Stratusphere™

Architecture Overview

Introduction

This guide has been authored by experts at Liquidware to provide an architecture overview of Liquidware's Stratusphere™ product, the leading product for Assessment and Diagnostics. This paper is intended for technical audiences who are already generally familiar with Stratusphere and the functions it provides.

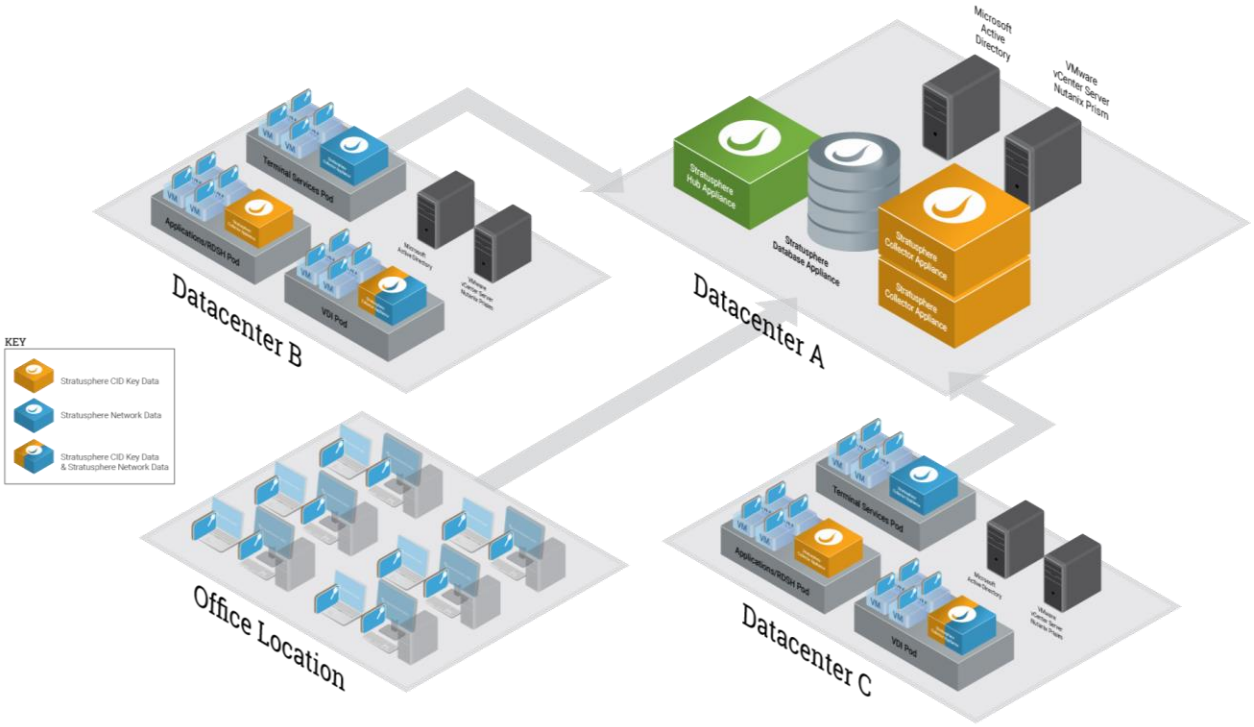
Liquidware Labs, Inc.
3600 Mansell Road
Suite 200
Alpharetta, Georgia 30022
U.S.A.
Phone: 678-397-0450
www.liquidware.com

Contents

Stratusphere Product Architecture & Components

Stratusphere is designed for use with most popular virtualization platforms including VMware, Citrix, Microsoft, KVM, Nutanix, and Amazon Web Services desktop virtualization platforms. It is available for download from the Liquidware website. The product includes three virtual appliances (pre-packaged and self-contained VMs), the Stratusphere Hub, Stratusphere Database and the Stratusphere Collector, and a software agent called the Connector ID Key that is delivered within the Stratusphere Hub.

Here is high level architecture diagram of Stratusphere:



- **Stratusphere Hub** —delivered as a virtual appliance (pre-configured VM), provides the central policy management, policy distribution, data collection, reporting and alerting system for Stratusphere. The main interface is accessed through a standard web browser, and the virtual appliance also has a command line console for appliance setup and administration.

- **Stratusphere Database –** delivered as a preconfigured virtual appliance, provides the central data storage option for the Stratusphere product line. This appliance is used for high performance architecture for larger number of desktop deployments. The Stratusphere Hub appliance saves all the data it received from other components into the database appliance.

- **Stratusphere Collectors**— delivered as a virtual appliance, provides the ability to collect CID Key data and network monitoring data for Stratusphere. The Stratusphere Collector appliance can collect CID Key Data, or Network Data or in small environments both forms of data. The CID Key Collector, can handle between 5-10K CID Keys calling back every hour. It is deployed in pairs to provide a form of high availability and redundancy for data collection. A single Stratusphere installation by default supports up to 10 CID Key Collectors. The Network Collector, is typically deployed one per virtual host where virtual desktops reside. Connected to the virtual switch and configured for passive monitoring, it tracks network latency, response

times and bandwidth consumption, enhanced by the user and machine information provided by the Advanced Connector ID Keys. The Collectors are controlled and managed by the Stratusphere Hub.

- **Connector ID Keys**—a small-footprint software agent installed on physical or virtual machines to gather end user experience metrics, endpoint configuration, and resource utilization & performance data. Its Advanced version is used to add tracking information to network connections to allow detailed monitoring of network latency, response times and bandwidth consumption per machine and per user. Connector ID Keys are managed through the Stratusphere Hub. Versions are available for 32-bit and 64-bit Microsoft Windows, Apple MAC OS, and for other Linux distributions such as RedHat, SUSE and Ubuntu.

Stratusphere Hub

The Stratusphere Hub virtual appliance is architected using an open source software stack. It is built using a hardened Linux 2.6 kernel OS, and uses Apache/Tomcat and Wicket for the user interface, PostgreSQL for configuration and audit data storage, and BIRT for report generation.

The Stratusphere Hub includes the following functions:

- **Web UI, Dashboards, Search-** provides ability to interact with the data & metrics collected, render it for display within UI & Dashboards, and provide searching ability for users, machines, application processes etc. across all the data collected.
- **Integration with Active Directory and LDAP**—optionally configure scheduled imports from directory server to obtain user group definitions, allowing user groups to be used for report and alert filters and policy rules.
- **Integration with VMware vCenter & Nutanix Prism**—optionally configure scheduled imports from VMware vCenter and/or Nutanix Prism to obtain machine grouping definitions (including host assignments, resource pools and folders), allowing these groups to be used for report and alert filters and policy rules. Also imported are the SAN and LUN mappings, used by Stratusphere for storage reports and alerts.
- **Policy Definition**—define rules for required service levels, performance monitoring, security validation, even environment usage billing, and automatically distribute policies to all Connector ID Keys and Collectors. Policies can easily be exported, imported, backed up or restored.
- **Stratusphere API, Reporting and Alerting**—API access, interactive dashboards and reports, configurable alerts, scheduled reports including report review and approval workflow. Create and save report filters. Customize reports or alerts using BIRT open source report designer. Alerts can be delivered via email, and secure RSS feeds are available for alerts and scheduled reports for integration with other systems (more below).
- **Administrative Change Log**—complete log of all system events and administrator actions, so that policy changes and administrative actions in Stratusphere can be audited and system errors can be quickly detected.

Security and Access Control

The Stratusphere Hub is built using a security modified Linux kernel. Access to the appliance functions is only through the browser user interface and the console interface, both of which require an administrator user name and password. Administrator names and passwords are set securely within the administrator user interface. In addition, a very limited number of channels are open for the communications with Connector ID Keys and Collectors. As described previously, these channels are secured and encrypted.

Data Collection

The Stratusphere Hub aggregates and stores the data collected from Connector ID Keys and Collectors. The data is stored in the Postgres database, which is used for reporting and alerting. The Postgres database sits on its own data partition.

The Stratusphere CID Key Collectors receive data from CID Keys and store it on a FIFO disk based queue. The queue is processed, and data is stored into the Stratusphere Database directly. Stratusphere Network Collectors sniff network traffic and attempt to send their data to the Stratusphere Hub once a minute. The Stratusphere Hub receives this network data and stores it into the Stratusphere database. By default, the Connector ID Keys send their data once an hour. The timing of delivery can be adjusted in the Hub's administrator interface. The Stratusphere Hub & Collector have a pool of threads to receive incoming data. In cases where the Stratusphere Hub or Collector are too busy or unavailable, the components will store data and attempt redelivery later. In most environments, components will be able to store up to two weeks of data without contacting the Stratusphere Hub, without any data loss. The method also allows for data collection on machines that are not always connected to the corporate network, such as notebooks.

The amount of data stored will vary based on size of environment, the configuration settings and the amount of activity in the environment. The Stratusphere Hub disk storage space can be adjusted using standard means for a virtual machine. For sizing guidelines, see the Stratusphere Sizing Guide.

The Stratusphere Hub includes many features to manage the collected data. This includes the ability to:

- Export manually through the Inspectors, Reporting and API
- Roll-up and summarize data from callback level detail to summarized by day, week, month, and year for faster performance and long-term retention.
- Ability to set auto-delete policies for data over a certain age, or to set auto-delete when the storage amount reaches a certain threshold. Auto-deletion policies also apply to saved alerts and scheduled reports.

Integration with Other Systems

As mentioned above, the Stratusphere Hub provides integration with Active Directory, LDAP, VMware vCenter, and Nutanix Prism. The Stratusphere Hub also includes the following options for integration with other systems, including systems management products or IT help desk systems from vendors such as IBM, HP, BMC and NetIQ:

- **SNMP Alerts**—alerts can be delivered to other systems using SNMP. The SNMP delivery mechanism is a small software agent that can be installed on any server, and that pulls alerts or other information from Stratusphere Hub through the secure RSS feeds.
- **Secure RSS Feeds**—secure RSS feeds are available for alerts, scheduled reports and the administrative change log. Using the RSS feeds, administrators can receive notification in standard RSS readers. Furthermore, it is straightforward to write connectors that pull information from Stratusphere RSS feeds and push them into other systems or applications. For example, Stratusphere performance data reports could be connected to an enterprise portal.

Stratusphere Database Appliance

The Stratusphere Database appliance is used when the number of CID Keys deployed on machines exceeds 500-1000 installations. To provide high performance and enhanced usability, the Stratusphere product can scale better by storing its data from an internal built-in database to an external appliance based database. This appliance is a simple, software-only, stripped down Linux based platform with Postgres RDBMS deployed. The Database appliance is configured to communicate with the Stratusphere Hub based on secure password authentication and key material exchange. The Stratusphere Hub connects to the Stratusphere Database appliance using the TCP protocol on port 5432 on which the Postgres Database process is listening.

Stratusphere Collector Appliance

The Stratusphere Collector appliances are responsible for CID Key data collection & insertion, network monitoring, gathering detailed information on network latency, response times and bandwidth consumption. Collectors are architected using an open source software stack. They are built using a hardened Linux 2.6 kernel OS and network packet filtering libraries from netfilter.org. They are managed centrally through the Stratusphere Hub, and can be locally managed through a command line interface.

Stratusphere Collector appliances can operate in the following roles:

1. CID Key Collectors
2. Network Collectors
3. CID Key & Network Collectors

CID Key Collectors

CID Key Collectors are designed to collect incoming CID Key data for higher scale and performance of the Stratusphere installation. They free up resources on the Stratusphere Hub to mainly be the UI, Reporting, Alerting, and API engine for the installation. CID Keys are designed to report to the Hub for registration purposes. Once a CID Key Collector is deployed, the CID Keys are directed to begin uploading data to the CID Key Collectors instead of the Hub. If there are multiple Collectors, the CID Keys randomly select one from the list, and then round robin to the rest of the Collectors in the list providing load balancing and redundancy in case of failure. Multiple sets of CID Key Collectors can be deployed in various data centers to collect data from CID Key in that data center or region, and insert it into the central Stratusphere Database. A single Stratusphere installation is configured to handle up to 10 CID Key Collectors by default. Each CID Key Collector configured with 2 vCPUs and 4 GB of RAM, can handle between 5-10K CID Key callbacks/hour.

Network Collectors

Network Collectors are designed to monitor and audit high volumes of network traffic with extreme efficiency. They connect to the virtual switch for passive monitoring, and a single Collector can monitor multiple virtual switches or even monitor traffic rerouted from a physical switch via a network tap. With only a 1 GB memory footprint, and typically consuming less than 1% of the CPU resources of a dual-CPU virtual host, Collectors can typically monitor and audit more than 5,000 packets per second without missing packets. Collectors auditing activities and granularity of data collected is defined by policies in the Stratusphere Hub. The collected data is stored on the Collectors in binary format, and is transferred securely to the Stratusphere Hub at regular intervals, by default once every minute although the frequency of transfer can be changed by administrators.

Network Collectors can capture key information critical to ensure consistent operations and diagnose performance in virtual desktop deployments. The information gathered includes:

- **Network Latency**—calculated via network roundtrip time (NRT)
- **Application Response Time**—per connection response times
- **Bandwidth consumption**—detailed KB/s for all network activity and desktop streaming
- **Failed and dropped connections**—detect network or application problems
- **By user, by machine**—detailed tracking by user and machine, critical for comprehension

Network Collectors can monitor TCP and UDP connections, and all desktop streaming protocols including RDP, ICA, PCoIP, and ALP. The type and granularity of monitoring data collection is controlled by policies in the Stratusphere Hub.

CID Key & Network Collectors

The Stratusphere Collector appliances can operate in a dual mode to collect CID Key data and network data on a host's virtual switch. Liquidware recommends using dual role Collectors ONLY if you have a small environment with less than 5-10 hosts. As mentioned above, a single Stratusphere installation does NOT support more than 10 CID Key Collectors or Dual Role Collectors by default and would require changing internal settings within the database.

Connector ID Keys

Connector ID Keys are small footprint software agents that are responsible for gathering user experience metrics, machine hardware configuration information, software inventory, and collect detailed resource utilization & performance data on user and application activity. The software agent and associated elements, including diagnostic utilities, requires approximately 5 MB of disk space. Connector ID Keys are available for Windows, Apple and Linux machines.

The Standard version of the CID Key has three services that start and stop with the machine. The main service as mentioned above is responsible for gathering user experience metrics, machine hardware configuration information, software inventory, and collect detailed resource utilization & performance data on user and application activity. The user identification service is responsible for gathering user credentials, monitoring user logons and application processes, and communicating with Stratusphere Hub. The final portion, the update service, is responsible for obtaining software updates from the Stratusphere Hub when they become available (auto-update of Connector ID Keys is controlled by administrators in the Stratusphere Hub).

Using the Stratusphere Hub, administrators can configure individual or groups of Connector ID Keys. Features can be individually enabled or disabled, and the frequency of callbacks to Stratusphere Hub or Collectors can be set.

If CID Key Collectors are deployed within the environment, the CID Keys can be configured to callback to a group of CID Key Collectors globally or by individual machine groups. The CID Keys receive a list of these Collectors from the Hub and then start calling back to the CID Key Collectors instead of the Hub. The CID Keys randomly select a Collector from the list to start with, and then round robin through the list from that point forward. If a Collector is not available, it simply moves to the next Collector in the list. If no Collectors are available, then the CID Key falls back to the Hub in a last-ditch effort to upload data. If the Hub is not available either, then the CID Keys go into a back-off algorithm to keep checking back with the Hub or Collectors to see if they are available. When the Hub or Collectors are available again, normal operations are automatically resumed.

The CID Keys can be configured to store collected data locally if the machine is running offline or the Hub or the Collectors are unavailable or inaccessible. It is configured by default to store up to 14 days of data until it starts purging it in a FIFO queue. When the machine comes online again, or the Hub or Collectors are available or accessible again, the CID Keys are configured to upload queued data in a LIFO order to include the latest callback data along with 4 queued callback reports.

Connector ID Keys can collect a variety of data elements that are important to assessments, diagnostics, or both, including:

- **Machine configuration and age**—devices, CPU, memory, drives, and age
- **Application inventory**—versions and patch information for OS and used applications
- **User Logon Time, Delay, and Breakdown** — time, delay, all internal processes in each user logon
- **User Types**—detect administrator privileges for individual users
- **Application Load Time**—the time it takes an application to fully initialize
- **User and Application Resource consumption**—CPU, memory, disk, network
- **Non-responding Applications**—detect when applications are not responding
- **GPU & GDI utilization** —tracking the level of graphics for each process, user, and machine
- **Resource Utilization of each user, machine and application**
- **Performance Numbers of each user, machine, and application**
- **Browser metrics** - Internet Explorer, Google Chrome.
- **Display Protocol** – Microsoft Remote Display Protocol (RDP/RFX), Citrix ICA/HDX, PCoIP.

The rarely used Advanced version of the Connector ID Key also adds information on network packets to allow tracking of network latency, response times and bandwidth for individual users, machines and applications. The network driver portion of each Advanced CID Key is inserted into the IP packet processing stack of the operating system, and takes care of adding the tracking information to TCP and UDP network connections (described in detail in section below).

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

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 use public-private key cryptography and key exchange following the Diffie-Hellman model, where the key generation and exchange happens automatically and is hidden from users of the system.

All policy configuration information on machines with Connector ID Keys and inside Stratusphere Collectors is stored within encrypted X.509 certificates. The encryption relies on the public-private keys generated and exchanged during the activation process.

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. Through a secure activation process, the Stratusphere Hub obtains the public key for all Connector ID Keys and all Collectors and gives its public key to each component.
2. The Stratusphere Hub generates an X.509 certificate for each Connector ID Key and each Collector. The certificate is encrypted using the public key of the Connector ID Key or the

Collector, so that only those components can decrypt it, and it is signed with the Stratusphere Hub's private key. The recipient confirms that the certificate came from the Hub using the Center's public key. The certificate contains policy and configuration information, and may be updated periodically and sent to components at configured intervals.

3. Once activated, all communication between the Stratusphere Hub and the Connector ID Keys and Collectors is secured using the private-public keys and the FIPS-compliant 128-bit AES block cipher encryption algorithm. Each message is encrypted using the recipient's public key so that only the intended recipient can decrypt it, and it is signed with the sender's private key allowing the recipient to confirm that it came from the identified sender.

Connector ID Patented Technology

This section describes the elements of the patented Connector ID protocol that is used by Stratusphere to track user and machine activity more reliably and efficiently inside the virtual network.

User Tracking

User tracking starts by assigning a unique number to each user. User identification is a two-step process conducted by a Connector ID Key in conjunction with the Stratusphere Hub. The steps are:

1. Obtain for each outgoing TCP or UDP connection attempt the fully qualified domain name (or its equivalent) of the active user account initiating the connection attempt through inquiry of the host operating system; the fully qualified domain name is guaranteed to be unique in the domain where it is registered;
2. Associate the fully qualified domain name of the user with an identifier, issued by the Stratusphere Hub, that is unique within a given environment, so that no two users are ever granted the same identifier.

The fully qualified domain name of the active user may be obtained at the startup of the Connector ID Key or upon first detection of outgoing TCP or UDP packets by querying the host operating system. For every outgoing TCP or UDP packet, the Connector ID Key checks the associated user account (each check requires only milliseconds). Once it obtains the user account information, it queries the Stratusphere Hub (through secure communications as described above) to obtain the unique assigned user identifier, which may have originally been established by Stratusphere Hub after first import from a directory system (such as Active Directory).

The result is a unique user identifier that can be embedded in network communications to identify the actual user account associated with each network connection attempt. Such user identifying information is not normally available in the TCP and UDP network connection attempts, and cannot normally be obtained except by inspecting later data packets after a connection is established – the Connector ID method however is much more reliable and requires much less processing (host CPU).

User identifiers are assigned randomly, not sequentially, and a 24-bit number is used for the identifiers so that over 16 million user identifiers can be issued in a single environment. When users are removed from the environment, their identifiers are typically preserved for reporting purposes. Upon administrative determination, identifiers may be reclaimed for later use.

Machine Tracking

Machine tracking starts by assigning a unique tracking number to each machine (physical or virtual), one that is consistent even when IP addresses change or even in the case where a VM is destroyed and re-created (as when using non-persistent virtual desktops). Machine identification follows a two-step process conducted by the agent in conjunction with the Stratusphere Hub. The steps are:

1. Examine the various elements of the machine to obtain a unique "fingerprint";
2. Associate the fingerprint with an identifier, issued by the Stratusphere Hub, that is unique within a given environment, such that no two machines ever receive the same identifier.

The machine fingerprint is normally established when the Connector ID Key is first run on a machine, which may occur immediately after installation or in some cases – such as when creating virtual machines from templates – when the machine is first booted. The unique machine identifier is established when the Connector ID Key registers (through secure communications as described above) with the Stratusphere Hub. Subsequently, the fingerprint and associated machine identifier are rechecked each time the machine is restarted as well as at a configurable recheck interval.

The fingerprint is calculated by examining machine elements that either have unique identifiers themselves or have readable signatures. Applying a hash algorithm for each examined element and placing the results together establish the complete fingerprint. Some elements examined for the fingerprint include:

- VMware UUID (VMware environments only)
- Fully-qualified machine name
- CPU ID
- Motherboard serial number
- Chassis ID
- Boot drive ID
- BIOS serial number
- NIC addresses
- Hard Drive serial numbers
- IDE controller signature
- Graphics controller signature
- SCSI controller signature
- CPU model information

Once the fingerprint is established, a unique machine identifier is assigned. Unique identifiers are distributed randomly, not sequentially. The unique machine identifier is a 24-bit number, so over 16 million different machine identifiers can be issued in a single environment. When machines are removed from the environment, their identifiers are typically preserved for reporting purposes. Upon administrative determination, identifiers may be reclaimed for later use.

Tracking Users and Machines in Network Connections

When the Stratusphere administrator turns on Connector ID tracking, the machine identifier and user identifier are each placed by the Connector ID Key in outgoing TCP and/or UDP connection attempts using Liquidware Lab's patented approach. In the case of TCP, these identifiers are placed in the TCP SYN packet header and are fully compliant with the IETF TCP specification. In the case of UDP, these identifiers are

appended to the UDP data. Like TCP, this method is fully compatible with the IETF UDP specification. The identifiers are always encrypted and verifiable (see information on Encryption Signatures in the section below).

For TCP, the Connector ID Key embeds the identifiers in unused portions of the TCP SYN packet header, including areas in the sequence number, acknowledgement number, window and urgent pointer fields. By embedding the identifiers into each TCP SYN packet or UDP packet (when Connector ID is enabled for TCP or UDP), Stratusphere enables continuous and highly efficient tracking of machine and user activity inside the virtual network. Since Connector ID complies fully with TCP and UDP specifications, destinations that receive TCP or UDP packets with embedded Connector ID identifiers work as normal and applications are unaffected.

Verification and Security

Encryption is used to protect identifiers and as a signature mechanism to validate the authenticity of the identifiers included in the network connection attempts. This is done by applying a strong cryptographic signature along with the embedded identifiers, where the signature is used to authenticate the machine sending the packet and the embedded identifiers within the packet. Each Connector ID Key applies a unique signature that can be fully verified by any Collector or the Stratusphere Hub.

Replay protection is also available for user and machine tracking in TCP communications. By default, this protection is not on, however administrators can turn it on in the Stratusphere Hub console. Replay protection is not typically required when using Stratusphere for assessment or diagnostic purposes, but may be required when using Stratusphere network activity tracking to validate security or provide compliance audit trails for internal systems, when there are concerns that hackers might attempt to obtain access to sensitive systems by replaying captured network traffic.

Conclusion

Stratusphere provides the most advanced solution for assessments and diagnostics on physical and virtual environments. As described in this paper, the solution is architected to be highly efficient, scalable and secure.

Many of the methods discussed in this document are represented in Liquidware's patent filings. Liquidware currently holds and owns three US patents (7,386,889 and 7,549,159 and 7,552,323) which were originally issued to Trusted Network Technologies and vmSight who were acquired by Liquidware. Liquidware also has over 10 other patents pending in the US and abroad.

For more information or details, please contact your Liquidware account representative.