AES
aesclever.com

CLEVERDetect® for IDS 1.2
Empowering IT Cloud Security Anywhere, Anytime

Key Features

- **z/OS Intrusion Detection Service (IDS) message capture and transfer** providing immediate insight into malicious activities or policy violations.
- **Mobile and browser interfaces** ensure real-time notification of problems leading to increased IDS activity visibility.
- Strengthen **z/OS security for File Transfer Program (FTP)** with online FTP session logon failure in real-time and through historical reports.
- Improve operator effectiveness with **integrated Command** functions allowing deeper inspection into potential problems.
- Interrogates **TCP and UDP protocols for IDS attack** detection including malformed packets, violation of outbound RAW restrictions, UDP perpetual echo, and restrictions placed on IPv4, IPv6, ICMP and IP fragments.
- **Transfer syslog, FTP Logon failure, or IDS messages** as SNMP traps to Security Information and Event Manager (SIEM) and as notifications to mobile devices.

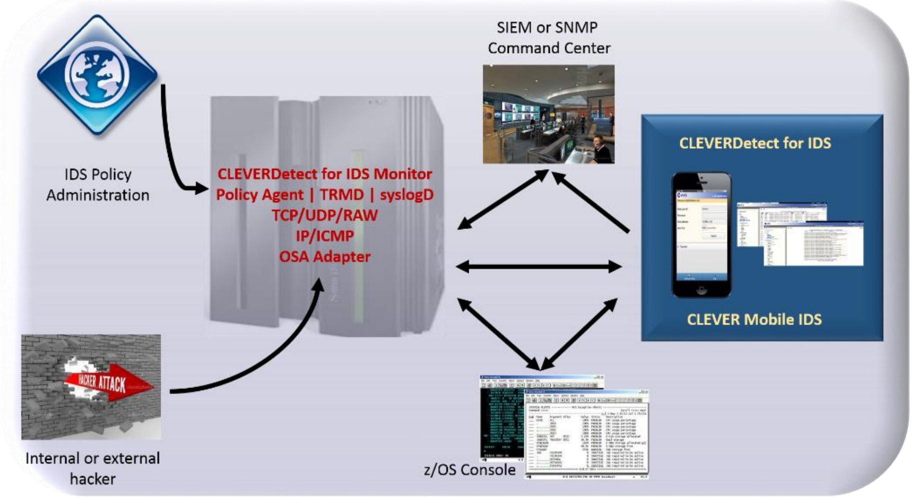
AES
P.O. Box 50927,
Palo Alto, CA 94303
650-617-2400
www.aesclever.com
info@aesclever.com

CLEVER® Business Cloud Security Management

Intrusion Detection is a very dynamic security activity impacting the network infrastructure and any IP enabled thing (IOT). Enterprise data centers are most concerned about intrusion detection at the network level and on servers. At its most basic an Intrusion Detection Service (IDS) device is passive, watching packets of data traverse the device, comparing the packets to configured rules (called policies), and setting off an alarm if there is anything suspicious. An IDS can detect several types of malicious traffic that would slip by a typical firewall.

A comprehensive baseline must be established to understand the 'normal' activity. A risk assessment follows prioritizing the impact on the business of an intrusion, defining the critical systems on which to implement intrusion detection services, and defining the intrusion detection policies to be implemented. Implementation follows with critical information like defined message, information, alert, and event handling to specific SNMP managers and SIEM systems established. Consistent visibility to these information flows is required to stop malicious traffic.

CLEVERDetect for IDS 1.2 has a new Dashboard feature providing a high level overview of events monitored. IDS Analyzer allows events to be viewed with extensive filtering options allowing a reduction of details shown to focus on specific elements. IDS Policy Explorer displays active policies and their details including policy rule, policy action, or route table names. If specific IDS attack types are selected and the 'Show Details' option is selected, then policy details will be displayed. IDS Status is based on a selected TCP/IP stack, summary, TCP or UDP IDS. LogView allows access to log data using the 'trmdstat' command. Using a menu driven interface, input is derived to build the 'trmdstat' commands and display the results.


IDS Policy Administration
CLEVERDetect for IDS Monitor
Policy Agent | TRMD | syslogD
TCP/UDP/RAW
IP/ICMP
OSA Adapter
SIEM or SNMP Command Center
CLEVERDetect for IDS
CLEVER Mobile IDS
HACKER ATTACK
Internal or external hacker
z/OS Console

CLEVER   IBM Business Partner   Microsoft Partner Network   Business Partner hp   redhat READY ISV PARTNER

Applied Expert Systems - The Business Cloud Security Company

Highlights of CLEVERDetect for IDS

The IDS service gives deep visibility into activity allowing it to also pinpoint problems with security policy, document existing threats, and discourage users from violating security policy. Other functions in applications also aid in intrusion detection. Awareness of unauthorized access attempts at logon is another way of understanding potential intrusions.

- **z/OS IDS message capture and transfer** providing immediate insight into malicious activities or policy violations.
- **Mobile and browser interfaces** ensures real-time notification of problems leading to increased Intrusion Detection Service (IDS) activity visibility.
- **Dashboard** providing a high level overview of events monitored.
- **IDS Analyzer** allows events to be viewed with extensive filtering options allowing a reduction of details shown to focus on specific elements.
- **IDS Policy Explorer** displays active policies and their details including policy rule, policy action, or route table names. If specific IDS attack types are selected and the 'Show Details' option is selected, then policy details will be displayed.
- **IDS Status** is based on a selected TCP/IP stack, summary, TCP or UDP IDS.
- **LogView** allows access to log data using the 'trmdstat' command. Using a menu driven interface, input is derived to built the 'trmdstat' commands and display the results.
- Strengthen **z/OS security for File Transfer Program (FTP)** with online FTP session logon failure in real-time and through historical reports.
- Improve operator effectiveness with **integrated Command** functions allowing deeper inspection into potential problems.
- Interrogate **TCP and UDP protocol for IDS attack** detection including malformed packets, violation of outbound RAW restrictions, UDP perpetual echo, and restrictions placed on IPv4, IPv6, ICMP and IP fragments.
- **Transfer IDS messages and FTP Logon Failures** as SNMP traps or syslog messages to Security Information and Event Manager (SIEM) and as notifications to mobile devices.

System Requirements

- **System z:** z/OS V2R2 or later
- **Web Server:**
  - Operating Systems - z/OS V2R2 or later, Windows Server 2016, Windows 10, Red Hat Enterprise Linux 6 or higher, and SUSE Linux Enterprise Server 11 or higher
  - JAVA Platform: WebSphere for z/OS 7.0 or later, Apache Tomcat 7.0 or later, JRE **must** be 7.0 or higher
- **PC Workstation:**
  - : Windows Server 2008 and 2012, Windows 10, 8, or 7, RHEL 6 or higher, SLES 11 or higher
- **Browser Applications:** Internet Explorer 8.0 or later, Edge, Firefox 31 or later
- **Optional feature CLEVER Mobile for IDS System Requirements**
  - **Android:** 4.x or above
  - **iOS:** 5.x or above

AES
P.O. Box 50927, Palo Alto, CA 94303 USA
Phone: (650) 617-2400
Fax: (650) 617-2420
Website: www.aesclever.com Email: info@aesclever.com

Copyright © 2022 Applied Expert Systems LLC. CleverView, CLEVER, CLEVER Mobile, CLEVERDetect, CLEVER TCPIP, CLEVER *e*Route, CLEVER cTrace, CLEVER Buffer, CLEVER Web, CLEVER/SNA and CLEVER ePerformance are registered trademarks of Applied Expert Systems LLC. The IBM logo, Business Partner emblem, zEnterprise, z/OS, and z/VM are trademarks of International Business Machines Corporation in the United States, other countries, or both. The HP Business Partner logo is a trademark of Hewlett-Packard Development Company, L.P. The Red Hat Ready ISV Partner logo is a trademark of Red Hat, Inc. in the U.S. and other countries. Used under license. The Novell PartnerNet Silver Partner logo is a trademark of Novell, Inc. in the U.S. and other countries. Microsoft and the Microsoft Partner Network logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Android is a trademark of Google Inc. iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple under license. Ubuntu and Canonical are registered trademarks of Canonical Ltd. All other trademarks are the property of their respective owners.