector-Baum in die Spalte „Startskripts“. Die Skripts werden in der Reihenfolge ausgeführt, in der sie in der Spalte aufgeführt werden, von oben nach unten.
4. Um die Skriptreihenfolge zu ändern, ziehen Sie die Skripts aus der Spalte oder klicken Sie mit der rechten Maustaste auf das Feld *Startskripts* und wählen Sie die Option *Reihenfolge der Startskripts ändern.*

Erstellen eines Wizard-Ports

Sie können mehrere Ports für einen Sammler erstellen. Bei einigen Sensortypen müssen Sie möglicherweise mehrere Instanzen desselben Collector erstellen und jede Instanz einem anderen Port zuweisen.

Der Verbindungstyp eines Ports legt fest, wie Sicherheitsdaten gelesen werden, welche Informationen gelesen werden und wann eine Verbindung hergestellt wird. Es gibt folgende Verbindungstypen:

- Serieller Verbindungstyp
- Socket-Verbindungstyp
- Verbindungstyp „Datei neu“
- Verbindungstyp „Datei alle“
- Verbindungstyp „Permanenter Vorgang“
- Verbindungstyp „Temporärer Vorgang“
- Verbindungstyp „SNMP-Trap“
- Verbindungstyp „Ohne“

Serieller Verbindungstyp

Der serielle Verbindungstyp wird verwendet, wenn Daten über einen seriellen RS-232C-Anschluss gelesen werden (entweder über ein serielles Kabel oder eine serielle Modemverbindung). Sie müssen den ensprechenden seriellen Anschluss (z. B. COM1, COM2) im Feld „Rx/Tx-Wert“ angeben. Der Host, auf dem das zu überwachende Produkt ausgeführt wird, muss außerdem über eine serielle Verbindung mit dem Host des Collector verfügen, entweder über ein serielles Kabel oder über Modems auf beiden Seiten der Verbindung.

Bei Verwendung dieses Verbindungstyps können andere Bearbeitungen und Einträge erforderlich sein.

Socket-Verbindungstyp

Der Socket-Verbindungstyp wird verwendet, wenn Daten über eine TCP-Socket-Verbindung gelesen werden. Sie müssen die IP-Adresse und die TCP-Portnummer des Remote-Host im Feld „Rx/Tx-Wert“ angeben. Die IP-Adresse und die TCP-Portnummer müssen durch einen Doppelpunkt getrennt sein. Um beispielsweise den SMTP-Port anzugeben, geben Sie Folgendes im Feld „Rx/Tx-Wert“ ein:

```
<IP-Adresse>:<Port>
```

Außerdem müssen Sie möglicherweise einen TCP-Socket-Server-Prozess auf dem Remote-Host installieren und ihn so konfigurieren, dass er Daten an den TCP-Port liefert.

Weitere Informationen zur Konfiguration von Collectors mit diesem Verbindungstyp finden Sie in der Dokumentation zum Collector (z. B. Collectors Snort, Cisco PIX und Solaris Syslog) unter

```
%workbench_home%\elements\<Collector-Name>\docs
```

Verbindungstyp „Datei neu“

Der Verbindungstyp „Datei neu“ wird verwendet, um ausschließlich Sicherheitsereignisdaten zu lesen, die einer Datei hinzugefügt werden, nachdem das Skript gestartet wurde. „Datei neu“ öffnet die betreffende Datei und beginnt den Lesevorgang am Dateiende. Sie müssen im Feld „Rx/Tx-Wert“ den Pfad zur Protokolldatei angeben.

Weitere Informationen zur Konfiguration von Collectors mit diesem Verbindungstyp finden Sie in der Dokumentation zum Collector (z. B. Collector Solaris Syslog) unter

```
%workbench_home%\elements\<Collector-Name>\docs
```

Verbindungstyp „Datei alle“

Der Verbindungstyp „Datei alle“ wird verwendet, um alle Sicherheitsereignisdaten in einer Datei zu lesen.

Wenn Sie „Datei neu“ oder „Datei alle“ wählen, können Sie als „Rx/Tx-Wert“ entweder „inputfile“ oder „outputfile“ eingeben. Das Format lautet wie folgt:

```
inputfile, outputfile
```

oder

```
inputfile
```

oder

```
outputfile
```

Wenn Sie „Datei neu“ oder „Datei alle“ auswählen und die Datei kleiner wird, wird die Datei von Anfang an gelesen.

Weitere Informationen zur Konfiguration von Collectors mit diesem Verbindungstyp finden Sie in der Dokumentation zum Collector (z. B. Collectors Solaris Syslog und Windows 2000-Ereignisprotokoll) unter:

```
%workbench_home%\elements\<Collector-Name>\docs
```

Verbindungstyp „Permanenter Vorgang“

Der Verbindungstyp „Permanenter Vorgang“ dient zum Starten eines permanenten Prozesses beim Start des Ports. Der Prozess sorgt durch Empfangs- und Übertragungsstatusangaben für die Kommunikation zwischen dem diesem Port zugewiesenen Collector und einer externen Anwendung.

Ein permanenter Vorgang wird beim ersten Lese-/Schreibstatus gestartet und während der gesamten aktiven Dauer des Ports fortgesetzt. Der Prozess wird vom Port im Rahmen des Herunterfahrens beendet. Wenn der Port stoppt, wird ein Ereignis der Stufe 5 gesendet. Beim Starten des Ports wird ein Ereignis der Stufe 1 gesendet.

Weitere Informationen finden Sie im Abschnitt Permanente und temporäre Prozesse. Informationen zur Konfiguration des Rx/Tx-Werts für diesen Verbindungstyp finden Sie im Abschnitt Konfigurieren des Rx/Tx-Werts für eine permanente bzw. temporäre Verbindung (Rx/Tx-Typ). Weitere Informationen zur Konfiguration von Collectors mit einem permanenten Verbindungstyp finden Sie in der Dokumentation zum Collector (z. B. Collector Check Point Firewall & VPN) unter

```
%workbench_home%\elements\<Collector-Name>\docs
```

Verbindungstyp „Temporärer Vorgang“

Der Verbindungstyp „Temporärer Vorgang“ dient zum Starten eines temporären Prozesses beim Start des Ports. Der Prozess sorgt durch Empfangs- und Übertragungsstatusangaben für die Kommunikation zwischen dem diesem Port zugewiesenen Collector und einer externen Anwendung.

Temporäre Vorgänge können mehrmals gestartet werden. Der Prozess wird vom Port im Rahmen des Herunterfahrens beendet.

HINWEIS: Bei Auswahl von „Permanenter Vorgang“ bzw. „Temporärer Vorgang“ muss „Rx/Tx-Wert“ den Pfad und den Dateinamen des auszuführenden Prozesses enthalten. Sie können entweder den vollständigen Pfad und Dateinamen oder einen relativen Pfad und Dateinamen (für %WORKBENCH_HOME%) angeben. Beispiel:

Vollständiger Pfad:

```
C:\Programme\Cisco\Csids_client – start
```

Relativer Pfad:

```
.\elements\Cisco\Csids_client – start
```

Beim permanenten Prozess wird von einem relativen Pfad ausgegangen, es sei denn „Rx/Tx-Wert“ wird als vollständiger Pfad eingegeben.

Beenden des temporären Prozesses – Wenn der temporäre Prozess vor Beendigung des Parsers stoppt, wird er beim nächsten Lese- oder Schreibstatus neu gestartet, ohne dass ein Ereignis gesendet wird.

Weitere Informationen finden Sie im Abschnitt Permanente und temporäre Prozesse. Informationen zur Konfiguration des Rx/Tx-Werts für diesen Verbindungstyp finden Sie im Abschnitt Konfigurieren des Rx/Tx-Werts für eine permanente bzw. temporäre Verbindung (Rx/Tx-Typ).

Verbindungstyp „SNMP-Trap“

Der Verbindungstyp „SNMP-Trap“ dient zum Empfang von Traps der SNMP v1-, v2- und v3-Traps. Diese Traps werden von Sensoren an die Server-IP-Adresse von Wizard gesendet. Anhand der IP-Adresse und des Object Identifier (OID) des sendenden Geräts aktiviert Collector Manager die Analyse über den entsprechenden Collector. Der Rx-(Analyse-)Zustand leitet eingehende SNMP-Trap-Daten an den Collector weiter.

Alle zum Sammeln und Analysieren von SNMP v1- und v3-Traps verwendeten Informationen können konfiguriert werden:

- SNMP v1-Traps werden mithilfe der IP-Adresse und des Object Identifier (OID) sowie mit einem Trap-Code identifiziert.
- SNMP v2-/v3-Traps werden mithilfe von IP-Adresse, Sicherheitsnamen, Engine-ID, Authentifizierung und Verschlüsselungsschlüsseln (wenn im Trap aktiviert) sowie des Object Identifier (OID) des Trap identifiziert.

Das ursprüngliche Format des Trap wird hinsichtlich der Trap-Werte so weit wie möglich beibehalten. Das Format wird ursprünglich in der MIB (Management Information Base) für den Sensor definiert, von dem das Trap ausging.

Weitere Informationen finden Sie unter Einrichten des SNMP-Trap.

Verbindungstyp „Ohne“

Der Verbindungstyp „Ohne“ wird ohne Kommunikationsport verwendet. Er ist effizienter, da er nicht versucht, eine Verbindung herzustellen. Dieser Verbindungstyp sollte verwendet werden, wenn ein Collector nicht den Status „Empfangen“ verwendet und lediglich Befehle verarbeitet.

Detailliertere Informationen zur Einrichtung von Collectors mit dem Verbindungstyp „Ohne“ finden Sie in der Collector-Dokumentation (z. B. Collectors ISS RealSecure und ISS SiteProtector) unter

```
%workbench_home%\elements\<Collector-Name>\docs
```

Erstellen, Zuweisen, Starten und Stoppen eines Wizard-Ports

Erstellen eines Wizard-Ports

1. Informationen zur Collector-Konfiguration finden Sie in der Collector-Dokumentation unter %workbench_home%\elements\<Collector-Name>\docs.
2. Klicken Sie auf die Registerkarte *Collectors* und wählen Sie einen Collector aus.
3. Klicken Sie in Collector Builder auf die Registerkarte „Wizard-Hosts“ und wählen Sie einen Host aus.
4. Doppelklicken Sie im Bereich „Portinformationen“ auf der rechten Seite auf *Neu*, geben Sie den Namen des Ports ein und drücken Sie die Eingabetaste.
5. Wählen Sie einen *Rx/Tx-Typ* aus.
6. Geben Sie Einrichtungsoptionen auf der Grundlage des Verbindungstyps an:
   - Bei seriellen Verbindungen und Socket-Verbindungen: klicken Sie im Feld „Portname“ mit der rechten Maustaste auf den Namen des Anschlusses und wählen Sie *Rx/Tx-Wert bearbeiten* aus. Geben Sie eine der folgenden Optionsmengen an:
     - Bei seriellen Verbindungen: Wählen Sie Baudrate, Wortgröße, Parität und Stop-Bits aus. Klicken Sie auf „OK“.
     - Bei Socket-Verbindungen: Geben Sie die IP-Adresse und die Portnummer des Hostcomputers durch Doppelpunkt getrennt ein. Wenn kein Empfangsstatus verwendet wird, setzen Sie den Typ auf „Ohne“ und klicken Sie auf *OK*.

- Bei allen anderen Verbindungstypen: Doppelklicken Sie in die Zelle *Rx/Tx-Wert*, geben Sie die entsprechenden Informationen ein und drücken Sie die Eingabetaste.
- Informationen zum Verbindungstyp „SNMP-Trap“ finden Sie unter Einrichten des SNMP-Trap.

7. Doppelklicken Sie auf die Collector-Zelle und wählen Sie einen Collector-Namen aus.
8. Klicken Sie mit der rechten Maustaste auf *Portname* und klicken Sie dann auf *Andere Portoptionen*. Das Dialogfeld „Andere Portoptionen“ wird angezeigt.
9. Aktivieren bzw. deaktivieren Sie im Dialogfeld *Andere Portoptionen* das Kontrollkästchen *Port beim Start ausführen*, wählen Sie eine *Startsequenz* aus und klicken Sie auf *OK*.
10. Wenn Sie einen Port für den lokalen Host erstellen, klicken Sie auf *Datei* > *Speichern* und wählen Sie *Portinformationen*.

    Wenn Sie einen Port für einen Remote-Host verwenden: Klicken Sie auf *Datei* > *Heraufladen/Herunterladen*.

    Der Port wird zum Bereich „Portinformationen“ hinzugefügt. Zur Implementierung des neuen Ports braucht das System nicht neu gestartet zu werden. Klicken Sie auf *Starten*, um den Status des neuen Ports von „Aus“ in „Ein“ zu ändern.

Permanente und temporäre Prozesse

Mithilfe von „Permanenter Vorgang“ oder „Temporärer Vorgang“ kann Wizard eine Schnittstelle zu einer anderen Anwendung herstellen. Dazu werden Skripts verwendet, die Daten empfangen oder übertragen und Antworten analysieren. Jedes dieser Skripts wird auf einem eigenen Port ausgeführt und jeder Port ist mit einer bestimmten Anwendung verbunden.

HINWEIS: Im Feld „Rx/Tx-Wert“ ist „Andere Anwendung“ angegeben.

Die Prozessnamen können folgende Elemente enthalten:

- Leerzeichen
- Schrägstriche und umgekehrte Schrägstriche (für die verschiedenen Betriebssysteme)
- Befehlsargumente
- Absolute und relative Pfade (die Umgebungsvariable WORKBENCH_HOME wird als relativer Wert HOME betrachtet)

Wenn ein Empfangs-/Übertragungsstatus (Rx/Tx) auftritt, wird der im Feld „Rx/Tx-Wert“ angegebene Prozess gestartet. Wenn der Parser beendet wird, wird auch der Prozess beendet.

Wenn ein permanenter Prozess beendet wird, wird ein Ereignis der Stufe 5 gesendet. Wenn ein permanenter Prozess startet, wird ein Ereignis der Stufe 1 gesendet.

Die Standardausgabe (stdout) des permanenten/temporären Prozesses ist mit dem Empfangsstatus „Lesen“ des Parsers verbunden. Die Standardeingabe (stdin) des permanenten/temporären Prozesses ist mit dem Übertragungstatus „Schreiben“ des Parsers verbunden.

Konfigurieren des Rx/Tx-Werts für eine permanente bzw. temporäre Verbindung (Rx/Tx-Typ)

Bei der Konfiguration permanenter und temporärer Verbindungen stehen drei Connector-Prozesse zur Verfügung. Hierbei handelt es sich um:

- DBConnector (JDBC-Prozess-Connector)
- Lea Client
- Remote Data Exchange Protocol (RDEP)

Verwenden Sie im Feld „Rx/Tx-Wert“ für die permanenten und temporären Prozesse keine Anführungszeichen. Wenn es sich bei dem Prozess um einen absoluten Pfad zu einer ausführbaren Datei mit einem langen Namen handelt, der Leerzeichen enthält, geben Sie ihn ohne Anführungsstriche ein. Beispiel:

```
%WORKBENCH_HOME%\e-security\elements\checkpoint\lea_clien
   t checkpoint\lea_client.conf –new
```

Verwenden Sie keine Leerzeichen in Argumenten für die ausführbare Datei im Feld „Rx/Tx-Wert“. Diese Argumente sind durch Leerzeichen getrennt. Wenn sie also Leerzeichen enthalten, geht die Software von zwei Argumenten aus, obwohl es sich tatsächlich nur um ein einziges handelt. Wenn die Argumente zum Speicherort einer Konfigurationsdatei übergehen, wie beispielsweise bei Check Point, müssen Sie einen relativen Pfad von %WORKBENCH_HOME% verwenden. Beispiel:

```
checkpoint/\lea_client checkpoint/\lea_client.conf -new
```

DBConnector

DBConnector (ein JDBC-Prozess-Connector) führt einen Client aus, der eine Verbindung mit einem Datenbankserver herstellt, eine SQL-Abfrage auf dieser Datenbank ausführt und das Ergebnis im Format Name-Wert-Paar in der Standardausgabe ausgibt. Die auszuführende SQL-Abfrage wird entweder aus der Standardeingabe oder aus einer Datei gelesen. Der Name im Name-Wert-Paar-Ergebnis wird aus dem Spaltennamen des Ergebnissets übernommen. Aufgrund dessen sollte der gewünschte Spaltenname explizit in der SQL angegeben werden. Die genaue Syntax variiert je nach Datenbankserver.

Diese Anwendung wird zusammen mit Collector Manager in $WORKBENCH_HOME/dbconnector installiert.

Weitere Informationen zur Verwendung von DBConnector finden Sie in der README-Datei zu der Anwendung, in der Sentinel Collector-Dokumentation für Entercept Host IDS 4.0 (über JDBC) oder im eSecurity-Kundenportal unter http://www.esecurityinc.com.

Lea Client

Sentinel lea_client verwendet die Log Export API von OPSEC, um Daten aus Check Point Firewall-1 zu entnehmen und im Format Namen-Wert-Paar auszugeben. Der Client lea_client wird normalerweise verwendet, um Daten an den Sentinel Check Point Firewall-1-Collector zuzuführen, wo die Daten normalisiert werden und, je nach der Aktion des Ereignisses (z. B. verwerfen, ablehnen oder akzeptieren) wird eine Warnung an den Sentinel-Server gesendet.

Diese Anwendung wird zusammen mit Collector Manager in $WORKBENCH_HOME/checkpoint installiert.

Weitere Informationen zur Verwendung von Check Point lea_client finden Sie in der README-Datei zu der Anwendung, in der Sentinel Collector-Dokumentation für ECheck Point Firewall & VPN Collector (über OPSEC) oder im eSecurity-Kundenportal unter http://www.esecurityinc.com..

Remote Data Exchange Protocol (RDEP)

Die Java-Anwendug rdep_client ruft Daten aus Cisco IDS v4.0-Remote-Sensoren ab, auf denen RDEP ausgeführt wird. Der Client rdep_client stellt mithilfe von HTTP bzw. HTTPS eine Verbindung zu einem IDS-Remote-Sensor her. Nachdem der Client die Verbindung hergestellt hat, öffnet er ein Abonnement oder verwendet ein zuvor geöffnetes Abonnement. Das Abonnement beschreibt die Art der Daten, die der IDS-Sensor an den Client sendet. Die Art der Daten, die ein neues Abonnement abruft, kann durch Bearbeitung der rdep_client-Konfigurationsdatei geändert werden. Mithilfe des Abonnements initiiert der Client eine Anforderung für Ereignisdaten vom IDS-Sensor. Die Ereignisdaten werden vom IDS-Sensor im XML-Format zurückgegeben, vom Sentinel RDEP-Client in Namen-Wert-Paare konvertiert und anschließend vom Collector analysiert und normalisiert. Der Collector sendet schließlich das normalisierte Ereignis weiter an Sentinel.

Diese Anwendung wird zusammen mit Collector Manager in $WORKBENCH_HOME/cisco/rdep_client installiert.

Weitere Informationen zur Verwendung von RDEP finden Sie in der README-Datei zu der Anwendung, in der Sentinel Collector-Dokumentation für Cisco IDS 4.0 Collector (über RDEP) oder im eSecurity-Kundenportal unter http://www.esecurityinc.com..

Einrichten des SNMP-Trap

Sentinel kann SNMP-Traps empfangen, die Sicherheitsereignisse darstellen, die bei einem Sensor in einem Netzwerk aufgetreten sind. Diese Ereignisse werden mithilfe des SNMP-Protokolls über ein Netzwerk an Sentinel gesendet. Die SNMP-Versionen v1, v2 und v3 werden unterstützt. Um Sentinel für den Empfang von SNMP-Traps zu aktivieren, muss eine Wizard Collector-Instanz erstellt werden, die den SNMP-Trap-Verbindungstyp (Rx/Tx) verwendet.

Sie können die Einstellungen des SNMP-Trap konfigurieren, um die Parameter anzugeben, mithilfe deren Wizard-SNMP-Collectors Traps als binäre Ereignisse an Sentinel weitergeben können.

Das Fenster „SNMP-Trap-Einstellung“ dient zur Konfiguration der Einstellungen für Wizard-SNMP-Collectors, einschließlich des für SNMP-Traps verwendeten Traps, der Trap-Codes der Authentifizierung und der Verschlüsselungsinformationen.

So können Sie auf das Fensters „SNMP-Trap“ zugreifen:

1. Weisen Sie in Collector Builder Ihrem SNMP-Collector einen Portnamen zu.
2. Wählen Sie für „Rx/Tx-Typ“ „SNMP-Trap“.
3. Klicken Sie mit der rechten Maustaste auf den Portnamen und wählen Sie die Option *Rx/Tx-Wert bearbeiten*.

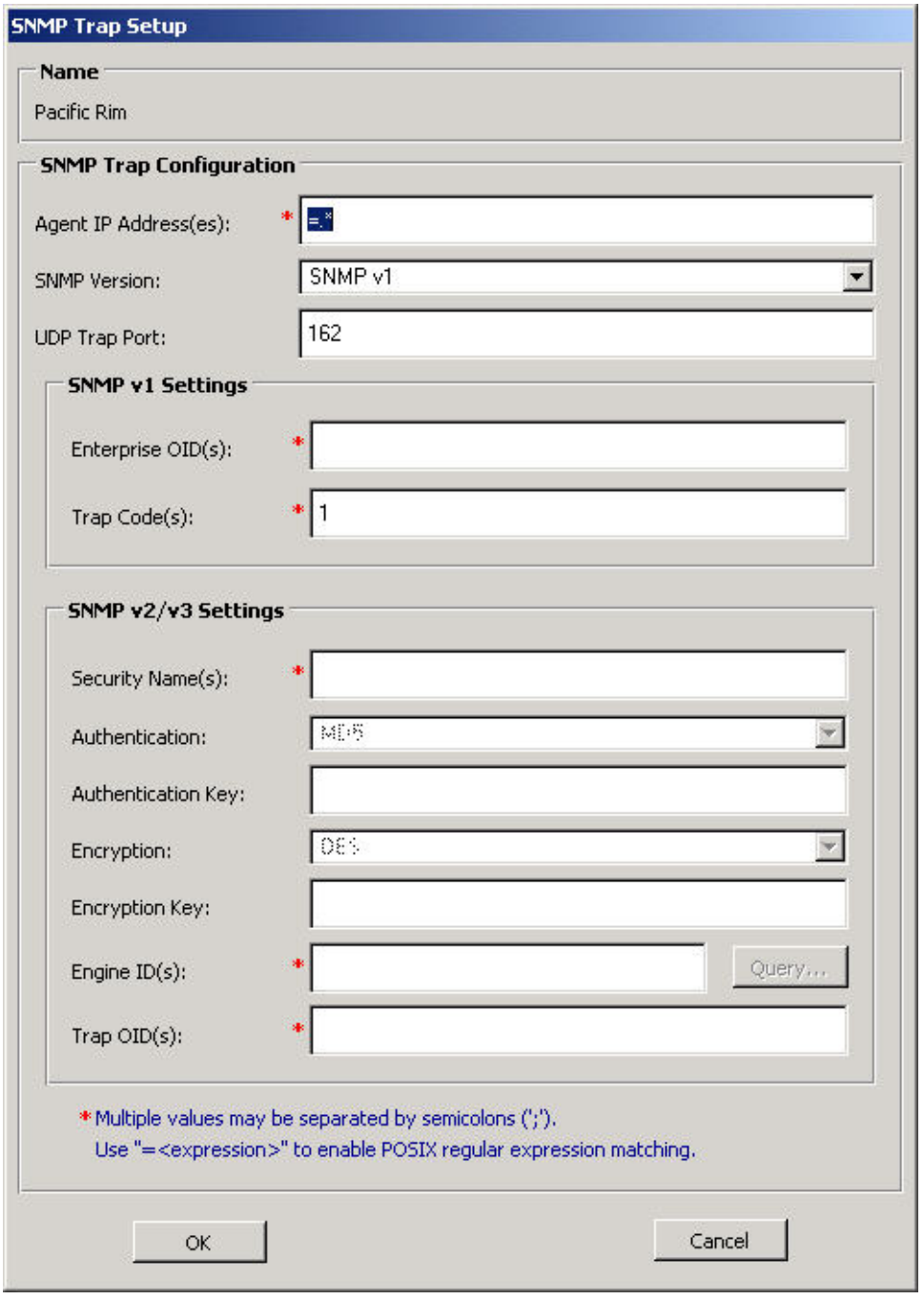
4. Geben Sie Ihre SNMP-Informationen ein.

HINWEIS: Der Standardport für das UDP-Trap ist162. Vergewissern Sie sich, dass dieser Port verfügbar ist. Anderenfalls können Sie eine andere Portnummer auswählen.

HINWEIS: Anders als bei anderen Collector-Ports wird das Feld „Rx/Tx-Wert“ ausgefüllt, gemäß Ihren Einstellungen im Fenster für die Einrichtung des SNMP-Trap. Bei einem SNMP-Collector kann das Feld Rx/Tx-Wert nicht manuell bearbeitet werden.

5. Speichern Sie den SNMP-Collector und laden Sie ihn herauf.
6. Aktivieren Sie diesen Collector, indem Sie Collector Manager stoppen und erneut starten.

HINWEIS: Zur Aktivierung dieses Collector müssen Sie Collector Manager, wie in Schritt 6 angegeben, stoppen und erneut starten.



Die SNMP-Einrichtung besteht aus folgenden Elementen:

- Collector-IP-Addresse(n)
- SNMP-Version
- UDP-Trap-Port
- SNMP v1-Einstellungen
  - Enterprise-OID(s)
  - Trap-Code(s)

- SNMP v2/v3-Einstellungen
  - Sicherheitsname(n)
  - Authentifizierung
  - Authentifizierungsschlüssel
  - Verschlüsselung
  - Verschlüsselungsschlüssel
  - Engine-ID(s) mit Abfrageschaltfläche
  - Trap-OID(s)

Im Dialogfeld „SNMP-Trap-Einstellung“ (wird durch Rechtsklick auf den Informationsbereich für den Collector Builder-Port und anschließendes Klicken auf „Rx/Tx-Wert bearbeiten“ geöffnet) können Sie Wizard für folgende Aktionen konfigurieren:

- Empfang von Traps auf anderen Ports als dem UDP-Port 162 (Standard).
- Erstellen eines einzelnen Wizard-Analyseskripts zur Verarbeitung von Traps aus mehreren IP-Adressen mit Informationen wie mehreren Trap-Codes und mehreren Trap-OIDs (Object Identfiers).
- Ermöglichen eines Abgleichs regulärer POSIX-Ausdrücke auf den Feldern für IP-Adresse, Enterprise Object Identifier (OID), Trap-Code und Trap-OID.
- Nach der Dekodierung des Trap legt Wizard Werte für die im Skript enthaltenen Variablen fest.

Collector-IP-Addressen

Collector-IP-Adressen sind IP-Adressen, die Traps empfangen sollen. Trennen Sie mehrere Werte durch Semikolon (;). Mithilfe des Formats =<Ausdruck> können Sie POSIX-kompatible reguläre Ausdrücke abgleichen. Das Sternchen (*) ist ein Modifikator für das vorstehende Zeichen bzw. den vorstehenden Ausdruck. Der Punkt (.) kann als Platzhalterzeichen verwendet werden und bei Verwendung regulärer Ausdrücke überall in der Zeichenkette auftreten.

Die häufigsten regulären Ausdrücke, die Sie wahrscheinlich verwenden werden, sind folgende:

`=`	entspricht einer beliebigen Zeichenkette beliebiger Länge
`= 192\.168.*`	entspricht einer beliebigen Zeichenkette, die 192.168 enthält Um nur Zeichenketten zu finden, die mit diesem Wert beginnen, verwenden Sie: ^192.168... Dabei muss ^ der Zeilenanfangs-Anker sein. Um nur Zeichenketten zu finden, die mit diesem Wert beginnen, verwenden Sie 0.47$... Dabei muss $ der Zeilenend-Anker sein.
`= [abc]`	entspricht a oder b oder c
`= [a-zA-Z0-9]`	entspricht einem beliebigen Einzelbuchstaben im Alphabet (Groß- oder Kleinbuchstabe) bzw. einer beliebigen Ziffer von 0 bis 9

Im Grunde lauten die Regeln in den obigen Beispielen für übliche reguläre Ausdrücke wie folgt:

. entspricht einem beliebigen Zeichen

* entspricht null oder mehr Vorkommnissen des vorstehenden Musters

[] entspricht einem beliebigen Einzelzeichen aus dem in Klammern definierten Muster

HINWEIS: Diese Regeln können kombiniert werden.

SNMP-Version

Es kann nur eine einzige SNMP-Version konfiguriert werden. Die Optionen in den Bereichen für die Einstellungen von SNMP v1 und SNMP v2/v3 werden gemäß der von Ihnen ausgewählten Version aktiviert.

UDP-Trap-Port

Der Standardwert für den Zielport des UDP-Ports lautet 162.

SNMP v1-Einstellungen

Diese Einstellungen sind nur aktiviert, wenn Sie SNMP v1 aus der Liste der SNMP-Versionen auswählen.

- Enterprise-OID(s) – Object-ID(s) zur Identifizierung des Collector-Typs, der das Trap gesendet hat. Trennen Sie mehrere Werte durch Semikolon (;).
- Trap-Code(s) – Trap-Codes für Sensors, die die SNMP-Traps senden. Diese Trap-Codes repräsentieren die vom jeweiligen SNMP-Collector gesendeten Trap-Typen. Trennen Sie mehrere Werte durch Semikolon (;).

SNMP v2/v3-Einstellungen

- Sicherheitsname(n) – Der für den Zugriff auf den Collector verwendete Benutzername. Bei Sicherheitsnamen muss die Groß- und Kleinschreibung beachtet werden. Trennen Sie mehrere Werte durch Semikolon (;).
- Authentifizierung – Authentifizierungsmethode. Es gibt folgende Werte:
  - Keine – Bei SNMP v3-Traps wird keine Authentifizierung durchgeführt.
  - MD5 – „Sicherheitsname“ wird so konfiguriert, dass der MD5-Algorithmus zur Erstellung einer digitalen Signatur für die Authentifizierung verwendet wird.
- Authentifizierungsschlüssel – Das zur Authentifizierung des Benutzers auf dem Collector verwendete Passwort. Nur Aktiviert, wenn „Authentifizierung“ auf „MD5“ gesetzt ist. Muss mindestens acht Zeichen lang sein. Bei Authentifizierungsschlüsseln muss die Groß- und Kleinschreibung beachtet werden. Derselbe Schlüssel muss auf dem sendenden SNMP-Collector konfiguriert werden.
- Verschlüsselung – Verschlüsselungsmethode. Es gibt folgende Werte:
  - Keine – Bei SNMP v3-Traps wird keine Verschlüsselung durchgeführt.
  - DES – Erwartet, Traps zu erhalten, die mit der Verschlüsselungsmethode DES (Data Encryption Standard) verschlüsselt sind.

- Verschlüsselungsschlüssel – Der zur Verschlüsselung der an Wizard-Collectors gesendeten Traps verwendete Schlüssel. Muss mindestens acht Zeichen lang sein. Beim Verschlüsselungsschlüssel muss die Groß- und Kleinschreibung beachtet werden. Nur aktiviert, wenn in der Verschlüsselungsliste „DES“ ausgewählt wurde.
- Engine-ID(s) – Eine eindeutige Kennung für einen SNMP v3-Collector. Es gibt eine Abfrageschaltfläche für Engine-IDs, mit der die abzufragende IP-Adresse gefunden werden kann. Eine erfolgreiche Abfrage gibt die Informationen zurück und fügt die Engine-ID hinzu. Wenn bereits eine Engine-ID im Feld vorhanden ist, wird eine weitere angehängt.
- Trap-OID(s) – Die Objekt-ID des Trap, das den speziellen Typ des empfangenden Trap angibt.

HINWEIS: Wenn Sie mehrere Sicherheitsnamen und Engine-IDs angeben, wird für alle dasselbe Authentifizierungs- und Verschlüsselungsschema verwendet.

HINWEIS: Wenn verschiedene Authentifizierungs- und Verschlüsselungsschlüssel für verschiedene SNMP-Collectors benötigt werden, muss für jeden Collector ein separater Port konfiguriert werden.

SNMP-Trap-Variablen

Einige Trap-Variablen gelten für alle Traps (SNMP v1 und v3), andere nur für eine einzige Version. In den folgenden Tabellen werden alle SNMP-Trap-Variablen aufgelistet. Diese sind nach der SNMP-Version gruppiert, mit der sie arbeiten:

- SNMP-Trap-Variablen für SNMP v1 und v3
- SNMP-Trap-Variablen für SNMP v1
- SNMP-Trap-Variablen für SNMP v3

SNMP-Trap-Variablen für SNMP v1 und v3

Variable	Beschreibung
`s_Trap_IP`	IP-Adresse des Collector/Sensors, der das Trap gesendet hat.
`s_Trap_Time`	Aktivzeit-Wert, der vom Collector/Sensor gemeldet wurde, der das Trap gesendet hat. Normalerweise gibt dieser Wert an, wie lange der Collector bereits ausgeführt wird. Format: D:HH:MM:SS.ss (Tage, Stunden, Minuten, Sekunden, Hundertstelsekunden).
`i_Trap_Version`	Wert für eine bestimmte SNMP-Version: 1 = SNMP v1 3 = SNMP v3
`i_Trap_Vars`	Anzahl der Variablenbindungen im Trap.

Variable	Beschreibung
s_Trap_OID[]	Ein Array (der Größe „i_Trap_Vars“) mit den Namen der in der Trap-Meldung gebundenen MIB-Variablen. Jedes Element des s_Trap_OID-Array ist eine OID, beispielsweise „.1.3.6.1.4.1.4286....“
s_Trap_Value[]	Ein Array (der Größe „i_Trap_vars“) mit den Werten der in der Trap-Meldung gebundenen MIB-Variablen. Die Indizes dieses Array und des s_Trap_OID-Array entsprechen sich, sodass s_Trap_OID[0] der Name und s_Trap_Value[0] der Wert ist.

SNMP-Trap-Variablen für SNMP v1

Variable	Beschreibung
s_Trap_Ent	Enterprise Object Identifier (OID des Collector/Sensors, der das Trap gesendet hat.
s_Trap_Code_Generic	Generischer Trap-Code des Trap. Es gibt folgende Werte: 1–5 = Standardmäßige, IETF-definierte (Internet Engineering Task Force) Trap-Typen 6 = Unternehmensspezifische Trap (Code ist in s_Trap_Code_Specific definiert)
s_Trap_Code_Specific	Spezifischer Trap-Code des Trap. Nur relevant, wenn s_Trap_Code_Generic = 6.

SNMP-Trap-Variablen für SNMP v3

Variable	Beschreibung
s_Trap_Engine_ID	Engine-ID des SNMP v3-Collector, der das Trap gesendet hat.
s_Trap_OID	Object Identifier (OID) des Trap, das den Typ des empfangenden SNMP v3-Trap angibt. Zum Zwecke der Trap-Identifizierung übernimmt die OID für SNMP v3-Traps den Platz der SNMP v1-Enterprise-OID und der generischen/spezifischen Trap-Codes ein.
s_Trap_Security_Name	Sicherheitsname, der den SNMP v3-Collector kennzeichnet, der das Trap gesendet hat.

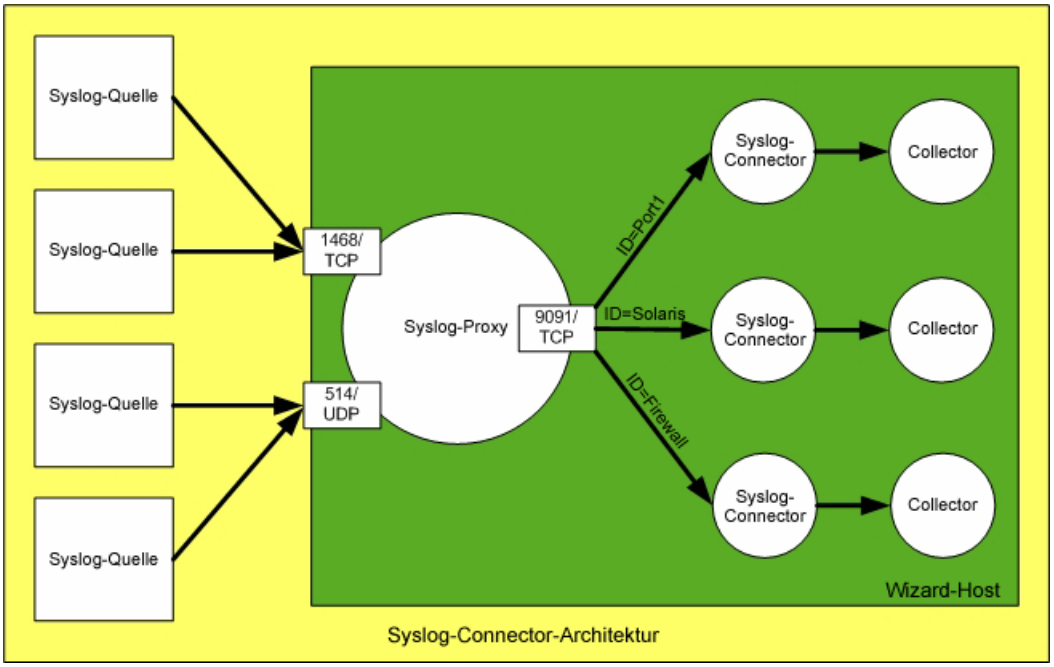
A Syslog Connector v1.0.2

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Novell hat diesen Syslog-Connector veröffentlicht, um eine reibungslose Integration zwischen Sentinel-Collectors und den Produkten zu ermöglichen, die in der Lage sind, Syslog-Meldungen zu generieren. Dieses Dokument soll Architektur, Installation, Verwendung und Optionen des Syslog-Connector erläutern.

Architektur

Der Syslog-Connector besteht aus zwei Teilen. Ein Teil ist der Syslog-Proxy und der andere der Syslog-Connector-Client. Der Syslog-Proxy überwacht ausgewählte UDP- und TCP-Ports. Der standardmäßige UDP-Port ist 514. Der standardmäßige TCP-Port ist 146. Dieser Port wird üblicherweise von Cisco PIX zum Senden von Syslog-Meldungen über das TCP-Protokoll verwendet.



Syslog-Connector-Architektur

Die von den einzelnen Syslog-Connector-Komponenten ausgeführten Funktionen werden im Folgenden beschrieben:

- Syslog-Proxy
  - Überwacht einen TCP- und/oder UDP-Port auf Syslog-Meldungen.
  - Analysiert die eingehende Meldung auf standardmäßige Syslog-Meldungskomponenten (Priorität, Datum, Hostname und Meldung)

- Falls die Meldungsquelle eine Meldung ohne Priorität, Datum oder Hostnamen sendet, wird RFC 3164 (BSD Syslog-Protokoll) befolgt und Daten zur Ergänzung werden eingefügt.
- Nach der Ermittlung von Komponente und Stufe aus der Priorität und dem Hostnamen veröffentlicht der Proxy die Meldung an die Syslog-Connector-Sitzungen, die daran interessiert sind.
- Falls die Sitzung des Syslog-Connector-Client endet, setzt der Syslog-Proxy die eingehenden Meldungen für diesen Client 10 Minuten lang in eine Warteliste. Dadurch soll sichergestellt werden, dass der Collector keine Meldungen verpasst, während er gerade neu gestartet oder vorübergehend angehalten wird.
- Der Syslog-Proxy überwacht einen TCP-Port, normalerweise 9091, um die Sitzungen des Syslog-Connector-Client zu warten.

- Syslog-Connector-Client
  - Der Connector wird als permanenter Prozess gestartet. Alle Laufzeitoptionen für den permanenten Syslog-Connector-Prozess sind unter „RX/TX-Wert“ eingegeben.
  - Ein Laufzeitparameter ist die ID. Die für einen bestimmten Syslog-Connector konfigurierte ID muss für alle Syslog-Connectors, die mit demselben Syslog-Proxy verbunden sind, eindeutig sein.
  - Zur Laufzeit kann ein Inhaltsfilter angegeben werden, um den Bereich der Meldungen zu begrenzen, die zur Analyse an den Collector gesendet werden.
  - Der Syslog-Connector stellt eine Verbindung zum Connector-Client-Service des Proxy her.
  - Der Syslog-Connector registriert seine ID und seinen Inhaltsfilter beim Syslog-Proxy.
  - Meldungen, die der Syslog-Proxy der ID zuordnet, werden vom Syslog-Connector gelesen und an dessen Standardausgabe weitergeleitet.
  - Zurzeit werden Struktur und Inhalt der Meldung unverändert an den Collector weitergeleitet. In Zukunft wird der Syslog-Connector die Meldung formatieren können, um die Analyseanforderungen des Collector zu erfüllen.

Das Syslog-Protokoll wurde herkömmlicherweise (und ist auch zurzeit noch) als UDP-basiertes Protokoll definiert. Da keine breite Palette verschiedener Anwendungen/Geräte vorhanden ist, die in der Lage sind, Meldungen über TCP zu senden und kein anerkannter Standard für Syslog über TCP existiert, wurde der Cisco PIX-Ansatz für die Beendigung von Syslog-Meldungen (Wagenrücklauf + Zeilenvorschub) übernommen. Die Meldungsbeendigung ist bei Syslog über TCP erforderlich, da es keinen definierten Standard oder eine natürliche Grenze zwischen Meldungen gibt. Syslog über UDP weist eine natürliche Meldungsbeendigung auf, da ein UDP-Paket eine einzelne Meldung transportiert und UDP verbindungslos ist.

Installation und Deinstallation

Der Syslog-Connector wurde für den Betrieb auf allen Wizard-Plattformen entwickelt. Aufgrund dieser Portierbarkeitsanforderung wurden beide Komponenten in Java geschrieben. Im Folgenden finden Sie eine Auflistung der Hardware- und Softwareanforderungen.

Systemanforderungen

Software

- Java 1.4.1 oder höher
- Wizard 4.2 oder höher
- Windows (2000/XP/2003), Solaris (8/9), RedHat Enterprise Linux (v3 ES/AS)

Hardware

- Zusätzlich 14 MB RAM (45 MB virtueller Arbeitsspeicher) für jede Instanz von Syslog-Connector und Proxy

Installation

Sowohl der Syslog-Proxy als auch die Connector-Client-Dateien werden automatisch bei der Installation des Collector-Service installiert. Die Syslog-Dateien befinden sich in folgendem Verzeichnis:

Bei UNIX:

```
$ESEC_HOME/wizard/syslog
```

Bei Windows:

```
%ESEC_HOME%\wizard\syslog
```

Wizard startet den Syslog-Proxy nicht automatisch. Wenn der Syslog-Proxy automatisch gestartet werden soll, muss er als Service installiert werden. Installieren Sie den Syslog-Proxy gemäß den folgenden Anweisungen als Proxy.

Installation als Windows-Service (Windows)

HINWEIS: Der Syslog-Proxy kann als automatisch auszuführender Windows-Service installiert werden. Um den Syslog-Proxy als Service zu installieren, müssen Sie folgende Befehle an der Eingabeaufforderung ausführen:

1. Wechseln Sie in das Verzeichnis /d “%ESEC_HOME%\wizard\syslog”
2. syslog-server.bat install

   Dadurch wird ein Windows-Service mit der Bezeichnung „eSecurity Syslog Server“ erstellt.

Installation als Service (UNIX)

HINWEIS: Der Syslog-Proxy kann als Service unter UNIX installiert werden, sodass er automatisch ausgeführt wird, wenn der Computer startet. Um den Syslog-Proxy als Service zu installieren, müssen Sie folgende Befehle ausführen:

1. Melden Sie sich als „root“ an.
2. Wechseln Sie in das Verzeichnis $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh install

Dadurch wird der Syslog-Proxy beim Start des Computers automatisch gestartet. Standardmäßig wird der Syslog-Proxy als Benutzer „root“ ausgeführt. Dies ist erforderlich, da der Syslog-Proxy standardmäßig an Port 514 gebunden wird, für den Root-Berechtigungen erforderlich sind. Um den Syslog-Proxy als einen anderen Benutzer als „root“ auszuführen, müssen Sie das Skript /etc/init.d/esyslogserver bearbeiten. Sie müssen sicherstellen, dass der betreffende Benutzer über die Berechtigungen zum Herstellen einer Bindung mit dem Port verfügt, der auf Meldungen überwacht werden soll. Hier einige Beispiele dafür, wie dies erreicht werden kann:

- Starten Sie den Syslog-Proxy über den Befehl „sudo“. Damit erhält der Benutzer „sudo“-Berechtigungen für die Bindung an den entsprechenden Port.
- Bearbeiten Sie die Syslog-Konfiguration (syslog.conf) so, dass der Syslog-Proxy an einen Port gebunden wird, für den keine Root-Berechtigungen erforderlich sind (d. h. >1024). In diesem Fall müssen Sie voraussichtlich die an Port 514 gesendeten Meldungen an den neuen Port umleiten, den Sie für die Verwendung ausgewählt haben.

Deinstallation

Um diesen Windows-Dienst zu deaktivieren, müssen Sie die folgenden Befehle an der Eingabeaufforderung ausführen.

Deinstallation als Windows-Service (Windows)

1. Wechseln Sie in das Verzeichnis /d “%ESEC_HOME%\wizard\syslog”
2. syslog-server.bat remove

Deinstallation als Service (UNIX)

Um den Syslog-Proxy als Service zu deinstallieren, müssen Sie folgende Befehle ausführen:

1. Melden Sie sich als „root“ an.
2. Wechseln Sie in das Verzeichnis $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

Syntax

Syslog-Proxyserver

Wizard startet den Syslog-Proxyserver nicht automatisch. Wenn der Syslog-Proxy automatisch gestartet werden soll, muss er als Service installiert werden. Befolgen Sie die Anweisungen in Abschnitt Installation, um den Syslog-Proxy als Service zu installieren.

Die Syslog-Proxy-Konfiguration wird in folgender Datei gespeichert:

Bei UNIX:

```
$ESEC_HOME/wizard/syslog/config/syslog.conf
```

Bei Windows:

```
%ESEC_HOME%\wizard\syslog\config\syslog.conf
```

Der Syslog-Proxy wird so eingerichtet, dass er standardmäßig folgende Konfiguration verwendet:

- Listener auf UDP-Port 514 für Syslog-Meldungen
- Listener auf TCP-Port 1468 für Syslog-Meldungen
- Listener auf TCP-Port 9091 für Connector-Verbindungen

Der Syslog-Proxy kann so konfiguriert werden, dass er andere Ports überwacht, um Syslog-Meldungen zu empfangen oder Client-Verbindungen zu akzeptieren. Die zugehörigen Schalter lauten:

-udp <Port>	Port für die Überwachung auf UDP-Meldungen von Geräten; Standard: 514
-tcp <Port>	Port für die Überwachung auf TCP-Verbindungen von Geräten; Standard: 1468
-connector <Port>	Port für die Überwachung auf TCP-Verbindungen von Connectors; Standard: 9091

Um diese Einstellungen zu bearbeiten, müssen Sie folgenden Abschnitt der Datei syslog.conf ändern:

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=1468
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
```

Beispiel: Sie möchten die Port-Einstellungen auf folgende Werte ändern:

- Listener auf UDP-Port 4514 für Syslog-Meldungen
- Listener auf TCP-Port 4168 für Syslog-Meldungen
- Listener auf TCP-Port 4991 für Connector-Verbindungen

In diesem Fall sollte der oben angegebene Abschnitt aus der Datei syslog.conf wie folgt geändert werden:

```
wrapper.app.parameter.3=-tcp
wrapper.app.parameter.4=4168
wrapper.app.parameter.5=-udp
wrapper.app.parameter.6=4514
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=4991
```

Standardmäßig wird die Syslog-Proxy-Konfiguration so eingerichtet, dass Client-Verbindungen von jedem Host akzeptiert werden. Zur Erhöhung der Sicherheit kann der Syslog-Proxy so eingerichtet werden, dass er nur Client-Verbindungen akzeptiert, die sich auf demselben Host befinden. Dies ist eine Sicherheitsmaßnahme, da zwischen den Client-Connectors und dem Proxy kein Datenschutz, keine Zugriffssteuerung und keine Authentifizierung in Kraft ist. Hierfür können folgende Schalter verwendet werden:

`-private`	Überwacht auf Connector-Verbindungen auf Loopback
-shared	Überwacht auf Connector-Verbindungen auf Localhost – Standardeinstellung

Der Schalter –shared weist den Proxy an, den Listener für die Client-Verbindung an ein Socket zu binden, auf das Remote-Hosts Zugriff haben.

Um diese Einstellungen zu bearbeiten, müssen Sie folgenden Abschnitt der Datei syslog.conf ändern:

```
wrapper.app.parameter.2=-shared
```

Um beispielsweise nur Client-Verbindungen vom selben Host zuzulassen, sollten Sie die Einstellungen wie folgt ändern:

```
wrapper.app.parameter.2=-private
```

Der Syslog-Proxy kann so konfiguriert werden, dass alle empfangenen Meldungen in einer Protokolldatei aufgezeichnet werden. Das Format der Meldungen wird in der Form angezeigt, die der Syslog-Proxy für die Weitergabe der Meldungen an einen anderen Syslog-Server verwenden würde. Daher wird <PRI>, also die Priorität, die der empfangende Syslog-Server für die Evaluierung der Komponente und die Stufe der Meldungen verwendet, am Anfang jeder Meldung angezeigt. Diese Art von Protokollierung wird durch den folgenden Schalter aktiviert.

`-log <Dateiname>`	Name der Protokolldatei, an die die Meldungen angefügt werden sollen.

Um diese Art von Protokollierung zu aktivieren, müssen Sie nach dem letzten Vorkommen von „wrapper.app.parameter“ die folgenden beiden Zeilen in die Datei syslog.conf einfügen:

```
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=<Dateiname>
```

Um beispielsweise diese Art von Protokollierung für die Datei $ESEC_HOME/wizard/syslog/messages.log zu aktivieren, müssen Sie die Einstellungen wie folgt ändern:

```
wrapper.app.parameter.7=-connector
wrapper.app.parameter.8=9091
wrapper.app.parameter.9=-messageSize
wrapper.app.parameter.10=5000
wrapper.app.parameter.11=-log
wrapper.app.parameter.12=messages.log
```

Wenn für den Dateinamen kein absoluter Pfad angegeben wurde, ist der Pfad relativ zum Verzeichnis $ESEC_HOME/wizard/syslog.

HINWEIS: Die Protokolldatei kann recht groß werden. Daher müssen Sie sicherstellen, dass das Verzeichnis, in das die Datei geschrieben wird, über genügend Speicherplatz verfügt (z. B. ein Verzeichnis, dass nicht unter $ESEC_HOME liegt).

Es wird empfohlen, den Syslog-Proxy mit mindestens 64 MB und höchstens 256 MB JVM-Heap-Speicher auszuführen. Bei dieser Konfiguration können Sie folgende Leistung erwarten:

Grenzwerte für den Proxyserver:

▪ Maximale Anzahl an Ereignissen:	500 E/s (Gesamtwert für alle Client-Ports)
▪ Maximale Größe von Connector Q:	5000 Meldungen (Standard, wenn nichts anderes angegeben ist)
▪ Maximale Anzahl an Connectors:	5

Um die Einstellungen für den Arbeitsspeicher zu bearbeiten, müssen Sie folgenden Abschnitt der Datei syslog.conf ändern:

```
# Initial Java Heap Size (in MB)
wrapper.java.initmemory=64

# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=256
```

Syslog-Connector-Client

Der Syslog-Connector-Client stellt eine Verbindung zum Syslog-Proxy her und sammelt dabei die Meldungen, die er abonniert hat. Die vom Client gesammelten Meldungen werden anschließend an die Standardausgabe weitergeleitet. Die Sitzung des Client mit dem Server endet erst, wenn der Client-Prozess bzw. der Syslog-Proxy beendet wird. Durch dieses Betriebs- und Ausgabeverhalten eignet er sich zur Verwendung als Connector für permanente Prozesse durch die Collector-Engine.

Konfigurieren Sie im Fenster für die Port-Konfiguration von Collector Builder einen Port mit dem Rx/Tx-Typ „Permanenter Vorgang“ und einem „Rx/Tx-Wert“, der der im Folgenden angegebenen allgemeinen Syntax ähnelt.

Bei UNIX:

```
syslog/SyslogConnectorAgent.sh <Argumente>
```

Bei Windows:

```
syslog\SyslogConnectorAgent.bat <Argumente>
```

Nach Abschluss des Rx/Tx-Werts müssen Sie den entsprechenden Collector aus der Bibliothek auswählen und die Port-Konfiguration sowie nach Möglichkeit den Collector auf den Remote-Wizard laden.

Der Syslog-Connector-Client verwendet eine Reihe von Standardargumenten zur Vereinfachung der allgemeinen Syntax. Die einfachste Befehlszeile für den Syslog-Connector-Client lautet:

Bei UNIX:

```
syslog/SyslogConnectorAgent.sh –id „MyUniqueID“
```

Bei Windows:

```
syslog\SyslogConnectorAgent.bat –id „MyUniqueID“
```

Die Interpretation dieser Befehlszeile lautet wie folgt:

- Verbindung zum Syslog-Proxy herstellen, der diese Verbindung überwacht (unter 127.0.0.1:9091)
- Alle Meldungen mit allen möglichen Syslog-Funktionen abonnieren
- Alle Meldungen mit allen möglichen Syslog-Stufen abonnieren
- Alle Meldungen unabhängig von der im IP-Header enthaltenen Quellen-IP-Adresse abonnieren.
- Alle Meldungen unabhängig von der Host-Angabe innerhalb der Meldung abonnieren.
- Diesen Sitzungsabonnementparametern die ID „MyUniqueID“ zuweisen

Die Sitzung des Syslog-Connector-Client wird mit dem oben angegebenen Abonnementfilter unter der ID „MyUniqueID“ beim Syslog-Proxy registriert. Die ID ist erforderlich. Die ausgewählte ID war willkürlich festgelegt, sie muss jedoch für alle Syslog-Connector-Client-Sitzungen mit demselben Syslog-Proxy eindeutig sein. Wenn ein anderer Syslog-Connector-Client mit derselben ID konfiguriert wird, wird eine der beiden Verbindungen mit derselben ID aufgegeben. Die letzte Sitzung, deren Verbindung mit dieser ID hergestellt wurde, bleibt erhalten.

Der generische Filter im vorherigen Filter führt eventuell zu nutzloser Collector-Verarbeitung. Dies ist der Fall, wenn die Meldungen, die die Filteranforderungen erfüllen (nämlich alle empfangenen Meldungen) für die Vorgänge des betreffenden Collector nicht relevant sind. Aus dem oben angegebenen Beispiel sollte hervorgehen, dass der Filterausdruck sehr vielseitig einsetzbar ist. Im folgenden Beispiel (UNIX) wird restriktiver, dafür jedoch auch genauer beschrieben, welche Meldungen für den Collector relevant sind.

```
syslog/SyslogConnectorAgent.sh -facilities „user,kernel“ -
   levels „warning,error“ -sender
   „192.16.0.12,192.16.0.0/16“ -host
   „17.16.8.0/24,10.1.1.13“ -id „MyOtherUniqueID“
```

Die Interpretation dieser Befehlszeile lautet wie folgt:

- Verbindung zum Syslog-Proxy herstellen, der diese Verbindung überwacht (unter 127.0.0.1:9091)
- (-facilities) Alle Meldungen abonnieren, die mit den Funktionen „user“ (Benutzer) oder „kernel“ (Kernel) gesendet wurden
- (-levels) Alle Meldungen abonnieren, die mit den Stufen „warning“ (Warnung) oder „error“ (Fehler) gesendet werden

- (-sender) Meldungen abonnieren, die durch die Quellen-IP-Adresse der eingehenden Meldungen an den Syslog-Proxy identifiziert werden. Dieses Argument führt dazu, dass der Syslog-Proxy die IP-Header-Informationen untersucht, um diese Kriterien zu evaluieren. Dadurch kann der Filter mit Syslog-Relay-Servern umgehen. Relay-Server identifizieren sich nicht in den Meldungen, die sie weiterleiten. Dieses Argument ist zwar eigentlich dazu gedacht, den Umgang mit weitergeleiteten Meldungen zu ermöglichen, es kann jedoch auch zum Filtern von Meldungen verwendet werden, die direkt aus der Syslog-Quelle gesendet wurden. Besonders relevante Relay-Server bzw. Syslog-Quellen sind 192.16.0.12 und 192.16.0.0/16. Das zweite Element steht tatsächlich für einen Bereich von IP-Adressen; solange die Quellen-IP-Adresse zwischen 192.16.0.0 und 192.16.255.255 liegt, erfüllen die betreffenden Meldungen die Filterkriterien. Hostnamem sind nicht gültig, da keine Hostnamen-Auflösung durchgeführt wird, um die Hostnamen der Quellen-IP-Adresse zu bestimmen.
- (-host) Meldungen abonnieren, die die Host-Bezeichner 17.16.8.0/24 bzw. 10.1.1.13 innerhalb der Syslog-Meldung aufweisen. Beim ersten Element handelt es sich um einen IP-Adressbereich. Wenn eine Meldung einen Host-Bezeichner in der Form einer IP-Adresse enthält, die im Bereich von 17.16.8.0 bis 17.16.8.255 liegt, erfüllt die Meldung diese Bedingung im Filter. Hostnamen werden vom Argument –host unterstützt. Der Hostname kann entweder wörtlich oder durch einen regulären Ausdruck angegeben werden. Denken Sie daran, dass auch für dieses Argument keine Hostnamen-Auflösung durchgeführt wird. Man kann nicht davon ausgehen, dass die Konfigurierung entweder eines Hostnamens oder einer IP-Adresse dazu führt, dass der Filter das jeweils andere Benennungsschema berücksichtigt. Beispiel: Die Konfiguration von „–host 172.16.0.90“ führt nicht zu einer Filterübereinstimmung für eine Meldung, die den Hostnamen „testbox1“ enthält, selbst wenn Namenauflösungs-Services 172.19.0.90 und „testbox1“ einander zuordnen würden. Bei der Host-Angabe als IPs werden also nur IP-Adressen gefunden und bei der Host-Angabe mithilfe von Hostnamen nur Hostnamen.

Der Filter aus dem obigen Beispiel lässt sich als folgender boolescher Ausdruck beschreiben:

```
(Facility=„user“ or Facility=„kernel“) and
   (Level=„warning“ or Level=„error“) and
   (Sender=„192.16.0.12“ or Sender=„192.16.0.0/16“) and
   (Host=„17.16.8.0/24“ or Host=„10.1.1.13“)
```

Die Anzahl der möglichen Kombinationen dieser Argumente ist das kartesische Produkt der Argumenttpyen, wobei jeder Argumenttyp ein Set ist. Gemäß PRINCIPIA CYBERNETICA WEB (http://pespmc1.vub.ac.be/ASC/CARTES_PRODU.html) ist das kartesische Produkt (hier in Übersetzung):

> „Die Sammlung aller geordneten n-Tupel, die gebildet werden können, sodass sie genau ein Element der ersten Menge, ein Element der zweiten,... und ein Element der n-ten Menge enthalten. Diese Sammlung kann so betrachtet werden, dass sie einen n-dimensionalen Raum darstellt, in dem jedes n-Tupel eine Zelle bildet. Das einfachste kartesische Produkt zweier Mengen ist eine zweidimensionale Tabelle (Kreuztabelle) mit Zellen zur Eingabe von Häufigkeiten, zur Angabe von Möglichkeiten (siehe „relation“) oder Unmöglichkeiten (siehe „constraint“) oder zur Darstellung der Übergänge, die das Verhalten eines Systems ausmachen. (Krippendorff)“

HINWEIS: Zum Zeitpunkt der Veröffentlichung des vorliegenden Dokuments war der oben aufgeführte Link zur Website korrekt.

Dies impliziert, dass theoretisch eine relativ große Anzahl verschiedener Meldungen den Filter durchlaufen können. Nur durch praktische, funktionsfähige Bedingungen wird die Anzahl der verschiedenen Meldungen tatsächlich festgelegt.

Neben den Befehlszeilenargumenten für den Filter gibt es noch folgende optionale Befehlszeilenargumente:

`-proxy <Serveradresse>:<Portnummer>`	Die Hostadresse des Syslog-Server-Proxy und die Portnummer für die Verbindung.
`-log <Dateiname>`	Aktiviert die Protokollierung in der angegebenen Datei.

Das Argument –proxy dient zur Konfiguration des Connector-Client zur Verbindung mit entweder einem nichtstandardmäßigen TCP-Port oder einem anderen Host als „localhost“. Der Syslog-Proxy erwartet, dass für eine Connector-Client-Verbindung standardmäßig 9091 verwendet wird. Wenn 9091 für den Host, auf dem der Syslog-Proxy ausgeführt wird, nicht geeignet ist, kann der Port während des Starts des Syslog-Proxy angepasst werden, und mithilfe des Arguments –proxy können die Clients angewiesen werden, eine Verbindung zu dem alternativen Port herzustellen. Außerdem kann der Ziel-Host des Connector-Client als ein anderer Host als das lokale System angegeben werden. Falls ein Syslog-Proxy Sitzungen von Remote-Connector-Clients akzeptiert, kann ein Syslog-Connector so konfiguriert werden, dass er eine Sitzung mit diesem Remote-Syslog-Proxy herstellt. Die IP-Adresse und der Connector-Client-Port des Syslog-Proxy werden mit dem Argument –proxy konfiguriert.

Das Argument –log aktiviert die Protokollfunktion des Connector-Client. Der Connector-Client gibt Meldungen aus, die er vom Syslog-Proxy empfängt. Anders als bei der Syslog-Proxy-Protokolldatei wird der Meldungsinhalt gemäß den registrierten Abonnementdetails gefiltert und die einzelnen protokollierten Meldungen enthalten nicht das Prioritätsfeld <PRI>. Der Inhalt stimmt mit dem Inhalt überein, den der Collector vom entsprechenden Syslog-Connector-Client empfängt.

HINWEIS: Die Protokolldatei kann recht groß werden. Daher müssen Sie sicherstellen, dass das Verzeichnis, in das die Datei geschrieben wird, über genügend Speicherplatz verfügt (z. B. ein Verzeichnis, dass nicht unter $ESEC_HOME liegt).

Ein Beispiel (unter UNIX) für die Verwendung der Argumente –proxy und –log ist Folgendes:

```
syslog/SyslogConnectorAgent.sh –proxy localhost:9091 –log
   connector_messages.log –id „MyUniqueID“
```

Konfigurieren der Protokollierung für den Syslog-Proxyserver

Der Syslog-Proxyserver schreibt Protokollierungsmeldungen in folgende Datei:

```
$ESEC_HOME/wizard/syslog/syslog_trace*.*.log
```

Der Protokollierumfang kann durch die Bearbeitung der Datei mit den Protokollierungseigenschaften geändert werden:

```
$ESEC_HOME/wizard/syslog/syslog_log.prop
```

Dies ist die Datei mit den Protokollierungseigenschaften, wie in der folgenden Zeile in der Datei syslog.conf angegeben:

```
wrapper.java.additional.1=-
   Djava.util.logging.config.file=syslog_log.prop
```

Nehmen Sie Änderungen an folgendem Abschnitt vor, um den Protokollierumfang anzupassen:

```
###### Configure the logging levels
   # Logging level rules are read from the top down. Start
   with the most general, then get more specific.
   …
   ######

   (###### Konfigurieren des Protokollierumfangs
   # Die Regeln für den Protokollierumfang werden von oben
   nach unten gelesen. Beginnen Sie mit der allgemeinsten
   und gehen Sie dann immer mehr ins Detail.
   …
   ######)
```

Beispiele für Befehlszeilenargumente

Der Syslog-Proxyserver und der Client-Connector können ohne die bei der Installation zur Verfügung gestellten Skripts ausgeführt werden. Dazu müssen Sie die Befehlszeilenargumente verwenden, die Sie in diesem Abschnitt finden.

Syslog-Proxy:

```
java –server –Xms64m –Xmx256m –
   Djava.util.logging.config.file=syslog-logger.prop -jar
   syslog.jar [-udp <Port>] [-tcp <Port>] [-connector
   <Port>] [-private|-shared] [-log <Dateipfad>]
   [-messageSize <Nummer>]
```

Gültige Argumente:

`–server`	Sollte immer verwendet werden. Wird von der JVM verwendet.
`–Xms64m`	Gibt die ursprüngliche Arbeitsspeichergröße des Syslog-Proxy an. Empfohlen: 64 Megabyte.
`–Xmx256m`	Gibt die maximale Arbeitsspeichergröße des Syslog-Proxy an. Empfohlener Standardwert: 256 Megabyte. Dadurch kann der Proxyserver mit Spitzen im Datenvolumen und mehreren Client-Connectors umgehen und mit Puffern arbeiten, wenn die Connectors die Verbindung wiederherstellen. Dieser Wert kann erhöht werden, wenn genügend Arbeitsspeicher verfügbar ist und das Datenvolumen sowie die Anzahl der Clients, die eine Verbindung herstellen, höher ist. Dieser Wert sollte 1,2 Gigabyte pro Syslog-Proxyserver nicht überschreiten, also „–Xmx1200m“.
`–Djava.util.logging.config.file`	Diese Eigenschaft gibt den Namen der Konfigurationsdatei (des Konfigurationspfads) für die Protokollierung der Fehlersuche an. Sie muss also auf die Stelle verweisen, an der sich die Datei befindet. Wenn kein Pfad angegeben wird, sucht sie im aktuellen Verzeichnis, von dem aus die JVM ausgeführt wurde. Beispiel: %workbench_home%\syslog-logger.prop
`-udp <Port>`	Port für die Überwachung auf UDP-Meldungen von Geräten; Standard: 514
`-tcp <Port>`	Port für die Überwachung auf TCP-Verbindungen von Geräten; Standard: 1468
`-connector <Port>`	Port für die Überwachung auf TCP-Verbindungen von Connectors; Standard: 9091
`-private`	Überwacht auf Connector-Verbindungen auf Loopback; Standardeinstellung
`-shared`	Überwacht auf Connector-Verbindungen auf Lokalhost. Wenn diese Eigenschaft nicht festgelegt ist, wird ein Kommunikationsfehler ausgegeben.
`-log`	Name der Protokolldatei, an die die Meldungen angefügt werden sollen.
`-help`	Zeigt diese Hilfemeldung an
`-version`	Gibt die Version des Proxy aus (0.91-poc)
`-messageSize`	Anzahl der gepufferten Meldungen, die für die vorübergehend nicht verfügbaren Verbindungen erneut gesendet werden sollen. Die maximale Größe ist 5000 ohne Kommas. Wenn der Optionswert nicht verwendet wird oder größer als 5000 ist, verwendet der Befehl standardmäßig den Wert 5000.

Syslog-Connector-Client:

```
java -jar syslogconnector.jar -id <UniqueId> [-proxy
   <Host:Portnummer>] [-facilities
   <facility1,facility2,…>] [-levels <level1, level2,…>]
   [-sender <Source IP1[/integer subnet mask], Source
   IP2[/integer subnet mask],…>] [-host < IP1[/integer
```

```
subnet mask]|Hostname1 | Hostname Regex1, IP2[/integer
subnet mask]|Hostname2 | Hostname Regex2, …>] [-log
<Dateipfad zur Protokolldatei>]
```

Gültige Argumente:

`-proxy <Host:Portnummer>`	Der Syslog-Proxy für die Verbindung mit Host:Port; Standard: 127.0.0.1:9091
`-facilities <facility1,facility2,…>`	Kommagetrennte Liste der gewünschten Komponenten; standardmäßig werden alle Komponenten verwendet.
`-levels <level1, level2,…>`	Kommagetrennte Liste der gewünschten Schweregrade; standardmäßig werden alle Stufen verwendet.
`-sender <Source IP1[/integer subnet mask], Source IP2[/integer subnet mask],…>`	Kommagetrennte Liste der gewünschten Sender; standardmäßig werden alle Sender verwendet.
`-host < IP1[/integer subnet mask]|Hostname1 | Hostname Regex1, IP2[/integer subnet mask`	Kommagetrennte Liste der gewünschten Hosts; standardmäßig werden alle Hosts verwendet.
`-log <Dateipfad zur Protokolldatei>`	Name der Protokolldatei, an die die Meldungen angefügt werden sollen.
`-id <UniqueId>`	Angabe der Connector-Identität (ERFORDERLICH)
`-help`	Zeigt diese Hilfemeldung an
`-version`	Gibt die Version des Connector aus (0.91-poc)

Tabelle der unterstützen Komponenten

Bei der Angabe in der Befehlszeile des Syslog-Connector-Client wird für Komponentennamen die Groß- und Kleinschreibung nicht berücksichtigt.

KERNEL	UUCP	LOCAL0
USER	CRON	LOCAL1
MAIL	SECURITY	LOCAL2
DAEMON	FTP DAEMON	LOCAL3
AUTH	NTP	LOCAL4
SYSLOG	LOG AUDIT	LOCAL5
LPR	LOG ALERT	LOCAL6
NEWS	CLOCK DAEMON	LOCAL7

Tabelle der unterstützen Stufen

Bei der Angabe in der Befehlszeile des Syslog-Connector-Client wird für Stufennamen die Groß- und Kleinschreibung nicht berücksichtigt.

EMERGENCY	WARNING
ALERT	NOTICE
CRITICAL	INFORMATIONAL
ERROR	DEBUG

Bereitstellungshinweise

An Syslog-Proxy weitergeleitete Meldungen

Die meisten Syslog-Server können die empfangenen Syslog-Meldungen an einen alternativen Syslog-Server weiterleiteten sowie die eingehenden Meldungen verarbeiten. In einem Bereitstellungsszenario kann es sinnvoll erscheinen, einen bestehenden Protokoll-Host zu ändern, um Meldungsweiterleitung an den Syslog-Proxy zu erzielen. Leider weisen einige Syslog-Server ungünstige Verhaltensweisen auf, die dies zu einer schlechten Wahl bei der Bereitstellung machen.

Es wurde beobachtet, dass Syslog-Serverbibliotheken unter Solaris 7, 9 und Linux 8 (die vermutlich dasselbe Verhalten zeigen wie andere bereitgestellte Versionen) nicht den Hostnamen bzw. die IP-Adresse des Hosts in die Meldungen aufnehmen, die sie Host-extern versenden. Der empfangende Syslog-Server verknüpft die Quellen-IP-Adresse bzw. den Hostnamen (über Namensauflösung) mit den empfangenen Meldungen in den von ihm generierten Protokolldateien. Wenn Solaris 9 als Relay zum Proxy fungiert, werden in die an den Proxy weitergeleiteten Meldungen weder die IP-Adresse noch der Hostname der ursprünglichen Meldungsquelle aufgenommen. Dies ist merkwürdig, da die Protokolldatei im Solaris 9-System eine IP-Adresse bzw. einen Hostnamen aufweist. Ohne den ergänzenden Hostnamen in der Meldung ist der Syslog-Proxy gezwungen, abzuleiten, dass die Meldung vom Relay-Server und nicht vom ursprünglichen Host stammte. Der Syslog-Proxy ergänzt bei jeder Meldung, die er von einem Solaris 9-Relay erhält, die Meldungen um die IP-Adresse des Relay-Host. Dies hat schwerwiegende Folgen. Der Ursprung eines Sicherheitsereignisses ist für den Collector und damit für Sentinel nicht sichtbar.

Es wird dringend empfohlen, dass der Proxy nicht als Empfänger von weitergeleiteten Meldungen fungiert, wenn die Meldungen nicht die IP-Adresse bzw. den Hostnamen des tatsächlichen Ursprungs enthalten. Diese Empfehlung kann schwerwiegende logistische Folgen haben, wenn der Proxy tatsächlich im Betrieb verwendet wird.

Beispiel:

Ein su-Ereignis findet auf ultrabookIIi (172.16.0.70) statt (unter Solaris 7). Dieser Computer sendet die Syslog-Meldungen an den Computer talkabout (172.16.0.72) (unter Solaris 9) weiter, der wiederum die Meldung an den Syslog-Proxy weiterleitet. Die folgenden Meldungen werden vom Sentinel-Connector generiert.

Proxy:

```
<37>Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0
```

Connector-Client:

```
Apr 02 06:54:11 [172.16.0.72.151.234] su: 'su root'
   succeeded for oespadm on /dev/pts/0
```

Im Folgenden finden Sie den Paket-Trace derselben Meldung, wenn sie zuerst bei talkabout ankommt und dann an den Syslog-Proxy auf pes020.esecurity.net weitergeleitet wird.

```
# snoop -x0 udp port 514
Using device /dev/dmfe0 (promiscuous mode)
```

```
ultrabookIIi -> talkabout    SYSLOG C port=42830
   <37>Apr  1 18:54:11

0: 0000 83cd 1395 0040 2082 202b 0800 4500
     .......@ . +..E.
16: 0061 fa09 4000 ff11 28d3 ac10 0046 ac10
   .aú.@...(....F..
32: 0048 a74e 0202 004d 5d7e 3c33 373e 4170
   .H.N...M]~<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    :
   'su root' succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0

talkabout -> pes020.esecurity.net SYSLOG C port=38890
   <37>Apr  1 18:54:11

0: 000a 5e02 a335 0000 83cd 1395 0800 4500
   ..^..5........E.
16: 0061 304b 4000 ff11 f031 ac10 0048 ac10
   .a0K@....1...H..
32: 02a6 97ea 0202 004d 6a82 3c33 373e 4170
   .......Mj.<37>Ap
48: 7220 2031 2031 383a 3534 3a31 3120 7375    r  1
   18:54:11 su
64: 3a20 2773 7520 726f 6f74 2720 7375 6363    :
   'su root' succ
80: 6565 6465 6420 666f 7220 6f65 7370 6164    eeded for
   oespad
96: 6d20 6f6e 202f 6465 762f 7074 732f 30      m on
   /dev/pts/0
```

Folgendes wurde auf talkabout aufgezeichnet:

```
Apr  1 18:54:11 ultrabookIIi su: 'su root' succeeded for
   oespadm on /dev/pts/0
```

B Konfigurieren eines Socket-Servers auf einem UNIX-Host

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Ein Socket-Server stellt einen Endpunkt für Socket-Verbindungen von UNIX Wizard Collector Manager zur Verfügung. Beispiel: Sie möchten eine Protokolldatei oder eine UNIX-Box von einer Wizard-Remote-Instanz aus überwachen und müssen eine Firewall passieren, um zum Port der UNIX-Box zu gelangen.

Die nachfolgenden Anweisungen dienen der Einrichtung eines Socket-Servers auf einem UNIX-(Uniplexed Information and Computing System-)Host; zudem basierend sie auf der Annahme, dass Sie auf dem UNIX-Host eine ASCII-(American Standard Code for Information Interchange-)Protokolldatei überwachen.

So richten Sie einen Socket-Server-Prozess auf einem UNIX-Host ein:

1. Erstellen Sie das Skript, das die Daten für die TCP-(Transfer Control Protocol-)Socket-Verbindung bereitstellt. Erstellen Sie hierzu eine neue Textdatei und kopieren Sie die nachfolgend angegebenen Zeilen in die Datei. Ersetzen Sie hierbei <Protokolldatei> mit dem vollständigen Pfadnamen der Datei, die Sie überwachen möchten:

   ```
   #!/bin/sh
   /bin/tail -f <Protokolldatei>
   ```

   Speichern Sie die Datei (Pfad und Dateiname können frei gewählt werden). Die Datei sollte jedoch an einem Ort gespeichert werden, an dem sie nicht gelöscht wird, und ihr Name sollte Aufschluss über ihre Funktion geben: Beispiel:

   ```
   /usr/local/bin/logfileserver
   ```

2. Wählen Sie einen nicht privilegierten TCP-Port auf dem UNIX-Host für den Serverprozess aus. Bei der Nummer des nicht privilegierten Ports handelt es sich um eine beliebige Zahl zwischen 1.025 und 65.535. Mithilfe des folgenden Befehls können Sie überprüfen, ob die von Ihnen gewählte Portnummer bereits verwendet wird (ersetzen Sie <Portnummer> hierbei mit dem gewünschten Port):

   ```
   netstat -an | grep LISTEN | grep <Portnummer>
   ```

   Wenn eine Zeile wie die nachfolgende ausgegeben wird, wird der Port zurzeit verwendet, Sie müssen also einen anderen Port auswählen.

   ```
   *.5555*.*0000 LISTEN
   ```

3. Bearbeiten Sie als Benutzer „root“ die Datei /etc/services und fügen Sie am Ende der Datei einen Eintrag für den neuen Socket-Service hinzu. Im nachfolgenden Beispiel wird eine Zeile für einen Service namens syslog_monitor hinzugefügt, der zur Überwachung von TCP-Port 5555 konfiguriert wurde:

   ```
   syslog_monitor5555/tcp
   ```

4. Bearbeiten Sie die Datei /etc/inetd.conf und fügen Sie am Ende der Datei einen Eintrag für den neuen Socket-Service hinzu. Im nachfolgenden Beispiel wird eine Zeile für einen Service namens syslog_monitor hinzugefügt, der zur Ausführung von Skript „/usr/local/bin/in.syslog_monitor“ konfiguriert wurde:

   Der nachfolgende Text sollte als durch Tabulatoren getrennte Felder in eine einzelne Zeile der Datei eingegeben werden, unabhängig von der Paginierung.

   ```
   syslog_monitor stream tcp nowait nobody
      /usr/local/bin/in.syslog_monitor in.syslog_monitor
   ```

5. Führen Sie folgenden Befehl aus, um den Socket-Server-Prozess zu aktivieren:

   ```
   kill -HUP `/bin/ps -ef | grep inetd | grep -v grep |
      awk '{print $2}'`
   ```

6. Testen Sie den Socket-Server. Stellen Sie hierzu eine Telnet-Verbindung zu dem von Ihnen ausgewählten Port her; daraufhin sollte der Inhalt Ihrer Protokolldatei angezeigt werden:

   ```
   % telnet localhost 5555
   ```

   Führen Sie zum Beenden der Telnet-Sitzung den ^] (control-])-Vorgang durch und geben Sie dann an der telnet>-Eingabeaufforderung „quit“ ein.