



Stratusphere FIT and Stratusphere UX Security Architecture Overview

Assessment, Diagnostics and Monitoring for Next-Generation Desktops

Whitepaper

INTRODUCTION

This whitepaper has been authored by experts at Liquidware Labs in order to provide guidance to adopters of desktop virtualization technologies. In this paper, we outline the security considerations designed into the architecture of our Stratusphere FIT and Stratusphere UX products.

Information in this document is subject to change without notice. No part of this publication may be reproduced in whole or in part, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any external use by any person or entity without the express prior written consent of Liquidware Labs.

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

CONTENTS

Introduction.....	2
Stratusphere FIT and Stratusphere UX Overview	4
Stratusphere Virtual Appliances	4
Connector ID Key (CID Key)	6
Track User Activity.....	6
Track Terminals and Virtual Desktops.....	6
Extreme Efficiency For Virtual Environments.....	7
Patents	7
About Liquidware Labs	7

STRATUSPHERE FIT AND STRATUSPHERE UX SECURITY OVERVIEW

Stratusphere FIT and Stratusphere UX are certified for use with VMware® and Citrix® desktop virtualization platforms, and are compatible with other desktop virtualization components such as third-party brokers. It is downloadable from the Liquidware Labs website. These products are comprised of two virtual appliances (pre-packaged and self-contained VMs), the Stratusphere Hub and the Network Station, and a software agent called the CID Key that is delivered along with the Stratusphere Hub.

STRATUSPHERE VIRTUAL APPLIANCES

The Stratusphere Hub and Network Station virtual appliances are based on a hardened stripped down version of the Red Hat 5 Linux 2.6 Operating System. Only essential software modules and services are retained onboard the appliances 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. All Stratusphere virtual appliances also have a command line console for appliance administrative controls, this interface is also password protected.

Stratusphere UX Offers True Cross Platform Support:

Hypervisors include VMware ESX 3.0 and higher, VMware ESXi 3.0 and higher, Citrix XenServer 5.5 and higher, and Microsoft Hyper-V on Windows 2008 R2 and higher. Desktop platforms (physical and virtual) include Windows operating systems including Windows 7 and Linux operating systems. Virtual desktop platforms include VMware View, Citrix XenDesktop and Citrix XenApp. Protocols: Citrix ICA, RDP and VMware PCoIP. Thin Application solutions supported include VMware ThinApp and Microsoft AppV.

Stratusphere UX runs as a virtual appliance. Resource requirements for its components are outlined as follows:

Stratusphere™ Hub Appliance (SHA)

- Hypervisors Supported VMware ESX 3.0 and higher, VMware ESXi 3.0 and higher, Citrix XenServer 5.5 and higher, and Microsoft Hyper-V on Windows 2008 R2 and higher.
- Download Size 605MB
- CPU 1 vCPU (capable of supporting multiple processors)
- Memory 2GB for Monitoring < 500 machines, 4GB for Monitoring < 1000 machines.
- Storage 6GB pre-allocated. Recommend adding a 30GB Drive for up to 1500 machines for 30days.

Stratusphere™ Database Appliance (SDA) – is an optional component used to store information when more than 1,000 CID Keys are deployed.

Connector ID Keys (Outlined in detail in the next section of this document)

Stratusphere™ Network Station (SNS)

- Hypervisors Supported VMware ESX 3.0 and higher, VMware ESXi 3.0 and higher, Citrix XenServer 5.5 and higher.
- Download Size 371MB
- CPU 1 vCPU
- Memory 512 MB.
- Storage 3.5GB pre-allocated

All communications between the Stratusphere components are encrypted using a PKI infrastructure where the Stratusphere Hub is the “Certifying Authority,” generating public and private key certificates for itself and each of the components (Network Stations and CID Keys on individual machines). Stratusphere product components 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 Active Directory, which are also secured).

The following ports and protocols are used by Stratusphere:

- TCP/443: HTTPS for the Stratusphere Hub management interface
- TCP/5501: CID Key communications to and from the Stratusphere Hub
- TCP/5502: Network audit data transfer between the Hub and Network Stations
- TCP/5444: Used to access Stratusphere Hub database when designing custom reports
- TCP/22: Secure shell console access to the command line console

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) and VMware® vCenter. 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 Labs only. Liquidware Labs Customer Support will notify customers when and if 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 Labs web site, and Network Stations and CID Key updates can either be automatically controlled through the Hub administrative interface or delivered through other software update or patch control services.

CONNECTOR ID KEY (CID KEY)

The Connector ID (CID) Key is installed on a physical desktop or within a guest virtual machine's operating system. Stratusphere currently supports current versions of Microsoft Windows operating systems, and supported Linux operating systems, including RedHat, SuSE and Ubuntu. The CID Key installation requires administrative privileges. The software runs as a service in the operating system that is configured to start automatically. Once installed, the CID 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 Key does not listen on any ports; it only sends information to the Stratusphere Hub on the secure channel (TCP/5501).

The CID Key functions are controlled by administrators through the Stratusphere Hub. When configured to monitor the machine configuration and processes, the CID Key sends information back to the Stratusphere Hub on a configurable timed basis. Also when configured, the CID 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 CD Keys in general, please refer to the Stratusphere architecture white paper.

CID Key is patented technology that differentiates Liquidware Labs Stratusphere FIT and Stratusphere UX solutions from all other assessment, diagnostics and monitoring solutions for virtual desktops. CID Key technology provides computer networks with a capability similar to "caller ID" for phone networks. With the CID Key software embedded in a thin client, on a physical or virtual desktop, each network connection includes an invisible fingerprint that allows real-time user and machine activity tracking at a virtual or physical network switch. With CID Keys for virtual desktops and applications, desktop administrators have unparalleled capabilities to track and profile end user activity and individual experience.

CID Key technology allows you to:

- Track devices and VMs and specific applications accessed by a user at any time
- Determine the exact application activity and user experience for individual users
- Efficiently assess and profile activity in real-time inside a virtual or physical network
- Profile RDP and ICA connections and service levels

The following are the key technology features found in Liquidware Labs products:

TRACK USER ACTIVITY

Track end user activity for virtual desktops and virtual applications using CID. Associate users and activity with their OS login ID. Track machine logons, application activity, network activity, performance, reliability and resource consumption by user or user group. Assess service level and other policies for individual users or user groups fully integrated with your user directory.

TRACK TERMINALS AND VIRTUAL DESKTOPS

Persistently identify machines, physical or virtual, in environments where these machines receive dynamic IP addresses (such as when using DHCP). Profile process activity within machines, users logging onto machines, and network activity to and from the machines, with the ability to track this data across a series of days even when IP addresses have changed. Establish and track service level and other policies for individual machines or groups of machines, and maintain consistency even if IP addresses change or machines are migrated.

EXTREME EFFICIENCY FOR VIRTUAL ENVIRONMENTS

To effectively ensure end user experience, reliability, security and regulatory compliance, it is highly desirable to provide continuous system data collection and auditing. In a virtual environment it is critical that data collection does not over-consume system CPU or memory. CID allows you to identify and track users and machines and all application activity to, from and between VMs on a single host without any noticeable effect on the efficiency or performance of the virtual host. This patented approach to activity tracking is much more efficient than other approaches that rely on guest VM polling or deep packet inspection of network connections.

PATENTS

CID is protected by U.S. Patent 7,386,889. There are 12 other patents pending in the U.S. as well as associated international filings.

ABOUT LIQUIDWARE LABS

Founded in 2009, Liquidware Labs™ is the leader in desktop transformation solutions for next-generation physical and virtual desktops, including VMware View, Citrix XenDesktop, and Microsoft Windows 7. The company's Stratusphere™ and ProfileUnity™ solutions have been described by analysts as the industry's first 'On-Ramp to VDI,' providing a complete methodology and software that enables organizations to decouple users and applications from the operating system and to cost-effectively assess, design, migrate, and validate the user experience for next-generation desktop infrastructure. Liquidware Labs products are VMware and Citrix certified, and are available through a global network of certified partners. Visit www.liquidwarelabs.com for further information