



System iNtrusion Analysis & Reporting Environment

SNARE Agent for MS SQL - Release Notes

SnareMSSQL is a program that facilitates the central collection and processing of MSSQL audit records. Log information, gathered from trace files, is converted to tab delimited text format, then delivered over UDP to a remote server.

SnareMSSQL is currently configured to deliver audit information to a SYSLOG server running on a remote (or local) machine. A configuration utility allows you to set the appropriate syslog target and priority, as well as the target DNS or IP address of the server that should receive the event information. It should be noted that many syslog servers are not designed to cope with the sorts of volume of data that multiplesnare agents can potentially generate.

The SnareMSSQL service will automatically start after you have completed the initial configuration process. We recommend that you configure appropriate access control on the SnareMSSQL registry entries using regedt32.exe - perhaps restricting the permission to read or modify the keys and values to Local or Domain Administrators only. SnareMSSQL stores its registry settings in: HKEY_LOCAL_MACHINE\SOFTWARE\InterSect Alliance\SnareMSSQLo 1.5.2.

- SnareMSSQL 0.2 - Beta release
- SnareMSSQL 0.3 - Added filtering for trace events generated by the agent
 - Improved resource handling
- SnareMSSQL 0.4 - Greatly improved functionality including support for named instances and the use of authentication settings
 - Added per-objective trace file handling
- SnareMSSQL 0.5 - Added support for database and instance name
 - Improved event display in remote control interface
- SnareMSSQL 0.5.4 - Recompiled to remove VC80 dependency
- SnareMSSQL 0.5.5 - Fixed bug in trace file management
 - Greatly improved trace file management
 - Minor speedups
- SnareMSSQL 0.5.6 - Added advanced trace filter
 - Added exception reporting to Query Tracking
- SnareMSSQL 0.5.7 - Extended field reporting
 - Expanded objective capabilities
 - Enhanced Error Reporting
- SnareMSSQL 0.5.8 - Fixed user filter
 - Added DatabaseName include/exclude filter
- SnareMSSQL 0.5.9 - Fixed backwards compatibility when updating agent
- SnareMSSQL 0.6.0 - Change Username to reflect LoginName, NTUserName and SessionLoginName added to Strings field. This will ensure SQL logins are captured correctly
 - Added Trace Path override field to Network Configuration
 - Added EventID lookup to remote control interface
 - Added local MSSQL enumeration (instance/DB/table) page to remote control interface
- SnareMSSQL 0.6.1 - Refined "use of user rights" logging, added ability to track Data Manipulation events, with or without tracking SELECT statements
 - Added Permissions field to output
 - Minor wording changes in the remote control interface
- SnareMSSQL 0.6.2 - Greatly improved SQL2000 support
 - Updated instance detection and enumeration
- SnareMSSQL 0.6.2.1 - Updated authentication routine to support Windows Authentication

For more information, contact your SNARE Server Sales Representative

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477 fax
snaresales@symtrex.com
www.symtrex.com
www.snare-server.com



Who's Watching Your Network?



System iNtrusion Analysis & Reporting Environment

- SnareMSSQL 0.7.0.0
 - Added ability to configure trace size, file count and location
 - Added "Audit to local file" feature and configuration options
 - Added ability to pull user names from a given domain group by placing the name in square brackets, e.g. [domain admins]. Currently on startup only
 - Added TDF configuration feature for SMO trace support
- SnareMSSQL 0.7.1.0
 - Added heartbeat capability. Each heartbeat contains a list of the currently monitored instances and their respective SQL versions. The heartbeat interval is variable.
 - Added a variable polling interval for the AD group lookup ability
 - Added ability to include Trace, Service and Debug log information in the regular stream of audit events for logging and analysis
 - Added support for running in a clustered environment
 - Added IA Supported features (e.g. TCP, multiple destinations)
- SnareMSSQL 1.0.0
 - Extended the AD Group Lookup feature to allow domain identification using either Netbios or full DNS syntax, e.g. [FLATNAME\group],[group@dns.name.local]
 - Added silent install features, including encryption of sensitive data
 - Added full cluster installation support
 - Added logging feature to installer
 - Added upgrade only and reinstall options to installer
 - Added /DomainInfo window to check domain trusts and domain controllers
- SnareMSSQL 1.0.1
 - Added the Success field to the capture list
- SnareMSSQL 1.0.1.1
 - Bug Fix, EventID Lookup

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477 fax
snaresales@symtrex.com
www.symtrex.com
www.snare-server.com



Who's Watching Your Network?