# Stratusphere™

## *Security Overview*

## Introduction

This guide has been authored by experts at Liquidware in order to provide a security overview of Liquidware's Stratusphere™ product, the leading product for VDI Assessment and Diagnostics. This paper is intended for IT Security and Operations audiences who want to understand the product from a security perspective within their IT environment.



**Liquidware Labs, Inc.**
3600 Mansell Road
Suite 200
Alpharetta, Georgia 30022
U.S.A.
Phone: 678-397-0450
www.liquidware.com

# Contents

**STRATUSPHERE OVERVIEW** ..... **3**

**STRATUSPHERE VIRTUAL APPLIANCES** ..... **3**

ACTIVATION AND SECURE INTER-COMPONENT COMMUNICATIONS ..... 3

**CONNECTOR ID KEY** ..... **5**

**DATA PRIVACY STATEMENT** ..... **5**

# Stratusphere Overview

Stratusphere is certified for use with VMware, Citrix, Microsoft, KVM, Nutanix, and Amazon desktop virtualization platforms, and is compatible with other desktop virtualization components such as third-party brokers. It is downloadable from the Liquidware website. The product includes three virtual appliances (pre-packaged and self-contained VMs), the Stratusphere Hub, Database and the Collector, and a software agent called the Connector ID Key that is delivered along with the Stratusphere Hub.

# Stratusphere Virtual Appliances

The Stratusphere Hub, Database and Collector virtual appliances are based on a hardened stripped-down version of the CentOS 6 Linux 2.6 Operating System. Only essential software modules and services are retained onboard the appliance with all other nonessential service modules being removed. Access to the Stratusphere Hub virtual appliance and administrative functions is provided through a web browser interface that is SSL encrypted and requires a user id and password to access. In addition, all Stratusphere virtual appliances have a command line console for appliance administrative controls, which is also password protected.

All communications between the Stratusphere components are encrypted using PKI infrastructure, where the Stratusphere Hub is the Certifying Authority generating public and private key certificates for itself and each of the components (Collectors and Connector ID Keys on individual machines).

## Activation and Secure Inter-Component Communications

Secure communications among the separate components of Stratusphere serve as a basis for communicating configuration and policy changes among those components and for establishing or obtaining identities or other data necessary for the functioning of the system. The communications between all components – Connector ID Keys to Hub/Collectors and between Hub and Collectors - uses straight SSL (TCP/443) with TLS 1.2.

All policy configuration information on machines with Connector ID Keys and inside Stratusphere Collectors is stored within X.509 certificates.

Steps for establishing and conducting secure inter-component communications are as follows:

1. Each component generates its own private-public 2048-bit RSA key pair. Using the standard SSL (TCP/443 using TLS 1.2) based secure communication channel, the Connector ID Keys and the Collectors connect to the Stratusphere Hub and provide their own public keys to the Stratusphere Hub for identification purposes for all future communications. As part of the same connection, the Connector ID Keys and Collectors receive the Stratusphere Hub's public key as part of a secure registration process.
2. Once a Connector ID Key or Collector has registered with the Stratusphere Hub, the Hub generates an X.509 certificate for each Connector ID Key and each Collector. The Hub signs the certificate with its private key and transmits it to the Connector ID Key or Collector as part of the activation process. The recipient Connector ID Key or Collector confirms that the certificate came from the Hub using previously obtained public key of the Hub. The certificate contains policy and configuration information. It may be updated periodically and sent to components at configured intervals.
3. Once activated, all ongoing communication between the Stratusphere Hub and the Connector ID Keys and Collectors is secured using SSL (TCP/443 with TLS 1.2). Each message is signed with the sender's private key allowing the recipient to confirm that it came from the identified sender.

Stratusphere virtual appliances do not actively ping, scan or broadcast traffic to any parts of the network. Stratusphere is a passive data collection system that only communicates among its own components (aside from specific import capabilities from management systems such as VMware vCenter, Active Directory, etc. which are also secured).

The following ports and protocols are used by Stratusphere 6.x:

- **TCP/22** : Stratusphere Hub, Database, and Collector Appliance SSH Console Management Interface.
- **TCP/443** : Stratusphere Hub Web User Management Interface.
- **TCP/443** : Connector ID Key communications.
- **TCP/443** : Collector communications.
- **TCP/5432** : Stratusphere Database appliance listening for database communication from Hub.

The following ports and protocols are used by legacy versions such as 5.x and older:

- **TCP/5501** : Stratusphere Hub listening for Connector ID Key communications (legacy).
- **TCP/5502** : Stratusphere Hub listening for Stratusphere Network Appliance communication (legacy).
- **TCP/5502** : Stratusphere Network appliance listening for Network Monitoring Policies from Hub (legacy).

The Stratusphere Hub can be configured to import information in a strictly read-only mode from enterprise infrastructure servers such as LDAP name stores (Microsoft Active Directory), VMware vSphere, and Nutanix Prism. If email based alerting is required it can also be configured to connect to a Mail Relay Server (Microsoft Exchange) to send out email alerts. The same alerts are also available to be sent to other systems monitoring solutions or via Stratusphere's secure RSS feeds (requires authentication with an administrator name and password to access).

Software updates and patches are provided by Liquidware only. Liquidware customer support will notify customers when there is an update available. Administrator username and password authentication is required for upgrades. The Stratusphere Hub can be updated with an automatic pull from the Liquidware web site, and Collectors and Connector ID Key updates can either be automatically controlled through the Hub administrative interface or delivered through other software update or patch control services.

The Stratusphere appliances can be configured to enable password complexity requirements on the Web User Interface as well as the Console Management Interface to comply with any organization's policies. It also supports secure certificate based access to existing infrastructure servers such as Active Directory, VMware vCenter, etc. The Web Server can also be configured to accept a SSL Certificate to guarantee the identity and owner of the website and application.

The Stratusphere appliance maintain keys and ciphers that comply with US Government's Department of Defense guidelines and is awaiting certification from Defense Information Systems Agency (DISA) Allowed To Operate (ATO) certificate for its CentOS based appliances that incorporate more than 700 Federal Security Technical Information Guides (STIGs).

The Stratusphere Hub, Database, and Collector Appliances all communicate securely with each other to maintain security and integrity with all data in motion. The Stratusphere Database appliance also provides options to encrypt data at rest. It can be configured to encrypt the entire disk to protect information at rest as well.

## Connector ID Key

The Connector ID Key is installed on a physical desktop or within a guest virtual machine's operating system. Stratusphere currently supports current versions of Microsoft Windows, MAC OS X & macOS, and Linux including Red Hat, CentOS, and Ubuntu distributions. The Connector ID Key installation requires administrative privileges. The software runs as a service in the operating system that is configured to start automatically. Once installed, the Connector ID Key automatically registers the machine (and the currently logged in user) with the Stratusphere Hub and receives an X.509 certificate back from the Stratusphere Hub. This certificate is non-transferable and is specific to the machine (physical or virtual) where it was generated. The CID does not listen on any ports; it only sends information to the Stratusphere Hub on the secure channel (TCP/443).

The Connector ID Key functions are controlled by administrators through the Stratusphere Hub. When configured to monitor the machine configuration and processes, the Key sends information back to the Stratusphere Hub on a configurable frequency. Also, when installed and configured, the prior versions of the Advanced version of the Connector ID Key embeds the identity of the user and machine on every network connection to uniquely and irrefutably identify the initiator of the connection (providing "Caller ID" for computer networks). For more details on this protocol and Connector ID Keys in general, please refer to the Stratusphere architecture white paper.

**Privacy:** The CID Key is not designed to collect passwords, nor personal information, nor patient health information, and nor credit card information. It does not keep track of the names of files or documents accessed or opened.

## DATA PRIVACY STATEMENT

Stratusphere is first and foremost a user experience-focused solution that uses resource utilization and performance metrics associated with users, machines and applications within the virtual architecture. Stratusphere gathers information and metrics on physical and virtual workloads, including details such as CPU and memory utilization as well as details on network and storage throughput. As noted above, Stratusphere accomplishes this task using virtual appliances and CID Keys.

While the Stratusphere solution can examine network packet header information (such as source and destination address details), at no time does Stratusphere expose network payload data—when organizationally required, the ability to track IP addressed can be disabled by the Stratusphere administrator. Stratusphere also gathers and provides information regarding desktop applications and processes, as well as relevant network applications and services to ensure appropriate performance and end user experience indicators are met. That said, at no time does Stratusphere examine specific data related to user-generated content. Related, Stratusphere does not capture any keystroke details, such as passwords, or accessed filenames. Further, all collected details remain within Stratusphere; no information or metrics are uploaded to any external location.