Table of Contents

1 INTRODUCTION ............................................................................................................................................. 3
  1.1 TOPICS COVERED ..................................................................................................................................... 3
  1.2 TARGET AUDIENCE ................................................................................................................................. 3

2 DIAGNOSTICS PREP 1: INSTALL AND CONFIGURE STRATUSPHERE ............................................................ 4
  2.1 INSTALL THE STRATUSPHERE HUB VIRTUAL APPLIANCE (VMWARE vSPHERE) ................................... 4
  2.2 INSTALL THE STRATUSPHERE HUB VIRTUAL APPLIANCE (CITRIX XENSERVER) ............................... 5
  2.3 INSTALL THE STRATUSPHERE HUB VIRTUAL APPLIANCE (MICROSOFT HYPER-V) ............................ 6
  2.4 CONFIGURE STRATUSPHERE™ HUB ....................................................................................................... 7
    2.4.1 Configure Stratusphere™ Hub using Web UI ..................................................................................... 7
    2.4.2 Configure Stratusphere™ Hub using the Console............................................................................. 11
  2.5 STRATUSPHERE™ DATABASE APPLIANCE .............................................................................................. 11
    2.5.1 Installing Stratusphere™ Database Appliance (VMware vSphere) .................................................... 12
    2.5.2 Configure Stratusphere™ Database Appliance .............................................................................. 12
    2.5.3 Transfer Database from Stratusphere™ Hub to Database Appliance using the Console .................. 14
    2.5.4 Complete Stratusphere™ Database Appliance configuration ......................................................... 15
  2.6 [OPTIONAL] SETUP USER GROUPS AND MACHINE GROUPS ................................................................. 15
  2.7 REVIEW DATA COLLECTION SETTINGS .................................................................................................... 17
  2.8 DISTIBUTE CONNECTOR ID KEYS TO TARGET DESKTOPS ...................................................................... 19
  2.9 [OPTIONAL] SETUP IMPORT FROM vCENTER FOR HOST STATISTICS .................................................. 20
  2.10 [OPTIONAL] INSTALL NETWORK STATIONS ON VIRTUAL HOSTS ......................................................... 21
    2.10.1 Configuring Network Monitoring on VMware Virtual Switch ......................................................... 22
    2.10.2 Configuring Network Monitoring on VMware Distributed Switch .......................................... 24
    2.10.3 Configuring Network Monitoring on XenServer ............................................................................. 26
    2.10.4 Configure Stratusphere™ Network Station using the Console ......................................................... 28

3 DIAGNOSTICS PREP 2: LEARN THE BASICS OF STRATUSPHERE .................................................................. 30
  3.1 DIAGNOSTICS DASHBOARD ..................................................................................................................... 30
  3.2 INSPECTOR ................................................................................................................................................ 31
  3.3 REPORTS .................................................................................................................................................. 31
  3.4 INVENTORY ............................................................................................................................................... 32
  3.5 VDI UX PROFILE ..................................................................................................................................... 35

4 DIAGNOSTICS 1: END-TO-END PERFORMANCE ANALYSIS ........................................................................ 36
  4.1 VIRTUAL MACHINE PERFORMANCE ANALYSIS ..................................................................................... 36
  4.2 HOST PERFORMANCE ANALYSIS .......................................................................................................... 38
  4.3 NETWORK PERFORMANCE ANALYSIS .................................................................................................. 39
  4.4 SAN PERFORMANCE ANALYSIS ........................................................................................................... 41

5 DIAGNOSTICS 2: TREND ANALYSIS AND ALERTS ...................................................................................... 42
  5.1 TREND ANALYSIS ..................................................................................................................................... 42
  5.2 ALERTS ..................................................................................................................................................... 43

6 DIAGNOSTICS 3: SUMMARY ANALYSIS AND RECOMMENDATIONS ......................................................... 45
  6.1 VDI UX ANALYSIS ..................................................................................................................................... 45
  6.2 PERFORMANCE TIME CHART AND COMPARISON .............................................................................. 46
  6.3 DIAGNOSTIC FINDINGS SUMMARY ......................................................................................................... 46

7 CONCLUSION ................................................................................................................................................. 49

8 APPENDIX: DEPLOYING CONNECTOR ID KEYS WITH AD GPO OR SMS ..................................................... 50
  8.1 DEPLOYING THE NETWORK CONNECTOR ID KEYS WITH AD GPO .................................................... 50
  8.2 DEPLOYING THE STANDARD CONNECTOR ID KEYS WITH AD GPO ................................................ 52
  8.3 DEPLOYING THE CONNECTOR ID KEYS WITH SMS ............................................................................. 57
  8.4 EMBEDDING CONNECTOR ID KEYS IN VMware View 4 Master Images ............................................. 58
1  Introduction

This document will walk you through an evaluation of Stratusphere UX (UX stands for User eXperience), the VDI diagnostics and performance monitoring solution from Liquidware Labs. This is not a complete training or user guide, but is meant to guide you through the basic steps to setup the product and to introduce you to key features, reports and capabilities, so that you can determine whether Stratusphere is suitable for your VDI monitoring needs. It is assumed you will use the evaluation license that comes with the free version of Stratusphere, allowing you to run the product for 10 days, and to assess up to 5 virtual desktops.

1.1  Topics Covered

During the course of this guide, you will:

✓ Learn how to install and configure the Stratusphere Hub virtual appliance
✓ Learn how to deploy Stratusphere Connector ID Keys and Network Stations
✓ Learn the key components of the Stratusphere diagnostics product module
✓ Learn how to review environment inventory and configuration for desktops, applications
✓ Learn how to review resource consumption data for desktops, users and applications
✓ Learn how to generate diagnostic findings and results

1.2  Target Audience

This document is meant for consultants and customers who are deploying desktop virtualization in pilots or production, and who may have use for a diagnostic tool to help measure user experience or identify performance issues. Technical skills required are minimal, however familiarity with deploying virtual desktops and virtual machines on VMware or XenServer is expected.
2 Diagnostics Prep 1: Install and Configure Stratusphere

This section describes the steps to setup monitoring for a target set of virtual desktops.

The Stratusphere Hub is a virtual appliance that you can install directly from the Liquidware Labs web site. It is the data collector and reporting system for VDI diagnostics and it also includes the data collection software agents that will be deployed within the desktop VMs. The first step is to install the Hub virtual appliance on an appropriate virtual host. Since this is a data collection and reporting appliance, it is recommended that you deploy it on a host appropriate for server applications, not a host used for virtual desktops (although for initial evaluation you may choose to share hosts but in this case note that Hub performance may be affected). The virtual appliance requires 1 gigabyte of memory and 4 gigabytes of disk space, and for larger product assessments you may choose to expand memory up to 4 gigabytes of memory and may require larger disk space to keep all data. For larger environments it is also recommended that the Hub has at least one dedicated CPU, and a fast storage system (local storage can be a good solution).

The following sections describe how to configure the virtual switch and install the Stratusphere Hub virtual appliance on either VMware vSphere or Citrix XenServer, and subsequent installation and configuration steps.

2.1 Install the Stratusphere Hub Virtual Appliance (VMware vSphere)

The Stratusphere Hub virtual appliance can be downloaded directly from Liquidware Labs web site onto your VMware host. To do this, open the VMware vSphere Client and connect to your target VMware vCenter host. In the vSphere Client, select File > Deploy OVF Template… and provide the URL for the Stratusphere virtual
appliance (OVF) that is listed on the Liquidware Labs product download page. Complete the appliance install wizard by accepting the evaluation license terms, providing the name, selecting the host, data store, and network port. The virtual appliance will then automatically be downloaded and installed.

2.2 Install the Stratusphere Hub Virtual Appliance (Citrix XenServer)

To install on XenServer, download and install the virtual appliance onto your host. To do this, you will first need to download the XVA .zip file from the Liquidware Labs web site and un-zip the XVA. Next, open the XenCenter Client and connect to your target XenServer host. In the XenCenter Client, select File > Import VM and proceed through the wizard, specifying the location of the downloaded XVA file.
2.3 Install the Stratusphere Hub Virtual Appliance (Microsoft Hyper-V)

To install on Microsoft Hyper-V, download and install the virtual appliance onto your host. To do this, you will first need to download the .zip file from the Liquidware Labs web site and un-zip it.

Next, open the Microsoft Hyper-V Manager Client and connect to your target Hyper-V host. Right-click on the Hyper-V host and select the “Import Virtual Machine…” menu option.

Select the folder that contains the files that were extracted from the zip file above by clicking on the “Browse” button above.
Once imported, select the Settings link for the imported virtual machine. You can choose to update the amount of Memory and Processors associated with the Stratusphere™ Hub. You can also add an additional disk to an available hard disk controller. Please make sure the Network Adaptor is connected to a valid VM Network with the right VLAN ID tags. The virtual appliance is now ready; you can start it and move to the next step.

### 2.4 Configure Stratusphere™ Hub

On completion of the import into the virtual host, you can edit settings on the Hub to set the CPU/Memory settings. You can add an additional hard disk with the required amount of space based on the “LiquidwareLabs.Stratusphere.DatabaseDiskSizing” guide. Instructions to add the disk to the appliance are available at LiquidwareLabs.com. Now you can power ON the virtual appliance. You can open a console to the virtual appliance and watch the boot sequence. The Hub can now be configured using the Web UI as well as the Hub console.

#### 2.4.1 Configure Stratusphere™ Hub using Web UI

If DHCP is enabled on the local network subnet, the Stratusphere™ Hub will acquire a DHCP network address. On completion of the boot sequence, the appliance will provide information on how to connect to the Web based Administration interface of the virtual appliance. As shown in the image below, it will display the URL that can be used to connect to the Stratusphere™ Hub along with the default administrative credentials.
Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to your employer, to authorized site, government, and law enforcement personnel, as well as authorized officials of government agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of such personnel or officials. Unauthorized or improper use of this system may result in civil and criminal penalties and administrative or disciplinary action, as appropriate. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

Administration interface can be accessed at https://10.0.80.101
Default administrator name: ssadmin
Default administrator password: sspassword

localhost login: _

You can now open your browser and navigate to the URL as shown in the console above. You can log into the Administration module using the default user id and password as shown above.
On successfully logging in, you will need to accept the End User License Agreement (EULA).

Then enter all the required registration information. You can choose to “Generate a New License” or choose “I have a product license key” to paste in the license you may have received from Liquidware Labs.
Once you click on “Get Started” you will be presented with a page to configure the virtual appliance.

Here is a brief description on the fields on this page:

1. **Host Name**: Please enter a hostname for the appliance. It can be a short name or a fully qualified host name.
2. **IP Address**: Provide a static IP Address for the virtual appliance. Since the appliance booted up using DHCP it will potentially need to give up the same address unless it's reserved within the DHCP server. It is strongly recommended to change it to a Statically allocated IP Address.
3. **Network Mask**
4. **Default Gateway**
5. **DNS Name**: Please enter the fully qualified DNS entry name associated with this static IP Address. The CID Keys will call back to the Stratusphere™ Hub based on what is in this field. It is strongly recommended that you use a DNS Entry name here instead of IP Address so as to circumvent any future issues that may crop up due to reconfiguring the IP Address of the appliance.
6. **DNS Server Addresses**: Please enter 1 or more IP Addresses of your DNS server in a comma separated list.
7. **DNS Search Suffix**: Please enter the local DNS search suffixes available within your local network.
8. **Time Zone**: Please select your local time zone from the drop down list.
9. **Enable NTP**: Please enable this option to avoid time drift and keep the Stratusphere™ Hub’s time synched and accurate.
10. **Time Servers**: This field comes pre-populated with some public time servers. You can choose to enter your own comma separated list of time servers as well. These can be entered as IP Addresses and/or DNS entry names.

On “Save Changes” all these configuration fields will be saved and if you have configured the new Static IP Address correctly, the browser will redirect you to your new IP Address based URL. This initial Appliance Network Configuration page is only available on first run and will not be available subsequently.

In addition to using the browser based interface, the Stratusphere™ Hub virtual appliance can also be configured through the console.
2.4.2 Configure Stratusphere™ Hub using the Console

If DHCP is not available on the local subnet, then you can use the Console to configure the Stratusphere™ Hub. Open up the console to the Stratusphere™ Hub on VMware VI Client and vSphere Client as well as the XenCenter or XenServer. Once opened, use the following default credentials to log in:

User ID: ssconsole
Password: sspassword

Here is a list of commands to configure the appliance:

```
set management ip <static.ip.address>
set management netmask <network.mask>
set management default gateway ip <default.gateway.ip.address>
set dns server <dns.ip.address.1>[,<dns.ip.address.2>][,...]
set dns search <dns.suffix.1>[,<dns.suffix.2>,[,...]]
write
set system hostname <hostname>
set system hub dns name <hub.dns.or.ip>
set system mail relay server <mail.relay.ip.dns>
set system time <Continent/City>
set system time <yyyy/mm/dd hh:mm>
set ntp server <time.1.server.ip.dns>[,<time2.server.ip.dns>][,...]
set ssh ssconsole on
set ssh on
write
set ntp on
write
exit
```

These commands are used to configure or re-configure the appliance if it needs to change its IP Address or a new time server etc. Make sure you execute the “write” command before exiting the console as that actually saves the changes made so far.

2.5 Stratusphere™ Database Appliance

The Stratusphere™ Database Appliance is used when more than 1,000 CID Keys report back to the Stratusphere™ Hub using the default callback frequency of 60min. Liquidware Labs recommends using the database from the Stratusphere™ Hub 4.8.x to create the database on the Stratusphere™ Database Appliance. 

**NOTE:** Please upgrade the Stratusphere™ Hub to the latest 4.8.x version before installing the Stratusphere™ Database Appliance.

The process begins with importing the Stratusphere™ Database Appliance software from Liquidware Labs Download site. Once imported, configure the Database Appliance as a statically addressed virtual appliance. The user must then copy a script to the Stratusphere™ Hub. This script prepares the Stratusphere™ Hub for an external database. It exports the database into a backup file and shuts down the database service on the Stratusphere™ Hub. It then transfers this file to the Stratusphere™ Database Appliance. On the Stratusphere™ Database Appliance, run a similar script to accept and restore the database backup file, enable services, and configure communication services between the Stratusphere™ Hub and Database Appliances. Once configured, the two appliances can communicate with each other and are now configured for enhanced performance and scalability. For detailed instructions please refer to the “LwL.Stratusphere.InstallingDatabaseAppliance.pdf” document.
2.5.1 Installing Stratusphere™ Database Appliance (VMware vSphere)

The Stratusphere™ Database Appliance can be imported using VMware vSphere Client directly from Liquidware Labs web site. To do this, open the VMware vSphere Client and connect to your target VMware vCenter host. In the vSphere Client, select File > Deploy OVF Template… and provide the URL for the Stratusphere Database virtual appliance (OVF) that is listed on the Liquidware Labs product download page. Complete the appliance install wizard by accepting the evaluation license terms, providing the name, selecting the host, data store, and network port. The virtual appliance will then automatically be downloaded and installed.

2.5.2 Configure Stratusphere™ Database Appliance

Liquidware Labs recommends hosting the Stratusphere™ Database Appliance on the same virtual host, same virtual switch, and same port group as the Stratusphere™ Hub Appliance. This configuration will ensure fastest communication response time between the Hub and the Database for high performance and scalability. Please ensure that there are significant CPU/Memory/IO resources available on the host as these are major server class virtual machines. After downloading the Stratusphere™ Database Appliance, please assign 2 vCPUs, 8GB of Memory, set the required amount of disk space on the second disk (default is 30GB), and connect the NIC to the same virtual network switch and port group as the Stratusphere™ Hub. Then power ON the appliance and go to the console of the virtual machine to start the configuration of the appliance. The database appliance includes a wizard for configuring the database that will prompt for required information. If you wish to use the default value for any setting you may do so by pressing the Enter key to move directly to the next setting. The wizard will ask for:

1. Current Value of Hostname:
2. Do you want to use DHCP (Y/N)? If you choose No, it will prompt for static IP Address. Liquidware Labs recommends using static IP Addresses.
3. What Address IP do you want to use?
4. What Netmask do you want to use?
5. What is the default gateway?
6. What Primary DNS server do you want to use?
7. What Secondary DNS Server do you want to use?
8. What Tertiary DNS Server do you want to use?
9. Enable the NTP Time Server Service [Yes]?
10. What NTP Time Server do you want to use?

This is an example of a completed configuration. Please note that names and IP addresses will vary according to your environment.

Save your configuration using the “write” command. You will finish with a screen showing the status of your database.
The Stratusphere™ Database Appliance is not configured and ready to receive its database from the Stratusphere™ Hub.

2.5.3 Transfer Database from Stratusphere™ Hub to Database Appliance using the Console

Log in to the consoles of the Stratusphere™ Hub and Database Appliance using root/sspassword credentials. Keep these two console windows next to each other as instructions need to be executed on both these appliances during the transfer.

Switch to Stratusphere™ Database Appliance Console

1. Log in to the console of the Stratusphere™ Database Appliance using root/sspassword.
2. To prepare the Stratusphere™ Hub for transferring its data we need to copy a script over to the Hub. To do so, execute the following command:

```
$ scp /opt/lwl/bin/ext.preparehub.sh friend@<Hub.IP.DNS>:/home/friend/
```

The command will prompt whether to connect, accept keys and ask for a password. Use the default “sspasecond”. This script is now copied to the Stratusphere™ Hub. We need to log into the Hub and execute it.

Switch to Stratusphere™ Hub Appliance Console

1. Log in to the console of the Stratusphere™ Hub Appliance using root/sspasecond.
2. We now need to stop the Stratusphere™ Hub Appliance database services, backup the data to a file and move it over to the Stratusphere™ Database Appliance. Execute the following command:

```
$ /home/friend/ext.preparehub.sh
```

**Important:** Once the files are moved over, this command will pause or wait for you to execute the corresponding command below by switching consoles on the Stratusphere™ Database Appliance. DO NOT ENTER “yes” just yet.

The command will display status messages for stopping services etc. and will then prompt the user for the IP or DNS of the Stratusphere™ Database Appliance. This command too will prompt whether to connect, accept keys and ask for a password. Use the default “sspasecond”. The database is now stopped and backed up to a file which has been transferred over to the Stratusphere™ Database Appliance. The command will then pause until the database is restored on the Database Appliance below.

Switch to Stratusphere™ Database Appliance Console

1. Execute the following command:

```
$ /opt/lwl/bin/ext.preparedb.sh
```

The command will now start restoring the database backup file copied over from the Stratusphere™ Hub Appliance. If the database is of a large size this may take a significant amount of time. Once completed, the command will display the following message:

```
Importing database...ok
```

The database transfer and restore procedure is now complete.

Switch to Stratusphere™ Hub Appliance Console

1. The Stratusphere™ Hub console will be waiting for user confirmation if the Stratusphere™ Database Appliance command finished successfully. Now enter “Yes” to continue.
2. Just in case you entered “Yes” prematurely (i.e. before coming to this step and before completing the Stratusphere™ Database ext.preparedb.sh command), please log into the console of the Stratusphere™ Hub Appliance using ssconsole/sspasecond and execute “restart services” command.
2.5.4 **Complete Stratusphere™ Database Appliance configuration**

Once the procedure is complete please verify the integrity by logging into the Stratusphere™ Web UI. Log in to the Administration section using ssadmin/sspassword credentials. Navigate to the Hub Administration > Data Retention > Status tab and verify the free space available based on the configured space of the Stratusphere™ Database Appliance. The database transfer and restore procedure is now complete. If you see any other messages or errors please contact Support@LiquidwareLabs.com.

2.6 **[Optional] Setup User Groups and Machine Groups**

Now that you are logged into the Administration module, the first thing to consider is whether you will be defining any user groups or machine groups for your assessment. You may choose to setup groups if you have distinct sets of users or desktops that you want to analyze separately during the assessment. These groups do not need to be setup prior to the assessment, however if you set them up prior you can immediately use the groups as you proceed through later steps. Groups can be useful for production assessments especially in larger environments, but are optional for this evaluation.

Machine groups can be used to group desktops for assessment, for example by location or by department. To define machine groups, go to Inventory > Machines, select Groups, and then click the New button.
User groups can be similarly created by hand by going to Inventory > Users, selecting Groups, and then clicking on the New button. With user groups you also have the choice to import groups from your Active Directory or LDAP, or from a file. For this assessment, if you want to setup user groups either create them manually, or import from a file by going to Hub Administration > User Directories, and select Import From CSV File from under the Local Directory. Information on the file formats for user groups and users can be found there.
2.7 Review Data Collection Settings

The next step is to review your data collection settings. While logged in to the Administration module, click on Hub Administration > Connector ID Keys. The first thing you will see is a set of Properties that control the data collection functions. Some notes on key properties (and suggested defaults are in screen shot below):

- **Callback Frequency** – the frequency that the Connector ID Key software agents (discussed in next section) will send collected data back to the Hub; in environments where a single Hub is monitoring many desktops (more than 500) then you will want to be careful about setting the frequency too low, since it will increase the network traffic (about 30K to the Hub on each callback) and the load on the Hub along with the amount of disk space used; note that detailed sizing guidelines and Hub tuning recommendations can be obtained from Liquidware Labs customer support

- **Enable Machine Inspection** – indicates that configuration and usage data should be gathered from user desktops

- **Inspection Sample Interval** – the frequency at which the Connector ID Key software gathers data on application and user activity and resource consumption on the user desktop; if the Callback Frequency is 15 minutes or less, then it is recommended that you set the sample interval to 1 or 2 minutes, for longer callback frequencies it is good to use sample interval of 5 minutes

- **Inspect (All the Time, or Only when user logged on)** – specifies whether application activity should be inspected all the time, or only when user logged on if you want to focus strictly on user activity

- **File/Folder Size and Counts** – specify folders and document types, will cause the Connector ID Keys to gather data on the number of files and total file size for each folder or file type specified

- **Automatically uninstall Connector ID Key software** – for Keys that are installed locally on user desktops (more on install in next section) this setting allows you to specify number of days after which the software agents on user desktops should “dissolve” (automatically remove themselves). This setting takes effect as soon as the CID Keys download their settings at the next callback interval. 0 = NEVER.
- Enable Connector ID for TCP Connections – this allows more accurate tracking of the network latency between the user desktop and the Hub during the assessment, recommended to leave this on.
### 2.8 Distribute Connector ID Keys to Target Desktops

To begin capturing metrics within your target desktop environment, you will need to deploy the Connector ID Key software to the target desktops. You can find the software by logging in to the Administration module, proceed to Hub Administration > Connector ID Keys and click on the Software tab. Liquidware Labs recommends using the Standard CID Key installer that can be used interactively and distributed directly to desktops.

Connector ID Keys are small footprint (less than 3 MB) and run invisibly with minimal performance impact on the end user desktops. By default when using the Standard version, they will be installed in a folder named Liquidware Labs\Connector ID in the Program Files folder. The Windows Standard installer has information that allows it to call back to a Stratusphere™ Hub and register automatically. They communicate securely with your Hub over TCP and UDP on port 5501.

Note that the “local version” Connector ID Keys can be installed on machines (physical/virtual desktops/servers) that will be used remote or offline, as long as there are certain times (including initial installation) when the machines are connected to the network and can reach the IP address (or DNS) of the Stratusphere Hub. Data collection will continue while the machines are offline, and up to two weeks of information can be stored locally until the next time the machine is connected to the network.

If you are interested in other versions of the Connector ID Key for Linux operating systems or using the Network or Advanced versions of the CID Key then click on the “Other Versions” link at the bottom of the page and you will see all the remaining versions.

The local install EXE can be pushed using SMS or any other standard software distribution tool. It can also be embedded into the master image of the virtual desktop. The command line to install the Connector ID Key for Windows Standard version is:

```
Install-connectorID-Key-4.7_0-winStandard.exe /q [HUBADDRESS="hub-ip-or-dns-name"] [MACHINEGROUP="machine-group-name"] [USERGROUP="user-group-name"]
```

The Network Shared install can simply be un-zipped onto a network server in a shared folder. The command line to start the Network shared Connector ID Key is:

```
netcid start <"network-cid-folder-path"> [-ha "hub-ip-or-dns-name"] [-mg "machine-group-name"] [-ug "user-group-name"]
```

The command line to stop the Network shared Connector ID Key is:

```
netcid stop <"network-cid-folder-path”>
```
If you need to push out the CID Key using Active Directory Group Policy then you can also download the AD GPO version of the installer which is an MSI along with the Group Policy template that can be used for software installation. Detailed instructions for both types of install can be found in the Appendix of this document.

To confirm that the Connector ID Keys have been successfully installed on the desktops or servers, and that they are reporting data back to the Stratusphere Hub, login to the Administration product modules on your Stratusphere Hub, and go to Inventory > Machines. The machines with Connector ID Keys running should automatically show up registered in the inventory list and you should be able to see their Last Contact Date updating as they make their regular callbacks to send data to the Hub. If machines are not showing up properly in the list, review your installation steps, that the machine is connected to network (for registration) and can reach the Hub (using TCP and UDP on port 5501).

2.9 [Optional] Setup Import from vCenter for Host Statistics

To get performance statistics on the virtual hosts, such as CPU Ready and Memory Swap Rate statistics, it is necessary to configure the Stratusphere Hub to connect to your vCenter (or to multiple vCenters). This capability is only available for VMware in 4.6, future versions will support XenServer and XenCenter as well.

To configure the connection, login to the Administration section of your Stratusphere Hub. Navigate to the VM Directories tab, and click on the Create New VM Directory button (do this once for each vCenter you want to connect to). Specify the connection information, then Save Changes.
To allow Stratusphere to initialize the information for your hosts, you also need to do an Import. Click on Import from VM Directory, and click the Import button. Stratusphere will import the Host definitions and the information about the VMs assigned to each virtual host.

2.10 [Optional] Install Network Stations on Virtual Hosts

If you want to capture details on network traffic, bandwidth, latency, and server response times for your virtual desktops, then you can also deploy Stratusphere Network Stations onto the virtual hosts where the virtual desktops run. The Network Stations are virtual appliances, very similar to the Stratusphere Hub with similar
steps for installation. The Network Stations do not have their own browser interface; however, they are managed via the console or through the Stratusphere Hub. And because the Network Stations will monitor the traffic for the virtual desktops on each host, they must be connected to a promiscuous port group (mirror port) on the host virtual switch. One Network Station can monitor all the network traffic on an individual virtual switch on a single host. The details of traffic to be monitored are set within the Stratusphere Hub administration interface.

Once a Network Station is installed and started, it will automatically register with the Stratusphere Hub.

To install a Network Station, you will need to download the OVF or XVA.zip from Liquidware Labs web site. The Network Station has 2 NÍCs. NIC 1 is the management port that will accept the static IP Address of the appliance and NIC 2 is the promiscuous NIC that will be used to monitor network connections. The sections below describe how to configure the promiscuous port in VMware or XenServer. The steps to configure a Network Station are almost exactly the same as the Stratusphere™ Hub. However, during the configuration, the Network Station will prompt the user for information regarding the Stratusphere™ Hub’s address and administrative credentials.

The summary of steps to install a Network Station is:
- Configure a promiscuous port on the target virtual host(s) as described below
- Import the OVF or XVA (download from Liquidware Labs) as described in section above
- Connect the second port of the Network Station to the promiscuous port
- Power on the Network Station
- Run the console Quickstart, specifying the Station’s network connection information and also specifying the connection information to connect to the Stratusphere Hub

2.10.1 Configuring Network Monitoring on VMware Virtual Switch

To enable detailed network performance monitoring, the Network Station virtual appliance has a second port that must be connected to a promiscuous port group on your virtual host network switch (allowing it to monitor the network packets that are traveling to and from each of the virtual desktops). Here are the steps to configure a virtual switch:

1. To configure the virtual switch on a target host, for VMware open the VMware Infrastructure (VI) Client for the target host, select the Host and go to Configuration > Networking, and click Properties.

2. Set all existing production port groups on the virtual switch to “Reject” Promiscuous Mode.
3. Now edit the virtual switch itself and set it to “Accept” Promiscuous Mode.

![Virtual Switch Properties](image)

4. Now add a new Port Group and it will inherit the “Accept” Promiscuous Mode from the virtual switch. If there are multiple VLANs on this switch and you want to monitor only 1 provide that VLAN ID while configuring this promiscuous port group. If you want to monitor all the VLANs on this virtual switch, then set the VLAN ID to 4095. It will provide this promiscuous port group with network connections across all VLANs on that switch.

![Stratosphere Monitor Properties](image)

Once your virtual switch is configured, you are ready to download and install the Network Station virtual appliance onto your VMware host.
2.10.2 Configuring Network Monitoring on VMware Distributed Switch

Here are steps to create a promiscuous port group on VMware virtual Distributed Switch.

1. Add a new port group to the virtual distributed switch.

2. Give it an appropriate name such as “Monitor” or “dvPortGroupPro”. You can leave the default Number of Ports at 128 or reduce it to the number of hosts you have this distributed switch on in the cluster. Select the “VLAN Trunking” option for VLAN Type and enter 0-4094 VLAN trunk range to get all VLAN traffic or you can be more specific based on VLANs you want to monitor.
3. Once created, right click and select “Edit Settings” for the new port group.

4. Navigate to Policies > Security and change the Promiscuous Mode to “Accept”.

5. Now Navigate to Advanced and click on “Edit Override Settings…” and allow overrides for “Block Port” and “Security Policy”.
6. The promiscuous port group will now be available on each host that has this virtual distributed switch. Configure a Network Station on each Host and connect its Network Adaptor 1 to a port group with a static IP that can communicate with the Stratusphere™ Hub and connect the Network Adaptor 2 to this newly created promiscuous port group.

### 2.10.3 Configuring Network Monitoring on XenServer

To enable the network performance monitoring, the Network Station virtual appliance has a second port that must be configured in promiscuous mode on your virtual host network switch (allowing it to monitor the network packets that are traveling to and from each virtual desktop). After importing the XenServer XVA, you will need to configure the network monitoring. Configuring the Stations’s second network connection for promiscuous mode will not affect any other VMs on the Host. For XenServer, the first step is to access the console for the XenServer host. Click on the Host in the XenCenter Client and open the console.

In the XenServer console, you will need to perform the following steps. For each step, you can use the “–list” command to find the appropriate target and the appropriate UUID, and at the end of each step you can use the “–param-list” command to see that the changes were saved. Also note that the XenServer console will auto-complete the UUIDs if you type in the first 3 characters and then hit tab.

At the console command line, perform the following steps:

1. Modify the promiscuous setting for the Hub’s virtual interface
   
   ```bash
   xe vif-list vm-name-label=xen_hub
   xe vif-param-set uuid=<uuid-of-vif> other-config:promiscuous="true"
   xe vif-param-list uuid=<uuid-of-vif>
   ```

2. Modify the promiscuous setting for the server’s physical interface
   
   ```bash
   xe pif-list network-name-label=eth0
   xe pif-param-set uuid=<uuid-of-pif> other-config:promiscuous="true"
   xe pif-param-list uuid=<uuid-of-pif>
   ```

3. Modify the promiscuous setting for the host virtual network switch

   ```bash
   ```
xe network-list name-label=Pool-wide network associated with eth0
xe network-param-set uuid=<uuid-of-network> other-config:promiscuous="true"
xe network-param-list uuid=<uuid-of-network>

The Network Station virtual appliance is now ready to be configured.
2.10.4 Configure Stratusphere™ Network Station using the Console

The Stratusphere™ Network Station has two network adaptors. NIC #1 is the management port and receives the static IP Address to communicate over the network to the Stratusphere™ Hub. NIC #2 is the promiscuous port that plugs into the new port group created in the section above. It sniffs the traffic of this NIC and sends the data to the Stratusphere™ Hub over the management port. Once the Network Station is downloaded from the Liquidware Labs site, to configure these NICs, right click on the Network Station appliance and select “Edit Settings”. Select the appropriate network connection labels and assign them to each NIC.

Once configured, power ON the appliance and open the console to the appliance. The machine boot sequence will be visible within the console. After it finishes booting, it will prompt the user to configure the appliance as shown below.

```
Starting tnt-backend-priv: [ OK ]
Starting tntpolicy: [ OK ]
Starting crond: [ OK ]
Starting auditd: [ OK ]
Starting anacron: [ OK ]
Starting atd: [ OK ]
Starting jexec: [ OK ]

Security warning: root password is still set to system default.
Security warning: friend password is still set to system default.
Security warning: sssconsole password is still set to system default.

Please change passwords
Would you like to configure the appliance? [yes/no] 
```
The user would need to have the following ready items ready to configure the Network Station:

1. Hostname
2. Static IP Address
3. Network Mask
4. Default Gateway IP Address
5. DNS Servers
6. Stratusphere™ Hub’s IP or DNS
7. Administrative credentials on the Stratusphere™ Hub (ssadmin/sspASSWORD)

Proceed as shown below:

Once the user saves the configuration above, the Network Station will save these settings, configure itself on the network and then register with the Stratusphere™ Hub. Once registered it will give a brief status message and then provide a login prompt. Use the following default credentials to log in:

User ID: ssconsole
Password: sspASSWORD

Here is a list of commands to configure the appliance:

```
set dns search <dns.suffix.1>[,<dns.suffix.2>,[,...]]
set system timezone <Continent/City>
set ntp server <timel.server.ip.dns>[,<time2.server.ip.dns>[,...]]
set ssh ssconsole on
set ssh on
write
set ntp on
write
exit
```

These console commands are used to configure or re-configure the appliance. If the appliance needs to be reconfigured the user can issue the “quickstart” command. Make sure you execute the “write” command before exiting the console as that actually saves the changes made so far. The Network Station will now show up under the Stratusphere™ Hub’s Web UI Administration product under Station Administration tab. It can be managed from the Hub’s Web UI from that point onwards.
3  Diagnostics Prep 2: Learn the Basics of Stratusphere

This section provides an introduction to the key elements of the Stratusphere UX product. To log in to the product, open your browser and go to https://[your-virtual-appliance-ip-address], then select Stratusphere UX from the Product drop-down, and enter the default username: ssadmin and password: sspassword.

3.1  Diagnostics Dashboard

The first thing you will see is the UX dashboard. This provides an overview of the data collected along with real-time refreshing and drill-down options. See the screenshot below for notes on the sections and usage.
3.2 Inspector

Click on Diagnostics > Inspector, and you will find a list of interactive reports and graphs that you can use to explore the diagnostics data. Use the drop-down at the top of the page to select the view and then click on the Go button to move to that view. You can filter the data using controls at the top of the page, and dynamically sort or drill-down using controls on the data table. Data can also be exported to PDF, XLS, and other formats.

3.3 Reports

Click on Diagnostics > Reports and you will find the list of previously generated reports on your Hub (if you have just deployed there may not be any in the list). The full list of available reports can be found by clicking on the Report Library. In the Report Library, you can select and dynamically run individual reports, and you can Edit them to set-up schedules. Note that all reports are customizable using the open source BIRT Report Designer, and you can add custom reports to the library as well (for more information on report customization, as well as how to query the Hub database directly from Excel or other tools, contact Liquidware Labs support).
3.4 Inventory

In the Inventory section of the Stratusphere UX product, you can view information on the Machines (desktops), Users and Applications in your environment. Once you have installed your Hub and deployed Connector ID Keys to the target desktops, the Inventory information will automatically begin populating, and data will be updated regularly (according to the Callback Frequency defined for the Connector ID Keys as discussed in previous section above). Select individual items from the Inventory lists and click on the Edit button to view more details – for example select a Machine and click Edit to view the configuration data gathered from that machine. The Inventory section is also where you can create and manage groups.
### Machines

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>OS Version</th>
<th>Connector ID</th>
<th>Created On</th>
<th>Last Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>npnccd-2</td>
<td>Virtual</td>
<td>Microsoft Windows XP Professional, Service Pack 3</td>
<td>netcd-4.6.0-1</td>
<td>May 3, 2010 3:36:20 PM EDT</td>
<td>May 12, 2010 4:45:00 PM EDT</td>
</tr>
</tbody>
</table>

### Users

<table>
<thead>
<tr>
<th>Username</th>
<th>Domain</th>
<th>Email Address</th>
<th>Role</th>
<th>Enabled</th>
<th>Created On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Qa</td>
<td><a href="mailto:Administrator@ntqa.com">Administrator@ntqa.com</a></td>
<td>User</td>
<td>Yes</td>
<td>May 3, 2010 3:34:58 PM EDT</td>
</tr>
<tr>
<td>daisy</td>
<td>Qa</td>
<td><a href="mailto:daisy@ntqa.com">daisy@ntqa.com</a></td>
<td>User</td>
<td>Yes</td>
<td>May 4, 2010 1:03:04 AM EDT</td>
</tr>
<tr>
<td>glargey_NWHeath</td>
<td>Qa</td>
<td><a href="mailto:glargey_NWHeath@ntqa.com">glargey_NWHeath@ntqa.com</a></td>
<td>User</td>
<td>Yes</td>
<td>May 4, 2010 1:03:04 AM EDT</td>
</tr>
<tr>
<td>ira</td>
<td>Qa</td>
<td><a href="mailto:ira@ntqa.com">ira@ntqa.com</a></td>
<td>User</td>
<td>Yes</td>
<td>May 3, 2010 3:41:27 PM EDT</td>
</tr>
<tr>
<td>inatest1</td>
<td>Qa</td>
<td><a href="mailto:inatest1@ntqa.com">inatest1@ntqa.com</a></td>
<td>User</td>
<td>Yes</td>
<td>May 4, 2010 1:03:04 AM EDT</td>
</tr>
<tr>
<td>inatest2</td>
<td>Qa</td>
<td><a href="mailto:inatest2@ntqa.com">inatest2@ntqa.com</a></td>
<td>User</td>
<td>Yes</td>
<td>May 4, 2010 1:03:04 AM EDT</td>
</tr>
<tr>
<td>inatest3</td>
<td>Qa</td>
<td><a href="mailto:inatest3@ntqa.com">inatest3@ntqa.com</a></td>
<td>User</td>
<td>Yes</td>
<td>May 4, 2010 1:03:04 AM EDT</td>
</tr>
<tr>
<td>Ja</td>
<td>Qa</td>
<td><a href="mailto:Ja@ntqa.com">Ja@ntqa.com</a></td>
<td>User</td>
<td>Yes</td>
<td>May 4, 2010 1:03:04 AM EDT</td>
</tr>
</tbody>
</table>

### Desktop Applications

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Version</th>
<th>Machines Installed</th>
<th>Estimated size (KB)</th>
<th>Installs Services</th>
<th>Installs Device Drivers</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Flash Player 10 ActiveX</td>
<td>10.0.42</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>xme</td>
</tr>
<tr>
<td>Adobe Flash Player 10 Plugin</td>
<td>10.0.42</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>xme</td>
</tr>
<tr>
<td>Adobe Reader 9.2</td>
<td>9.2.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>xme</td>
</tr>
<tr>
<td>AntiVirus Service Executable</td>
<td>2.1.659</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>xme</td>
</tr>
<tr>
<td>Application Layer Gateway Service</td>
<td>5.1.2600</td>
<td>2</td>
<td>43</td>
<td>0</td>
<td>0</td>
<td>xme</td>
</tr>
<tr>
<td>CTF Leader</td>
<td>5.1.2600</td>
<td>3</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>xme</td>
</tr>
<tr>
<td>Citrix XenCenter</td>
<td>5.5.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>xme</td>
</tr>
<tr>
<td>Client Server Runtime Process</td>
<td>5.1.2600</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>xme</td>
</tr>
<tr>
<td>Client Server Runtime Process</td>
<td>6.1.7600</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>xme</td>
</tr>
<tr>
<td>Connector ID</td>
<td>4.6.0</td>
<td>4</td>
<td>3,774</td>
<td>Yes</td>
<td>Yes</td>
<td>xme</td>
</tr>
</tbody>
</table>
For more details on the configuration of individual machines, go to Inventory > Machines, select a machine and click on the Edit button. You can view details about the hardware, OS, installed applications and patches.
3.5 VDI UX Profile

The VDI UX Profile is part of Liquidware Labs’ patent-pending VDI UX rating system, used to continuously rate desktop and user activity on virtual desktops to help categorize the expected user experience. The rating system categorizes a desktop or user on nine metrics, each one rated Good, Fair or Poor according to thresholds defined in the profile. You can specify relative weights for each metric (zero to exclude a metric). Also, you can auto-generate thresholds based on statistical measures taken from recent historical data.

To view or change the profile settings, login to Stratusphere UX and navigate to Diagnostics > VDI UX Profile. At the top of the page, you can choose to calculate thresholds based on historical data, either one time (in which case the threshold changes will not be saved until you click Save Changes) or auto-adjusted in the background on a daily basis. Note that you can recalculate VDI UX ratings for previously collected data when you Save Changes.
4 Diagnostics 1: End-to-End Performance Analysis

Once you have deployed Stratusphere for monitoring, you are ready to begin generating reports and analyzing the environment. This section provides you information on the key Inspector views and reports from the Report Library that will help you analyze the performance of your VDI environment.

4.1 Virtual Machine Performance Analysis

To begin examining machine performance, navigate to Diagnostics > Inspector. Select the view Top Consumer Charts in the drop-down and generate the charts for the diagnostics date range. Using this chart you can quickly identify the top resource consumers.

To see summary details for each machine, select the Inspector view Machine Diagnostics Summary, change the Date Range to Last 24 Hours, and click the Go button. This shows one row for each machine.
To see further details, click on the drill-down button on the left side of a selected row, and drill-down to see the machine inspection history for a specific machine. This will show a breakdown for every report that the Connector ID Key sent back for the specified machine.

To get a complete view of the machine, host, SAN, and application data gathered for the specific machine during this period, select the Inspector view Desktop 360º View and click Go.
Next go to Diagnostics > Reports, click on Report Library, and run the following reports for the time period you are analyzing.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slow User Logins</td>
<td>Identifies logins taking longer than specified threshold</td>
</tr>
<tr>
<td>Slow Application Load Times</td>
<td>Identifies applications that took longer than specified number of seconds to load</td>
</tr>
<tr>
<td>Top CPU Consuming Applications</td>
<td>Shows the applications consuming the most CPU cycles</td>
</tr>
<tr>
<td>Top Memory Consuming Applications</td>
<td>Shows the applications using the most memory</td>
</tr>
<tr>
<td>Machines with High CPU Usage</td>
<td>Identifies machines using more than specified threshold percentage of CPU</td>
</tr>
<tr>
<td>Machines with High Memory Usage</td>
<td>Identifies machines using more than specified threshold percentage of Memory</td>
</tr>
</tbody>
</table>

### 4.2 Host Performance Analysis

To examine host performance, go to Diagnostics > Inspector and select the Host Performance Summary from the drop-down list of views, then click the Go button. To see details about the machines running on a specific host, drill-down on the row.

For the summary report on host performance, go to Assessment > Reports, click on Report Library, and run the following report for the diagnostics time period.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Performance Summary</td>
<td>Lists summary averages statistics for each virtual host</td>
</tr>
</tbody>
</table>
4.3 Network Performance Analysis

To gain a graphical view of network connections, with an ability to drill down on the performance data, navigate to Diagnostics > Inspector, select the Network Connection Map from the drop-down list of views, and click the Go button. Next you will need to select one of your VMs as the Target Machine, then click the Draw Map button.
To view overall network performance data by application (port/protocol), navigate to Diagnostics > Inspector and select the Network Application Summary from the view drop-down, click on the Go button. To view data for a specific application such as RDP, select the application from the filter drop-down at the top of the page.

<table>
<thead>
<tr>
<th>Application</th>
<th>Connection Attempts</th>
<th>Incomplete Connections</th>
<th>Unauthorized Connections</th>
<th>Failed SLA</th>
<th>Network Latency Roundtrip Avg.</th>
<th>Total Response Time Avg.</th>
<th>Total Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP over TLS/SSL (TCP/443)</td>
<td>23,662</td>
<td>0 (0%)</td>
<td>87</td>
<td>0 (0%)</td>
<td>338.11 µs</td>
<td>2.94 s</td>
<td>216.23 MB</td>
</tr>
<tr>
<td>VMware View Messaging (TCP/9001)</td>
<td>2,506</td>
<td>2,506 (100%)</td>
<td>0</td>
<td>0 (0%)</td>
<td>n/a</td>
<td>n/a</td>
<td>350.73 KB</td>
</tr>
<tr>
<td>Connector ID Key Communication   (TCP/5501)</td>
<td>1,217</td>
<td>61 (5%)</td>
<td>109</td>
<td>0 (0%)</td>
<td>1.61 ms</td>
<td>355.82 ms</td>
<td>82.58 MB</td>
</tr>
<tr>
<td>Network Station Communication    (TCP/5505)</td>
<td>233</td>
<td>0 (0%)</td>
<td>0</td>
<td>0 (0%)</td>
<td>957.88 µs</td>
<td>200.04 ms</td>
<td>3.88 MB</td>
</tr>
<tr>
<td>DHCP Server (UDP/67)</td>
<td>66</td>
<td>0 (0%)</td>
<td>0</td>
<td>0 (0%)</td>
<td>n/a</td>
<td>8.27 s</td>
<td>65.32 KB</td>
</tr>
<tr>
<td>World Wide Web (TCP/80)</td>
<td>36</td>
<td>0 (0%)</td>
<td>9</td>
<td>0 (0%)</td>
<td>324.94 ms</td>
<td>1.56 min</td>
<td>102.15 KB</td>
</tr>
<tr>
<td>SSH Remote Login (TCP/22)</td>
<td>13</td>
<td>0 (0%)</td>
<td>0</td>
<td>0 (0%)</td>
<td>751.08 µs</td>
<td>24.75 min</td>
<td>66.02 MB</td>
</tr>
<tr>
<td>Unmon (TCP/5544)</td>
<td>1</td>
<td>0 (0%)</td>
<td>1</td>
<td>0 (0%)</td>
<td>2.09 ms</td>
<td>452.95 ms</td>
<td>10.33 MB</td>
</tr>
</tbody>
</table>

To print reports on network performance, go to Diagnostics > Reports, click on Report Library, and run the following reports (note that the reports are in two categories, the category can be changed with the drop-down at the top of the library page).

<table>
<thead>
<tr>
<th>Category</th>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Performance</td>
<td>Machines with High Network IO</td>
<td>Identify machines with network IO exceeding specified threshold</td>
</tr>
<tr>
<td>Desktop Performance</td>
<td>Machines with High Network Latency</td>
<td>Identify machines with latency exceeding specified threshold</td>
</tr>
<tr>
<td>Desktop Performance</td>
<td>Top IO Consuming Applications</td>
<td>The top IO consuming applications</td>
</tr>
<tr>
<td>Network Activity</td>
<td>Network Activity by Application</td>
<td>Summary network performance by application (port/protocol)</td>
</tr>
</tbody>
</table>
4.4 SAN Performance Analysis

To view SAN performance data, with an ability to drill-down and find the specific machines and applications consuming SAN, go to Diagnostics > Inspector and select SAN Diagnostics Summary from the view drop-down and click the Go button. The list of datastores is displayed, and you can drill-down to see the trend graph and the VMs (that have Connector ID Keys) using the datastore during the specified period.

To print reports on the application and document inventory data, go to Diagnostics > Reports, click on Report Library, and run the following reports for the diagnostics time period:

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall SAN Performance</td>
<td>Summary of SAN performance information by datastore</td>
</tr>
<tr>
<td>SAN Activity by Machine</td>
<td>SAN performance and usage data by virtual machine</td>
</tr>
<tr>
<td>Machines with High Disk IOPS</td>
<td>Identify virtual desktops with IOPS exceeding a specified threshold</td>
</tr>
<tr>
<td>Top IO Consuming Applications</td>
<td>Top IO consuming applications for a specified time period</td>
</tr>
</tbody>
</table>
5  Diagnostics 2: Trend Analysis and Alerts

Stratusphere UX provides extensive capabilities to analyze trends, and also to setup alerts that can be delivered via email or RSS. This section provides an overview of the key features.

5.1 Trend Analysis

To examine performance trends, navigate to Diagnostics > Inspector and select the VDI UX Trends Chart view from the drop-down, then click the Go button. The trend chart allows you to select the timeframe, and to select the metrics to compare on the bar charts and the line graph. You can use this chart to view trends and to see how metrics are correlated.
5.2 Alerts

Stratusphere UX includes a set of pre-configured alert options. Alerts can be viewed in the Hub UI, and they can also be delivered via email or subscribed to using an RSS reader. To configure alerts, navigate to Diagnostic Alerts and click on the Configure Alerts button.

To configure alerts, specify how often Stratusphere should check alert thresholds, choose the type of alerts to configure and set the appropriate threshold for each alert. You can also specify one or more email addresses where alerts should be delivered.
It is also possible to generate alerts based on any scheduled report. This means that you can setup alerts based on existing reports in the Report Library, or create custom reports and generate custom alerts. To setup an alert based on a report, navigate to Diagnostics > Reports, click on the Report Library link, select a report from the list and click on the Edit button. In the Edit form, you will need to setup a schedule to run the report, and check the box to generate a custom alert. These alerts will be delivered and displayed exactly like other Alerts.

![Schedule, Email and Alert](image)
6  Diagnostics 3: Summary Analysis and Recommendations

The final step in using Stratusphere for VDI diagnostics and user experience analysis is to generate the summary analysis and findings reports. The VDI UX categorization (Good/Fair/Poor UX for VDI) used in many of the reports is based on the VDI UX Profile settings discussed in the prior section above. In this section we cover the key summary reports you can generate and use to construct your final diagnostic deliverables.

6.1 VDI UX Analysis

To examine the distribution of desktops or users falling into different categories of VDI UX (Good/Fair/Poor), go to Diagnostics > Inspector, select the view VDI UX Scatter Plot from the drop-down list and generate the chart. You can choose to display by Machine or by User. You can drill-down to see more details on individual users or machines by clicking on nodes on the chart. You can also choose to display Average fitness ratings, or the Lowest ratings (reflecting peak periods of resource consumption).
Next go to Diagnostics > Reports, click on Report Library, and run the following reports for your time period.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDI UX by Machine</td>
<td>Breaks down assessed machines into Good, Fair, and Poor VDI UX</td>
</tr>
<tr>
<td>VDI UX by User</td>
<td>Breaks down assessed users into Good, Fair, and Poor VDI UX</td>
</tr>
</tbody>
</table>

### 6.2 Performance Time Chart and Comparison

Two key reports that you can use to analyze the performance of a time period, or to compare the performance of one time period to another, are the Performance Time Chart and the Performance Comparison reports. These reports show you key performance metrics and identify top consumers for the machines, hosts and SAN, and can be used to help identify whether there are performance problems and what might be the specific causes.

Go to Diagnostics > Reports, click on Report Library, and run the following reports for your time period.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Time Chart</td>
<td>Detailed breakdown and performance analysis for a given time period</td>
</tr>
<tr>
<td>Performance Comparison</td>
<td>Detailed comparison of key performance characteristics for two time periods</td>
</tr>
</tbody>
</table>

### 6.3 Diagnostic Findings Summary

The Diagnostic Findings report is a single summary Microsoft Powerpoint that includes graphs and data from many of the reports listed in sections above, all combined into a single report designed for you to customize and adapt to fit your needs. It includes information on the overall diagnostic data, the findings and analysis, and placeholders for your final recommendations. This report can be useful as the basis for a summary report following a VDI health check project or a VDI pilot.

To generate the report, login to Stratusphere UX. On the Diagnostics dashboard, simply click on the Generate Summary Report button, then specify the start date and end date for the report. Optionally you can also specify a specific machine group or a specific user group to report on. Note that this report may take 5 minutes or more to run, depending on the period and the amount of data gathered. The final result file will be stored in the Reports archive, where you can access and download the Powerpoint report.
Desktop Virtualization Performance Analysis

<Insert Partner Name>
<Insert Consultant Name>

May 14, 2010

Findings for machine group: - All -
Findings for user group: - All -
7 Conclusion

In this document we have covered a complete set of steps to evaluate the Stratusphere product for use in VDI monitoring and diagnostics. You have been introduced to the installation, data gathering, analysis and reporting steps, and you have seen the advanced features of Stratusphere for VDI monitoring, analysis and planning.

For more information on the technical capabilities of Liquidware Labs’ Stratusphere or ProfileUnity Pro, and for partner or end-user pricing, please visit http://www.liquidwarelabs.com or contact us at:

Liquidware Labs
3600 Mansell Road, Suite 200
Alpharetta, GA 30022
Phone: 678-397-0450
Fax: 678-397-0339
Email: info@liquidwarelabs.com

Liquidware Labs Europe - EMEA
Phone: +41 800 897 114
Email: info@liquidwarelabs.com
Appendix: Deploying Connector ID Keys with AD GPO or SMS

As discussed above, Connector ID Key software is included inside your Stratusphere Hub virtual appliance, and must be launched on the end-user desktops to gather assessment data. For Windows, there are EXE based packages that can be installed locally on desktops, and there are also versions that can be installed on a network server and then launched remotely on the user desktops. The software can be found by logging into the Administration module of your Stratusphere Hub (at https://[your-hub-ip-address] with default username: ssadmin password: sspassword), then going to Hub Administration > Connector ID Keys > Connector ID Key Software.

For evaluation you can manually install the EXE on test desktops, but this section provides further details if you wish to distribute Connector ID Keys using Active Directory Group Policy or SMS. Local install and remote launch can all be done silently, without any intrusion for the end users. To remove the software, you can use the standard procedures to reverse the process described below, or as discussed in sections above you can simply set any locally installed Connector ID Keys to “dissolve” (auto-delete) themselves after a specified number of days.

If you have problems or questions regarding the steps described here, please contact support@liquidwarelabs.com for more information.

8.1 Deploying the Network Connector ID Keys with AD GPO

This section describes how to install the network version and then use Group Policy to automatically launch Connector ID Keys on desktops. We suggest using Group Policy to launch the Connector ID Key by assigning Connector ID Key to computers (Computer Group). For those computers, the Connector ID Key will be launched when the computer starts, and it is available to all users who log on to the computer. A procedure is also available to completely clean all information off the desktops when assessment is complete.

The steps below describe the installation and launch process.

Step One: Extract the network Connector ID Key

To install the Connector ID Key, download the network version and un-zip the files onto a network share:

1. Create a shared network folder where you will put the Connector ID Key files. (\file server\share)
2. Extract the network Connector ID Key files to the share.
3. Set permissions on the share to allow access to the files.
   a. Grant either “Authenticated Users” or “Everyone” read permission.

Step Two: Create a Group Policy that Starts Network CID

To start collecting data, create a Group Policy object (GPO) that will launch network Connector ID:

1. Assign netcid.exe as a startup script. This is a computer policy and should be applied to the OU(s) containing the computers that will execute network Connector ID. Please reference the figure below for further assistance.

   Script Name: C:\files\server\share\path\netcid.exe
   Script Parameters: start “\ unc \ path \ netcid.exe” -ha “hub_ip” [-mg “machine_group_name”] [-ug “user_group_name”]

   Note: The last two parameters are optional.
Step Three: Create a Group Policy that Stops Network CID
Once you have completed your data collection and want to stop collecting data and stop the CID Key process, you should stop network Connector ID.

1. Assign netcid.exe as a shutdown script. This is a computer policy and should be applied to the OU(s) containing the computers that will have network Connector ID removed. Please reference the figure below for further assistance.
   
   **Script Name:** `\\fileserver\share\path\netcid.exe`
   
   **Script Parameters:** `stop "\\unc\path\netcid.exe"`
8.2 Deploying the Standard Connector ID Keys with AD GPO

This section describes how to use Group Policy to automatically distribute the “locally installed” Connector ID Keys to desktop machines or users. We suggest using Group Policy to distribute the Connector ID Keys by assigning Connector ID Key MSI distribution to computers (Computer Group). For those computers, the Connector ID Key will be installed when the computer starts, and it is configured as a service and is available to all users who log on to the computer.

**Step One: Create a Distribution Point**
To assign the Connector ID Key MSI, you must create a distribution point on the publishing server:

1. Create a shared network MS folder where you will put the Connector ID Key MSI. (\file server\share)
2. Copy the Connector ID Key MSI file to the share.
3. Set permissions on the share to allow access to the MS file.
   a. Grant either “Authenticated Users” or “Everyone” read permission.

**Step Two: Load Group Policy ADM Template**
The ADM Template allows Connector ID options to be specified through Group Policy. Please reference the figures below for further assistance.

Right Click Administrative Templates under Computer Configuration and select Add/Remove Templates.

Select “Add” to load the Liquidware Labs template.
Browse to the location where the Liquidware Labs template is located. This template is available from the Administration section of the Hub. You will need to download it from the hub prior to completing this step.

Once the template has been loaded, close the dialog box.

Select View then Filtering.
Disable “Only show policy settings that can be fully managed”.

Specify Connector ID Options for your environment.

**Step Three: Deploy the Software**
Create a Group Policy that deploys the Connector ID MSI package. Please reference the figures below for further assistance.
Right Click the Software installation option under Computer Configuration and select New then Package.
Browse to the location the where the Connector ID MSI is located. This path should be the UNC path created in Step 1.

Select Assigned and then choose OK.

Double Click the Connector ID package to open the Properties dialog box.
Enable “Always wait for the network at computer startup and logon”.

[Group Policy Object Editor image]

<table>
<thead>
<tr>
<th>Setting</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don't display the Getting Started screen at logon</td>
<td>Not configured</td>
</tr>
<tr>
<td>Always use classic logon</td>
<td>Not configured</td>
</tr>
<tr>
<td>Run these programs at user logon</td>
<td>Not configured</td>
</tr>
<tr>
<td>Do not process the run once list</td>
<td>Not configured</td>
</tr>
<tr>
<td>Do not process the legacy run list</td>
<td>Not configured</td>
</tr>
<tr>
<td>Always wait for the network at computer startup and logon</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
8.3 Deploying the Connector ID Keys with SMS

In this example we will use the example folder name `\InstallerCache\CID` presumed on the SMS host machine named SMS01. Change these to the actual names in your environment.

Start the SMS Administrative Console and create a new package with the following attributes:
- **Name:** Connector ID Keys
- **Version:** 4.x.x (specify the actual version to be deployed)
- **Publisher:** Liquidware Labs, Inc.
- **This package contains source files:** True (checked)
- **Source directory:** `\SMS01\InstallerCache\CID`

Use the default or site specific settings for all remaining attributes.

Create a Distribution Point for this newly created package according to your site needs.

Create a Program specifying the executable installer package:
- **Name:** Connector ID Keys
- **Command line:**
  ```
  Install-connectorID-Key-4_x_x-winStandard.exe /q [HUBADDRESS=“hub-ip-or-dns-name”] [MACHINEGROUP=“machine-group-name”] [USERGROUP=“user-group-name”]
  ``
  *Note:* The last three parameters HUBADDRESS, MACHINEGROUP, and USERGROUP are optional. The EXE installer already has information regarding the address of the Stratusphere™ Hub it was downloaded from and has to register to. However, if you want to override this embedded information, then you must specify the HUBADDRESS parameter and the installer will ignore the information it has internally. Also, if you want to specify a machine group and/or user group for automatic registration then you need to specify the last two parameters.
- **Run:** Normal

The following is necessary to complete Connector ID Keys installation and registration.
- **Estimated memory:** 512 MB RAM or higher
- **Maximum allowed run time:** 20 minutes
- **Program can run:** Whether or not a user is logged on (suggest scheduling install when users are not logged on)
- **Run mode / Run with Admin rights:** True (selected)

You are now ready to create a new Advertisement. Use the following attributes:
- **Package:** Connector ID Keys
- **Program:** Connector ID Keys Installer
- **Mandatory assignments:** Create one or more of these to force the installation of the package without requiring the user to run advertised programs. Use the default or site specific settings for all remaining attributes.

Once the advertisement is created, and the scheduled time for deployment arrives, client machines receive the advertisements and program installation begins. As the installations progress, Stratusphere should display newly registered machines in Inventory > Machines.
8.4 Embedding Connector ID Keys in VMware View 4 Master Images

Overview
This document provides information about installing Stratusphere Connector ID Keys on VMware View 4 master images or templates.

Prerequisites
Important! You must be an Administrator with full administrative credentials while installing the Connector ID Key on your base image.

Preparation
Login to the Administration module of the Stratusphere Hub virtual appliance, at https://[your-hub-ip-address], and go to Hub Administration > Connector ID Keys > Connector ID Key Software. Download the appropriate install package for your target environment.

Connector ID Key Deployment in VMware View 4 Master Image
To install the Connector ID Key on a base image do the following:

1. Power on and log into your base desktop VM image.
2. Install the Connector ID Key manually.
3. Validate that the virtual machine registered correctly by logging in to the Administration module on your Stratusphere Hub, and making sure it is listed under the Inventory > Machines tab.
4. On the master image desktop, open the command prompt as an administrator. Navigate to C:\Program Files\Liquidware Labs\Connector ID\admin scripts and execute VMwareView_MasterImagePrep.bat.
5. Shut down the base desktop virtual machine, you are now ready to take a snapshot of the machine for the base image or template.
6. In View 4 Automated Desktop Pool configuration, specify the following as Post Synchronization script on the QuickPrep Settings page: C:\Program Files\Liquidware Labs\Connector ID\VMwareView_PostSyncScript.bat