

# StableNet®

## Automated Network & Service Management Overview

### EXECUTIVE SUMMARY

In today's complex network environments, managing a diverse array of technologies and devices from multiple vendors can be a daunting task. Infosim's StableNet offers a comprehensive solution to this challenge by providing automated network and service management that unifies disparate network elements into a single, cohesive platform.

StableNet operates on four foundational pillars: Discovery & Inventory, Configuration & Change Management, Fault Management & Root Cause Analysis, and Performance Management. These cover all aspects of network management, from initial discovery and inventory of network resources to ongoing performance monitoring and fault resolution.

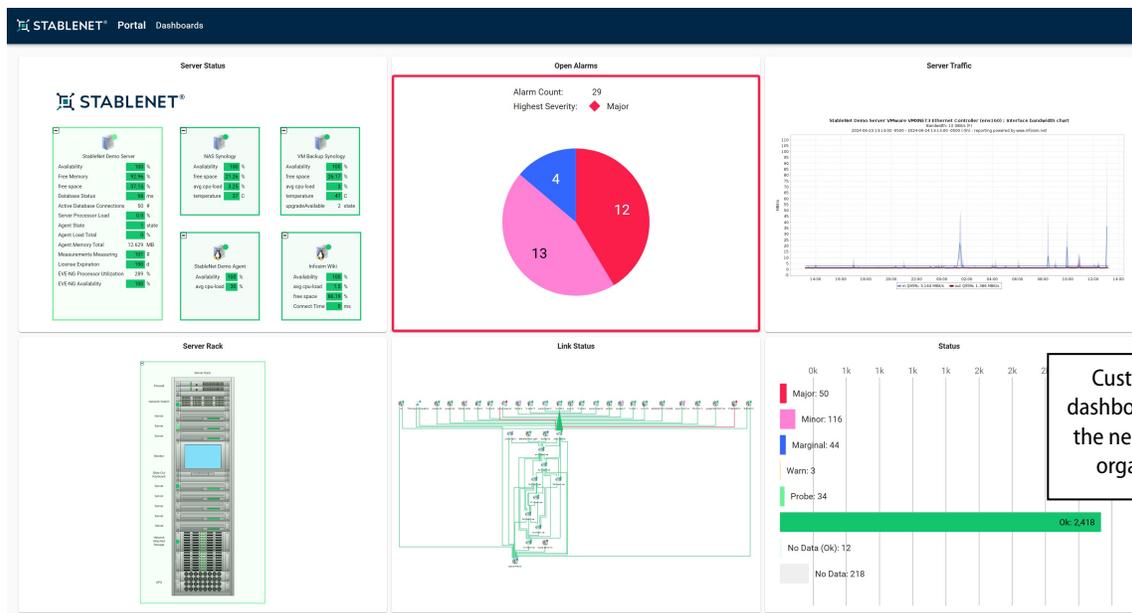
Infosim commissioned Tolly to evaluate the key functionalities of StableNet across these four pillars. The evaluation demonstrated that StableNet excels in providing an intuitive and user-friendly interface, robust automation capabilities, and extensive customization options. See Figure 1 for an example of the customizable StableNet dashboard.

### THE BOTTOM LINE

StableNet comprehensive multi-vendor functionality:

- 1 Automatically identifies and inventories all network resources providing an up-to-date network view
- 2 Eliminates manual configuration errors by automating device management and keeping change history
- 3 Quickly identifies and isolates the root cause of network issues, reducing downtime and improving network and service reliability
- 4 Continuously collects and analyzes real-time and historical performance data across real and virtualized environments

### StableNet Example Dashboard



Customizable dashboard to meet the needs of each organization

Source: Tolly, June 2024

Figure 1

StableNet's ability to integrate and automate critical network management functions makes it an invaluable tool for organizations looking to streamline their network operations, reduce operational costs, and improve overall network reliability and performance.

StableNet provides a comprehensive high-level overview of network performance and utilization through its dynamic visualization capabilities.

The system uses predefined colors to indicate the status of various network elements, ensuring that users can quickly and easily identify issues. For example, green may indicate normal operation, yellow may signal a warning, and red may denote a critical issue. Additionally, the width of the lines representing network links can be adjusted to reflect their utilization levels, with thicker lines indicating higher utilization.

To enhance user interaction and provide detailed insights, StableNet includes a feature where detailed information about a network element is displayed in a window when the mouse hovers over it. This hover-over functionality allows users to access real-time data and metrics without navigating away from the high-level view. The information provided can include metrics such as bandwidth usage, error rates, and latency, among others.

This intuitive and interactive approach ensures that network administrators have immediate access to critical information, enabling them to make informed decisions and respond to issues promptly.

## Test Results

### Discovery

StableNet simplifies the discovery process resulting in improved efficiency for the IT team and a network that remains robust and manageable as it scales.

The natural starting point for automated network and service management is discovery. StableNet agents query LAN segments and attached devices to build up the device inventory for display. StableNet's output is both visual and dynamic - and, thus, static screenshots can not do justice to the system but can provide an introduction to its capabilities.

### Topology

The left side of Figure 2 illustrates an example topology layout generated by StableNet in this test. That layout can be

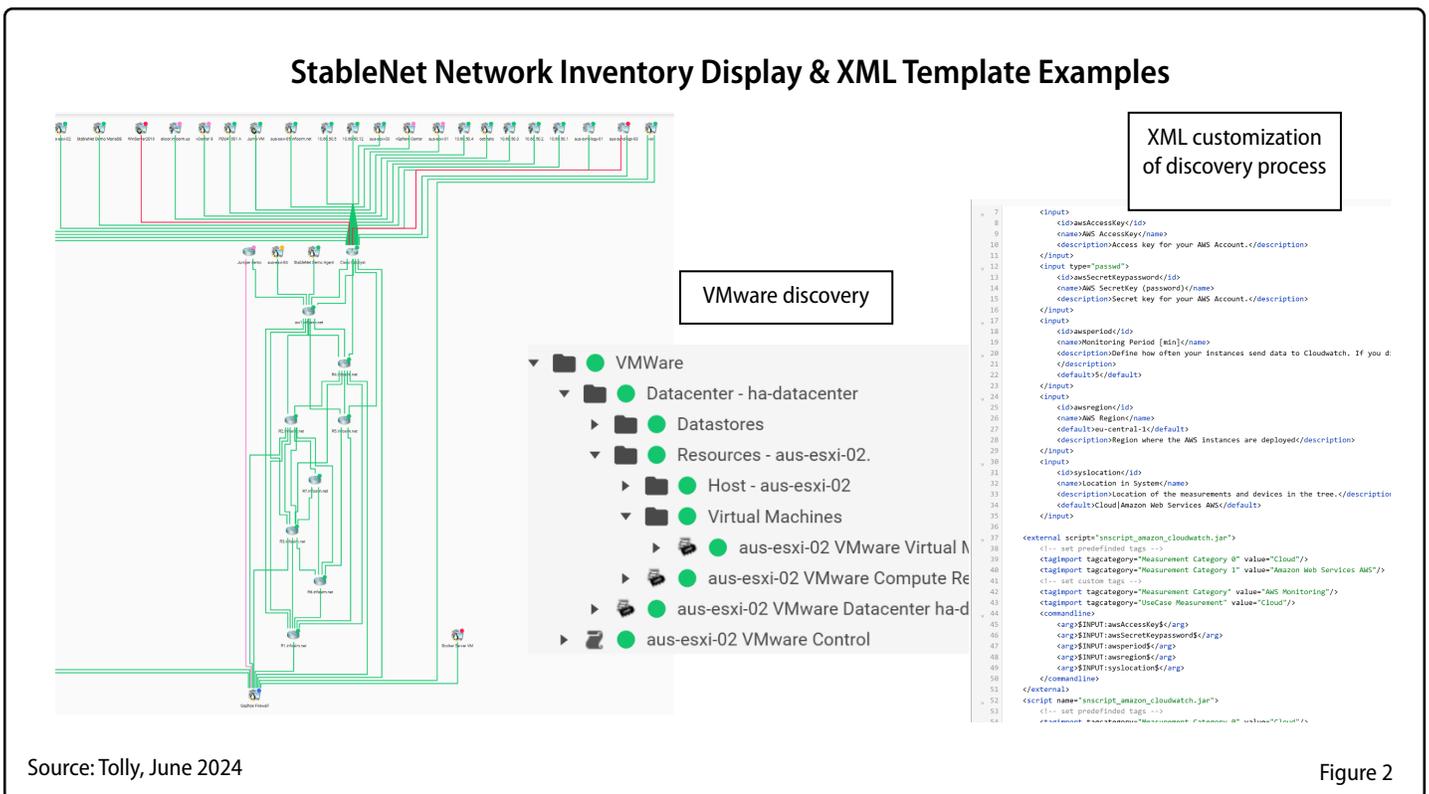


Figure 2



changed with a click to organize devices according to an organization's needs. The line color indicates trouble status.

### Virtualized Infrastructure

Virtualized infrastructure can be found in almost every organization. Thus, it is important to be able to extend discovery to virtualized devices and important resources such as storage. The partial screenshot in the lower middle of Figure 2 illustrates StableNet's ability to query and display VMware vCenter storage information.

### Discovery Customization via XML

The discovery process can be further customized and optimized by using industry-standard XML templates to guide the process. Among other things,

additional parameters and data can be statically mapped to devices and, thereby, become part of the StableNet database.

### Network Configuration & Change

Eliminating error-prone manual device management and configuration is arguably one of the greatest benefits of implementing a network automation solution.

### Configuration Differences

The most essential element of understanding the network is knowing what changed in the configuration of a network device. StableNet keeps a deep backup history of each configuration and

can generate a "Config Diff" dynamically for any device. The upper left side of Figure 3 illustrates one such example.

### Vulnerabilities

Unmediated vulnerabilities in network infrastructure software can open the entire network to attack.

StableNet provides vulnerability analysis for Cisco Systems and Juniper Networks infrastructure. The middle right side of Figure 2 depicts the output of a vulnerability assessment on a Cisco Systems device showing that a Denial of Service (DoS) vulnerability exists on that device.

## StableNet Network Configuration & Change Examples

```

Backup R2.infosim.net (2023-06-28 13:54:56 -0500)
96 -ip ospf 1 area 0
97 -speed 100
98 -full-duplex
99
100
101 !
102 interface FastEthernet0/1
103 -ip address 192.168.1.2 255.255.255.0
104 -ip nbar protocol-discovery
105 -ip flow ingress
106 -ip flow egress
107 -ip ospf hello-interval 1
108 -ip ospf 1 area 0
109 -speed 100
110 -full-duplex
111 !
112 interface FastEthernet1/0
113 -ip address 192.168.100.2 255.255.255.0
114 -ip nbar protocol-discovery
115 -ip flow ingress
116 -ip flow egress
117 -ip ospf hello-interval 1
118 -ip ospf 1 area 0
119 -speed 100
120 -full-duplex
121 !
122 router ospf 1
123 -log-adjacency-changes
124 !

Backup R1.infosim.net (2024-06-07 13:37:57 -0500)
96 -ip ospf 1 area 0
97 -speed 100
98 -full-duplex
99 auto_discovery qos
100 service-policy output DeemQoSPolicy
101 !
102 interface FastEthernet0/1
103 -ip address 192.168.1.1 255.255.255.0
104
105 -ip flow ingress
106 -ip flow egress
107 -ip ospf hello-interval 1
108 -ip ospf 1 area 0
109 -speed 100
110 -full-duplex
111 !
112
113
114
115
116
117
118
119
120
121
122 router ospf 1
123 -log-adjacency-changes
124 !

```

Configuration differences (left) visualizing added (green), changed (blue), and deleted (red) configuration statements

Vulnerability analysis (below) identifying a specific vulnerability in Cisco IOS that needs to be addressed

```

Job Result of Device "R1.infosim.net", Object ID: 114868

## Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Denial of Service Vulnerability
backup not found for Config Snippet "show ip sockets"

target: "show udp", using LINE based structuring ...
show udp (Rev.1)
[no context]
!! missing: ".*17'D.*(500|848|4500|4848).*" (1)

```

### End of Sales/Service/Life (below) for Cisco Systems components

Vendor	Model	Source	Bulletin ID	End-of-Sales	End-of-Service	End-of-Life	End-of-Extended-Service
Cisco	1-100GE-DWDM/C	Cisco - Provided by Infosim	EDL12504	2019-07-30	2020-07-29	2024-07-31	
Cisco	1-100GE-DWDM/C+++	Cisco - Provided by Infosim	EOL19773	2021-08-06	2022-08-06	2026-08-31	2024-08-05
Cisco	01FT562	Cisco - Provided by Infosim	EOL15093	2023-12-19	2024-12-18	2028-12-31	2025-12-18
Cisco	01FT571	Cisco - Provided by Infosim	EOL15093	2023-12-19	2024-12-18	2028-12-31	2025-12-18
Cisco	10C768-DPSK/C	Cisco - Provided by Infosim	EOL9330	2014-02-13	2019-02-28	2019-02-28	
Cisco	10C768-DPSK/C-0	Cisco - Provided by Infosim	EOL8629	2013-03-15	2014-03-15	2018-03-31	
Cisco	10C768-ITU/C EXP	Cisco - Provided by Infosim	EOL13773	2021-08-06	2022-08-06	2026-08-31	2024-08-05

Source: Tolly, June 2024

Figure 3

## EoX

Given the number of different devices and components in most network, keeping track of when products are no longer sold or supported can be an arduous task.

For Cisco Systems and Juniper Networks devices, StableNet maintains information on its database that can immediately inform the user of end-of-sales, end-of-support, and end-of-life for various products and components.

## Fault Management & Root Cause Analysis

Even the best managed network will experience problems from time to time - whether it is an interface failure, remote link, or some other issue. Responding to

that failure and remediating the situation is always the top priority.

### Root Cause

Even in simple networks, it is easy for a problem to become hidden as one failure typically triggers many more alarm or error conditions. Determining the root cause of the problem is essential to fixing the problem.

To test StableNet's root cause analysis capabilities, engineers disabled one interface of a Cisco Systems router.

Within a few seconds, StableNet identified the root cause correctly to be the interface that was intentionally disabled. The upper part of Figure 4 illustrates the "drill down" to the root cause which was identified by its object ID of 16409 which is circled in the screenshot.

Infosim

StableNet

Automated  
Network &  
Service  
Management

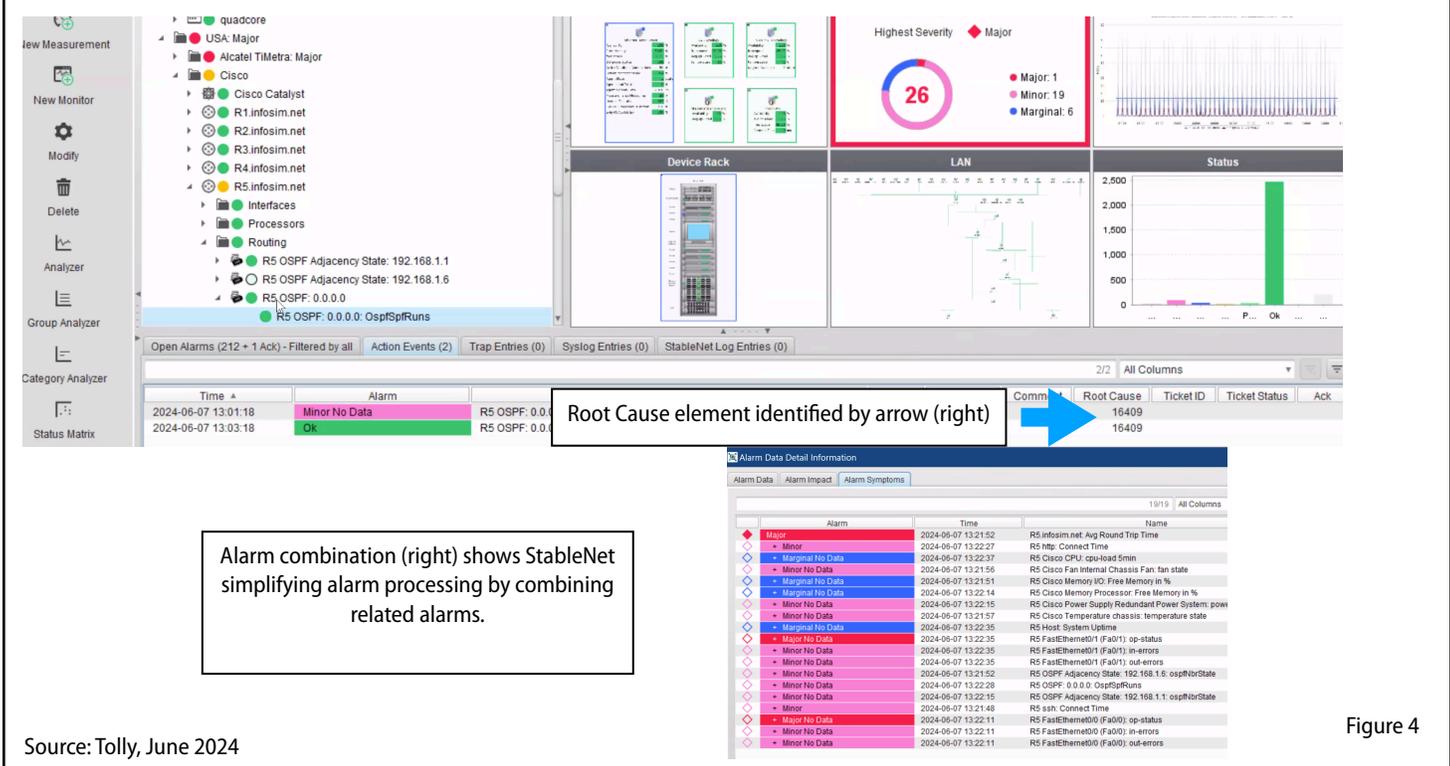


### Combined Alarms

One failure will typically cause multiple alarms as various elements being monitored are no longer reachable by the agent. Systems that only show each alarm as a separate event can make for a challenging management environment.

Intelligence in StableNet allows the system to group or combine alarms such that subsidiary alarms can be grouped under a

### StableNet Fault Management & Root Cause Analysis Examples



Source: Tolly, June 2024

Figure 4

heading for a major alarm that dramatically simplifying what the network manager has to view. The lower part of Figure 4 illustrates that capability.

### Alarm Customization

StableNet provides for extensive customization of conditions that will trigger alarms.

Alarms can be generated at various severity levels and trigger notification emails to the appropriate network management team members.

### Performance Services

User service level agreements, formal or informal, ultimately involve performance. Network components need to be shown to be delivering sufficient bandwidth and, thus, acceptable response time.

StableNet agents poll devices and StableNet server collects real-time and historical data in its database. That data are used dynamically by StableNet to provide insights into network performance from a “birds-eye” view down to details of traffic on individual interfaces of devices.

### High-Level Overview

The high-level view is shown in the left side of Figure 5. Here, StableNet provides an overview of link utilization between core networking equipment and a central switch.

### Low-Level Drill Down

Similarly, the data measurements stored by StableNet can be used to provide detailed traffic measurements down to the network interface level.

The right side of Figure 5 shows the inbound and outbound traffic loads for selected interfaces on a router.

## Test Setup & Methodology

### StableNet Overview

StableNet Server is the “brain” of the system. It processes and presents data, manages the database, and communicates with both end users and agents. It is deployed as software on a server and uses a relational database to store its information. Linux and Windows are supported server platforms. OracleDB and MariaDB are supported database environments and are provided by the customer.

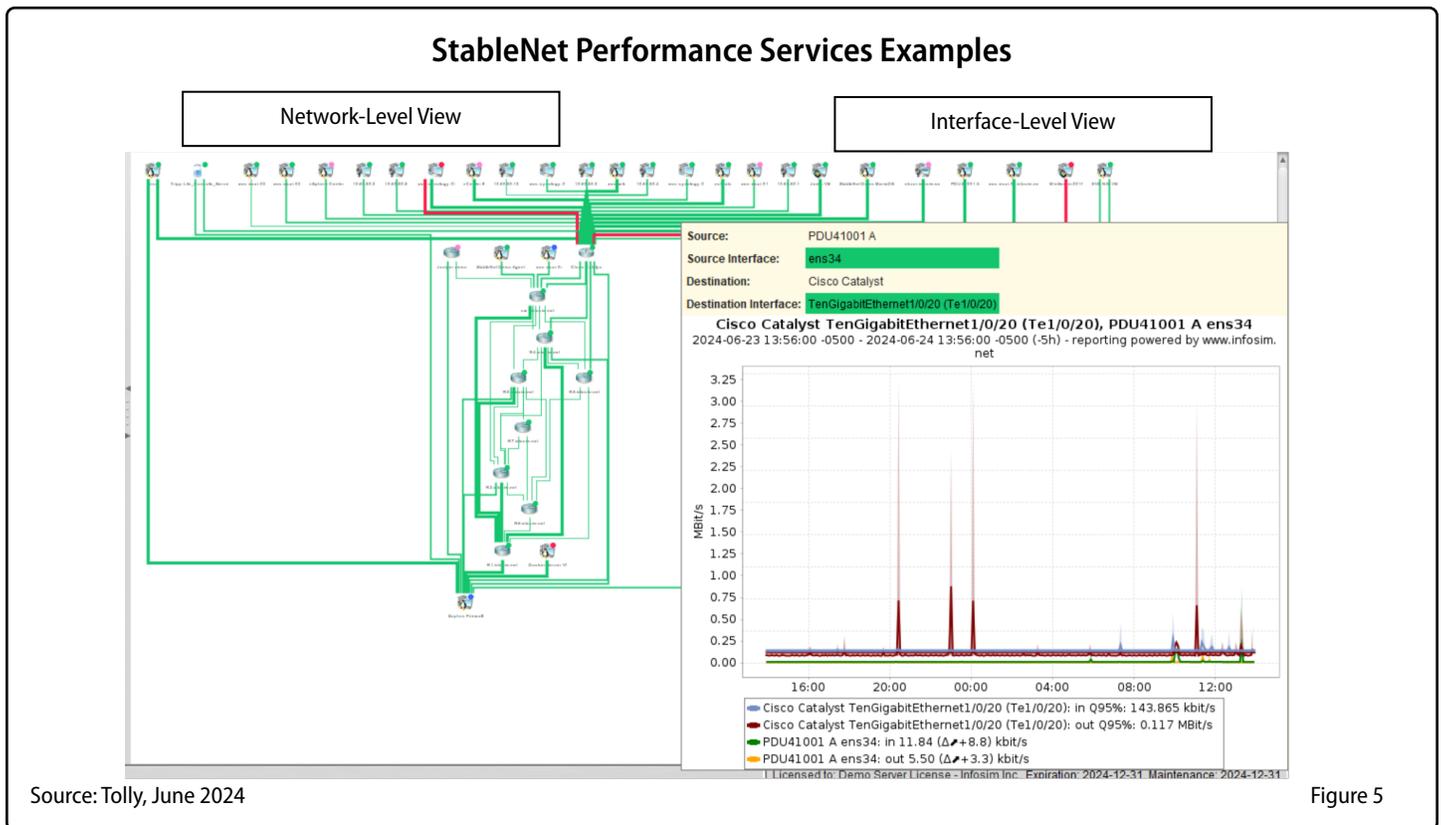


Figure 5



## StableNet High Level Overview

StableNet® by Infosim addresses the most pressing pain points faced by network managers through its comprehensive, unified approach to network and service management. The platform's four foundational pillars—Discovery & Inventory, Configuration & Change Management, Fault Management & Root Cause Analysis, and Performance Management—are designed to tackle key challenges:

**Alarm Floods:** StableNet®'s advanced alarm management capabilities intelligently group related alarms, reducing noise and simplifying the identification of critical issues.

**Network Visibility:** Automated discovery and dynamic topology mapping provide a clear, real-time view of all network resources, ensuring managers always know what is on the network.

**Multi-Vendor Integration:** By consolidating data from multiple vendors into a single platform, StableNet® streamlines problem tracking and root cause analysis, eliminating the need to switch between multiple applications.

**Configuration Management:** Automated configuration and change management features, including configuration backups and dynamic "Config Diff" analysis, minimize errors and ensure network stability.

**Data Presentation:** Customizable dashboards, weather maps, and detailed reports offer intuitive and flexible data presentation, enabling network managers to access the information most relevant to their roles quickly.

By integrating these critical functions into one cohesive application, StableNet® simplifies network management, enhances operational efficiency, and improves overall network reliability, making it an indispensable tool for modern network operations.

Source: Infosim, June 2024

StableNet gathers information and interacts with network devices via StableNet agents. Agents are implemented in software (Linux or Windows) and are the intermediary between network endpoints and the StableNet Server. As there is no "per agent" charge, customers can deploy agents as they see fit on their networks.

StableNet provides a Java-based GUI that can run on Windows or Linux. StableNet also offers a web-based portal that provides nearly the same feature set and is moving towards feature parity.

Rather than charge "by device" monitored, StableNet takes a different approach. InfoSim charges by "measurements" - a measurement being any particular element that is being monitored. Customers can

assign their quota of purchased "measurements" to any attributes of any devices and can re-assign them at any time.

## Test Environment

StableNet 24 Service Pack 3 was tested along with MariaDB version 10.4.25.

The environment consisted of a multiple LANs that had connections to Cisco Systems, Juniper Networks, and other vendor devices. Devices were real and virtualized with routed interfaces to adjacent LANs.

## Test Methodology

The tests run for this test are self-explanatory and do not require a formal methodology.



## About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 35 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at [sales@tolly.com](mailto:sales@tolly.com), or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:  
<http://www.tolly.com>

## Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

js-1-wt-2024-06-26-VerF