

Table of Contents

Stratusphere™ Requirements	2
Stratusphere™ Hub Appliance (SHA)	2
Stratusphere™ Database Appliance (SDA).....	2
Stratusphere™ Software Download.....	2
Stratusphere™ Installation Preparation.....	3
Stratusphere™ Hub Deployment Models for Assessments	4
Stratusphere™ Assessment Time Estimates	5
Stratusphere™ Hub Upload for Analysis & Assessment Deliverable	6

Stratusphere™ Requirements

Liquidware Labs Stratusphere™ has three components: Hub, Connector ID Key, and Network Station. The Hub and Connector ID Keys are the only components used during assessments – Network Stations are NOT REQUIRED. Here are some of the requirements for these components.

Stratusphere™ Hub Appliance (SHA)

Stratusphere™ Hub Appliance is a required component and forms the central management and reporting core of the Stratusphere™ platform.

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. <i>Note: In an unlikely scenario where the appliances need to be run on VMware Player, VMware Server, and VMware Workstation we recommend the use of VMware Converter 4.x to convert the appliance file formats.</i>
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)

Stratusphere™ Database Appliance (SDA) is an optional component used to store information when more than 1,000 CID Keys are deployed. This option allows a higher volume of CID Keys to call back to the Stratusphere™ Hub and a high performance option for better user interface response times.

Hypervisors Supported	VMware ESX 3.0 and higher, VMware ESXi 3.0 and higher, Citrix XenServer 5.5 and higher. <i>Note: In an unlikely scenario where the appliances need to be run on VMware Player, VMware Server, and VMware Workstation we recommend the use of VMware Converter 4.x to convert the appliance file formats.</i>
Download Size	350MB
CPU	2 vCPU (capable of supporting multiple processors)
Memory	8GB for Monitoring < 5,000 machines, 16GB for Monitoring < 10,000 machines.
Storage	30GB Drive for up to 1500 machines for 30days.

Stratusphere™ Software Download

1. Use our Download site: <http://www.liquidwarelabs.com/download>. Fill in the requested information and you can use the links to download our software for VMware and Citrix platforms.

2. If you are part of our Apache Partner Program, you can use your credentials to log into our Partner Portal at http://www.liquidwarelabs.com/project_apache/login.asp. Navigate to the software download page and download the appropriate files directly.

Stratusphere™ Installation Preparation

1. Each Stratusphere™ virtual appliance needs the following during configuration:
 - a. Hostname
 - b. IP Address (static) (Required)
 - c. Network mask
 - d. Default Network Gateway IP Address
 - e. DNS Server IP Addresses
 - f. Mail Relay Servers (Optional)
 - g. NTP Servers (Recommended)
 - h. **DNS entry name for the Stratusphere™ Hub IP Address (Strongly Recommended)**
 2. Distribution of the Connector ID Key (CID) to the target desktops needs to be handled by the infrastructure team at the end user. The Standard CID Key local version installer in the form of an EXE will be provided to the software distribution team who would then be responsible for packaging, distribution, and installation of the CID Key on all targeted desktops. If the Standard CID Key Network version is used then the Active Directory Domain Administrators would be needed to create a new Group Policy Object to create Startup/Shutdown scripts to invoke our Network CID Key from a shared folder such as NETLOGON folder on an Active Directory Controller. Documentation for installation of the CID Key in various scenarios can be provided on request.
 3. The Stratusphere™ software components communicate between each other using TCP connections. Please ensure these ports are open and accessible between the components. Here is a list of TCP network ports used in communication between the Stratusphere™ Hub, Network Station and Connector ID Keys:
 - a. Stratusphere™ Hub TCP/22 (SSH) : Console access to Stratusphere™ Hub
 - b. Stratusphere™ Hub TCP/443 (HTTPS) : Management UI
 - c. Stratusphere™ Hub UDP/5501 (CID Key) : Connector ID Key Communications
 - d. Stratusphere™ Hub TCP/5501 (CID Key) : Connector ID Key Communications
 - e. Stratusphere™ Hub TCP/5502 : Network Station Communications
 - f. Stratusphere™ Hub TCP/5444 : Reporting Database Access
 - g. Network Station TCP/5502 : Policy Communications
 4. The Stratusphere™ UI can import user group and machine group information from any LDAP compliant name store (Microsoft Active Directory, Novell eDirectory). We can use a standard domain user account or better yet, a service account to import user group membership information. This account should be read-only permissions only since we do not update any information on the name store. However, in most organizations the group memberships may not be exactly what you expect to use since they may not be populated in the way we want to use them. Liquidware Labs recommends creating a CSV file with grouping information for users and machines which can then be imported into the Stratusphere™ UI. This form of import

provides a better focus on how the output of the assessment deliverable can be grouped together. Here is the format of the UNIX based CSV text file:

- a. Machine Group/User Group CSV used by import script
machine-name1,group-name1
machine-name2,group-name1;group-name2;...;group-nameN
machine-name3,group-name2
machine-name4,group-name2;group-name3
- b. User Group CSV used in the UI
group-name,user-name1;user-name2;...;user-nameN

Note: There is a difference in formats of the two files. To create a UNIX based text file, you can use open source applications like [NotePad++](#) that can convert to UNIX based text files.

Stratusphere™ Hub Deployment Models for Assessments

Liquidware Labs recommends three models of how the Stratusphere™ Hub can be deployed:

1. Customer ESX Infrastructure:

This is our most common deployment scenario. Most large customers have existing ESX infrastructure that can host the Stratusphere™ Hub during the pre-VDI planning assessment phase. We download and install the Stratusphere™ Hub on that ESX infrastructure at same location where the Virtual Desktops are to be hosted in future. CID Keys are downloaded from the Stratusphere™ Hub and distributed to the physical desktops and laptops using any standard software distribution tools or group policy. Once the assessment data collection period is over, the CID Keys are automatically uninstalled or dissolved from the physical desktops/laptops. We then shutdown and export the Stratusphere™ Hub, compress it and upload it to the Liquidware Labs FTP Servers for help with the analysis for the VDI Assessment Deliverable.

2. Mobile Infrastructure:

Stratusphere™ Hub can be preinstalled on an ESXi platform on a small server or on VMware Server/Workstation on a laptop. The Stratusphere™ Hub is powered on, given an IP Address and is available for use as a standard Stratusphere™ Hub. CID Keys are downloaded from the Stratusphere™ Hub and distributed to the physical desktops and laptops using any standard software distribution tools or group policy. Once the assessment data collection period is over, the CID Keys are automatically uninstalled or dissolved from the physical desktops/laptops. We then shutdown the Stratusphere™ Hub and the laptop it's on and ship it back to the partner offices. Here the partner can export it and upload it to the Liquidware Labs FTP Server for help with analysis for the VDI Assessment Deliverable.

3. Partner hosts the Stratusphere™ Hub for the customer:
 The Partner hosts the Stratusphere™ Hub for the customer if they are also going to provide managed or hosted desktops for their customers. The partner provides a CID Key to the customer software distribution team. The CID Keys call over the web back to the Stratusphere™ Hub, register and provide all necessary assessment data. When the assessment data collection period is over, the CID Keys are automatically uninstalled or dissolved from the physical desktops/laptops. Initially the partner can export it and upload it to the Liquidware Labs FTP Server for help with analysis for the VDI Assessment Deliverable.

Stratusphere™ Assessment Time Estimates

Step	Task	Time Estimate
1.	Initial conference call with customer to explain the concept, requirements and preparation for the Assessment.	1 Hour. (T-1week before installation)
2.	Downloading of 1 Stratusphere™ Hub. Partner should ask the customer to download before we get on site or bring the software with on a DVD/USB Stick.	5min to 1 Hour depending on customer bandwidth.
3.	Install and configure 1 Stratusphere™ Hub.	1 Hour.
4.	Import Active Directory/LDAP user and group information. If large numbers of user groups exist, we recommend using a manually created CSV file import.	1 Hour – depends on size.
5.	Provide the CID Key installer to customer Software Distribution team for pushing out to physical desktops.	
6.	Perform health check #1 after one day.	1 Hour.
7.	Perform health check #2 after two days.	1 Hour.
8.	Perform health check #3 after three days.	1 Hour.
9.	Export the Stratusphere™ Hub to OVF/VMDF.	1 Hour.
10.	Upload the Stratusphere™ Hub to Partner FTP Site.	Variable depending on customer bandwidth.
11.	Download and import OVF/VMDK into lab for analysis.	Variable depending on partner bandwidth.
12.	Perform analysis and assess the data collected over collection period to create VDI Assessment Findings and Recommendations deliverable document.	3-5 days.
13.	Present Assessment deliverables to customer.	1 Hour.

Stratusphere™ Hub Upload for Analysis & Assessment Deliverable

Here are simple instructions on what to do after the Stratusphere™ Assessment data collection period concludes:

1. Gracefully shutdown the Stratusphere™ Hub. Use any **one** of the following options to do so:
 - a. In the Virtual Infrastructure Client or vSphere 4.0 Client right click on the Stratusphere™ Hub, and select “Shutdown Guest”.
 - b. Log into the Stratusphere™ Hub console using `ssconsole/sspassword`. Execute the “`shutdown`” command. The Stratusphere™ Hub will shut down after that.
2. Use any **one** of the following two options to export the appliance:
 - a. Log into the ESX Host’s console and zip up the contents of the Stratusphere™ Hub folder. Use the “`tar cvzf ../hub.tar *.*`” command to zip up the folder. Then use either the Data Browser or [WinSCP](#) to copy the tar file to your local desktop.
 - b. From the Virtual Infrastructure Client use the **File->Virtual Appliance->Export** option. It will create an OVF/VMDK set of files on your local desktop folder. Zip these files together to compress their size.
3. Upload the tar zip file or the OVF/VMDK files to our FTP site. We recommend using [FileZilla](#) FTP client. Here are the details:
 - a. FTP: `tam-ftp.liquidwarelabs.com`
 - b. User: `<username>` Provided by Liquidware Labs
 - c. Pass: `<password>` Provided by Liquidware Labs
 - d. Folder: `\Partner\Customer`
4. Download the same files down into your lab environment. Use the same option used in item 2 above to import the appliance into your lab environment:
 - a. Use the Data Browser or WinSCP to copy the tar file to your ESX’s VMFS from your local desktop. Log into the ESX Host’s console and unzip up the contents of the tar file in the Stratusphere™ Hub folder. Use the “`tar xvzf hub.tar`” command to unzip the tar file within the folder. Using the Data Browser you can then select the `.vmx` file and add it to the inventory.
 - b. Unzip the file into a folder. From the Virtual Infrastructure Client use the **File->Virtual Appliance->Import** option and browse to your local folder where you unzipped the zip file. Select the OVF file and import it within your lab infrastructure.
5. Edit the settings of this new appliance to point to your local VM Network. Power on the appliance. Log into the console using the default credentials `ssconsole/sspassword` or acquire the changed password for `ssconsole`. Run the following commands to re-ip the appliance:
 - a. `set management ip <new.ip.address>`
 - b. `set management netmask <new.netmask>`
 - c. `set management default gateway <new.gateway.ip>`
 - d. `write`
6. Your appliance is now ready to use.