



SNIF



Symphion Network Instrumentation Framework

SNIF Configuration Item Reporting Features Overview

SNIF's Comprehensive Configuration Management Database (CMDB) - What is it?

Provides comprehensive web-based current and historical configuration details about all enterprise IP enabled assets. Offers enterprise-wide configuration item visibility and one single view to track and manage it all.

What problems does it solve?

Effective IT organizations must have up-to-date, accurate and accessible inventories and information about all IT assets. Without that information, they encounter problems such as inability to effectively perform essential operations practices, inability to effectively trouble shoot, delayed problem resolution, failure to identify failing components and diminishing or excess capacities and many more scenarios that can cripple organizations. SNIF's advanced scheduler enables periodically scans of the entire enterprise IT asset base (or arbitrary focused groupings of assets or locations) and keeps up-to-date track of all of your asset details and how they change to allow you to significantly reduce problems.

What platforms does SNIF CMDB support?

All IP enabled devices. All vendors. SNIF CMDB supports virtual machines, Linux, MS SQL and Oracle databases.

What are some of the Configuration Item features that SNIF provides and how do you use them?

Upon installation, SNIF™ enables effective daily systems management reporting tasks such as: configuration management, software portfolio management, capacity planning, utilization, security management, network management, database management and trouble management.



S Y M P H I O N

5910 N. Central Expressway
700 Premier Place
Dallas, TX 75206
t. 214.522.4000
f. 214.522.4009
www.symphion.com



Configuration Management

A key tenet of effective desktop and server management is the ability to easily audit enterprise configurations.

SNIF™ provides the configurations of each enterprise device (desktops, servers, network elements, storage area networks, printers and other devices) and allows you to version and compare configurations.

Software Management

Effective and routine software management is an essential IT best practice. Whether managing license utilization of desktop applications or key server OS licenses or auditing to determine where software has been installed or not installed in the enterprise, effective software management is a key component to IT success. SNIF distinguishes and enables various aspects of Software Management. SNIF maintains information about general software and software usage, specific high value software that includes licensing information and the required patches for a healthy, safe, reliable and productive computing environment. SNIF supports many Software Management scenarios. Several of those scenarios are:

- How many licenses of specific software do we own?
- Where are X licenses located?
- How many products of X vendor do we own?
- Has the latest critical patches been deployed to all desktops?
- How many versions of SQL Server are running within the user managed environment?

SNIF™ provides a software library that includes detailed software information both enterprise-wide and for each specific computing device. SNIF™ reports information such as where specific software is used, where it is not used, duplicate licenses, where particular versions are installed, banned software and, for each device, what software is installed, when it was installed, the version installed, when the software was last changed and when the software is running, regardless of manufacturer or version of the software. SNIF™ differentiates between types of software such as operating systems, desktop software, application drivers and patches. SNIF™ has proven especially effective in identifying where important patches have and have not been properly installed.

Capacity Planning

Successful IT best practices include routine enterprise capacity auditing and planning to determine if under or over utilization is occurring.



SNIF™ provides readily available accurate information about enterprise capacity regarding all devices. SNIF™ provides detailed information such as processor utilization, processors per devices, disk capacity and utilization, database sizing, users per domain, devices per domain operating system licenses and, device age and installation date to automate capacity auditing and planning.

Security Management

Security management includes all activities that protect the organization's IT assets from external and internal threats. Successful implementation of enterprise security standards necessarily requires regular management and auditing of those standards. Security management includes providing a complete inventory of devices, comprehensive analysis and disposition of security risks posed by individual devices with open ports, unpatched security holes, open network connections, and enabling user access, identifying unauthorized access, creating and establishing access control lists to give only authorized users access to technical resources, maintaining access control lists and identifying rogue devices not previously known or controlled by IT that pose security risks such as unauthorized wireless devices.

SNIF™ makes security management easier. SNIF™ identifies and inventories all the configurations of all devices on the network and allows managers to identify rogue (and potentially dangerous or unsecure) servers, desktops, network elements and other devices. SNIF™ provides valuable automation to enable IT personnel in regularly auditing against established corporate security standards. With respect to servers and other IP enabled devices in the enterprise regardless of location, SNIF™ provides users with:

- active directory information
- account name, groups
- number of failed log in attempts
- last failed attempt
- open ports (including which device has the open port, remote port information, vulnerabilities per port and port description)
- database accounts
- logged in users
- new IP addresses on the network
- last login
- security patches installed and security logs



Database Management

Effective IT organizations manage their database management systems and respective databases for growth, size, backup schedules, adhering to corporate policies, and user access.

SNIF™ provides administrators and managers with the ability to remotely report on database management systems and their respective databases. SNIF™ provides detailed information about most popular databases including RDBMS configuration, database sizing, database configuration, RDBMS error logs, user access information and provides special support for Microsoft SharePoint™.

Network Management

LAN/WAN network infrastructure management incorporates the design, implementation, administration and monitoring of a company's network infrastructure. SNIF™ affords effective network management by allowing you to define different scanning techniques and characteristics by SNIF™ IP range or by each individual device. SNIF™'s flexibility allows users to manage network segments by enterprise, locations, function or type. SNIF™ users can manage all available IP addresses and report active and inactive (unused) addresses, report device MAC addresses and NIC cards (including speed and manufacturer) and all such metrics as new devices are added to the network. SNIF™ provides NIC errors, protocol errors, primary and secondary DNS server information, and DHCP capabilities by network adapter.

Problem Diagnosis and Trouble Management

Problem Diagnosis and Trouble Management are core IT best practices. In time, all systems will experience some type of breakage resulting from factors such as tampering, mismanagement, end of service life, external disruption, poorly executed implementation or obsolescence. ,

SNIF assists in mitigating disruptive forces in your data center, on your network, with your trading partners and within your end user community. SNIF can assist in averting disaster, in providing key metrics for forensic studies after a disaster and by providing tools to manage to to your service level agreements.

Immediately upon your first enterprise scan with SNIF™, you have a platform



for problem diagnosis and trouble management. SNIF™ provides key diagnostic information such as:

- executing software
- installed software and patches
- services packs, system event log and size
- file system types and errors
- new devices since last scan
- last user login, number of bad logins
- system uptime
- which devices communicate with the device
- allocated IP addresses
- CPU, kernel time of executing software
- system resources such as memory
- disk capacity, utilization
- time of last login attempted
- CPU utilization at time of scan
- open ports
- last communication with device and port used

Some of the questions answered by SNIF are:

- How do we know how many Microsoft Office licenses do we have deployed?
- What software is executing on the end user's machines?
- How much capacity do we have in the data center?
- What is the average uptime of our production servers?
- What wireless devices do we have in our network and where are they deployed?
- Which devices are no longer plugged into our network?
- Which devices participate in delivering a customer service?
- Where do I get the metrics to size my disaster recovery site?
- How many times have there been a failed attempts to log on to our payroll server?
- What software changed on the computer having the problem?
- When was the last patch applied to our SAN farm?

SNIF can help answer these reactive and proactive questions and many more. SNIF's versioned CMDB repository gives everyone easy, accurate, up-to-date information on a need-to-know basis when they need it. It is operational 24x7 collecting data on the schedule that you set. With SNIF's unparalleled performance, if needed, it can scan your entire enterprise several times per day to assist you in detecting and isolating anomalies with the SNIF blueprinted enterprise. With SNIF's comprehensive interface, first response personnel can access its knowledge base and perform like more

