Stratusphere™ FIT and Stratusphere™ UX

Installation & Configuration Guide

Introduction

This guide has been authored by experts at Liquidware to provide information and guidance concerning the installation and configuration of Stratusphere™ FIT and Stratusphere™ UX.

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 is expected.

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

CONTENTS

Stratusphere Overview

Liquidware's Stratusphere™ is a cornerstone desktop transformation and management solution for both physical and virtual environments. The Stratusphere solution is made up of two products—Stratusphere™ FIT and Stratusphere™ UX. As an assessment solution, Stratusphere FIT gathers a wide range of data about your existing infrastructure to give a clear picture about how resources are currently consumed. Stratusphere UX is a unique monitoring and diagnostics desktop management solution that independently defines and collects data metrics about desktop user experience performance as well as the entire desktop infrastructure from endpoints, hosts, network and storage.

When making computing resource decisions, organizations typically do not know what users have on their desktops or where to start from a hardware or software perspective, performance perspective, or from a user experience perspective. Without an assessment, they will either allocate minimal resources to the target environment, leading to performance problems later, or over-provision resources, incurring higher costs. Stratusphere FIT is the solution for the IT Manager or Director who is responsible for transforming the current environment into the next generation of desktops.

Stratusphere FIT provides a sound assessment foundation on which management can make solid planning decisions and will be able to set baselines in order to validate success at the project's end. Stratusphere FIT:

- Assesses and baselines desktops, users, applications and infrastructure resources
- Measures endpoint to datacenter network latency
- Rates user, machine, and application fitness levels for virtualization: Good/Fair/Poor
- Supports capacity planning (CPU, Memory, Storage, IOPS)
- Enables design of optimum shared-image strategy
- Allows creation of remediation plans before migrating desktops to virtual platforms

From the day-to-day operations perspective, Stratusphere UX provides desktop administrators with a single pane-of-glass to monitor ALL desktops—physical and virtual—to ensure they are performing to user expectations and corporate SLAs. Desktop administrators can proactively monitor desktops through inspectors and dashboards. If significant issues arise, Health Checks can be performed to troubleshoot the environment as well as optimize desktop images and infrastructure design for best performance. Stratusphere UX delivers an ongoing and constant rating of enterprise desktop performance—by application, group, or user—and independently tracks hundreds of metrics on all integral layers of the infrastructure to ensure quality and consistent user experience across all desktops. Stratusphere UX:

- Provides end-to-end visibility - desktop to data center
- Proactively monitors and rates user experience: Good/Fair/Poor
- Allows admins to identify, diagnose, and solve the root-cause of issues in the infrastructure
- Validates pilot and production infrastructure changes to ensure optimal performance
- Offers cross-platform support for physical and virtual machines on mixed platforms
- Operates as "read-only" for secure no touch access to critical data center systems
- Supports Hyper-V and XenServer based virtual machines and provides advanced support for VMware vSphere Server, VMware View PCoIP and VMware ThinApp

The Stratusphere solution is designed to save organizations time and money while boosting productivity. It eliminates the guesswork associated with resource planning and allows administrators to proactively monitor performance to keep users productive.

Software Requirements

Stratusphere is available as a virtual appliance which is imported into your infrastructure's hypervisor. Stratusphere consists of three pre-packaged, self-contained virtual appliances: the Hub, the optional Database, and the optional Collector. The Stratusphere Hub provides the central policy management, policy distribution, data collection, reporting and alerting system for Stratusphere. The Stratusphere Connector ID (CID) Key software is a lightweight agent that is distributed to the devices in your environment that you wish to monitor. The CID Key Agent collects machine configuration and performance information from those devices and reports back either directly to the Stratusphere Hub or, in larger environments, to Collector appliances that send data from grouped CID Keys back to the Hub. The Stratusphere Database appliance is an optional add-on for larger environments. It provides a central storage option for the Hub's data collection and allows administrators to navigate and report on larger amounts of data more efficiently. The Stratusphere Collector appliance is another optional add-on that can be configured to not only collect CID Key data but also monitor all the network activity of virtual desktops tracking stats including network latency, response times and bandwidth consumption.

Stratusphere Hub Appliance Requirements

The primary user interface for the Hub is accessed through a standard web browser, but the virtual appliance also has a command line console for appliance setup and administration. The Stratusphere Hub appliance requires the following for installation:

Component	Requirements
Hypervisors Supported	VMware ESXi 5.5 and higher, Citrix XenServer 6 or higher, Microsoft Hyper-V on Windows Server 2012 and higher & Azure, AWS EC2, Google Cloud Platform, Red Hat KVM, and Nutanix Acropolis 2016.04.19 and newer **Note: VMware vSphere Virtual Machine Hardware Version** Based on some recently published vulnerabilities, VMware has recommended using higher virtual machine hardware versions. Please make sure to upgrade the Stratusphere appliance virtual machine hardware version to at least 10 and higher as supported by your infrastructure. Please reference this Knowledge Base article from VMware for additional information on how to upgrade virtual machine hardware versions. *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.*
Integrates with	VMware vSphere 5.5 and higher, Nutanix Prism, and Microsoft Active Directory 2003 and higher
Browsers Supported	Chrome 22.x, Firefox 12.x, or Internet Explorer 11 and higher versions.
CPU	4 virtual CPUs — Larger installations may require more.

Component	Requirements
Memory	8GB RAM (default) — Please use the Stratusphere Sizing Guide to determine your optimal configuration.
Storage	57.2 GB pre-allocated hard disk space — Larger installations may require more disk space depending on data retention needs and a fast storage system (local storage can be a good solution).
Languages	US English

NOTE: Should you see performance issues with a 4-vCPU configuration, you may want to decrease from 4 to 2 vCPUs—we have seen instances where the hypervisor will not schedule a machine with 4 vCPUs as often as a machine with 2 vCPUs. Related, 4 vCPUs may not provide maximum benefit if the Hub and Database appliances are not completely utilizing available CPU resources (assuming no other VMs are running on the same host).

Stratusphere Connector ID Key Requirements

The Connector ID Key software is a lightweight agent distributed to all end-point devices in your environment that you want to monitor, whether they are virtual or physical. Please note that the Windows Advanced CID Key development has been paused.

Component	Requirements
Operating Systems Supported	Windows 7/8/8.1/10, Windows Server 2008/2008 R2/2012/2012 R2/2016/2019, Linux (RHEL 5/6/7/8; CentOS 5/6/7/8; Ubuntu 10/12/13/14/16/18; Fedora 12/13; SUSE 11/12), Apple macOS (El Capitan & higher), 32-bit and 64-bit where applicable on desktops, servers, thin clients (IGEL, Stratodesk, 10Zig), physical & virtual machines
Display Protocols Supported	Remote Desktop, VMware PCoIP stats on ESX 5.1 and higher, Citrix ICA stats on Presentation Server 6.5 and higher, VMware BLAST on View Horizon Agent 7.3 and higher
CPU	1 CPU at 1 gigahertz (GHz) or faster. The agent consumes less than 1.0% of the CPU resources.
Memory	20-40 MB RAM
Storage	15-20 MB available hard disk space
Languages	US English

Stratusphere Database Appliance Requirements (Optional)

The Stratusphere Database appliance is an optional add-on used in environments dealing with larger amounts of data collection. The Database appliance requires the following for installation:

Component	Requirements
Hypervisors Supported	VMware ESXi 5.5 and higher, Citrix XenServer 6 and higher, Microsoft Hyper-V on Windows Server 2012 and higher & Azure, AWS EC2, Google Cloud Platform, Red Hat KVM, and Nutanix Acropolis 2016.04.19 and newer **Note: VMware vSphere Virtual Machine Hardware Version** Based on some recently published vulnerabilities, VMware has recommended using higher virtual machine hardware versions. Please make sure to upgrade the Stratusphere appliance virtual machine hardware version to at least 10 and higher as supported by your infrastructure. Please reference this Knowledge Base article from VMware for additional information on how to upgrade virtual machine hardware versions. *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.*
CPU	4 virtual CPUs — Larger installations may require more.
Memory	16 GB RAM (default) — Please use the Stratusphere Sizing Guide to determine your optimal configuration.
Storage	91.85 GB pre-allocated hard disk space, expandable as per sizing guidelines
Languages	US English

Note: When using the Database appliance, the Database appliance must be on the same host as the Hub to ensure fast network access. The Hub and Database must be on separate datastores with fast disk IO, especially for the database.

Stratusphere Collector Appliance Requirements (Optional)

The Stratusphere Collector appliance requires the following for installation:

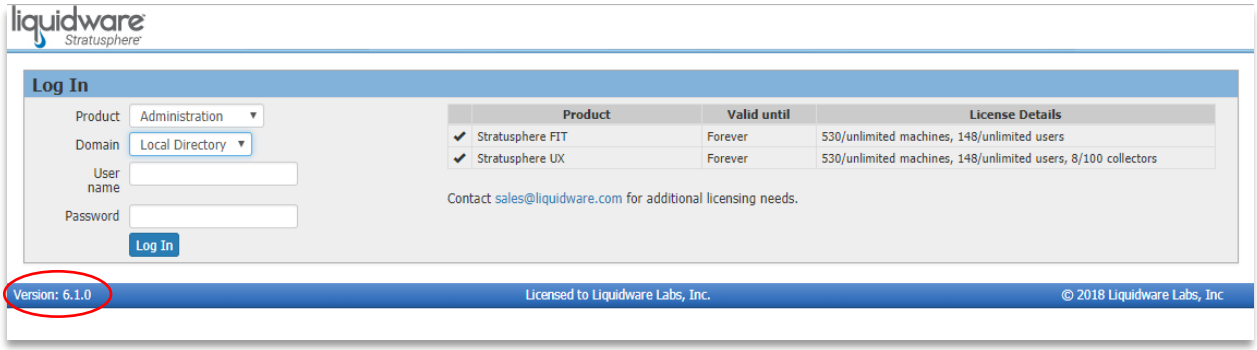
Component	Requirements
Hypervisors Supported	VMware ESXi 5.5 and higher, Citrix XenServer 6 and higher (bonded NICs not supported), and Microsoft Hyper-V on Windows Server 2012 and higher & Azure, AWS EC2, Google Cloud Platform, Red Hat KVM, and Nutanix Acropolis 2016.04.19 and newer, **Note: VMware vSphere Virtual Machine Hardware Version** Based on some recently published vulnerabilities, VMware has recommended using higher virtual machine hardware versions. Please make sure to upgrade the Stratusphere appliance virtual machine hardware version to at least 10 and higher as supported by your infrastructure. Please reference this Knowledge Base article from VMware for additional information on how to upgrade virtual machine hardware versions. *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.*
CPU	2 virtual CPUs or higher
Memory	4 GB RAM — Please use the Stratusphere Sizing Guide to determine your optimal configuration.
Storage	31.40 GB pre-allocated hard disk space
Languages	US English

Upgrading Stratusphere

On-Premises Versions: If the current on-premises (VMware vSphere, Microsoft Hyper V, Citrix XenServer, Nutanix) installed version of Stratusphere is at 6.1.x, or 6.0.x, or 5.8.5 or higher, please use the instructions in *Migrating to Stratusphere 6.5.0 Appliances*, to migrate network settings, certificates, and data from 5.8.5 and higher appliances to the 6.5.0 appliances. If the current installed version is earlier than 5.8.5, please upgrade to 5.8.5 and then perform a migration using the instructions mentioned above. Alternatively, contact Support@Liquidware.com for further assistance.

Cloud Platform versions: If the current installation of Stratusphere is on any of our supported Cloud Platforms (AWS, Azure, Google Cloud Platform), the 6.5.0 versions of the appliances are still in the onboarding process within each cloud platform vendor. As soon as they become available, the Migrating to Stratusphere 6.5.0 Appliances guide will be updated with relevant instructions for each platform.

To find out which version of the Stratusphere appliance you are running, start the Stratusphere Web UI and look in the lower left-hand corner for the version number. You can compare this version number with what is available on Liquidware Software Download Area (https://www.liquidware.com/Download/).



Alternatively, the version number is also shown on the console when the Stratusphere Hub virtual machine is powered on.

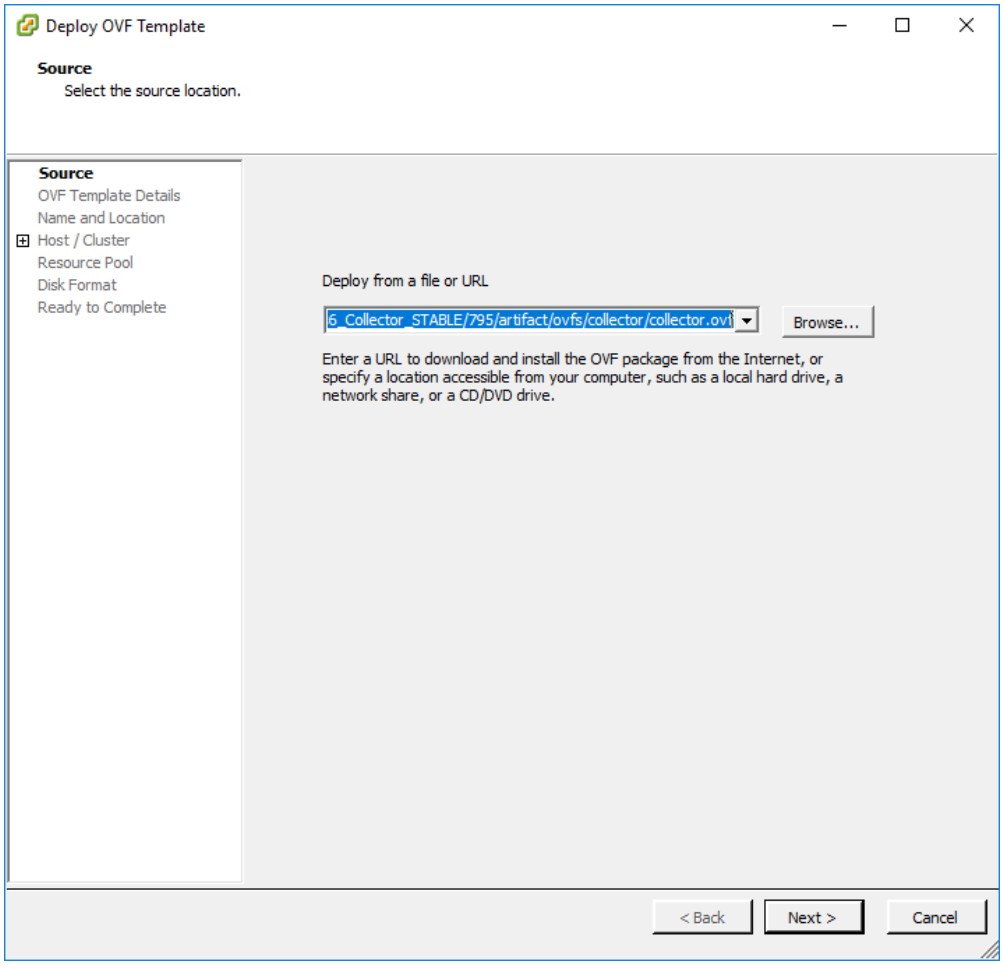
Installing the Stratusphere Virtual Appliances

The Stratusphere Hub, Database, and Collectors are all virtual appliances that can be installed directly from the Liquidware web site. The Stratusphere Hub 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 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 following instructions can be used to install the Hub as well as other optional appliances within your virtual environment.

For VMware Virtual Environments

To install the Stratusphere appliances directly onto your VMware host:

1. Open the VMware vSphere Client and connect to your target VMware vCenter host.
2. In the vSphere Client, select **File > Deploy OVF Template…** and provide the URL for the Stratusphere appliance (OVF) that is listed on the Liquidware Product Download page. (Visit http://www.liquidware.com/Download/ to register and get access to fully functional evaluation copies of the Stratusphere software.)

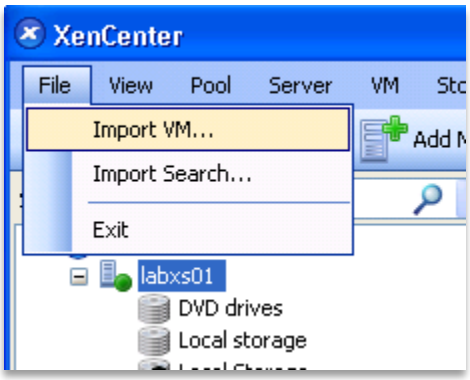


3. Complete the appliance installation wizard by:
    a. accepting the evaluation license terms,
    b. providing the name, and
    c. selecting the host, data store, and network port.
4. The virtual appliance will then automatically be downloaded and installed.

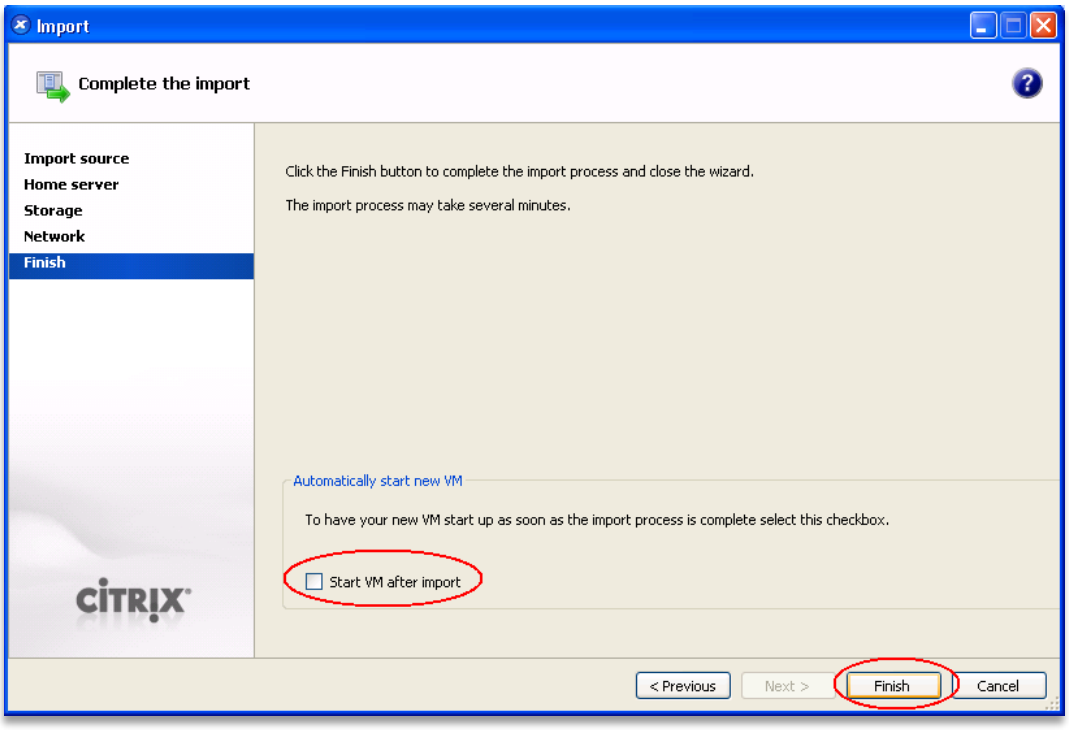
For Citrix XenServer Virtual Environments

To install the Stratusphere appliances directly onto your XenServer host:

1. Download the XVA ZIP file from the Liquidware Product Download page and un-zip the file. (Visit http://www.liquidware.com/Download/ to register and get access to fully functional evaluation copies of the Stratusphere software.)
2. Open the XenCenter Client and connect to your target XenServer host.
3. In the XenCenter Client, select **File > Import VM…** and proceed through the wizard, specifying the location of the downloaded XVA file.



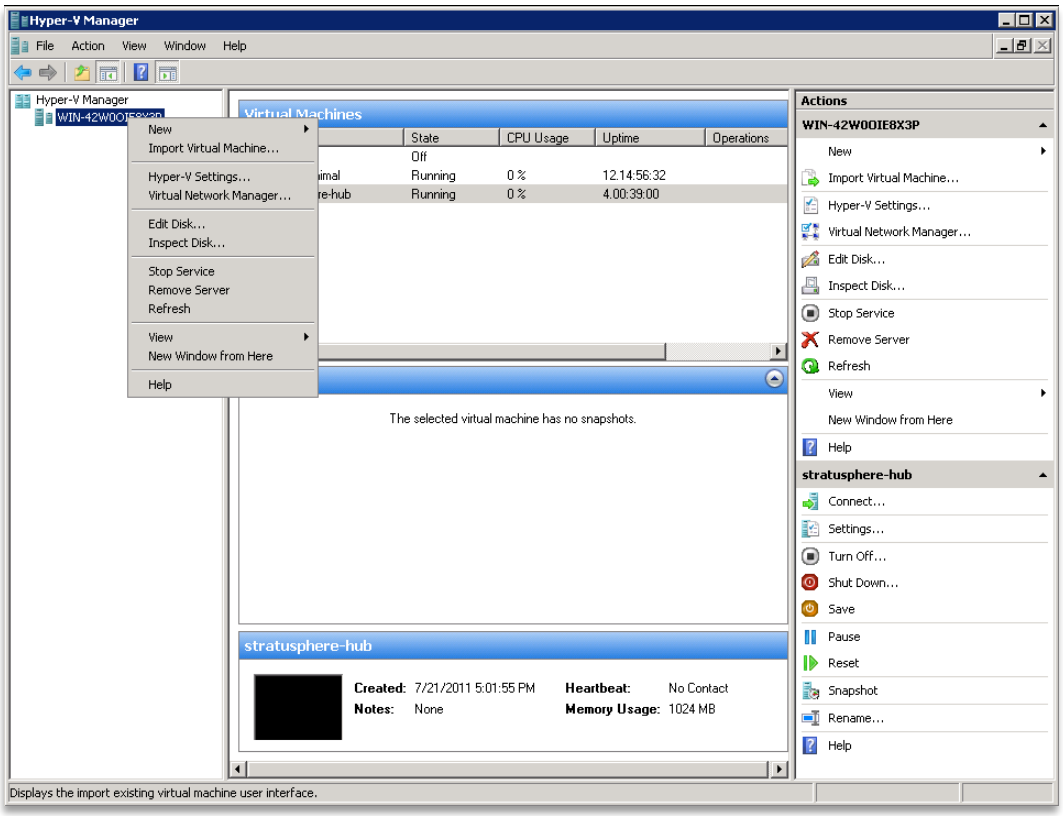
4. For VM resizing purposes, make sure **Start VM after import** is unchecked. Then click **Finish**.



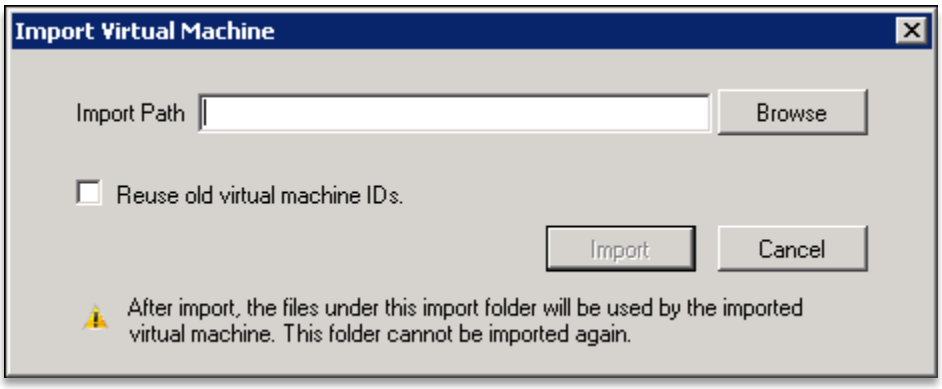
For Microsoft Hyper-V Virtual Environments

To install the Stratusphere appliances directly onto your Microsoft Hyper-V host:

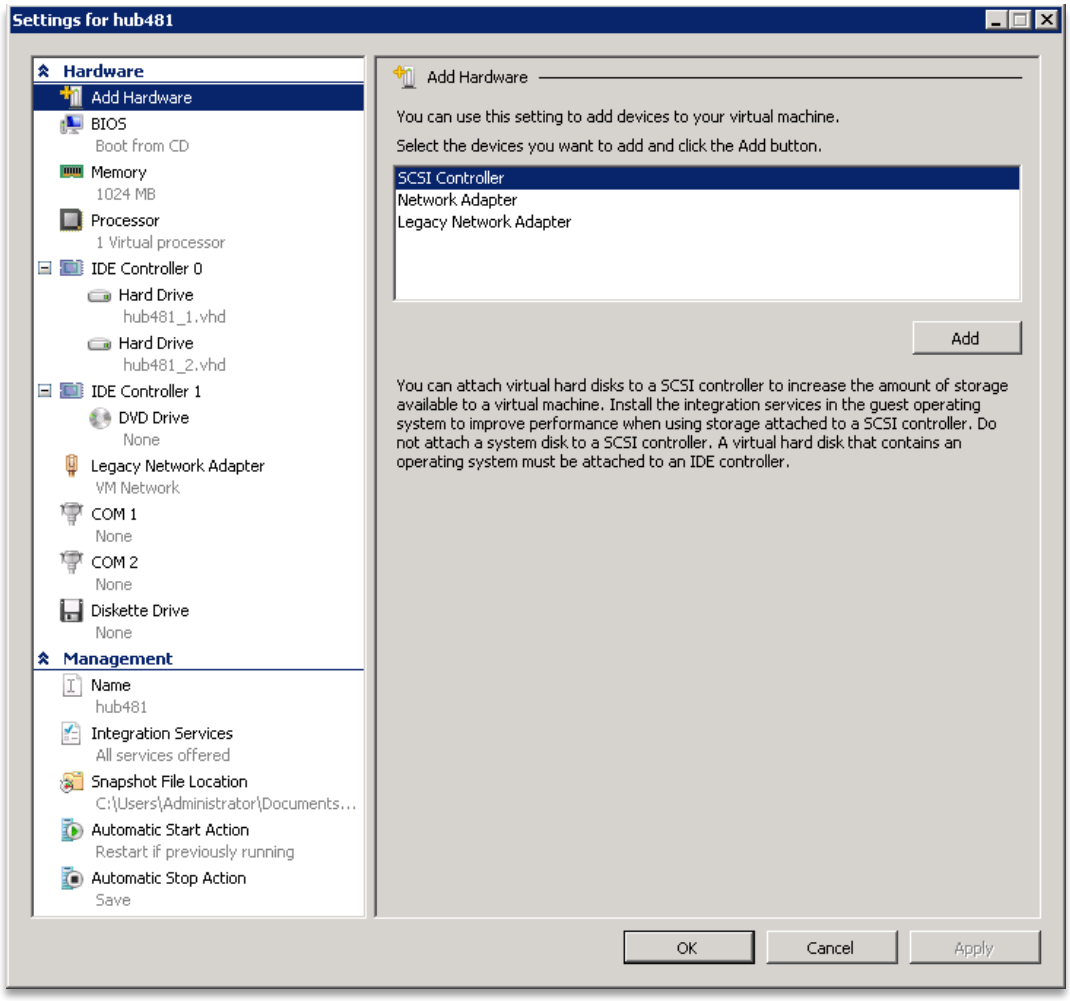
1. Download the Hyper-V ZIP file from the Liquidware Product Download page and un-zip the file. (Visit http://www.liquidware.com/Download/ to register and get access to fully functional evaluation copies of the Stratusphere software.)
2. Open the Microsoft Hyper-V Manager Client and connect to your target Hyper-V host.
3. Right click on the Hyper-V host and select the **Import Virtual Machine…** menu option.



4. Click on the **Browse** button to select the folder that contains the files that were extracted from the ZIP file.



5. 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.



For Other Virtual Environments

To install the Stratusphere appliances in other virtual environments, you will need to provide your virtual host with the URL for the OVF Stratusphere appliance that is listed on the Liquidware Product Download page. The OVF versions of the Stratusphere appliances are generic virtual machines that should work on most other virtualization platforms. (Visit http://www.liquidware.com/Download/ to register and get access to fully functional evaluation copies of the Stratusphere software.)

Installing Stratusphere Appliances on Amazon Web Services

The Stratusphere Hub, Database & Collector appliances can also be installed easily on Amazon Web Services (AWS) using Amazon Machine Image (AMI) names available in each data center within AWS. The Stratusphere Hub appliance is available as a Bring Your Own License (BYOL) and an Hourly Metered Marketplace appliance. Depending on your licensing and usage scenarios, you can select any one of these types of appliances.

The Stratusphere Hub appliance is the data collector and reporting system for diagnostics and it also includes the data collection software agents that will be deployed within the machines. The Stratusphere Database appliance is a dedicated database appliance for higher performance and scale for larger installations. The Stratusphere Collector appliance is a dedicated data collector appliance that is used to offload this load from the Hub appliance. Please use the Liquidware Stratusphere Sizing Guide to determine resource sizing guidelines for the Hub and CID Collector appliances. The first step is to install the Hub appliance and, if the sizer states based on your configuration, install the Database and Collector appliances as well. Since these virtual appliances are basically server appliances with a web front end, data collection and storage, and reporting appliance, it is recommended that you deploy them on AWS Instance Tiers appropriate for high performance server applications. The following instructions are meant to install the Stratusphere Appliances within your AWS data center location within your Virtual Private Circuit (VPC).

Note: Since the instructions for the Hub, Database and Collectors are the same, please use the appropriate AMIs and note the differences in AWS Instance Types, models as well as resource requirements regarding vCPUs, RAM, number of disks and disk space required between the Hub, Database and Collector appliances.

Stratusphere BYOL & Hourly Metered Marketplace Hub Appliances

Liquidware provides BYOL and Hourly Metered Marketplace Hub appliances. If you already have a perpetual Stratusphere license, you can use it to migrate your data from your on-premises installation into AWS. Contact Liquidware to migrate the license to the new Stratusphere Hub appliance when you need to apply the new BYOL license to this new Hub in the cloud. If you chose to use the Hourly Metered Stratusphere Hub, you can simply subscribe to it using AWS subscription. AWS will charge you as part of your standard billing cycle based on a User per Hour charging model. The Stratusphere Database and Collector appliances are only available as public AMIs in each region. They can be used with the BYOL or Hourly Metered Hub appliances.

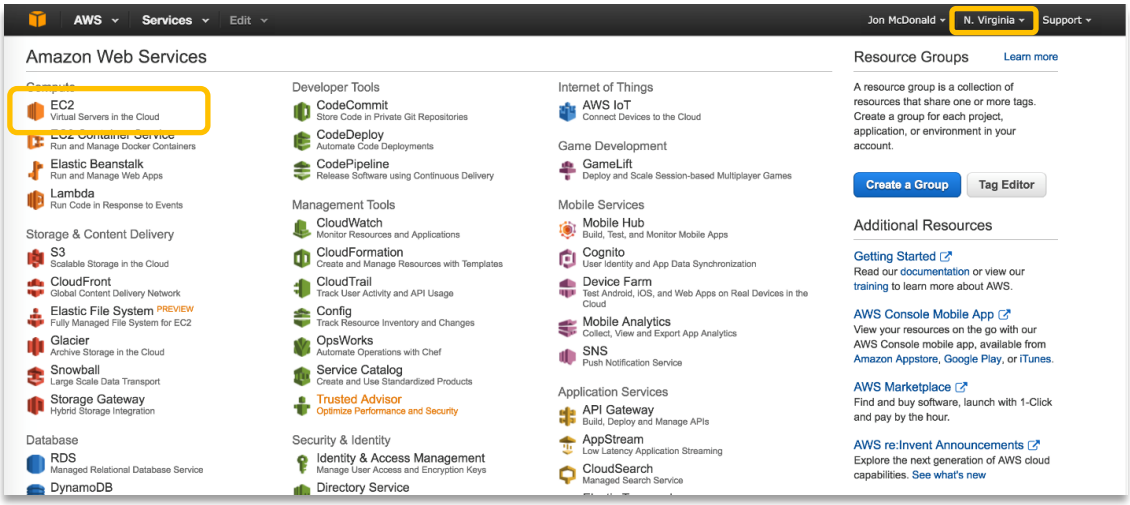
Preparation

1. Please acquire administrative credentials to the Amazon Web Services EC2 environment for your organization.
2. Please use the Liquidware Stratusphere Sizing Guide to appropriately size the Stratusphere Hub and Collector appliance for your installation base.

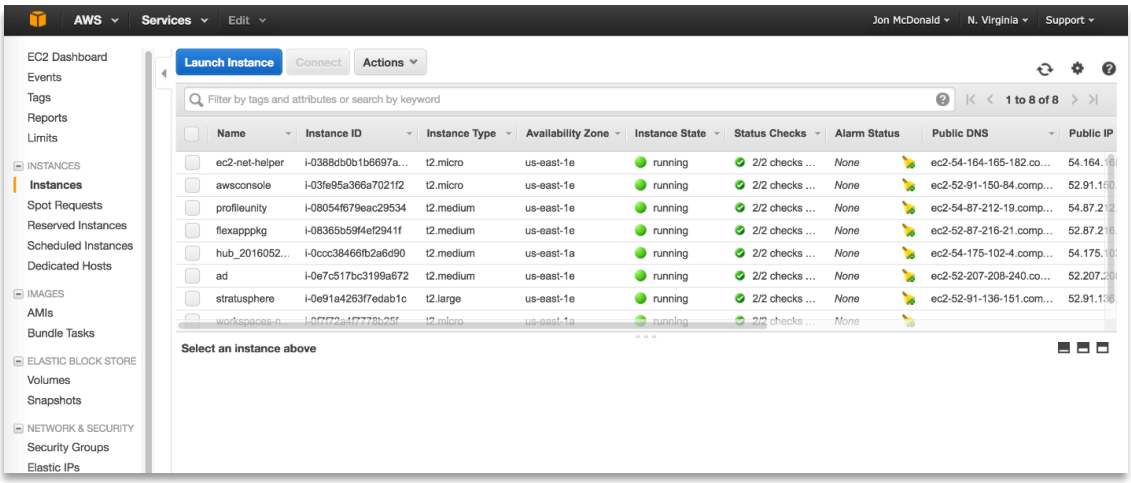
Instructions

1. Please refer to the Liquidware Product Download page for the most up to date Stratusphere Hub, Database, and Collector AMIs for your data center.
2. Log into your Amazon Web Services EC2 site using your administrative credentials.

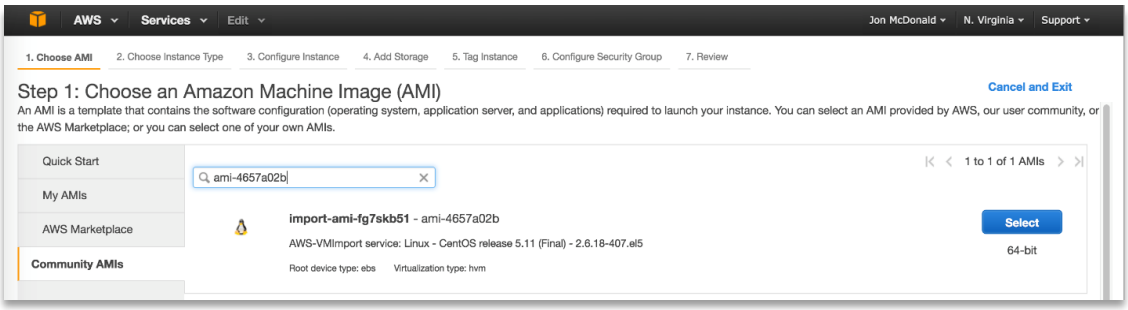
3. Make sure you select the appropriate **Data Center Location** on the top right of the page. Click on the **EC2** link to manage all your virtual machines in the cloud.



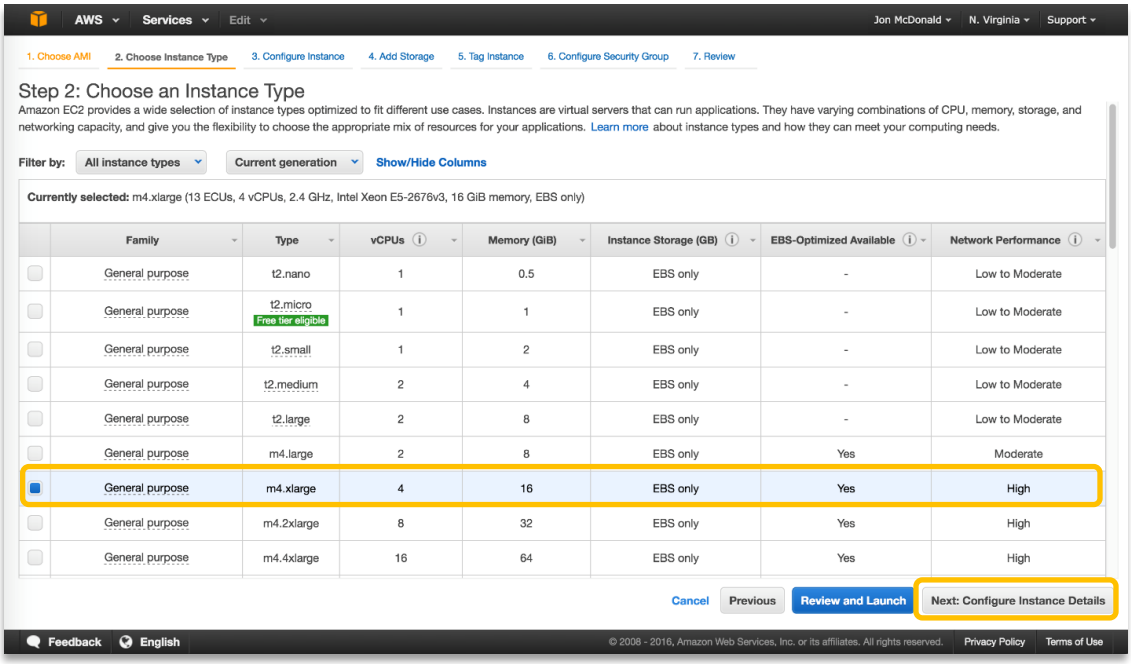
4. Then select the **Instances** link on the left side list. To create a new virtual machine, without selecting any existing machine, click on the **Launch Instance** button to begin.



5. As part of this wizard, on STEP 1: CHOOSE AN AMAZON MACHINE IMAGE (AMI) page. Select **Community AMIs** or **AWS Marketplace** on left side. Search for the AMI ID (Hub, Database or Collector) for your region and select it. Click **Select** to proceed.



6. On STEP 2: CHOOSE AN INSTANCE TYPE page, for the Hub we recommend selecting the **m4.xlarge** instance for starters. Depending on the Stratusphere Sizing Guide, please select the appropriate model with adequate number of vCPUs and RAM. Click on the **Next: Configure Instance Details** button.

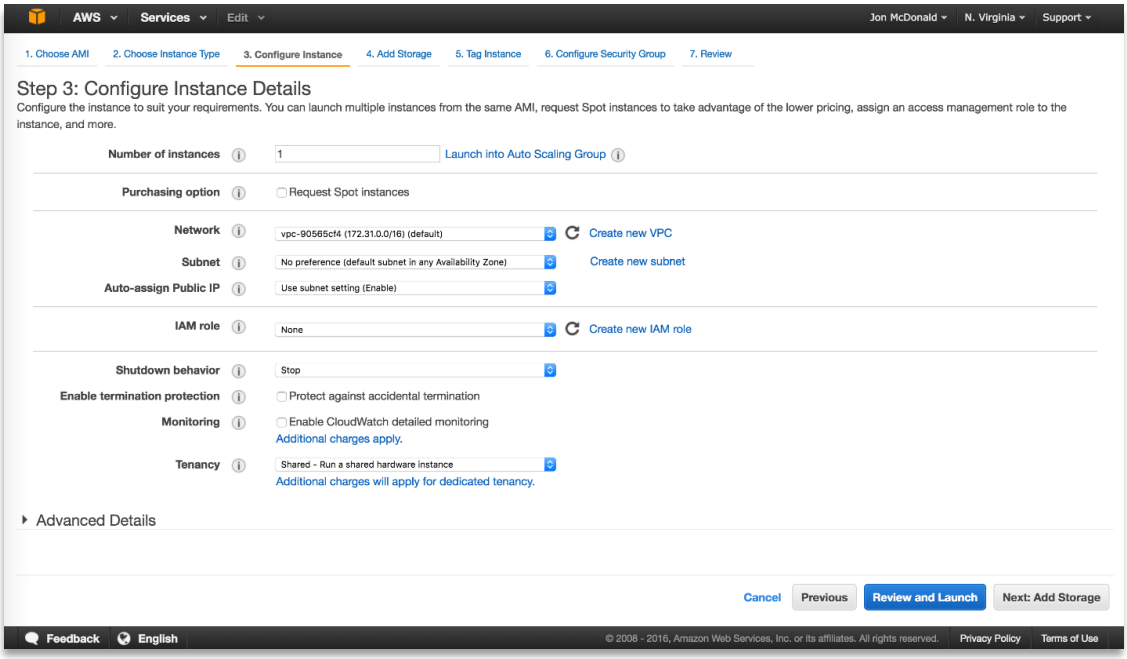


The following chart shows which Amazon EC2 Instance Types and minimum model sizes are supported to run Stratusphere UX Hub appliances. Please choose one of these Instance Types using the minimum model size or higher as needed to accommodate the CPU and RAM requirements calculated by the Stratusphere Sizing Guide.

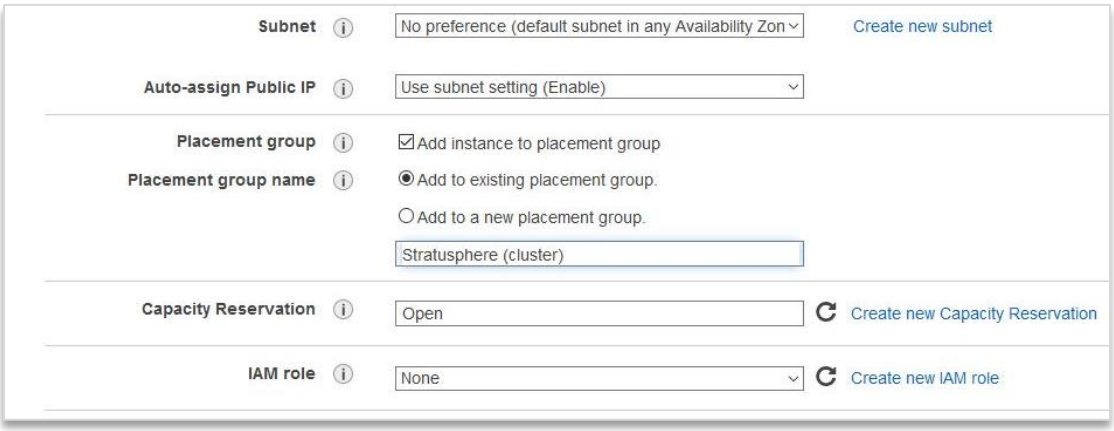
Instance Type	Description	Minimum Model	Recommended	Supported	Tested
M4	General Purpose	xlarge	Yes	Yes	Yes
M5	General Purpose	xlarge	Yes	Yes	Yes
M5a	General Purpose	xlarge	Yes	Yes	Yes
M5d	General Purpose	xlarge	Yes	Yes	Yes
T3	General Purpose	xlarge	Yes	Yes	Yes

The Stratusphere Collector appliances on AWS require 2 vCPUs and at least 4 GB of RAM. Liquidware recommends using the **m4.large** model for Collector appliances that have 2 vCPUs and 8 GB of RAM. Please set the disk space requirements as per the Sizing Guide mentioned above.

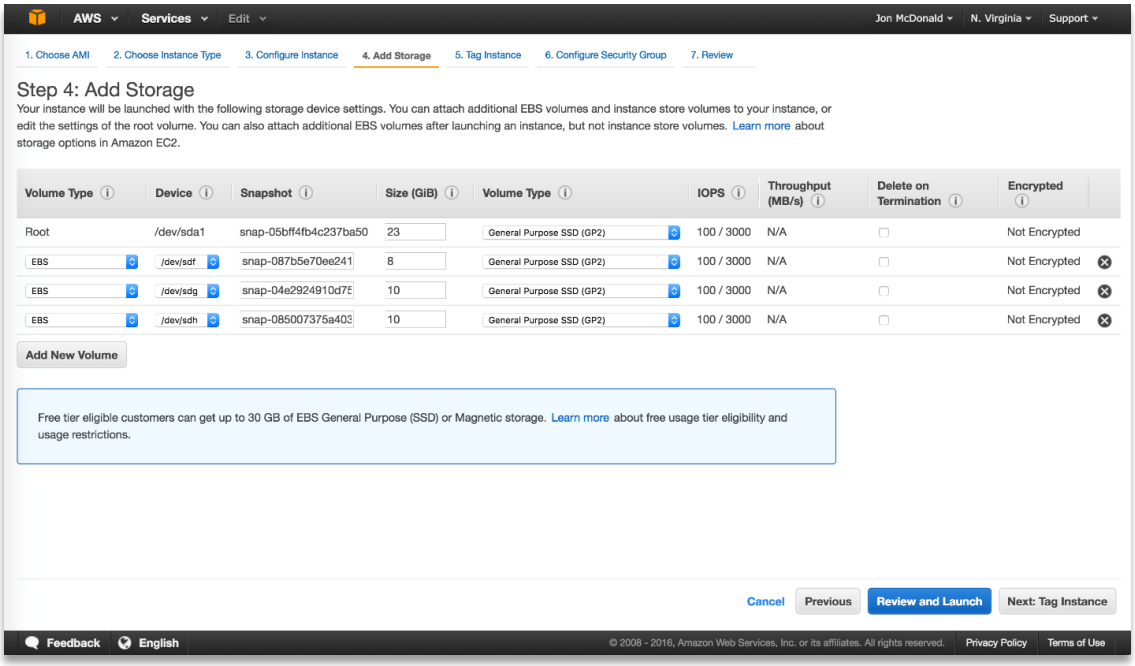
7. On STEP 3: CONFIGURE INSTANCE DETAILS page, enter 1 as N**umber of instances** and select the appropriate **Network VPC** as shown below and then click on the **Next: Add Storage** button.



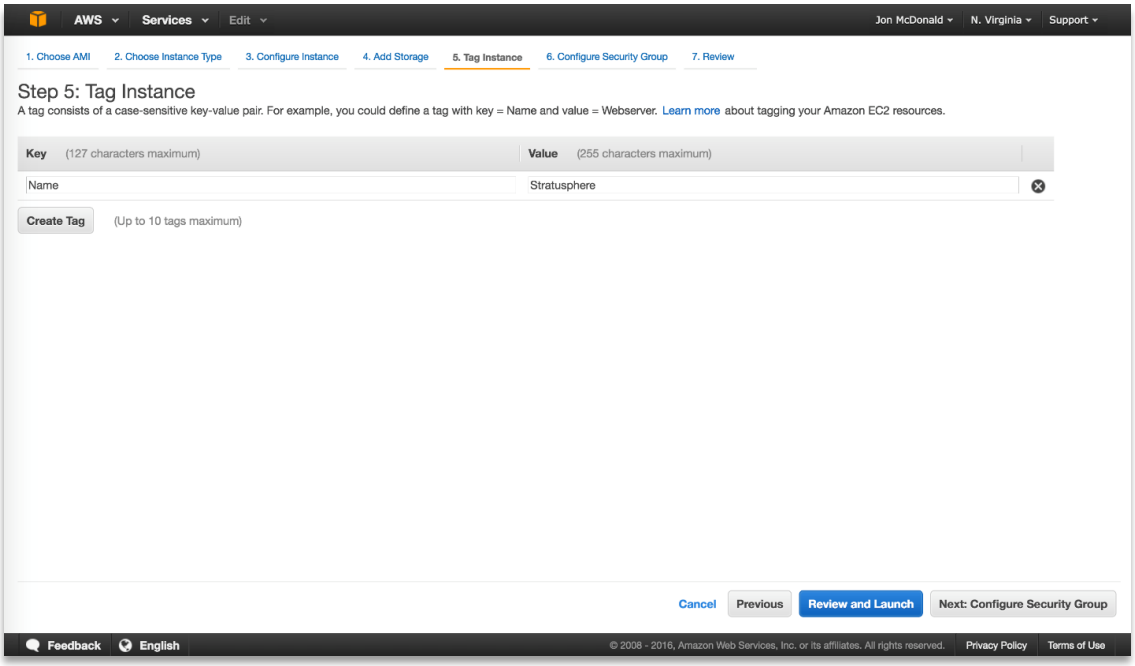
If you are installing multiple Stratusphere appliances, such as a Hub and a Database or a Collector, AWS provides **Placement Groups** to enhance network connectivity and reduce latency between the Stratusphere appliances. Liquidware recommends creating a Cluster based Placement Group and adding each Stratusphere appliance to this Placement Group during configuration itself. Here is an example, with an appropriately named **Stratusphere** Placement group:



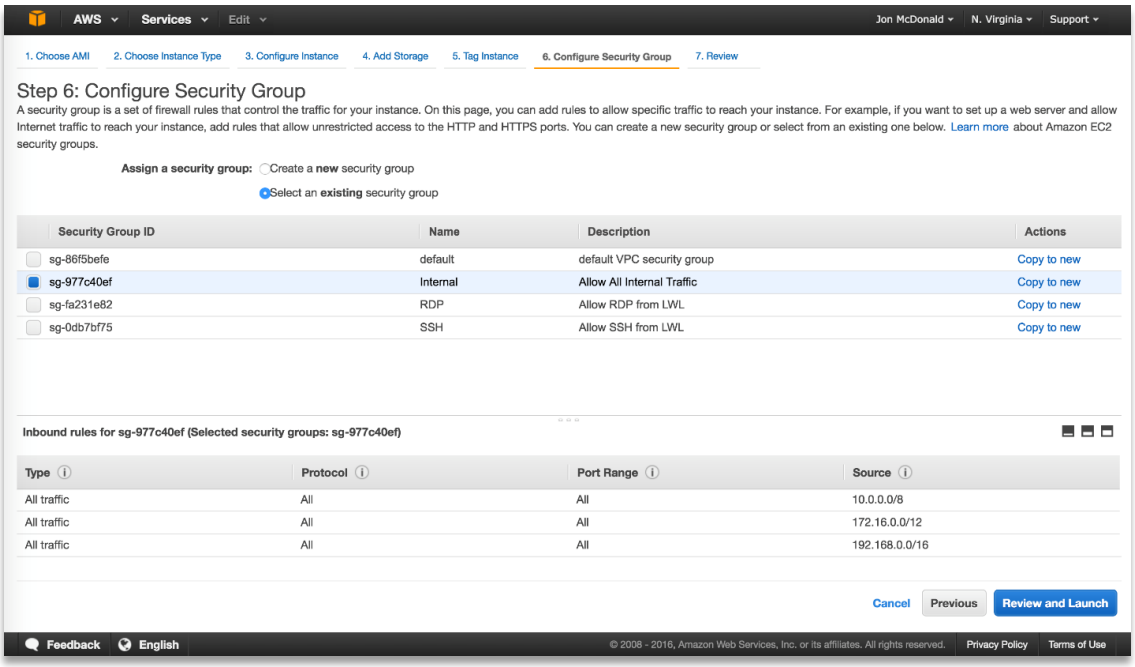
8. On STEP 4: ADD STORAGE page, enter the appropriate hard disk sizing details based on Stratusphere Sizing Guide recommendations, an example of which is shown below. Please note that the AWS storage devices may not be listed in alphabetical order. Make sure the AWS label matches the Sizing Guide. For example, "/dev/sdg" is "HD 3", which is to be used for database storage. Click on **Next: Tag Instance** to proceed.



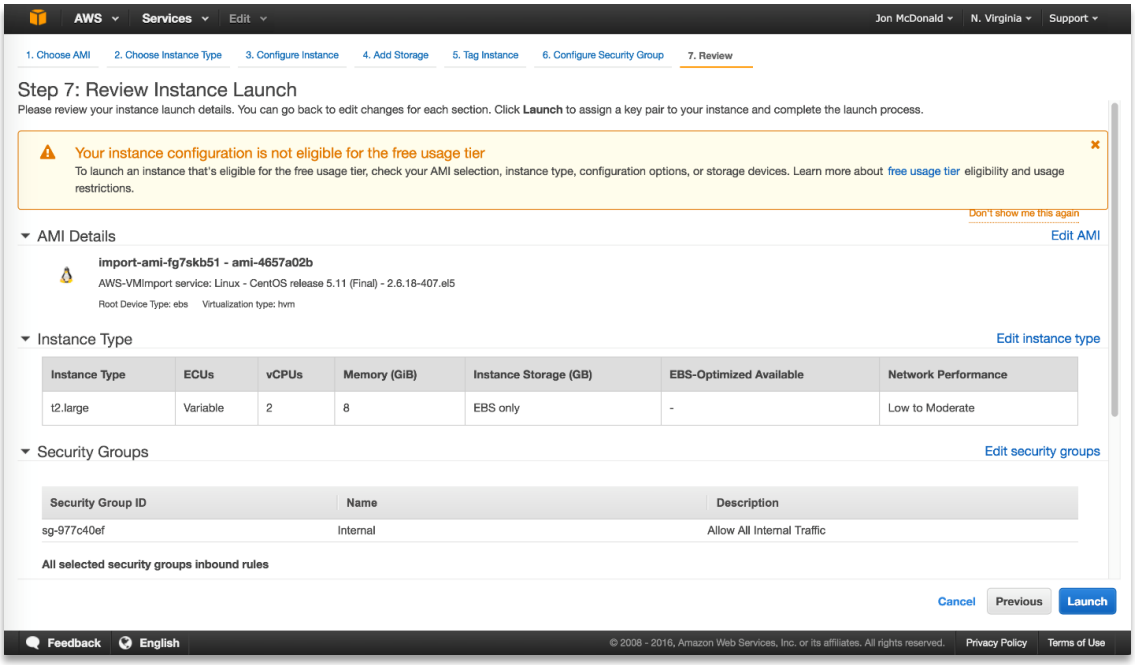
9. On STEP 5: TAG INSTANCE page, enter ***Stratusphere*** or ***Hub*** or ***CIDCollector*** or a similar value for the **Key, Value** pair to tag the virtual appliance properly. Click on **Next: Configure Security Group** to proceed.



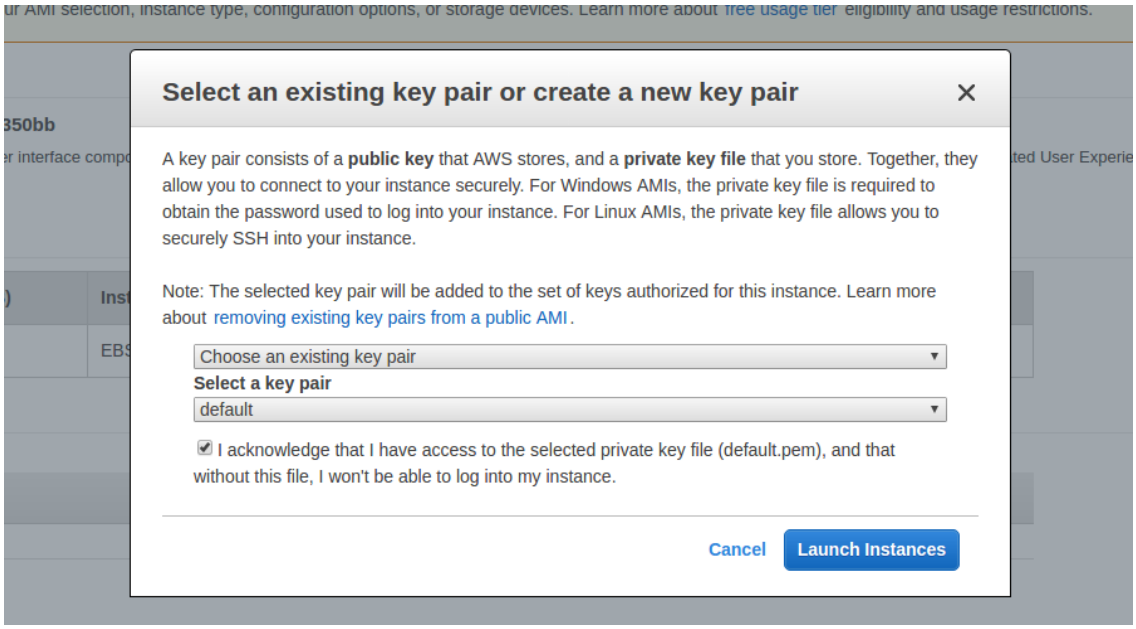
10. On STEP 6: CONFIGURE SECURITY GROUP page, select or create an appropriate security groups that would allow traffic to the Stratusphere Hub appliance. For convenience, you could create a sample security group that allows ALL INTERNAL TRAFFIC to this appliance for now and then come back later to allow only the protocols and ports that are required for the Stratusphere Hub appliance. Click on **Review and Launch** to proceed.



11. On STEP 7: REVIEW INSTANCE LAUNCH page, review and verify the selection of the right AMI, all the Instance settings and Security Group configurations. Once validated, click on the **Launch** button to create, install, configure and launch the Stratusphere Hub or Collector Appliance.

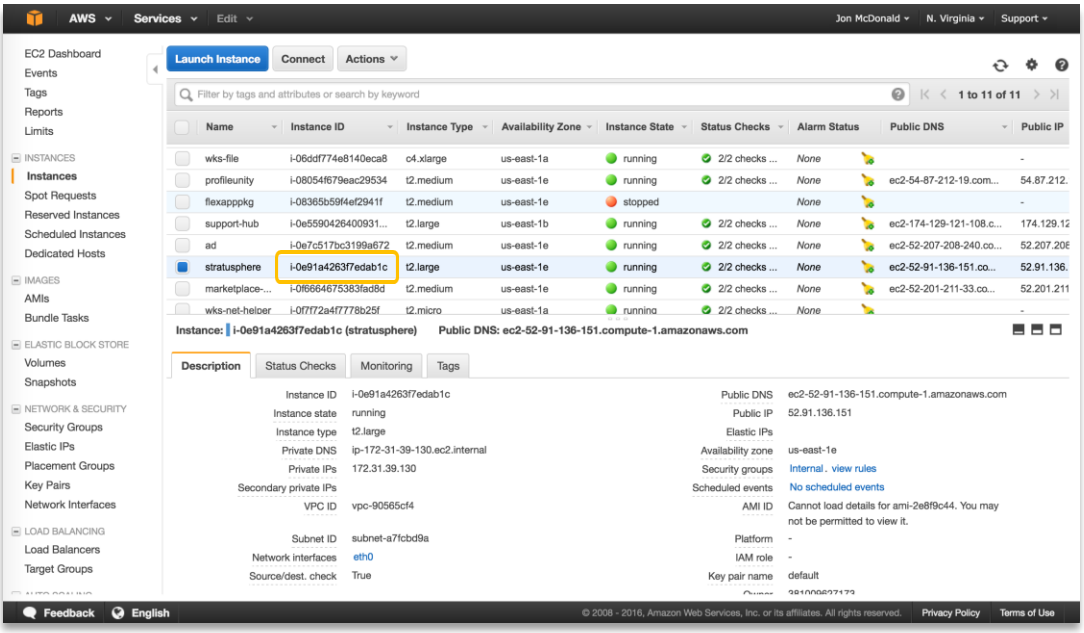


12. Amazon recommends usage of key pairs for accessing AMIs. Please make a selection from the options provided:



13. The AWS EC2 UI will now return to the list of your AMIs. It will show the Stratusphere appliance being prepared with a **State** showing *pending* and once finished will switch to the *running* state. The **Instance Status** column will display *Initializing…* for some time and will then perform some checks to show *Check 2/2*. The entire import, install, and configuration process should take about 10-15min after Launch time. It needs some time to perform some startup configuration tasks before it is ready for use.
14. Make note of the Local IP address, DNS Name, and host name for the appliance. For a Hub appliance, use the Local IP address of the appliance displayed in the bottom half of the AWS UI and use your preferred browser to navigate to the following address: **`https://<enter.hub.ip.address>`**.

15. While following the instructions in the standard documentation that follows, we would like for you to note the following differences:
    a. AWS does NOT allow default passwords for appliances i.e. *sspassword*. So anywhere you see ***sspassword*** please replace it with the **Instance ID** of the virtual machine as seen on the EC2 page for the details of the Hub appliance. This applies to the default *ssadmin* user on the Web UI of Stratusphere Hub.



    b. If using PuTTY to SSH into the Stratusphere Hub, as per AWS recommendations, we recommend using SSH key pairs associated with the automatically created AWS User ID: **`ec2-user`**. If you want to switch to root user while logged into the console for Stratusphere Hub, you should use '*sudo <command>*' to execute commands that require elevated permissions.
16. Please use the standard documentation to now log into the Hub Web UI and configure the appliance.
17. Before beginning use of Stratusphere appliances in production, Liquidware would like to remind you to please use the Liquidware Stratusphere Sizing Guide to appropriately size the Stratusphere Hub appliance and Collector appliance for your installation base.
18. After installing the Hub, repeat these same instructions to install the Database and Collector appliance(s). Once installed, please see the instructions below to establish trust between a Database & a Hub before using the standard process of joining them together, as well as how to add and register Collector appliances to the Stratusphere Hub.

Establish trust between Stratusphere Hub and Database

AWS does not allow usage of standard passwords to log into appliance consoles. As documented above, SSH keys must be setup to establish trust between appliances before the join can be performed. For the join to work:

A. The **`ec2-user`** on the Hub must be able to SSH without a password to the **`ec2-user`** on the Database, and
B. The **`root`** user on the Hub must be able to SSH without a password to the **`ec2-user`** on the Database for upgrade purposes.
C. The **`root`** user on the Database must be able to SSH without a password to the **`ec2-user`** on the both the Hub and Database appliances

Here is the list of items to prepare for and instructions to establish trust between these appliances before you can use the standard join process:

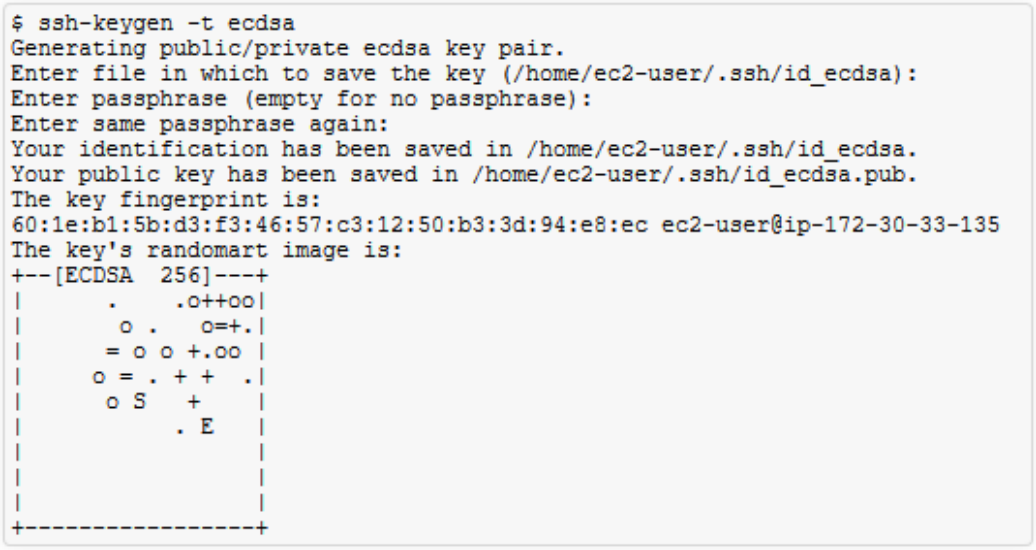
Preparation

1. Ensure the security policy of each appliance allows SSH connections between the Hub & Database.
2. Ensure the security policy of the Hub appliance allows connections to the Database appliance on port TCP/5432.

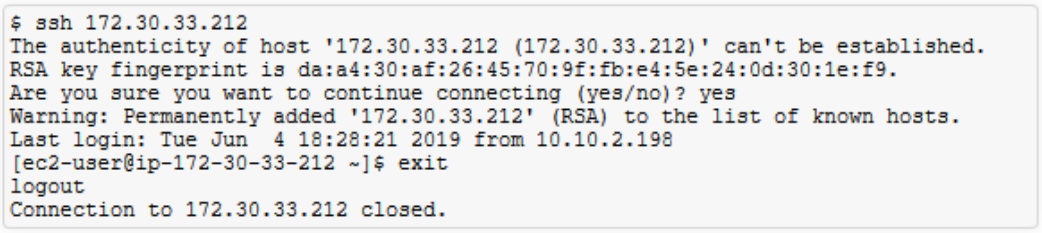
Instructions

In some commands below, `<right-click-mouse-to-paste>` is a placeholder for the action of right-clicking the mouse within PuTTY – this action automatically pastes the contents of the clipboard into the PuTTY command line. Neither the actual characters such as < and > nor the text, `right-click-mouse-to-paste`, should be typed in on the command line. This merely represents the action that should be taken at that point in the command line.

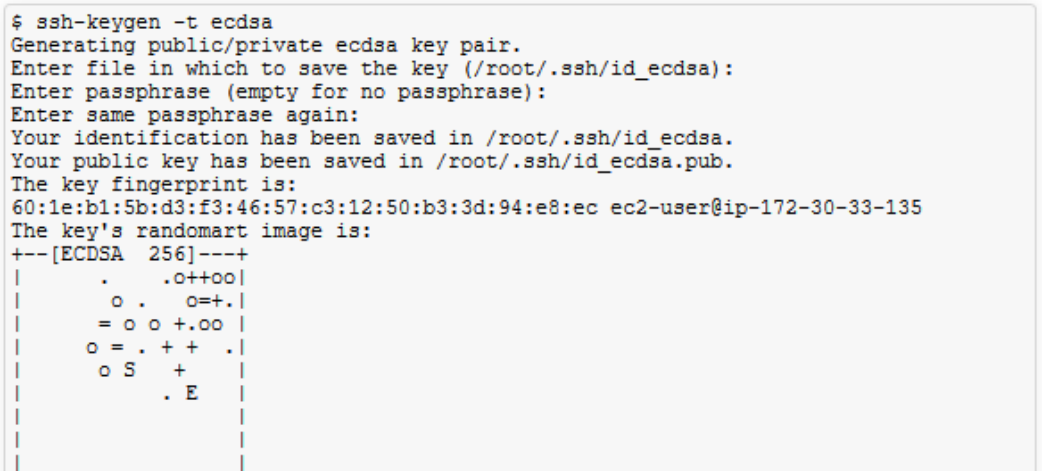
#	Hub Instructions	Database Instructions
1	Using a tool like PuTTY, open two SSH connections to each appliance and place them side by side. Connect to the Stratusphere appliance consoles using the standard **`ec2-user`** with the associated AWS keys. Here is a link to a quick refresher on how to do so from the AWS documentation.	
	To address point (A) above:	
2	Within the SSH console of the Hub appliance, while logged in as the **`ec2-user`**, generate a new SSH key by executing the following command and accepting the defaults by pressing ENTER: **`ssh-keygen -t ecdsa -q -N ""`** DO NOT enter a passphrase if prompted by the keygen command. Leave the field empty.	

#	Hub Instructions	Database Instructions
		
3	Within the same SSH console of the Hub appliance, print the contents of the SSH public key by executing the following command, and then use your mouse to select the entire sequence of characters displayed, that forms the public key, to copy it to your clipboard: ➢ **`cat .ssh/id_ecdsa.pub`**	
		
4		Now switch to the SSH console on the Database appliance, and add the Hub's **`ec2-user`** public key to the authorized list of keys that can connect as the **`ec2-user`** by using the echo command and pasting the key copied from above, and sending it to the `authorized_keys` file: ➢ **`echo "<right-click-mouse-to-paste>" >> .ssh/authorized_keys`**
5	Now, from within the SSH console on the Hub appliance, verify whether the Hub can now connect without a password to the Database as	

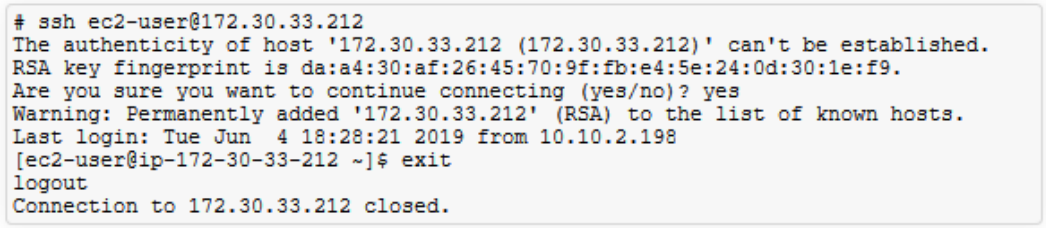
#	Hub Instructions	Database Instructions
	the **ec2-user**. You will have to accept the SSH keys and then logout from the connection: ➢ **ssh <db.ip.or.dns>**	

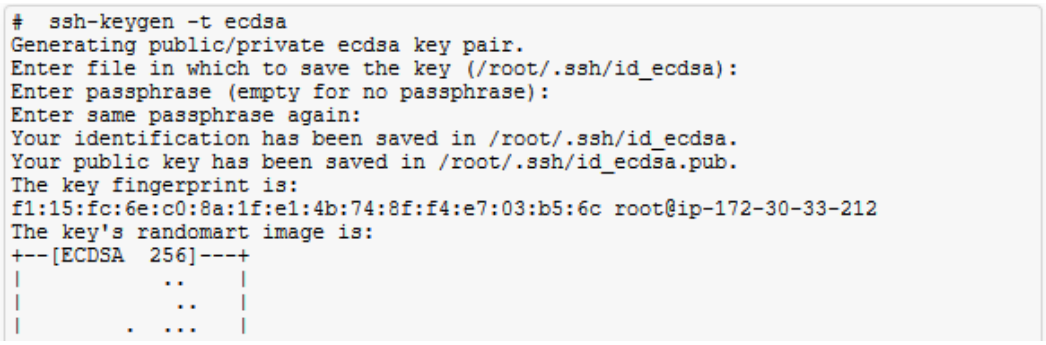
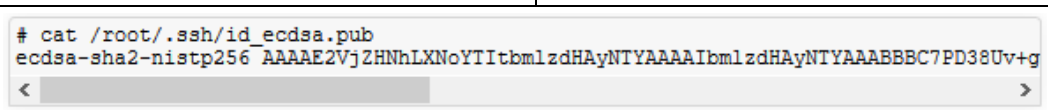
	
	`$ ssh 172.30.33.212`
	`The authenticity of host '172.30.33.212 (172.30.33.212)' can't be established.`
	`RSA key fingerprint is da:a4:30:af:26:45:70:9f:fb:e4:5e:24:0d:30:1e:f9.`
	`Are you sure you want to continue connecting (yes/no)? yes`
	`Warning: Permanently added '172.30.33.212' (RSA) to the list of known hosts.`
	`Last login: Tue Jun 4 18:28:21 2019 from 10.10.2.198`
	`[ec2-user@ip-172-30-33-212 ~]$ exit`
	`logout`
	`Connection to 172.30.33.212 closed.`	

	To address point (B) above:	
6	Now that we have confirmation for **ec2-user**, we need to redo the same process for the **root** user. Within the SSH console on the Hub, switch to **root** and generate a new SSH key. Press ENTER to accept the defaults: **sudo bash** **ssh-keygen -t ecdsa -q -N ""** DO NOT enter a passphrase if prompted by the keygen command. Leave the field empty.	

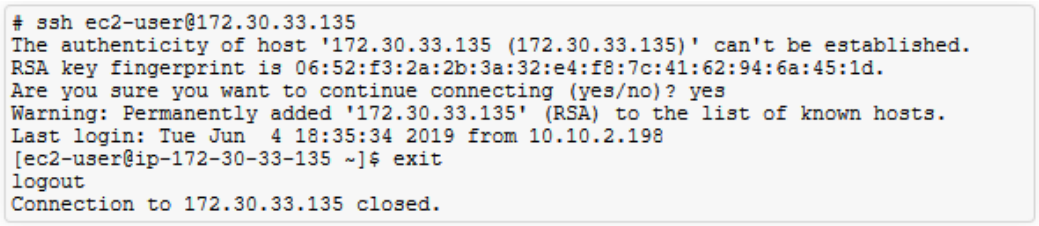
	
	`$ ssh-keygen -t ecdsa`
	`Generating public/private ecdsa key pair.`
	`Enter file in which to save the key (/root/.ssh/id_ecdsa):`
	`Enter passphrase (empty for no passphrase):`
	`Enter same passphrase again:`
	`Your identification has been saved in /root/.ssh/id_ecdsa.`
	`Your public key has been saved in /root/.ssh/id_ecdsa.pub.`
	`The key fingerprint is:`
	`60:1e:b1:5b:d3:f3:46:57:c3:12:50:b3:3d:94:e8:ec ec2-user@ip-172-30-33-135`
	`The key's randomart image is:`
	`+--[ECDSA 256]---+`
	`|  .  .o++oo|`
	`|  o .  o=+.|`
	`| = o o +.oo |`
	`| o = . + +  .|`
	`|  o S  +  |`
	`|  . E  |`
	`|  |`
	`|  |`
	`|  |`	

7	Within the same SSH console of the Hub appliance, print the contents of the SSH public key by executing the following command, and then use your mouse to select the entire sequence of characters displayed, that forms the public key, to copy it to your clipboard:	

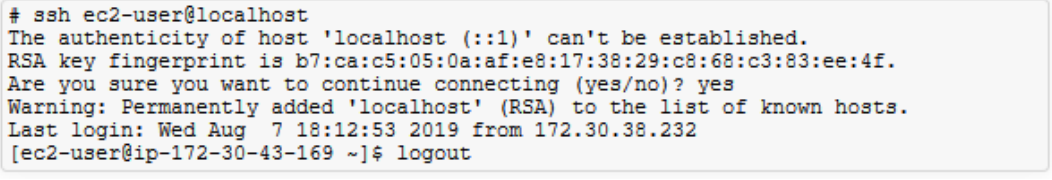
#	Hub Instructions	Database Instructions
	➢ **cat /root/.ssh/id_ecdsa.pub**	
		
8		Now switch to the SSH console on the Database appliance, and add the Hub's **root** user public key to the authorized list of keys that can connect as the **ec2-user** by using the echo command and pasting the key copied from above, and sending it to the authorized_keys file: ➢ **echo "<right-click-mouse-to-paste>" >> .ssh/authorized_keys**
9	Now, from within the SSH console on the Hub appliance, verify whether the Hub can now connect without a password to the Database as the **ec2-user**. You will have to accept the SSH keys and then logout from the connection: ➢ **ssh ec2-user@<db.ip.or.dns>**	
		
10	Now, from within the SSH console on the Hub appliance, log out as **root** to return to the **ec2-user** to prepare for the next set of commands below. ➢ **exit**	
	To address point (C) above:	
11		Within the SSH console of the Database, switch to **root** user using the command: ➢ **sudo bash**

#	Hub Instructions	Database Instructions
12		Within the same SSH console on the Database, generate a new SSH key as the **root** user by executing the following command and accepting the defaults by pressing ENTER: **ssh-keygen -t ecdsa -q -N ""** DO NOT enter a passphrase if prompted by the keygen command. Leave the field empty.
		
13		Within the same SSH console of the Database appliance, print the contents of the **root** user's SSH public key by executing the following command, and then use your mouse to select the entire sequence of characters displayed, that forms the public key, to copy it to your clipboard: ➢ **cat /root/.ssh/id_ecdsa.pub**
		
14		Within the same SSH console on the Database appliance, add the Database's **root** user public key to the authorized list of keys that can connect as the **ec2-user** by using the echo command and pasting the key copied from above, and sending it to the `authorized_keys` file: ➢ **echo "<right-click-mouse-to-paste>" >> /home/ec2-user/.ssh/authorized_keys**

#	Hub Instructions	Database Instructions
15	Now, from within the SSH console on the Hub appliance, add the Database's **root** user public key to the authorized list of keys that can connect as the **ec2-user** by using the echo command and pasting the key copied from above, and sending it to the `authorized_keys` file: ➢ **echo "<right-click-mouse-to-paste>" >> /home/ec2-user/.ssh/authorized_keys**	
16		From within the SSH console of the Database, verify whether the **root** user of the Database can now connect without a password to the Hub as the **ec2-user**. You will have to accept the SSH keys and then logout from the connection: ➢ **ssh ec2-user@<hub.ip.or.dns>**

	
	`# ssh ec2-user@172.30.33.135`
	`The authenticity of host '172.30.33.135 (172.30.33.135)' can't be established.`
	`RSA key fingerprint is 06:52:f3:2a:2b:3a:32:e4:f8:7c:41:62:94:6a:45:1d.`
	`Are you sure you want to continue connecting (yes/no)? yes`
	`Warning: Permanently added '172.30.33.135' (RSA) to the list of known hosts.`
	`Last login: Tue Jun 4 18:35:34 2019 from 10.10.2.198`
	`[ec2-user@ip-172-30-33-135 ~]$ exit`
	`logout`
	`Connection to 172.30.33.135 closed.`	

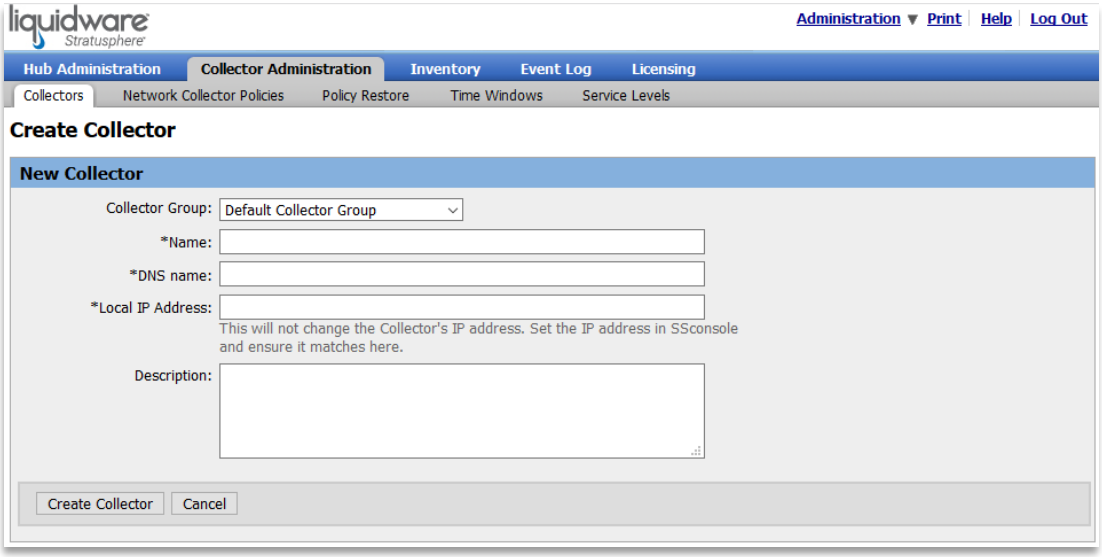
17		From within the same SSH console of the Database, we must also verify whether the **root** user of the Database can connect to itself as the **ec2-user** user. Again, you will have to accept the SSH keys and then logout from the connection: ➢ **ssh ec2-user@localhost**

	
	`# ssh ec2-user@localhost`
	`The authenticity of host 'localhost (::1)' can't be established.`
	`RSA key fingerprint is b7:ca:c5:05:0a:af:e8:17:38:29:c8:68:c3:83:ee:4f.`
	`Are you sure you want to continue connecting (yes/no)? yes`
	`Warning: Permanently added 'localhost' (RSA) to the list of known hosts.`
	`Last login: Wed Aug 7 18:12:53 2019 from 172.30.38.232`
	`[ec2-user@ip-172-30-43-169 ~]$ logout`	

#	Hub Instructions	Database Instructions
18	Now that the trust connections between the Hub and Database using the **`ec2-user`** and **`root`** user have been verified, you can now proceed to the instructions provided in the Connecting the Hub and Database appliances section to formally join a Hub and Database together.	

Add & Register a Stratusphere CID Key Collector to the Hub

1. Once a Stratusphere CID Key Collector is up and running within your AWS EC2 VPC environment, log into ADMINISTRATION product of the Stratusphere Hub's Web UI. Use the default credentials and the Instance ID as password to log in.
2. Navigate to **Collector Administration > Collectors** tab.
3. Click on **New** to add a new Collector.
4. On the following form, add the host name as **Name**, **DNS Name** and **Local IP Address** as observed on the AWS EC2 page for the Collector's details.



5. Click on **Create Collector** to save and create a new Collector.
6. The Hub will reach out to the Collector and help register it. Once registered, the Collector may potentially reboot, get the registration information from the Hub, and then show up as a CID Key Collector within the main **Collector Administration > Collectors** page.
7. Repeat these same instructions for adding and registering additional Collectors.

Installing Stratusphere Appliances on Microsoft Azure

The Stratusphere Hub, Database & Collector appliances can also be installed easily on Microsoft Azure available in each data center within Azure. The Stratusphere Hub appliance is available as a Bring Your Own License (BYOL) appliance.

The Stratusphere Hub appliance is the data collector and reporting system for diagnostics and it also includes the data collection software agents that will be deployed within the machines. The Stratusphere Database appliance is a dedicated database appliance for higher performance and scale for larger installations. The Stratusphere Collector appliance is a dedicated data collector appliance that is used to offload this load from the Hub appliance. Please use the Liquidware Stratusphere Sizing Guide to determine resource sizing guidelines for the Hub and CID Collector appliances. The first step is to install the Hub appliance and, if the sizer states based on your configuration, install the Database and Collector appliances as well. Since these virtual appliances are basically server appliances with a web front end, data collection and storage, and reporting appliance, it is recommended that you deploy them on Azure Instance Types appropriate for high performance server applications. The following instructions are meant to install the Stratusphere Appliances within your Azure data center location.

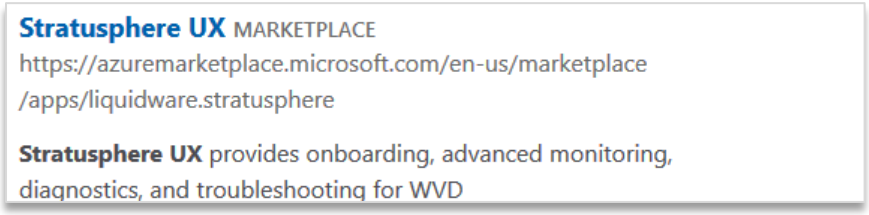
Note: Since the instructions for the Hub, Database and Collectors are the same, please use the appropriate option and note the differences in Instance Types as well as resource requirements regarding vCPUs, RAM, number of disks and disk space required between the Hub, Database and Collector appliances.

Stratusphere BYOL Marketplace Hub Appliances

Liquidware provides BYOL Marketplace Hub appliances. If you already have a perpetual Stratusphere license, you can use it to migrate your data from your on-premises installation into Azure. Contact Liquidware to migrate the license to the new Stratusphere Hub appliance when you need to apply the new BYOL license to this new Hub in the cloud. The Stratusphere Database and Collector appliances are available in each region and can be used with the BYOL Marketplace Hub appliances.

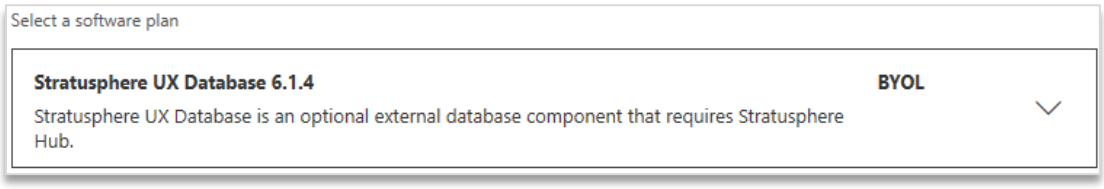
Preparation

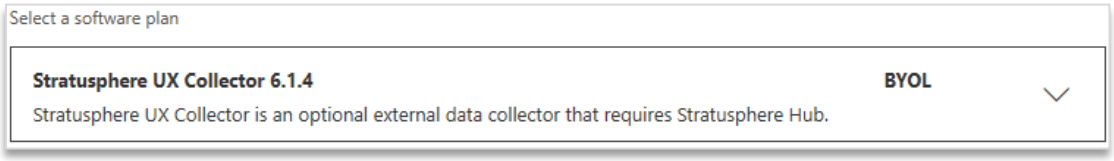
1. Please acquire administrative credentials to the Microsoft Azure environment for your organization.
2. Please use the Liquidware Stratusphere Sizing Guide to appropriately size the Stratusphere Hub, Database and Collector appliance for your installation base. Stratusphere best practices strongly recommend having the Hub and Collectors as close to the Database as possible, at least within the same region and preferably on the same host. If the sizing guide recommends or requires a Database and Collector appliances, Liquidware strongly recommends:
    a. Creating a HOST GROUP within Azure (may result in additional charges)
    b. Creating a PROXIMITY PLACEMENT GROUP within Azure.
3. From a planning perspective, if you need to understand some of the resources associated with the Stratusphere UX solution, please go to the Stratusphere UX App on Microsoft's Azure Marketplace or search for **'Stratusphere UX'** on the Microsoft Azure website, and select the following on the page:



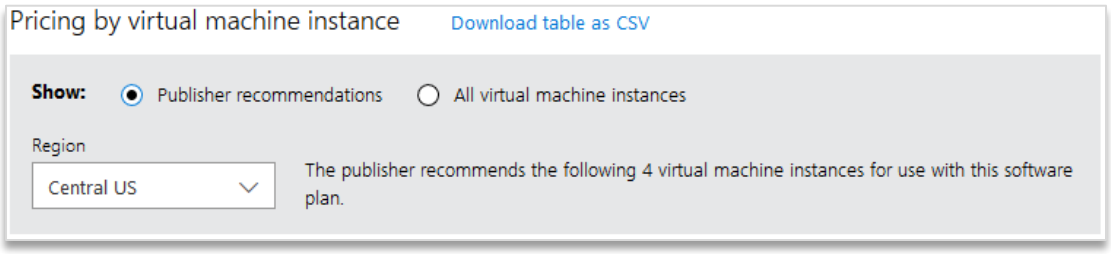
4. On the main PRODUCTS > STRATUSPHERE UX page, it will start by displaying the basic OVERVIEW tab with introductory information on Stratusphere including links to release notes, installation and configuration guides, sizing guide, etc. Click on the PLANS + PRICING tab to see the available software plans. Start with the drop down under **Select a software plan** and select **Stratusphere UX (x.x.x)** option. This is the main component of the solution called the Hub. The other two plans are optional software components called Stratusphere UX (x.x.x) Database and Collector.

After using the instructions below for installing the Hub, depending on the recommendations of the Stratusphere Sizing Guide, please use the Stratusphere UX Database and Stratusphere UX Collector options for installing the other appliances – the instructions below remain the same.





5. To verify it is available within your region, choose the region that you want to deploy the Stratusphere UX solution within.



6. Use the Stratusphere Sizing Guide to enter the number of machines that need to be monitored, and based on its recommendations, determine the right instance out of the suggested machine instances under the Publisher recommendations. Liquidware has already chosen a list of instances for each of its appliances running on Azure.
   Here are instances recommended for the Stratusphere Hub:

Virtual Machine		Configuration				Cost per hour	
Instance	Category	Cores	RAM	Disk Space	Drive Type	Infrastructure Cost	Software Cost
D4SV3*	General Purpose	4	16GB	32GB	SSD	$0.22	BYOL
D8SV3*	General Purpose	8	32GB	64GB	SSD	$0.44	BYOL
D16SV3*	General Purpose	16	64GB	128GB	SSD	$0.88	BYOL
D32SV3*	General Purpose	32	128GB	256GB	SSD	$1.76	BYOL

*Premium storage is available for this type of virtual machine. Learn more

   Here are the instances for the Stratusphere Database:

Virtual Machine		Configuration				Cost per hour	
Instance	Category	Cores	RAM	Disk Space	Drive Type	Infrastructure Cost	Software Cost
D4SV3*	General Purpose	4	16GB	32GB	SSD	$0.22	BYOL
D8SV3*	General Purpose	8	32GB	64GB	SSD	$0.44	BYOL
D16SV3*	General Purpose	16	64GB	128GB	SSD	$0.88	BYOL
D32SV3*	General Purpose	32	128GB	256GB	SSD	$1.76	BYOL

*Premium storage is available for this type of virtual machine. Learn more

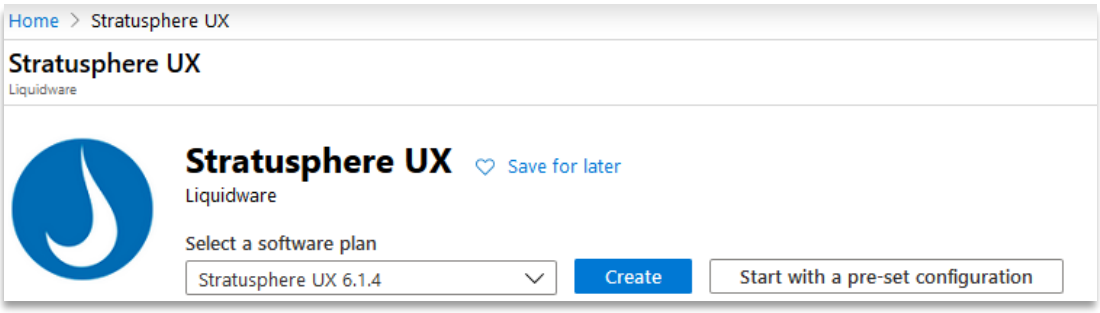
   Here are the instances for the Stratusphere Collector:

Virtual Machine		Configuration				Cost per hour	
Instance	Category	Cores	RAM	Disk Space	Drive Type	Infrastructure Cost	Software Cost
B2S*	Standard	2	4GB	8GB	SSD	$0.052	BYOL
D2SV3*	General Purpose	2	8GB	16GB	SSD	$0.11	BYOL

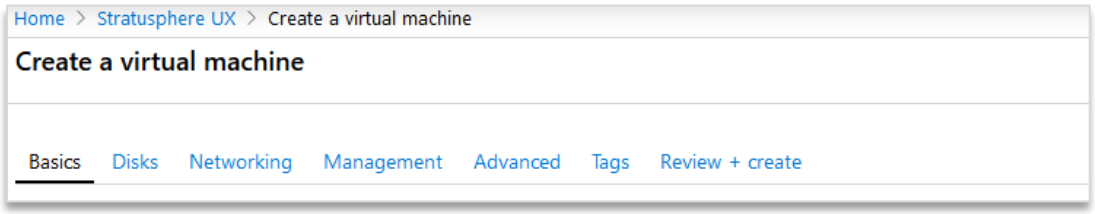
*Premium storage is available for this type of virtual machine. Learn more

Instructions

1. To begin the installation process, log into the Microsoft Azure Portal and click on the **CREATE A RESOURCE** button at the top of the home page.
2. Search for **'Stratusphere UX'** within the search box provided and select the Stratusphere UX search result.
3. It should take you to the following page. If you are starting your Stratusphere UX installation, select **STRATUSPHERE UX X.X.X** option from the SELECT A SOFTWARE PLAN dropdown. If you are adding a Database or Collector, then select the appropriate option under the SELECT A SOFTWARE PLAN dropdown. Then click on the **CREATE** option button.



4. The **Create** option will present a new wizard based CREATE A VIRTUAL MACHINE page with a series of tabs that can be used to customize the installation for your environment.



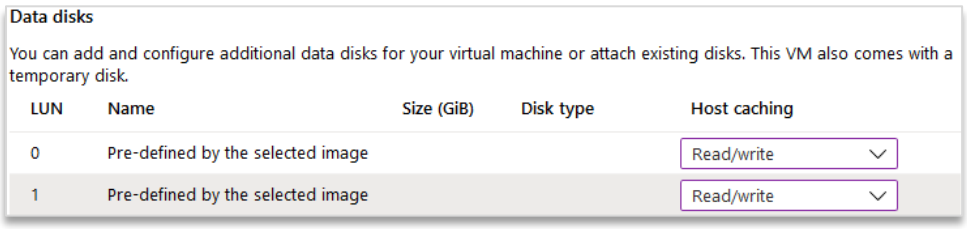
5. Under the BASICS tab:
   a. Select your SUBSCRIPTION ACCOUNT and your RESOURCE GROUP.
   b. INSTANCE DETAILS:
      i. **VIRTUAL MACHINE NAME:** Enter a Virtual machine name that meets the criteria for host names. Please do NOT use periods within the host name.
      ii. **REGION:** Select a Region for your organization.
      iii. **AVAILABILITY OPTIONS:** Select the default NO INFRASTRUCTURE REDUNDANCY REQUIRED option.
      iv. **IMAGE:** Use the preselected with STRATUSPHERE UX X.X.X to install and start with the Stratusphere UX Hub.
      v. **AZURE SPOT INSTANCE:** No.
      vi. **SIZE:** Select the default selected instance Standard D4s v3 or the one closest to what the Stratusphere Sizing Guide recommended.
   c. ADMINISTRATOR ACCOUNT:
      i. **AUTHENTICATION TYPE:** SSH public key. Liquidware recommends using SSH public keys although passwords are supported as well.
      ii. **USERNAME:** az-user. Liquidware recommends using an easy to remember username for logging into the appliance. We **require** the same username/password on both the Hub and the Database. The two appliances cannot be joined unless their credentials match.
      iii. **SSH PUBLIC KEY:** Paste the public part of your SSH key into this field. For information on how to create SSH keys, please refer to this article published by Microsoft to Create &

use SSH keys for Azure. You can also use the following article which uses PuTTYgen - SSH Key generator on Windows.

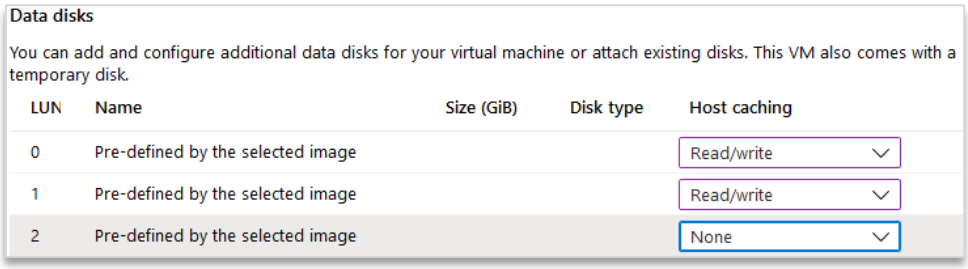
d. Click **NEXT : DISKS >** button.

6. Under the DISKS tab:
   a. DISK OPTIONS
      i. **OS DISK TYPE:** Premium SSD (across all appliances)
      ii. **DATA DISKS:** These options are appliance dependent:

Hub Data Disks:



Database Data Disks:



   b. ADVANCED can be ignored.
   c. Click **NEXT : NETWORKING >** button.

7. Under the NETWORKING tab:
   a. NETWORK INTERFACE:
      i. **VIRTUAL NETWORK:** You may choose to create a new virtual network or use an existing virtual network.
      ii. **PUBLIC IP:** If the Stratusphere Hub is going to be accessible over the Internet, please use a Public IP.
      iii. **NIC NETWORK SECURITY GROUP:** Advanced is auto selected as there are preconfigured NSG rules for Stratusphere Hub, Database and Collector appliances already.
      iv. **CONFIGURE NETWORK SECURITY GROUP:** Choose an existing group or create a new one.
      v. **ACCELERATED NETWORKING:** Off
   b. LOAD BALANCING:
      i. **PLACE THIS VIRTUAL MACHINE BEHIND AN EXISTING LOAD BALANCING SOLUTION?** No.
   c. Click **NEXT : MANAGEMENT >** button.

8. Under MANAGEMENT tab:
   a. AZURE SECURITY CENTER: Your subscription determines mostly includes this option.
   b. MONITORING:
      i. **BOOT DIAGNOSTICS:** On
      ii. **DIAGNOSTICS STORAGE ACCOUNT:** Choose new or existing storage account.

c. IDENTITY:
    i. **SYSTEM ASSIGNED MANAGED IDENTITY:** Off (Note: This is not available in Azure Government Cloud)
d. AUTO-SHUTDOWN:
    i. **ENABLE AUTO-SHUTDOWN:** Off
e. Click on **NEXT : ADVANCED >** button.

9. Under ADVANCED tab:
    a. EXTENSIONS: Liquidware does not require or support any VM extensions as of now.
    b. CLOUD INIT: Liquidware does not require or support Cloud init.
    c. HOST:
        i. **HOST GROUP:** Liquidware recommends hosting all Stratusphere UX appliances on the same host for best performance. If there is a host group available, Liquidware strongly recommends using it to assure best performance of the Stratusphere UX solution by hosting the Hub, Database and Collector on the same host group. This may result in additional charges.
    d. PROXIMITY PLACEMENT GROUP: Liquidware recommends placing the Stratusphere UX Hub, Database and Collector within a proximity placement group so that they are physically closer together in the same region. Please create one prior to installation if possible. Note: This is not available in Azure Government Cloud. Please use these instructions to place the virtual machine in a Proximity Placement Group post-deployment.
    e. VM GENERATION: No change as these are Gen 1 VMs.
    f. Click on **NEXT : TAGS >** button.
10. Under the TAGS tab: Liquidware does not require or recommend any specific tags as of now but will support any standard operating procedures your organization uses for tagging virtual machines. Click on **NEXT : REVIEW + CREATE >** button.
11. The REVIEW + CREATE page will perform some basic validations and provide all the information entered in the prior tabs for review purposes. Please ensure all information and settings are as entered. Then click the **CREATE** button and wait for the instance to be created.
12. Please repeat these instructions to install optional Stratusphere UX Database or Stratusphere UX Collector appliances on Azure based on the Stratusphere Sizing Guide recommendations.

The Azure Create Instance page will display the progress of how the appliances are being created and will display basic information when they are live and ready for use. Liquidware recommends the use of the Boot diagnostics under Support + Troubleshooting to see the console boot up. Liquidware has seen this the boot up process take anywhere up to 10 minutes sometimes. In case of the Stratusphere Hub, use the public or private IP Address / DNS to connect to the web UI for the Hub and proceed as shown in the sections below. In case of the Database and Collector appliance, proceed to the sections below.

Establish trust between Stratusphere Hub and Database

Microsoft Azure supports usage of standard passwords and SSH keys to log into appliance consoles. As documented above, Liquidware recommends the usage of SSH keys and uses them to establish trust between appliances before the join can be performed. For the join to work:

A. The **`az-user`** (Azure user) on the Hub must be able to SSH without a password to the **`az-user`** (Azure user) on the Database, and
B. The **`root`** user on the Hub must be able to SSH without a password to the **`az-user`** on the Database for upgrade purposes.
C. The **`root`** user on the Database must be able to SSH without a password to the **`az-user`** on the both the Hub and Database appliances

Here is the list of items to prepare for and instructions to establish trust between these appliances before you can use the standard join process.

Preparation

1. Liquidware has already preconfigured a set of Network Security Group rules that allows access to the Hub appliance on SSH (TCP/22), HTTP (TCP/80), and HTTPS (TCP/443) ports. Similarly, NSG rules for the Database SSH (TCP/22) & Postgres (TCP/5432) and Collector SSH (TCP/22) and HTTPS (TCP/443) are also preconfigured.
2. Please make sure you download and install an SSH client such as PuTTY on your computer prior to beginning the process below.

Instructions

In some commands below, `<right-click-mouse-to-paste>` is a placeholder for the action of right-clicking the mouse within PuTTY – this action automatically pastes the contents of the clipboard into the PuTTY command line. Neither the actual characters such as < and > nor the text, `right-click-mouse-to-paste`, should be typed in on the command line. This merely represents the action that should be taken at that point in the command line.

#	Hub Instructions	Database Instructions
1	Using a tool like PuTTY, open two SSH connections to each appliance and place them side by side. Connect to the Stratusphere appliance consoles using the standard **`az-user`** **with the associated keys**, **skipping password authentication** deployment. Here is a link to a quick refresher on how to do so from the Azure documentation.	
	To address point (A) above:	
2	Within the SSH console of the Hub appliance, while logged in as the **`az-user`**, generate a new SSH key by executing the following command and accepting the defaults by pressing ENTER: **`ssh-keygen -t ecdsa -q -N ""`**	

#	Hub Instructions	Database Instructions
	DO NOT enter a passphrase if prompted by the keygen command. Leave the field empty.	
		
3	Within the same SSH console of the Hub appliance, print the contents of the SSH public key by executing the following command, and then use your mouse to select the entire sequence of characters displayed, that forms the public key, to copy it to your clipboard: ➢ **`cat .ssh/id_ecdsa.pub`**	
		
4		Now switch to the SSH console on the Database appliance, and add the Hub's **`az-user`** public key to the authorized list of keys that can connect as the **`az-user`** by using the echo command and pasting the key copied from above, and sending it to the `authorized_keys` file: ➢ **`echo "<right-click-mouse-to-paste>" >> .ssh/authorized_keys`**
5	Now, from within the SSH console on the Hub appliance, verify whether the Hub can now connect without a password to the Database as	

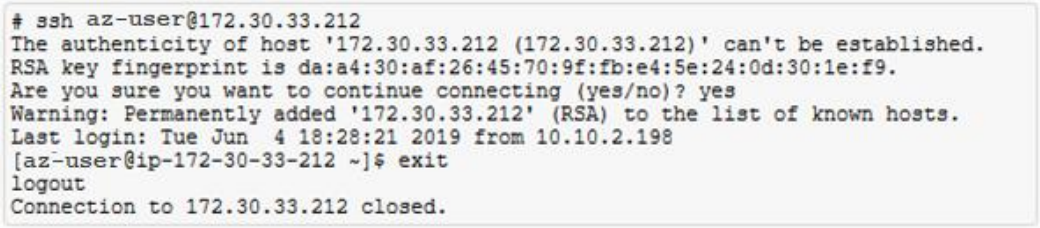
#	Hub Instructions	Database Instructions
	the **az-user**. You will have to accept the SSH keys and then logout from the connection: ➢ **ssh <db.ip.or.dns>**	

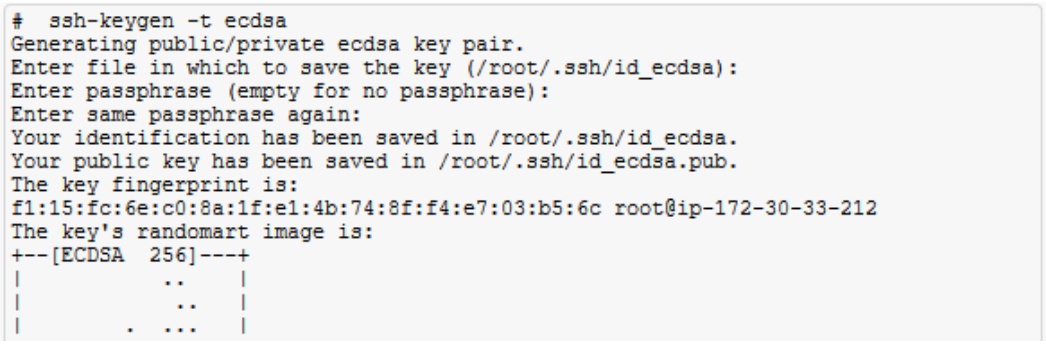
	`$ ssh 172.30.33.212`
	`The authenticity of host '172.30.33.212 (172.30.33.212)' can't be established.`
	`RSA key fingerprint is da:a4:30:af:26:45:70:9f:fb:e4:5e:24:0d:30:1e:f9.`
	`Are you sure you want to continue connecting (yes/no)? yes`
	`Warning: Permanently added '172.30.33.212' (RSA) to the list of known hosts.`
	`Last login: Tue Jun 4 18:28:21 2019 from 10.10.2.198`
	`[az-user@ip-172-30-33-212 ~]$ exit`
	`logout`
	`Connection to 172.30.33.212 closed.`	

	To address point (B) above:	
6	Now that we have confirmation for **az-user**, we need to redo the same process for the **root** user. Within the SSH console on the Hub, switch to **root** and generate a new SSH key. Press ENTER to accept the defaults: **sudo bash** **ssh-keygen -t ecdsa -q -N ""** DO NOT enter a passphrase if prompted by the keygen command. Leave the field empty.	

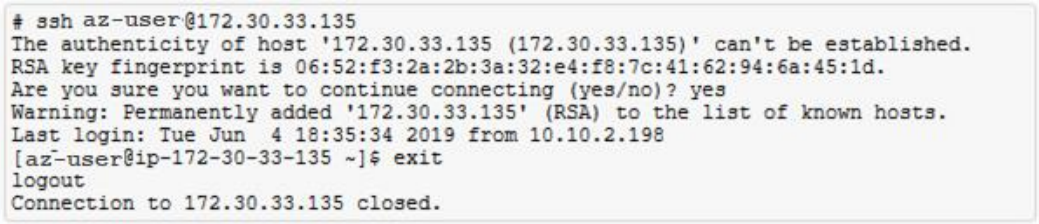
	`$ ssh-keygen -t ecdsa`
	`Generating public/private ecdsa key pair.`
	`Enter file in which to save the key (/root/.ssh/id_ecdsa):`
	`Enter passphrase (empty for no passphrase):`
	`Enter same passphrase again:`
	`Your identification has been saved in /root/.ssh/id_ecdsa.`
	`Your public key has been saved in /root/.ssh/id_ecdsa.pub.`
	`The key fingerprint is:`
	`60:1e:b1:5b:d3:f3:46:57:c3:12:50:b3:3d:94:e8:ec az-user@ip-172-30-33-135`
	`The key's randomart image is:`
	`+--[ECDSA 256]---+`
	`|  .  .o++oo|`
	`|  o .  o=+.|`
	`|  = o o +.oo |`
	`|  o = . + +  .|`
	`|  o S  +  |`
	`|  . E  |`
	`|  |`
	`|  |`
	`|  |`	

7	Within the same SSH console of the Hub appliance, print the contents of the SSH public key by executing the following command, and then use your mouse to select the entire sequence of characters displayed, that forms the public key, to copy it to your clipboard:	

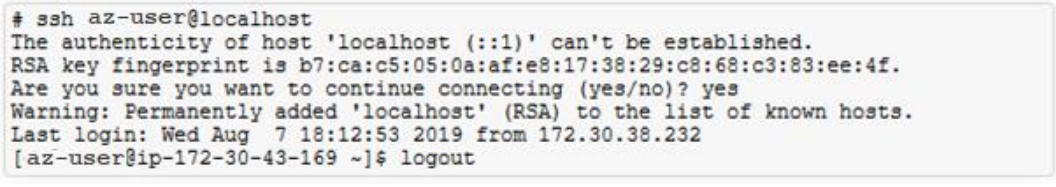
#	Hub Instructions	Database Instructions
	➢ **cat /root/.ssh/id_ecdsa.pub**	
		
8		Now switch to the SSH console on the Database appliance, and add the Hub's **root** user public key to the authorized list of keys that can connect as the **az-user** by using the echo command and pasting the key copied from above, and sending it to the authorized_keys file: ➢ **echo "<right-click-mouse-to-paste>" >> .ssh/authorized_keys**
9	Now, from within the SSH console on the Hub appliance, verify whether the Hub can now connect without a password to the Database as the **az-user**. You will have to accept the SSH keys and then logout from the connection: ➢ **ssh az-user@<db.ip.or.dns>**	
		
10	Now, from within the SSH console on the Hub appliance, log out as **root** to return to the **az-user** to prepare for the next set of commands below. ➢ **exit**	
	To address point (C) above:	
11		Within the SSH console of the Database, switch to **root** user using the command: ➢ **sudo bash**

#	Hub Instructions	Database Instructions
12		Within the same SSH console on the Database, generate a new SSH key as the **root** user by executing the following command and accepting the defaults by pressing ENTER: **ssh-keygen -t ecdsa -q -N ""** DO NOT enter a passphrase if prompted by the keygen command. Leave the field empty.
		
13		Within the same SSH console of the Database appliance, print the contents of the **root** user's SSH public key by executing the following command, and then use your mouse to select the entire sequence of characters displayed, that forms the public key, to copy it to your clipboard: ➢ **cat /root/.ssh/id_ecdsa.pub**
		
14		Within the same SSH console on the Database appliance, add the Database's **root** user public key to the authorized list of keys that can connect as the **az-user** by using the echo command and pasting the key copied from above, and sending it to the `authorized_keys` file: ➢ **echo "<right-click-mouse-to-paste>" >> /home/az-user/.ssh/authorized_keys**

#	Hub Instructions	Database Instructions
15	Now, from within the SSH console on the Hub appliance, add the Database's **root** user public key to the authorized list of keys that can connect as the **az-user** by using the echo command and pasting the key copied from above, and sending it to the `authorized_keys` file: ➢ **echo "<right-click-mouse-to-paste>" >> /home/az-user/.ssh/authorized_keys**	
16		From within the SSH console of the Database, verify whether the **root** user of the Database can now connect without a password to the Hub as the **az-user**. You will have to accept the SSH keys and then logout from the connection: ➢ **ssh az-user@<hub.ip.or.dns>**

	
	`# ssh az-user@172.30.33.135`
	`The authenticity of host '172.30.33.135 (172.30.33.135)' can't be established.`
	`RSA key fingerprint is 06:52:f3:2a:2b:3a:32:e4:f8:7c:41:62:94:6a:45:1d.`
	`Are you sure you want to continue connecting (yes/no)? yes`
	`Warning: Permanently added '172.30.33.135' (RSA) to the list of known hosts.`
	`Last login: Tue Jun 4 18:35:34 2019 from 10.10.2.198`
	`[az-user@ip-172-30-33-135 ~]$ exit`
	`logout`
	`Connection to 172.30.33.135 closed.`	

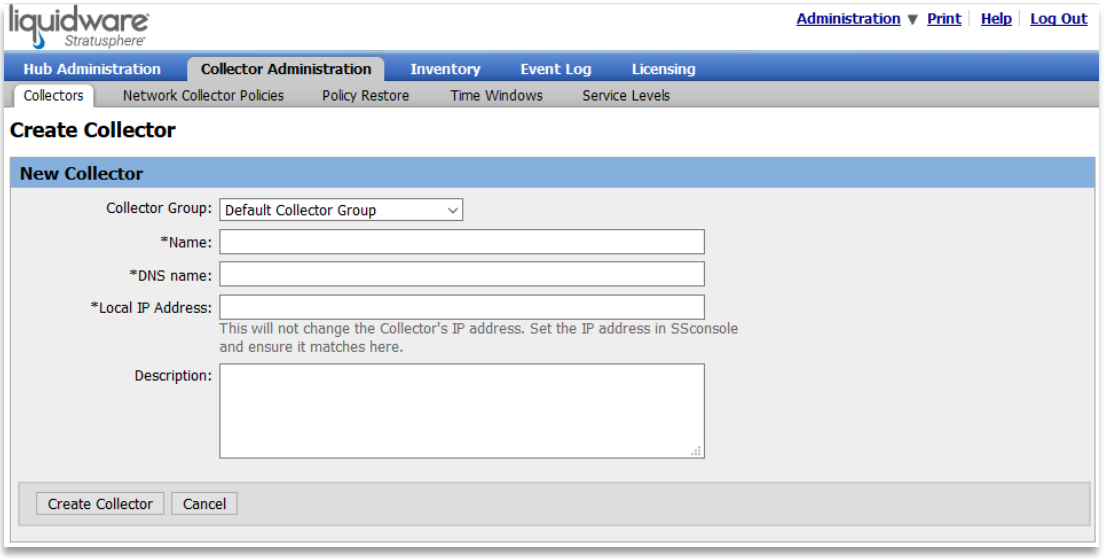
17		From within the same SSH console of the Database, we must also verify whether the **root** user of the Database can connect to itself as the **az-user** user. Again, you will have to accept the SSH keys and then logout from the connection: ➢ **ssh az-user@localhost**

	
	`# ssh az-user@localhost`
	`The authenticity of host 'localhost (::1)' can't be established.`
	`RSA key fingerprint is b7:ca:c5:05:0a:af:e8:17:38:29:c8:68:c3:83:ee:4f.`
	`Are you sure you want to continue connecting (yes/no)? yes`
	`Warning: Permanently added 'localhost' (RSA) to the list of known hosts.`
	`Last login: Wed Aug 7 18:12:53 2019 from 172.30.38.232`
	`[az-user@ip-172-30-43-169 ~]$ logout`	

#	Hub Instructions	Database Instructions
18	Now that the trust connections between the Hub and Database using the **`az-user`** and **`root`** user have been verified, you can now proceed to the instructions provided in the Connecting the Hub and Database appliances section to formally join a Hub and Database together.	

Add & Register a Stratusphere CID Key Collector to the Hub

1. Once a Stratusphere CID Key Collector is up and running within your Microsoft Azure environment, log into ADMINISTRATION product of the Stratusphere Hub's Web UI. Use the default credentials to log in.
2. Navigate to **Collector Administration > Collectors** tab.
3. Click on **New** to add a new Collector.
4. On the following form, add the host name as **Name**, **DNS Name** and **Local IP Address** as observed on the Azure page for the Collector's details.



5. Click on **Create Collector** to save and create a new Collector.
6. The Hub will reach out to the Collector and help register it. Once registered, the Collector may potentially reboot, get the registration information from the Hub, and then show up as a CID Key Collector within the main **Collector Administration > Collectors** page.
7. Repeat these same instructions for adding and registering additional Collectors.

Installing Stratusphere Appliances on Nutanix Acropolis Hypervisors

The Stratusphere Hub, Database, and Collectors are all virtual appliances that can be installed directly from the Liquidware web site on Nutanix Acropolis Hypervisor. The Stratusphere Hub 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 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 following instructions can be used to install the Hub as well as other the other appliances within your virtual environment.

Please note that only CID Key Collectors are currently supported on the Nutanix Acropolis platform. Network Collectors are not supported at this time.

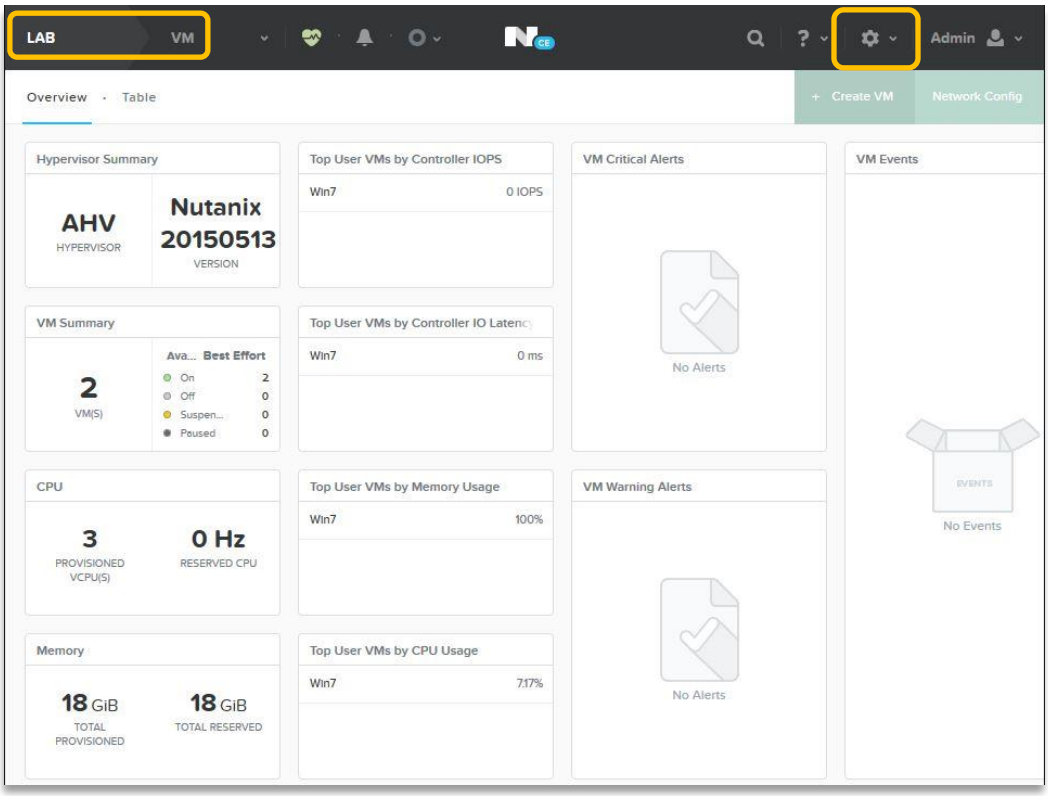
Preparation

1. Please acquire administrative credentials to the Nutanix Acropolis environment for your organization.
2. Please use the Liquidware Stratusphere Sizing Guide to appropriately size the Stratusphere Hub appliance and Database appliance for your installation base.
3. Identify the links to the Nutanix Acropolis files for the Hub, Database, and Collector appliances on the Liquidware Stratusphere Download page and keep them handy. If your Nutanix Acropolis Cluster does NOT have direct access to the Internet, please download the QCOW2 files to your local environment in preparation to be uploaded to Acropolis.
4. Nutanix does NOT provide a virtual container format such as OVF or XVA. Thus, each QCOW2 must be uploaded separately first, and then virtual resources such as vCPUs, RAM, Disks, NICs, etc. need to be manually configured for each appliance.

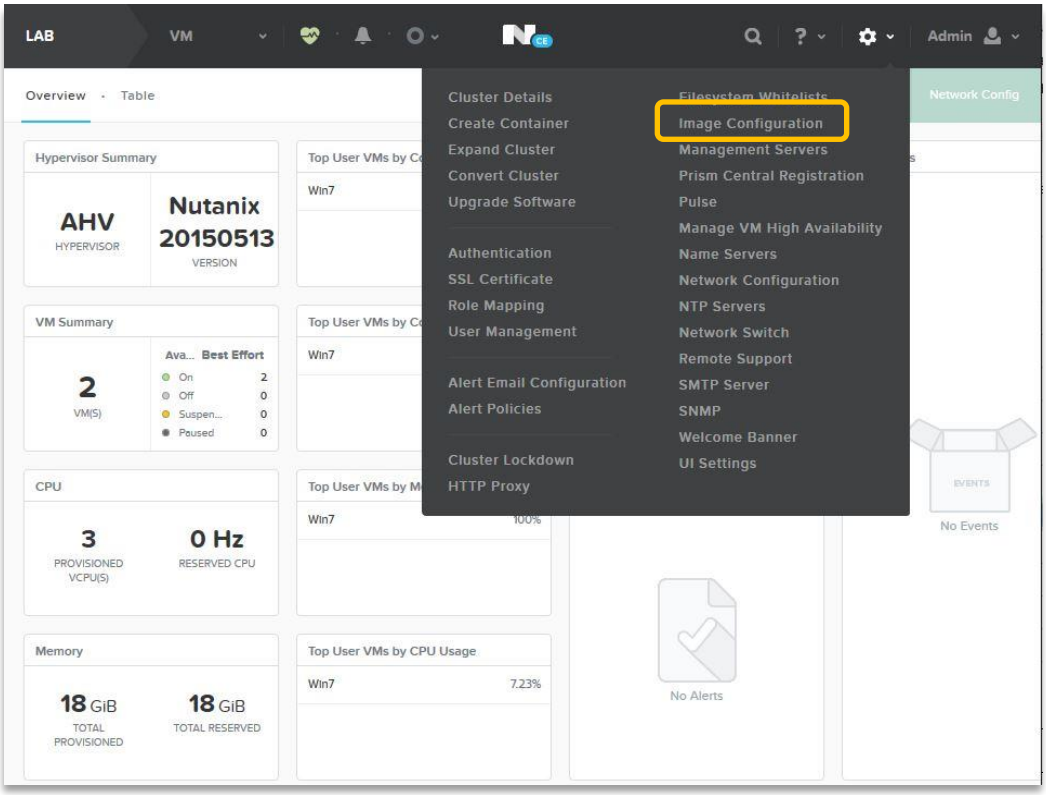
Instructions

1. Log into your Nutanix Acropolis cluster using your administrative credentials.

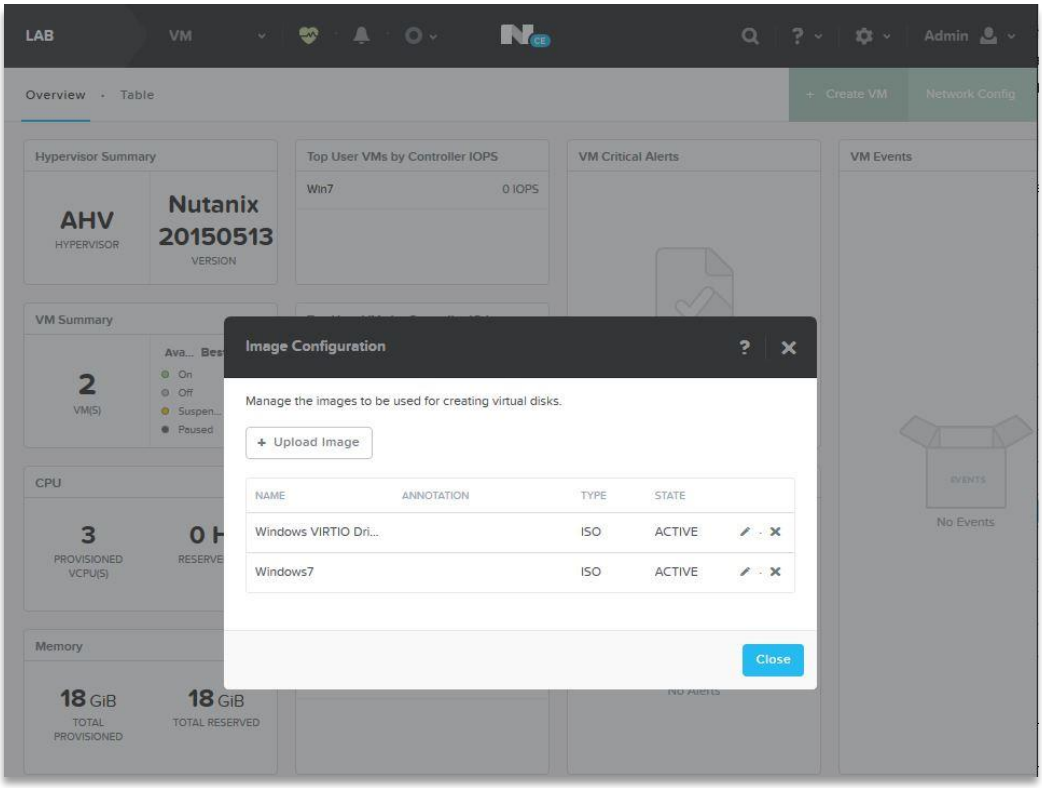
2. Make sure you select the appropriate **Cluster > Home** on the top left of the page.



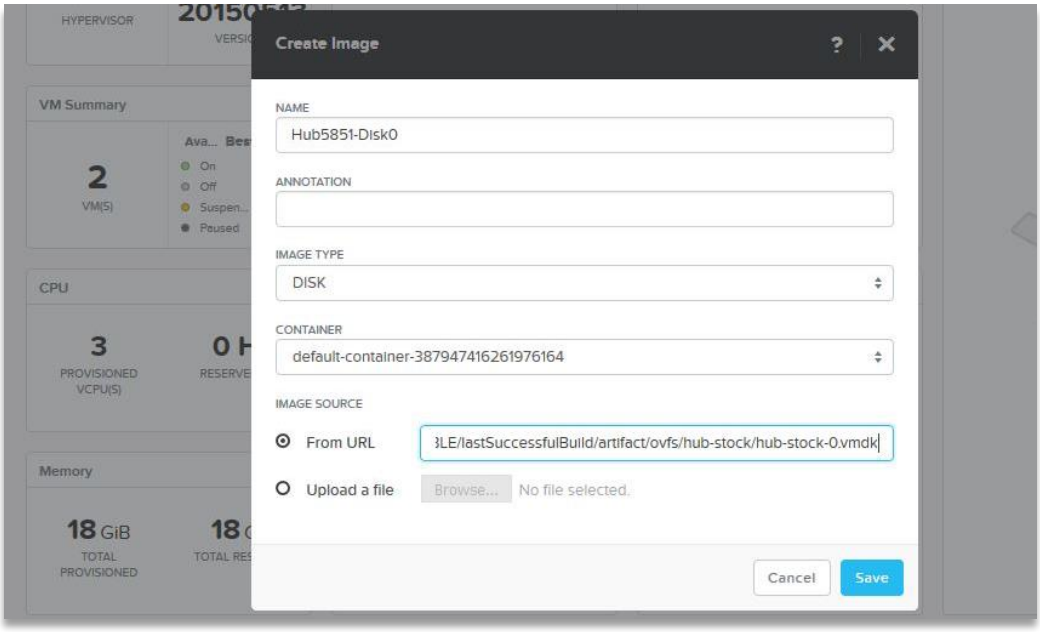
3. Then click on the gear icon on the top right and select **Image Configuration**.



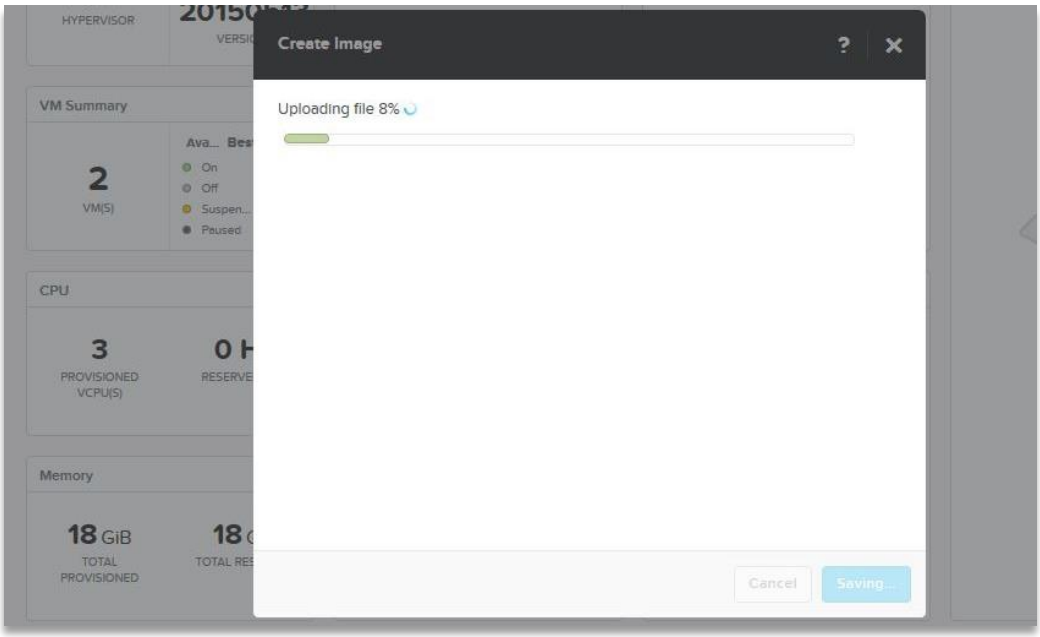
4. In the **Image Configuration** window, click on the **+ Upload Image** button to upload the appliance VMDK images.



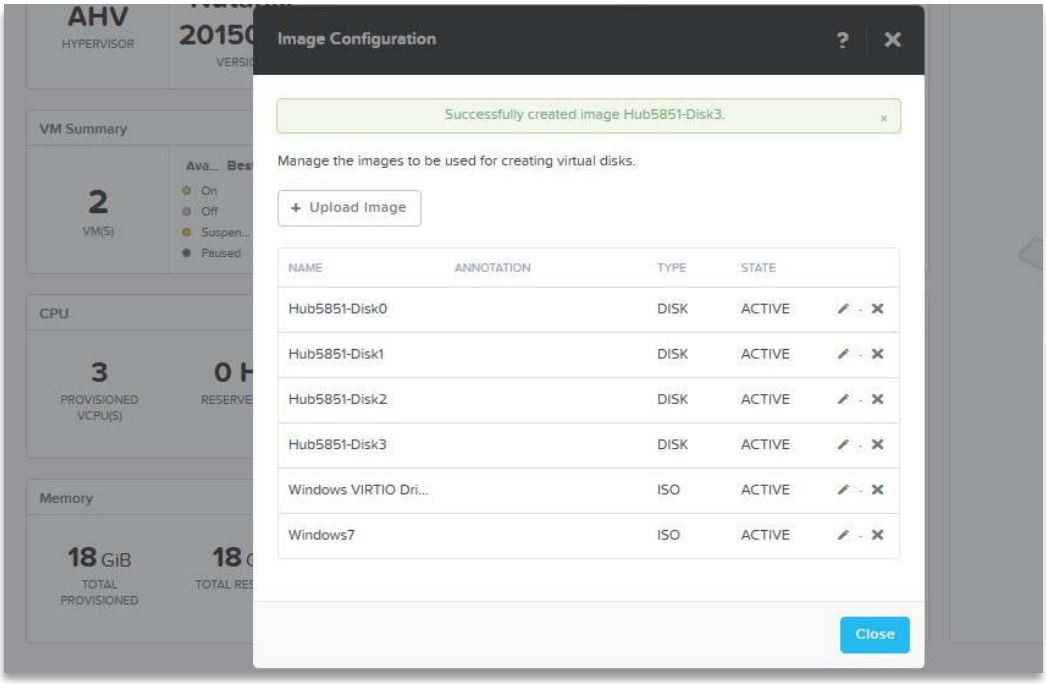
5. In the **Create Image** window, enter a unique name for this disk image for **Name**, select **Disk** for **Image Type**, and leave the **default container** selected for **Container**. For **Image Source**, if your Nutanix Acropolis cluster has access to the Internet, choose the **From URL** option and paste in the link to the first disk or Disk0 of the appliance. Alternatively, if your environment is isolated from the Internet, please choose the second option **Upload a file**, and browse to your local desktop to upload the Disk0 VMDK to your Nutanix cluster. Repeat this step for each disk for each appliance you intend to use.



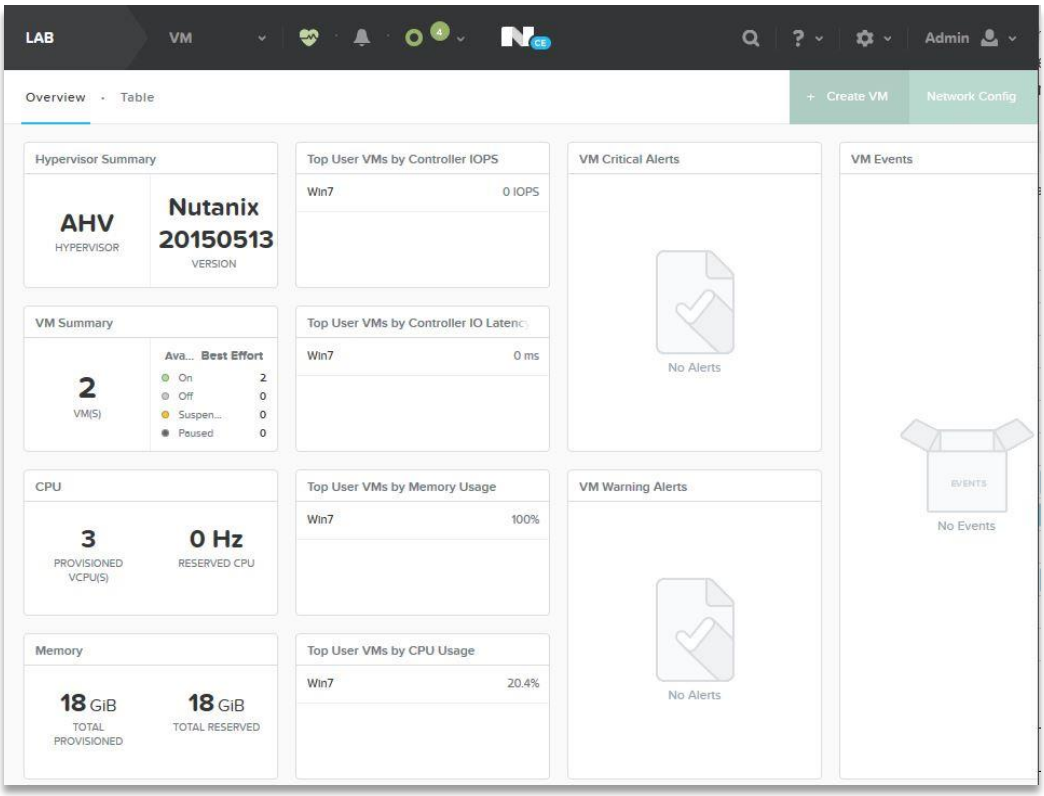
6. On clicking **Save**, the disk image will be uploaded from the Stratusphere Download location to your cluster. Depending on the bandwidth available, this may take a minute or more.



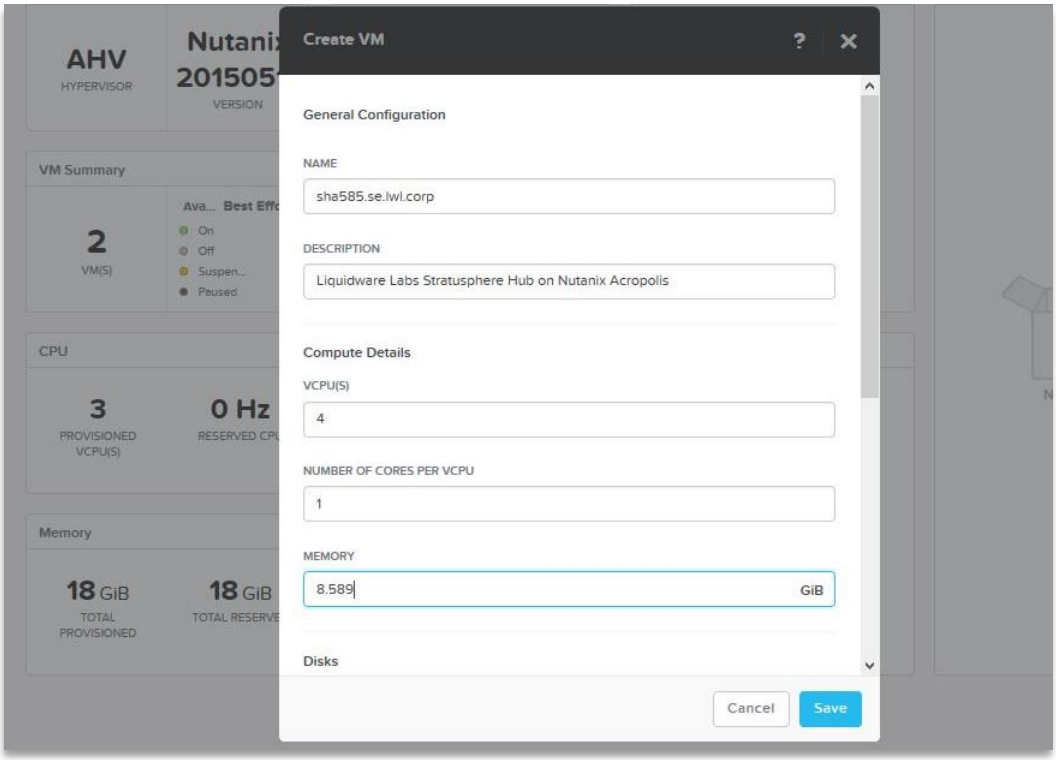
7. After uploading Disk0 for the Hub, follow the same process to upload remaining 3 disks for the Hub, about 5 Disks for the Database appliance if required, and for the Collector as well. Please keep in mind that these disk images need to be added to the Stratusphere Hub virtual machine in the right order so please make sure you use an appropriate naming convention for Hub, Database, & Collector QCOW2 images. After adding all 4 disks for the Stratusphere Hub appliance, it should look like the example below. Click **Close** button to finish adding disk images.



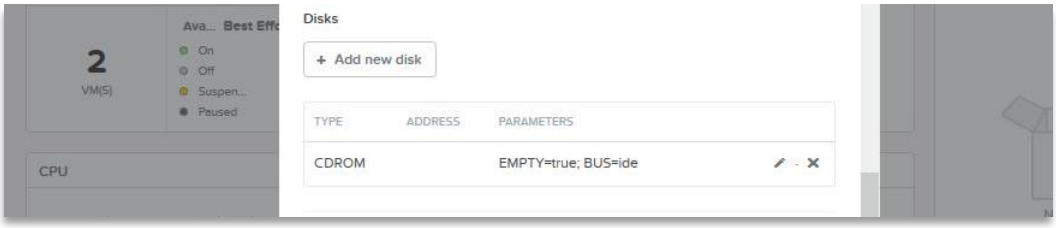
8. Navigate to **Cluster > VM** and select the **+ Create VM** option.



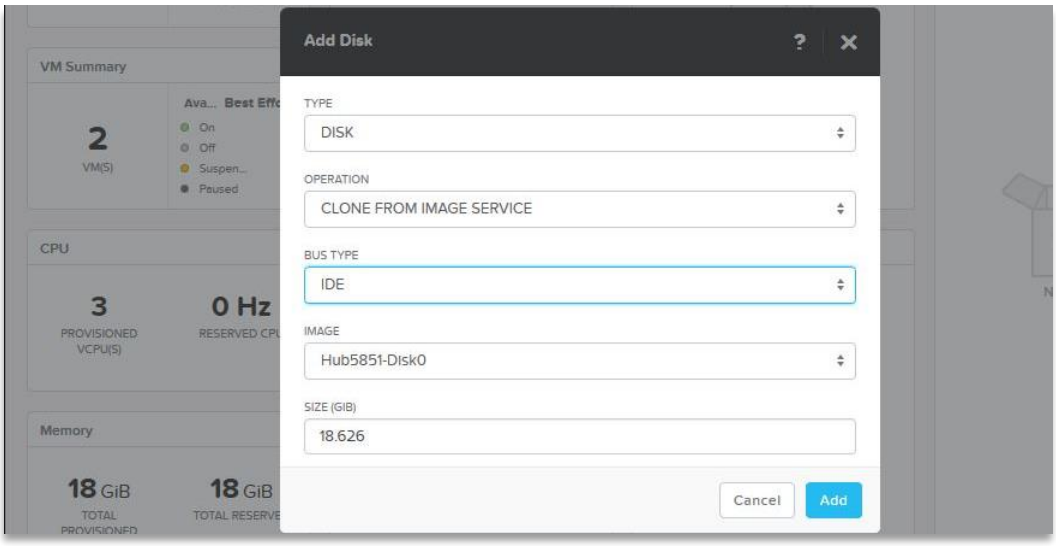
9. In the **Create VM** window, enter a **Name** for the Stratusphere Hub appliance and **Description** for it. Based on the Stratusphere Sizing Guide, enter the number of **vCPUs** and **Memory** recommended.



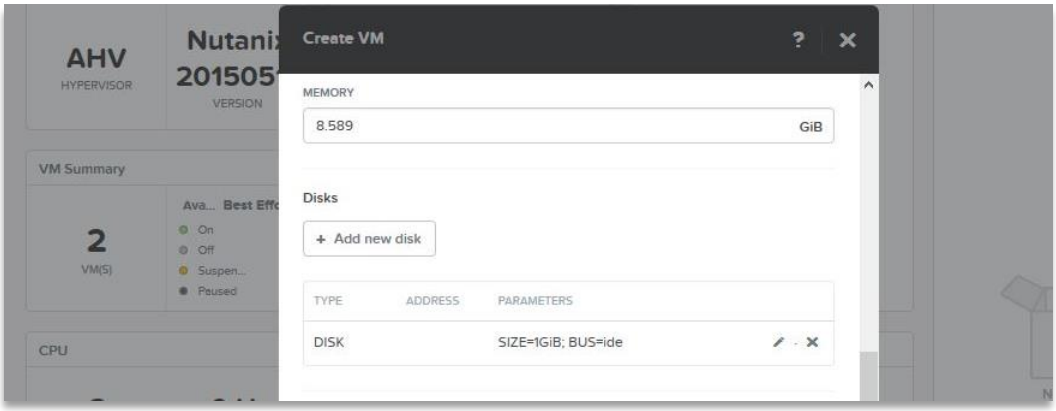
10. Scroll down to see the **Disks** section. Click on the x to remove the **CDROM**. It will prompt you for confirmation.



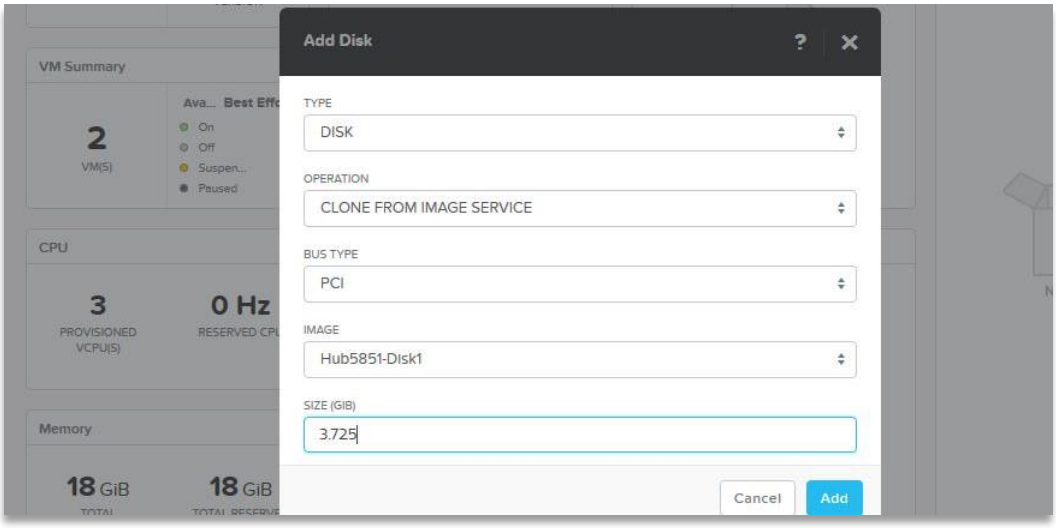
11. To add the first Disk0 for the Hub appliance. Click on **+ Add new disk** button.
12. On the **Add disk** window, select **DISK** for **Type**, **CLONE FROM IMAGE SERVICE** for **Operation**, and **IDE** or **SCSI** for the **Bus Type**. In older versions of Nutanix, the first disk i.e. Disk0 HAD to be of type **IDE**. Each subsequent disk can be of type **PCI** for performance, but the first disk had to be of type **IDE**. There is no such requirement in the newest version of Nutanix. Then select the appropriately named Hub Disk0 and give it the same size recommended by the Stratusphere Sizing Guide. Click **Add**.



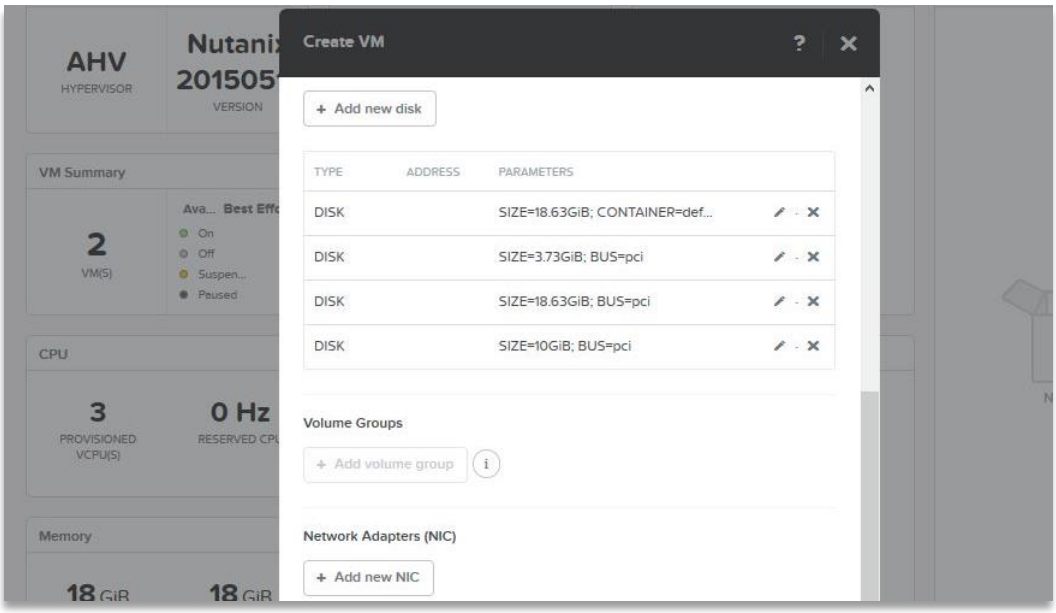
13. After the first disk is added, it will look as shown below.



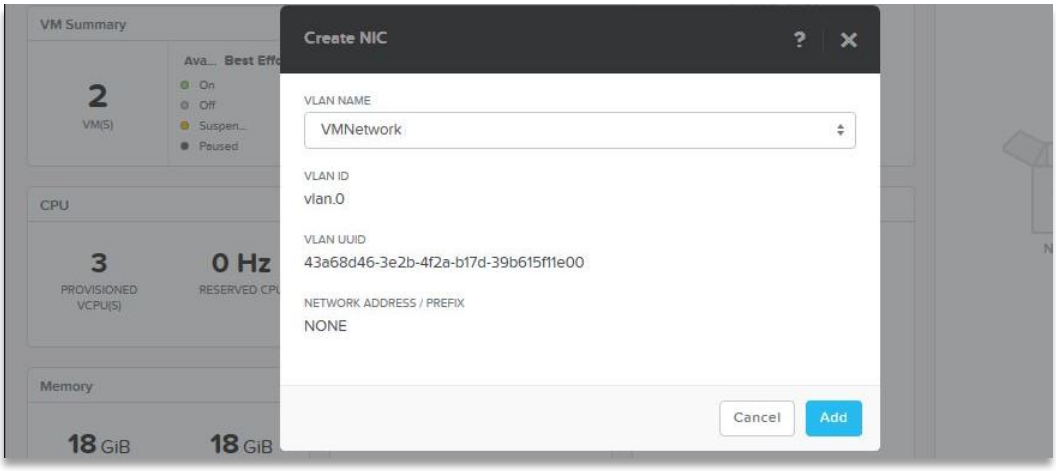
14. Please repeat the steps to add 3 additional disks to the Stratusphere Hub appliance, 5 disks for the Database appliance if required, and ones for the Collector appliance. Here is an example of the second disk Disk1 being PCI of Bus Type.



15. Once all the disks have been added, it should look like the example below. Now click on the **+ Add new NIC** button.



16. On the **Create NIC** window, select the appropriate **VLAN Name** you want the Hub to be on and click on **Add** button to finish adding the NIC.

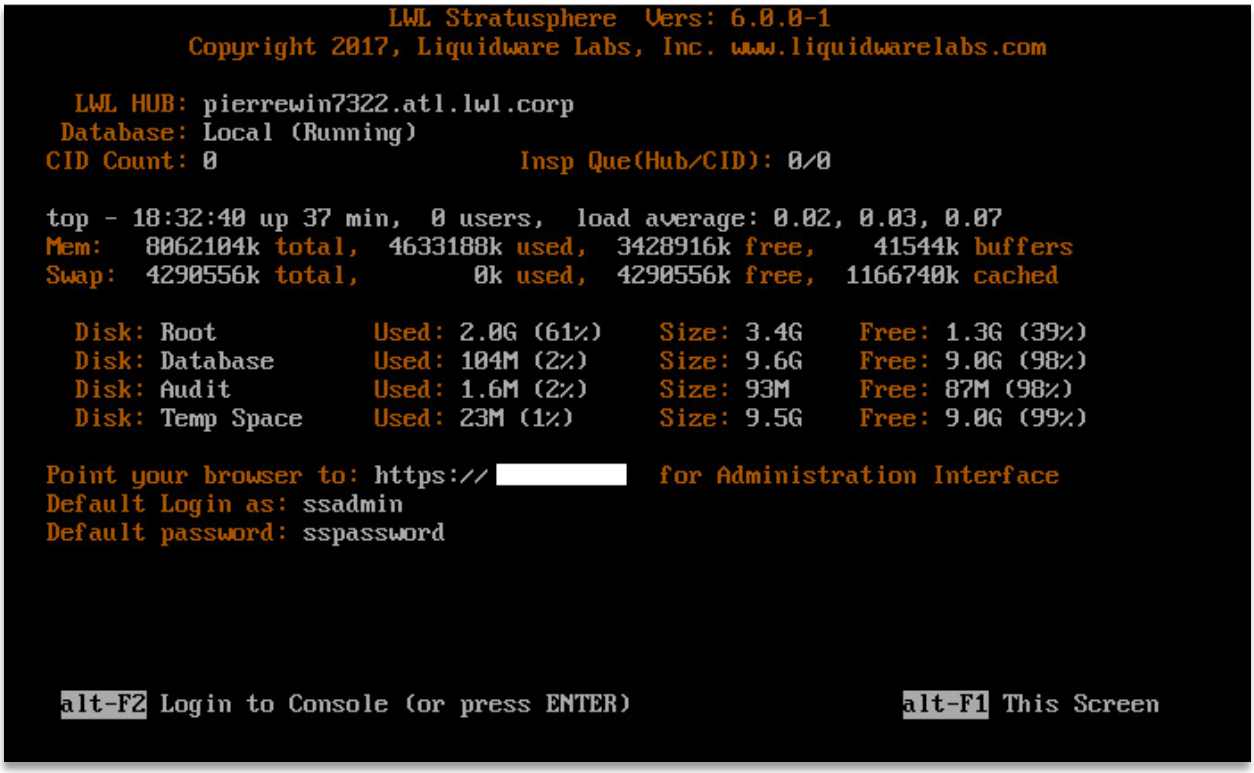


17. The Stratusphere Hub virtual machine is now fully created. Click on **Save** to finish creation of the VM.
18. Before beginning use of Stratusphere appliances in production, Liquidware would like to remind you to please use the Liquidware Stratusphere Sizing Guide to appropriately size the Stratusphere Hub appliance and Database appliance for your installation base.
19. Use the same instructions to install the Database and Collector appliances. Then use the standard instructions to configure and join/register them with the Stratusphere Hub appliance.
20. Now select the Table view under the Cluster > VM tab. Select the newly created Stratusphere Hub appliance and chose the Power On option to boot the Stratusphere Hub appliance.
21. Then click on the Launch Console link to open a browser-based console of the Hub appliance. If you need to configure the appliance, we recommend using PuTTY to SSH to the appliance as outlined in the next section.

Configuring Stratusphere Hub Appliance Settings

After the Hub import into the virtual host completes, you can customize the Hub settings for your environment. In addition to other configuration options, you can edit settings on the Hub to set the CPU/Memory settings. If you would like to expand an existing disk or add an additional hard disk, please see our online Stratusphere Sizing Guide to calculate the required amount of space. The sizing guide and instructions are available on our Stratusphere FIT and UX documentation pages on the Liquidware Support Portal.

To get started with the configuration process, power ON the virtual appliance and open a console to watch the boot sequence. Once the Hub is booted, you will see something like the console view below. The Hub can be configured by either using the Web UI or the Console UI.

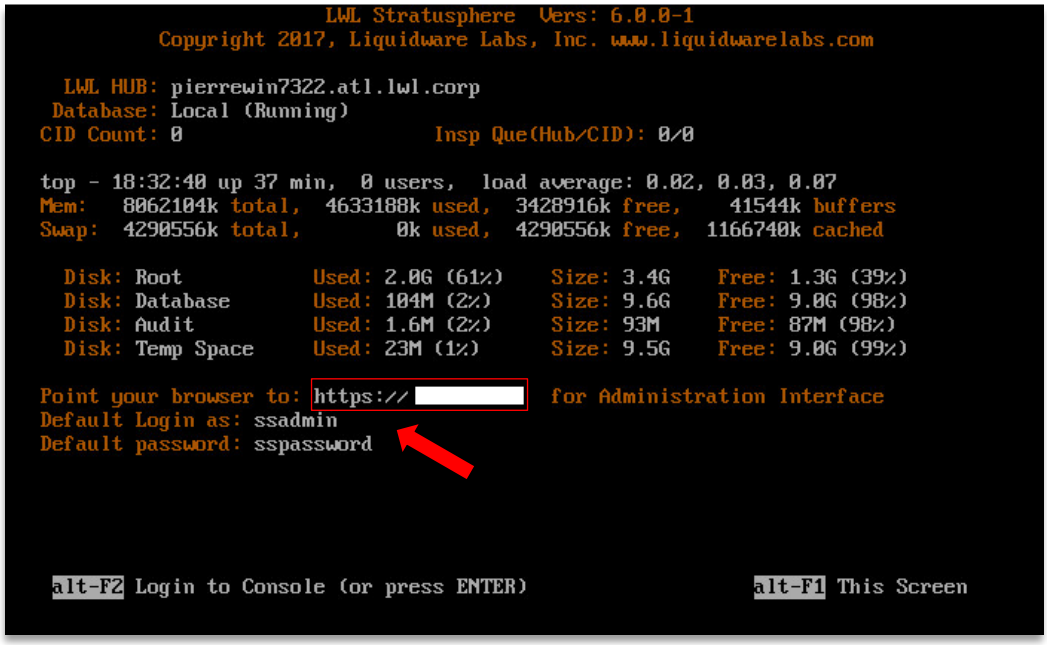


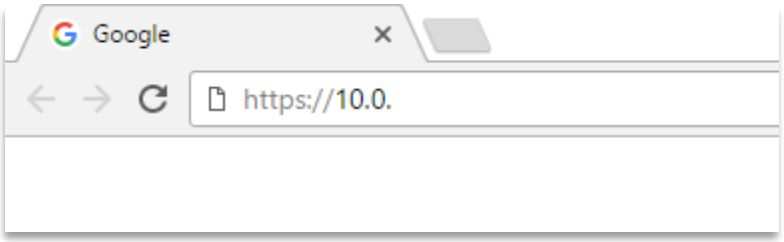
Using the Web UI

If Dynamic Host Configuration Protocol (DHCP) is enabled on the local network subnet, the Stratusphere Hub will acquire a DHCP network address. On completion of the boot sequence, the virtual appliance will provide a URL to connect to the web-based Administration Interface.

To configure the Stratusphere Hub using the Web UI:

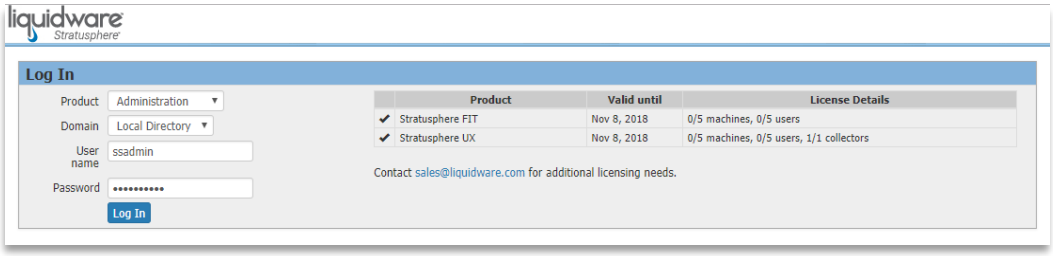
1. Enter the Administration Interface URL found in the console view into a browser.



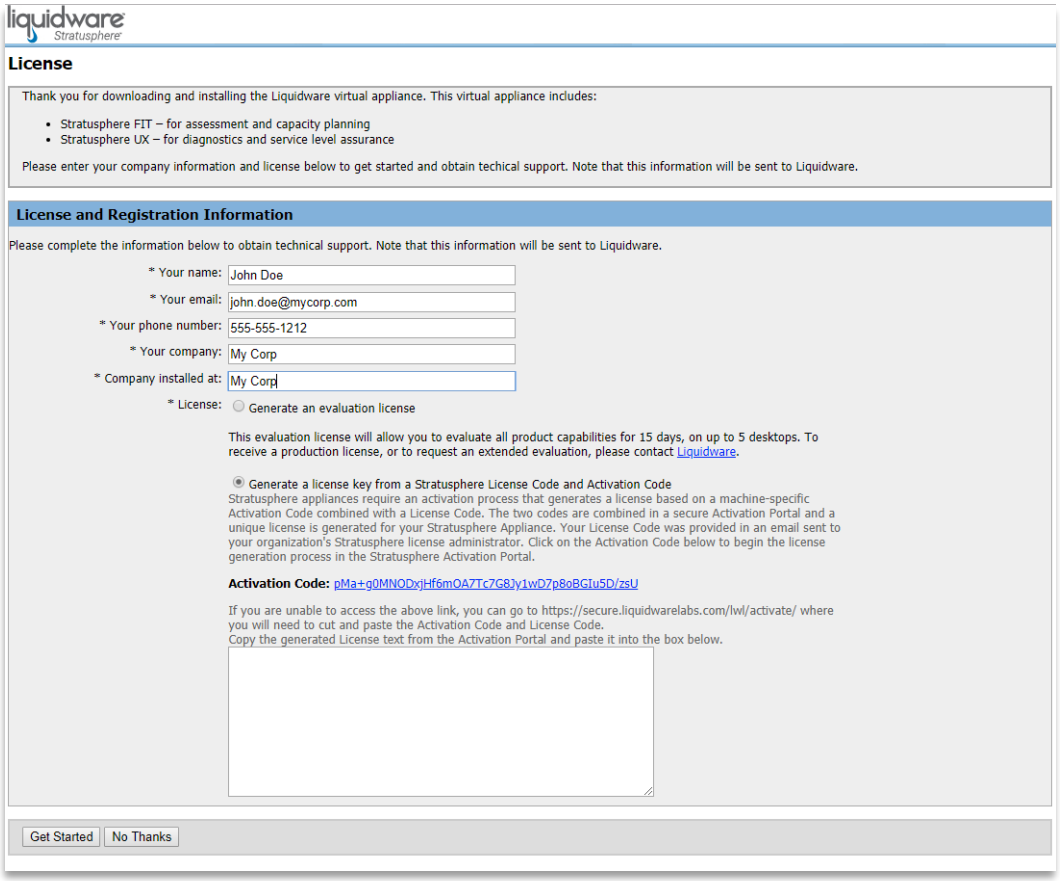


2. At the web login page, enter your **User name** and **Password**.

> ***The default Administration Interface credentials for the Stratusphere Hub web version are:***
>
> ***User name: ssadmin***
>
> ***Password: sspassword***
>
> ***Note: For AWS, use your VM Instance ID for the password.***



3. Please enter the required product registration information.

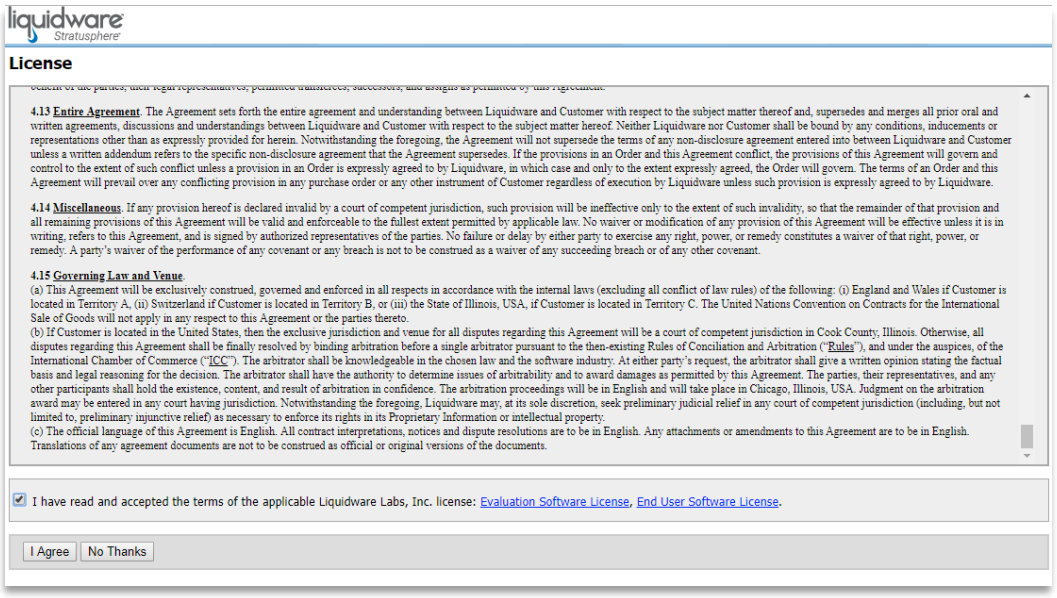


   a. If you have not received a License Code and are evaluating the software, choose to **Generate an evaluation license**. Then click **Get Started**.

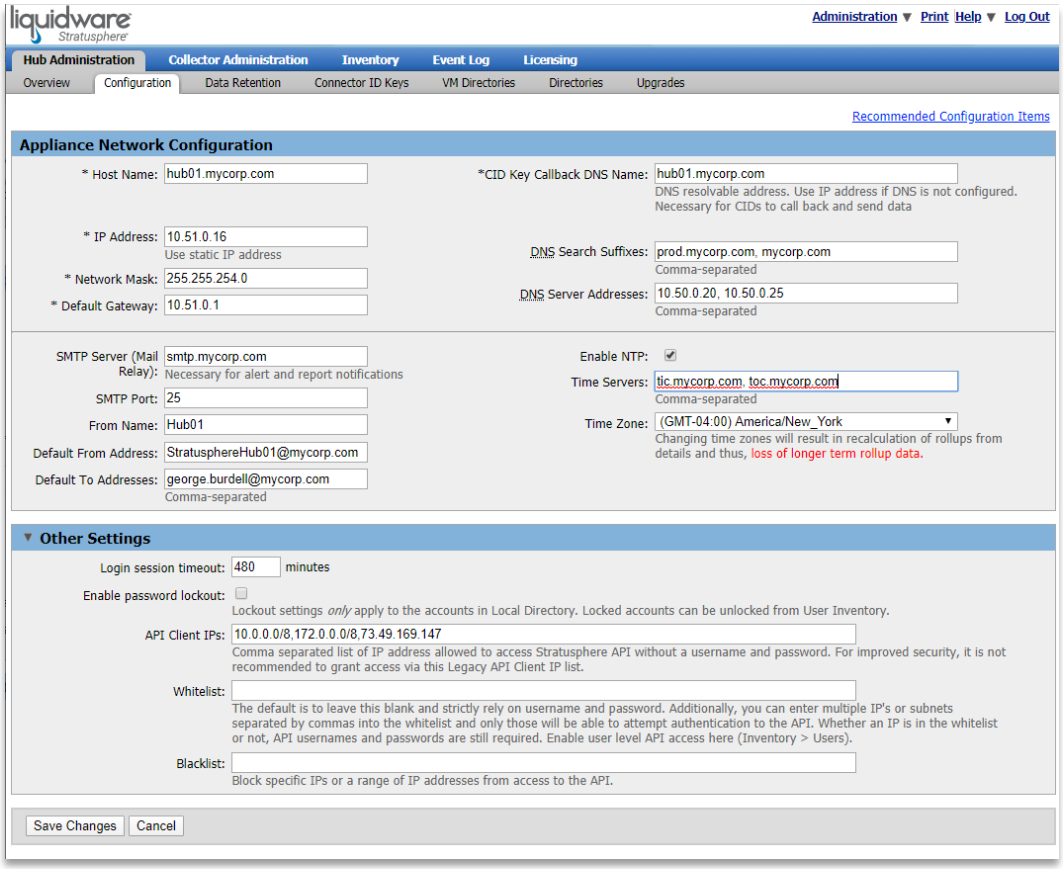
b. If you have purchased the software and received a License Code, choose **Generate a license key from a Stratusphere License Code and Activation Code**. Then click on the Activation Code link. This **Activation Code** is unique, and the link will take you to the Liquidware Stratusphere License Activation Portal where your Activation Code will be prefilled for you.

i. Enter your unique **License Code** that was sent to you by email from Liquidware and click **Proceed**.
ii. Copy the generated License text from the Activation Portal and paste it into the box on the **Update License** tab in the Hub Administration module.
iii. Click **Get Started** to finish.

4. Read through the End User License Agreement (EULA). If you agree to the terms and wish to continue, check the checkbox indicating you have read all license agreements that apply to you. Then click on the **I Agree** button.



5. Now you can customize the Hub's network configuration. When you are done, click **Save Changes** to save your configuration settings. If you have configured the new Static IP address correctly, the browser will redirect you to your new IP address-based URL.



Appliance Network Configuration

Host Name:
Enter a **DNS resolvable fully qualified host name** for the appliance. Underscores are not allowed.

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. Changing it to a statically allocated IP address is strongly recommended.

Network Mask:
Enter the appropriate netmask for your network. Example: 255.255.255.0

Default Gateway:
Enter the default gateway for your network. Example: 10.10.2.1

CID Key Callback 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 to circumvent any future issues that may crop up due to reconfiguring the IP address of the appliance.

DNS Search Suffixes:
Please enter the local DNS search suffixes available within your local network.

DNS Server Addresses:
Please enter 1 or more IP addresses of your DNS server in a comma separated list.

SMTP Server (Mail Relay):
Stratusphere Alerting provides SMTP based email alerts. Enter the address of an SMTP mail relay server accessible from the Stratusphere Hub.

SMTP Port:
Provide the port number that the Stratusphere Hub will send email alerts to. In most cases it should be the standard port for SMTP i.e. 25. However, if the SMTP Server is configured to listen on a custom port, please alter the port number as required.

From Name:
Enter the name that Stratusphere email alerts will be from. In case there are multiple Hubs within your organization, this field should be customized with something like the FQDN of the Stratusphere Hub or an easy name to be associated with the email from this Hub – otherwise all emails from all Stratusphere Hubs will display the default 'Stratusphere Hub Administrator' as the name in the email.

Default From Address:
Enter the default email address that Stratusphere email alerts will be from.

Default To Addresses:
Enter the default email addresses that Stratusphere email alerts will be sent to. This can be an administrator email or an email alias used to send email to a group of people. If more than one email address is used, they should be separated by commas.

Enable NTP:
Please enable this option to avoid time drift and keep the Stratusphere Hub's time synched and accurate.

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.

Time Zone:
Please select your local time zone from the drop-down list. Note that changing your time zone after Stratusphere has been in use collecting data will cause the recalculation of roll-up criteria used to display summary metrics and the loss of all previous roll-up data.

Other Settings

Login session timeout:
Based on your organizational security policies, please enter the session timeout duration. If the user is inactive within the Stratusphere Web UI for more than the duration specified in this field, the user session is invalidated, and the user will have to re-authenticate and log back into the Web UI.

Enable password lockout:
Based on your organizational security policies, the password complexity and lockout policy can be enabled. Enabling this option will ensure that the passwords used must be complex in nature and will also enforce the locking of an account based on a certain number of invalid login attempts. Lockout setting applies only to Local Directory accounts. Locked Accounts can be unlocked from User Inventory.

API Client IPs:
Stratusphere provides Database API to access and pull information out of the Stratusphere Database. Enter the specific IP address(es) or subnets that can access information from the Stratusphere Database using the API without using a username or password. For improved security, it is not recommended to grant access via this Legacy API Client IP list.

White List:

Enter the specific IP address(es) that can access information from the Stratusphere Database using the API through user and password authentication. The default is to leave this field blank for wider access. If any IP addresses are listed, API access is restricted to only those IP addresses in the white list that can authenticate their identity. Liquidware enhanced security around Stratusphere API by disallowing usage of the default **ssadmin** user or any password that contains 'password' in it. Liquidware recommends creating a

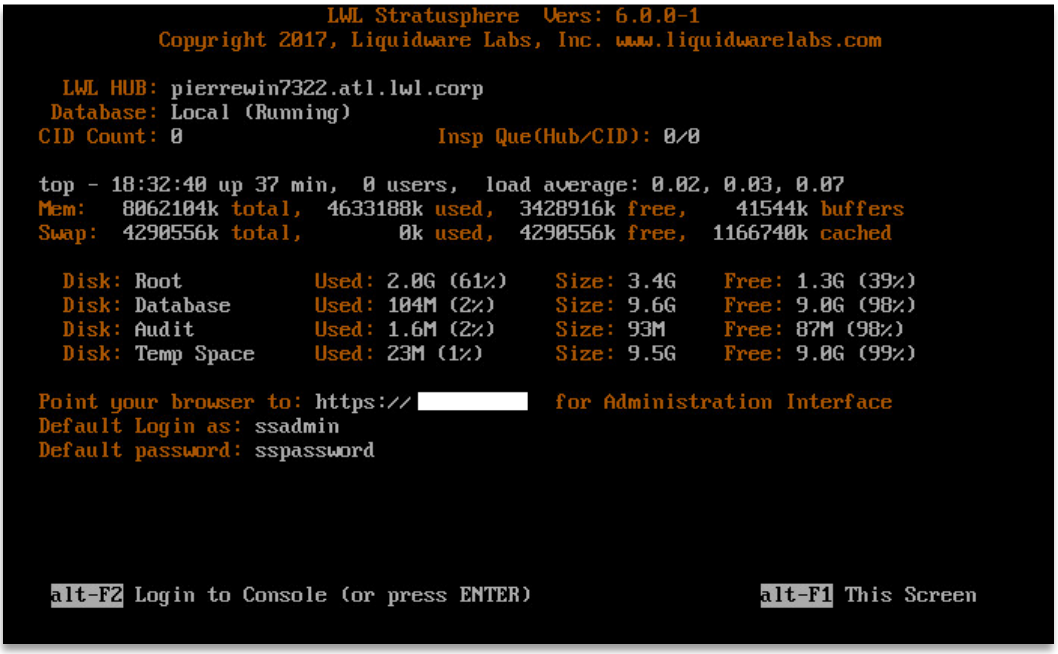
different set of users that are allowed API access using best practices around password security.

Black List:
Enter the specific IP address(es) that are blocked from having access to the Stratusphere Database using the API through user and password authentication.

Using the Console UI

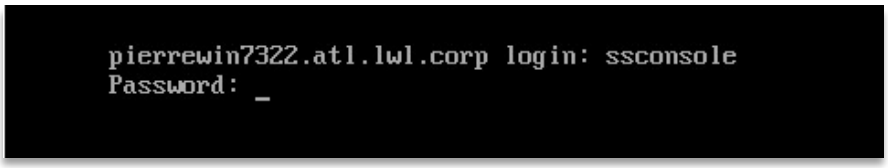
If DHCP is not available on the local subnet, you can use the Console to configure the Stratusphere Hub appliance.

1. Open a console view of the Hub appliance in your virtual environment.



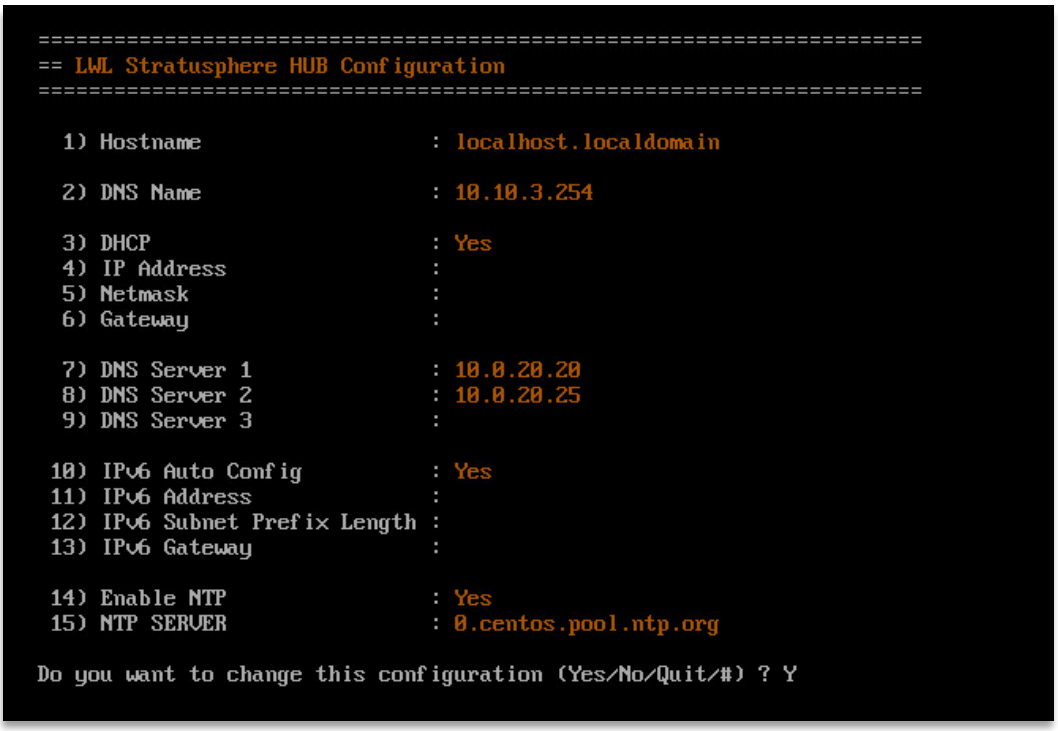
2. Press **Alt+F2** or **Enter** to login to the console with your credentials.

> ***The default login credentials for the Hub Console are:***
>
> ***User name: ssconsole***
>
> ***Password: sspassword***



3. Once logged in, the “LWL Hub” console-based menu will be launched as shown below. Choose the **N** option to configure the Network and hit **Enter**.

4. You will be presented with the following screen. It will ask for information to configure the network appliance. Enter **Y** to change the configuration of the appliance.



5. The appliance will then ask you a series of questions to configure the certain key items. It will ask for:
    a. Hostname (Must be a DNS Resolvable Fully Qualified Host Name)
    b. DNS Name
    c. DHCP (Y/N)
    d. IP Address
    e. Netmask
    f. Default Gateway
    g. DNS Server 1
    h. DNS Server 2
    i. DNS Server 3
    j. IPv6 Auto Configure option
    k. IPv6 Address
    l. IPv6 Subnet Prefix Length
    m. IPv6 Gateway
    n. Enable NTP
    o. NTP Server

6. After you answer all the questions the appliance will display what you entered back to you for your confirmation. If any item needs to be edited, simply enter the number of the item and the appliance will prompt you to edit it as needed.

7. Once satisfied with your configuration settings, chose the **W** option to write and save these settings permanently. The appliance will apply and save all the configuration settings and take you back to the initial menu options.

Using the Stratusphere Database Appliance (Optional)

Liquidware provides an optional Database appliance that can be used with Stratusphere. The Stratusphere Database appliance is an external database and thus enhances performance and capacity for receiving reports from devices deployed in your environment. As a rule of thumb, the Stratusphere Database appliance is used when more than 1,000 devices report back to the Stratusphere Hub using the default callback frequency of 60 minutes. However, if you would like more frequent callbacks, we would recommend using the Database appliance even if you are using fewer devices and have more than 1,000 callbacks per hour. Please visit our Support Portal for more recommendations on when to use the Database appliance. We also have an online Stratusphere Sizing Guide on our website to help you size your environment.

Installing the Database Appliance

Please follow the instructions given in the beginning for **Installing the Stratusphere Appliances** in your virtual environment to assist you in installing the Stratusphere Database appliance.

Configuring the Stratusphere Database Appliance

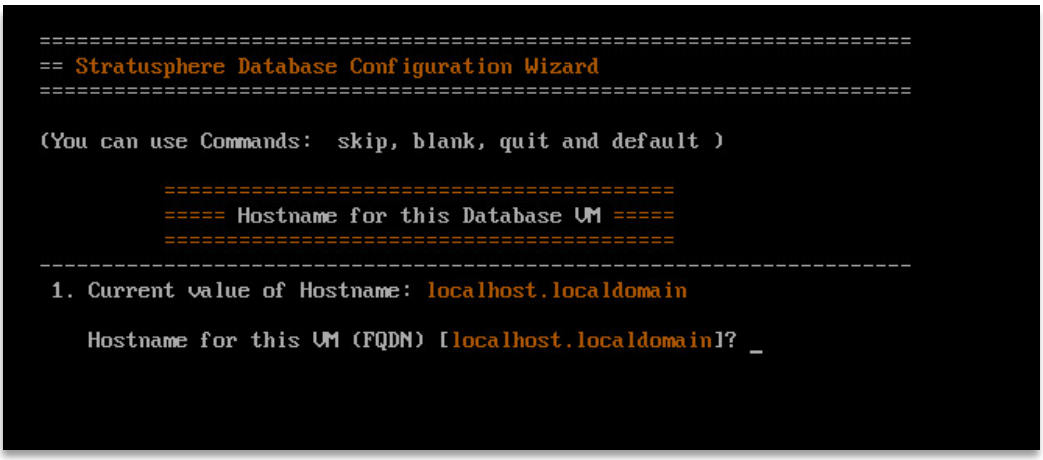
Liquidware recommends hosting the Stratusphere Database appliance on the same virtual host, same virtual switch, and same port group as the Stratusphere Hub appliance. This configuration will ensure the fastest communication response time between the Hub and the Database for high performance and scalability. Please ensure that there are significant CPU, memory, and I/O resources available on the host as these are major server-class virtual machines.

After installing the Stratusphere Database appliance into your virtual environment, please:

- assign 4 vCPUs or as stated in the online sizing tool,
- assign at least 8GB of Memory or as stated in the online sizing tool,
- set the required amount of disk space on all the disks as stated in the online sizing tool,
- and connect the NIC to the same virtual network switch and port group as the Stratusphere Hub.

To start the configuration of the Database appliance:

1. Power ON the Database appliance and go to the virtual machine console.
2. The Stratusphere Database Configuration Wizard will automatically start. 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.



3. The wizard will ask for:
    a. Current Value of Hostname: Please enter a DNS resolvable fully qualified host name.
    b. Do you want to use DHCP (Y/N)? If you choose No, it will prompt for static IP address. Liquidware recommends using static IP addresses.
    c. What IP address do you want to use?
    d. What Netmask do you want to use?
    e. What is the default gateway?
    f. What Primary DNS server do you want to use?
    g. What Secondary DNS Server do you want to use?
    h. What Tertiary DNS Server do you want to use?
    i. Do you want to auto config IPv6? If you choose Yes, you will not have to set items 10-12.
    j. What IPv6 Address do you want to use?
    k. What is the IPv6 subnet prefix length?
    l. What IPv6 gateway do you want to use?
    m. Enable the NTP Time Server Service [Yes]?
    n. What NTP Time Server do you want to use?

    The following is an example of a completed configuration that the wizard displays after all settings have been entered. Please note that names and IP addresses will vary according to your environment.

```
=====================================================================
== Stratusphere Database Pending Configuration
=====================================================================

* 1) Hostname                    : db.domain.com

* 2) DHCP                        : No
* 3) IP Address                  : 10.0.80.142
* 4) Netmask                     : 255.255.254.0
* 5) Gateway                     : 10.0.81.42

  6) DNS Server 1                : 10.0.20.20
  7) DNS Server 2                : 10.0.20.25
  8) DNS Server 3                :

* 9) IPv6 Auto Config            : Yes
 10) IPv6 Address                :
 11) IPv6 Subnet Prefix Length   :
 12) IPv6 Gateway                :

 13) Enable NTP                  : Yes
 14) NTP SERVER                  : 0.centos.pool.ntp.org

Do you want to save this configuration (Write/Edit/Abort/Quit/No/#) ?
```

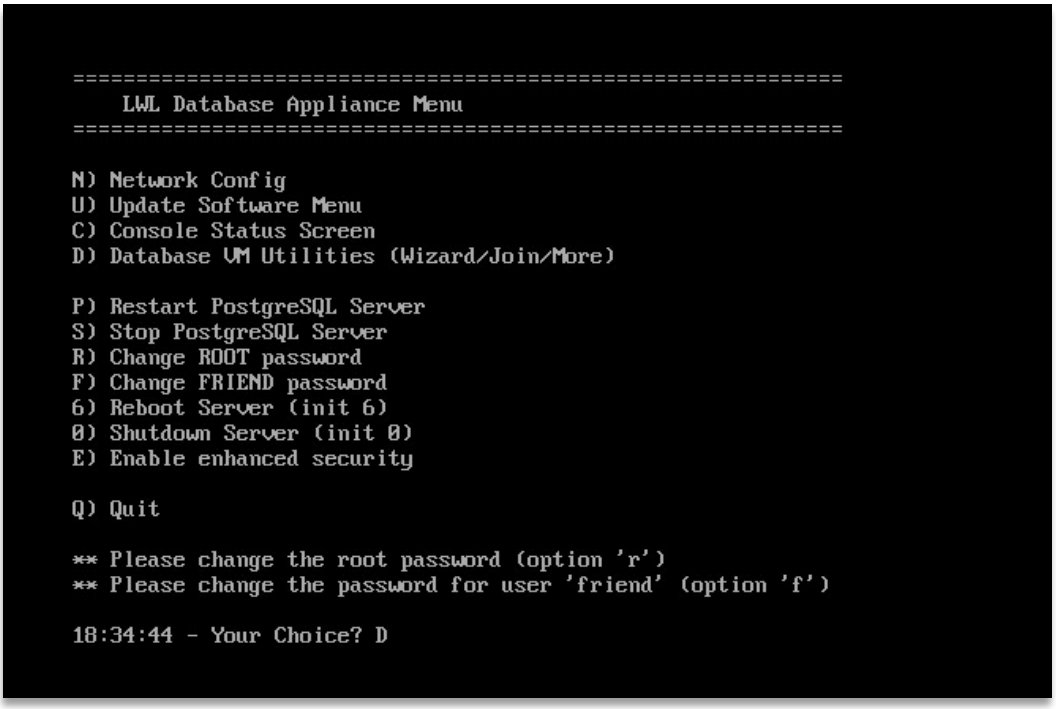
4. Type **`W`** or **`Write`** to save your configuration. You will finish with a screen showing the status of your database.

```
                    LWL Stratusphere  Vers: 6.0.0-1
          Copyright 2017, Liquidware Labs, Inc. www.liquidwarelabs.com

 LWL DATABASE: josephwin7322.atl.lwl.corp
       My IP: 10.0.80.142
      My HUB:
  Database: postgresql-9.6 (pid  6785) is running...

 top - 13:03:08 up 20 min,  0 users,  load average: 0.00, 0.00, 0.00
 Mem:  16335968k total,   738944k used, 15597024k free,    17792k buffers
 Swap:  8386556k total,        0k used,  8386556k free,   474612k cached
 Cpu(s):  0.8%us,  0.3%sy,  0.0%ni, 98.5%id,  0.4%wa,  0.0%hi,  0.0%si,  0.0%st

   Disk: Root          Used: 897M (15%)    Size: 6.3G    Free: 5.1G (85%)
   Disk: Database      Used: 71M (1%)      Size: 32G     Free: 30G (99%)









  alt-F2 Login to Console (or press ENTER)                alt-F1 This Screen_
```

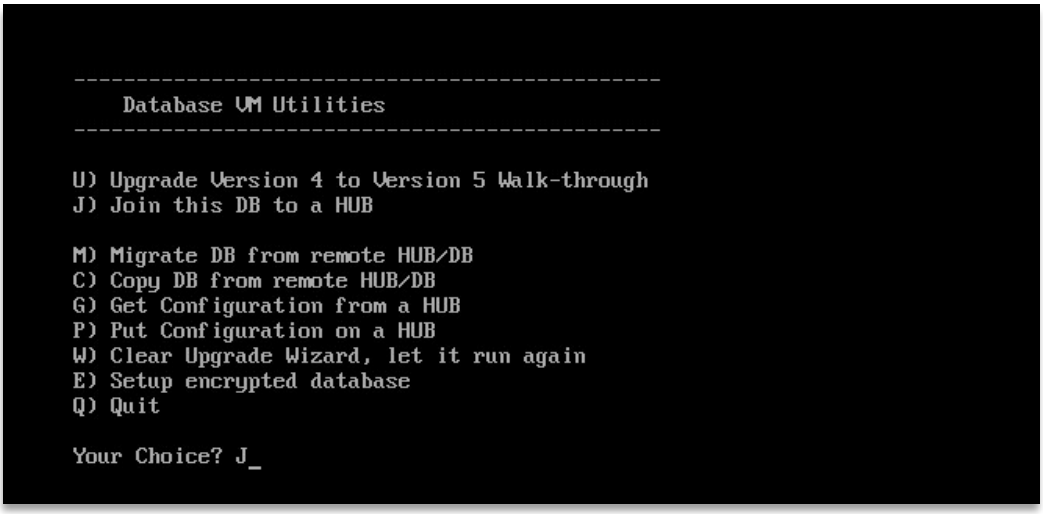
Connecting the Hub and Database Appliances

To connect the Database appliance with the Hub:

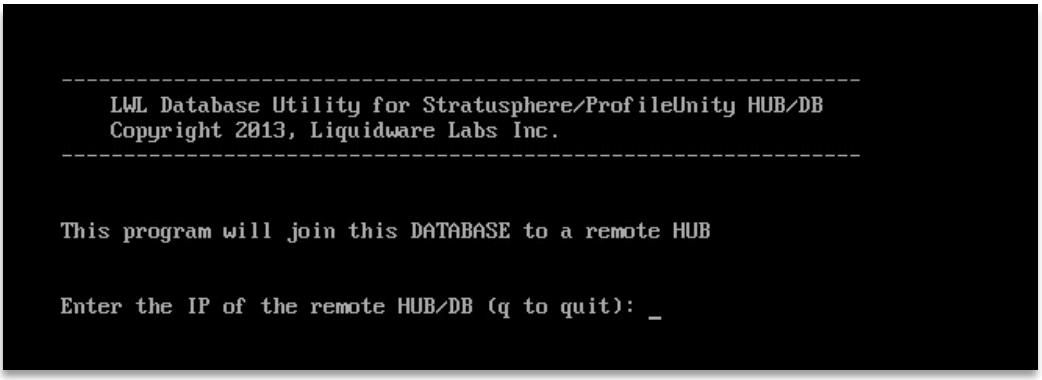
1. Make sure both the Hub and Database appliances are powered ON.
2. Open an SSH session to the Database appliance.
   Important Note: Liquidware recommends and for the purposes of these instructions assumes usage of the PuTTY SSH Client while connecting to Stratusphere appliances. Depending on your platform, use credentials such as:
   `friend` (VMware vSphere, Citrix XenServer, Microsoft Hyper V, Nutanix Acropolis, etc.)
   OR
   `ec2-user` (Amazon AWS)
   OR
   `az-user` (Microsoft Azure) or similar when appliance was created
   Use their respective passwords or SSH Keys (AWS & Azure) to log into the appliance. Then execute the following command to open the Liquidware Database Appliance Menu utility:
   - `sudo lwl`
3. The LWL Database Appliance Menu appears as shown below. Choose option **`D`** to go to the Database Utilities.



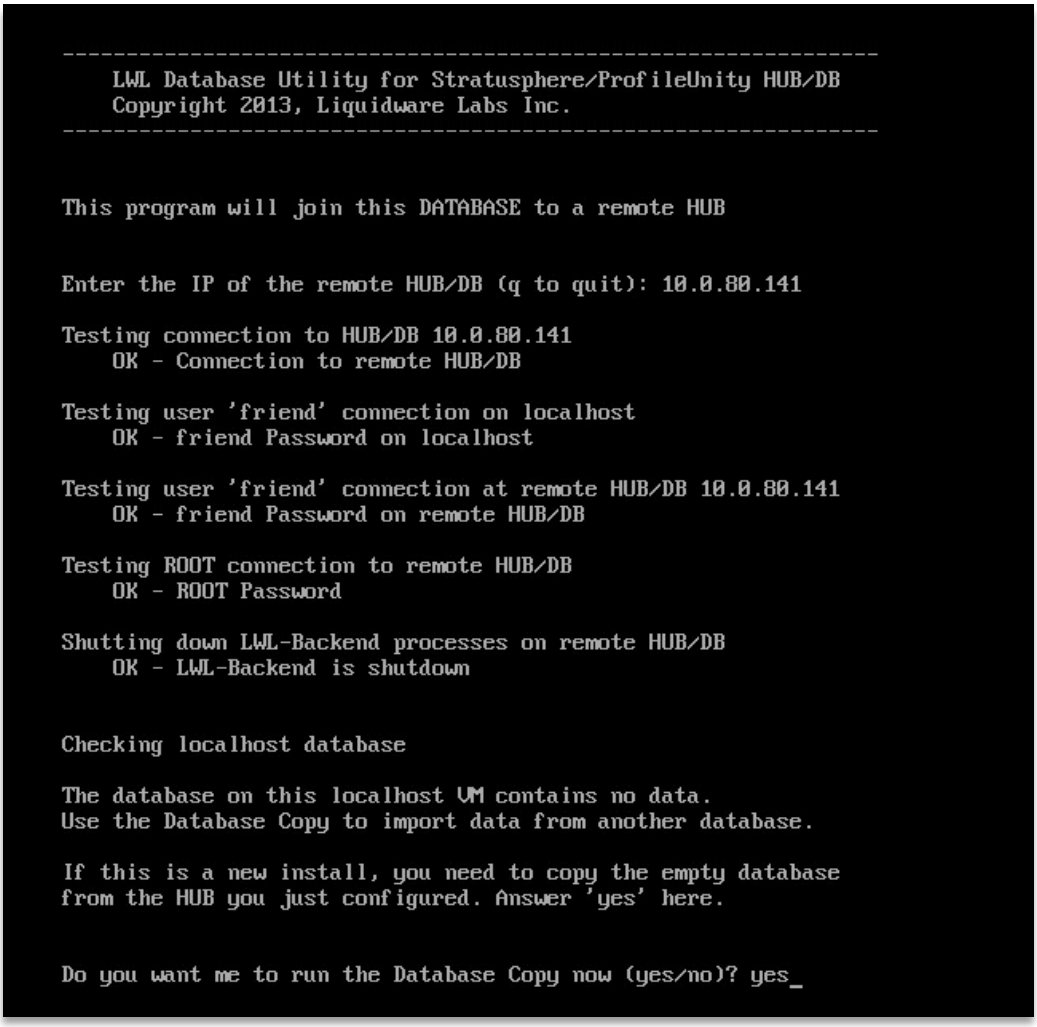
4. Choose option **J** to join the Database appliance with the Hub appliance.



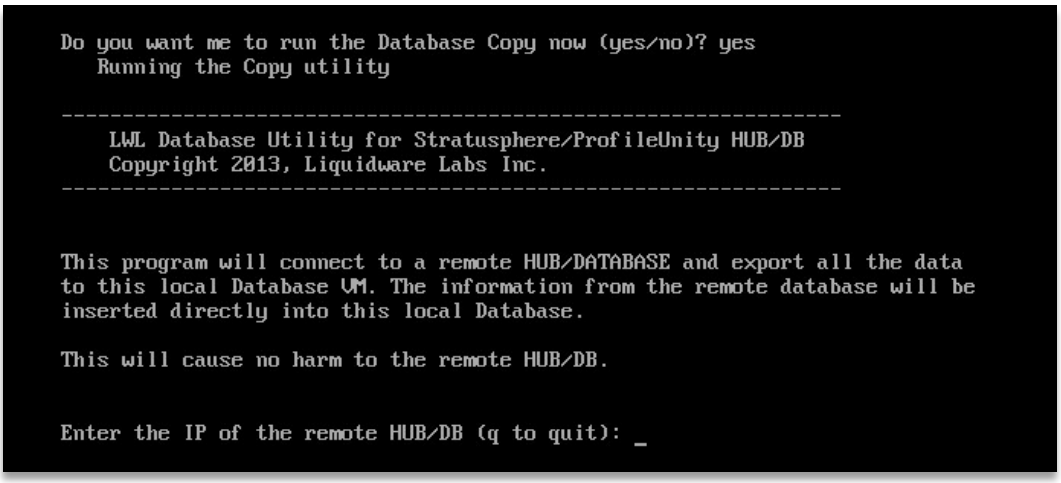
5. Type the IP address of the Hub you wish to connect to this Database and then press **Enter**. The Database will test the connection with the Hub.



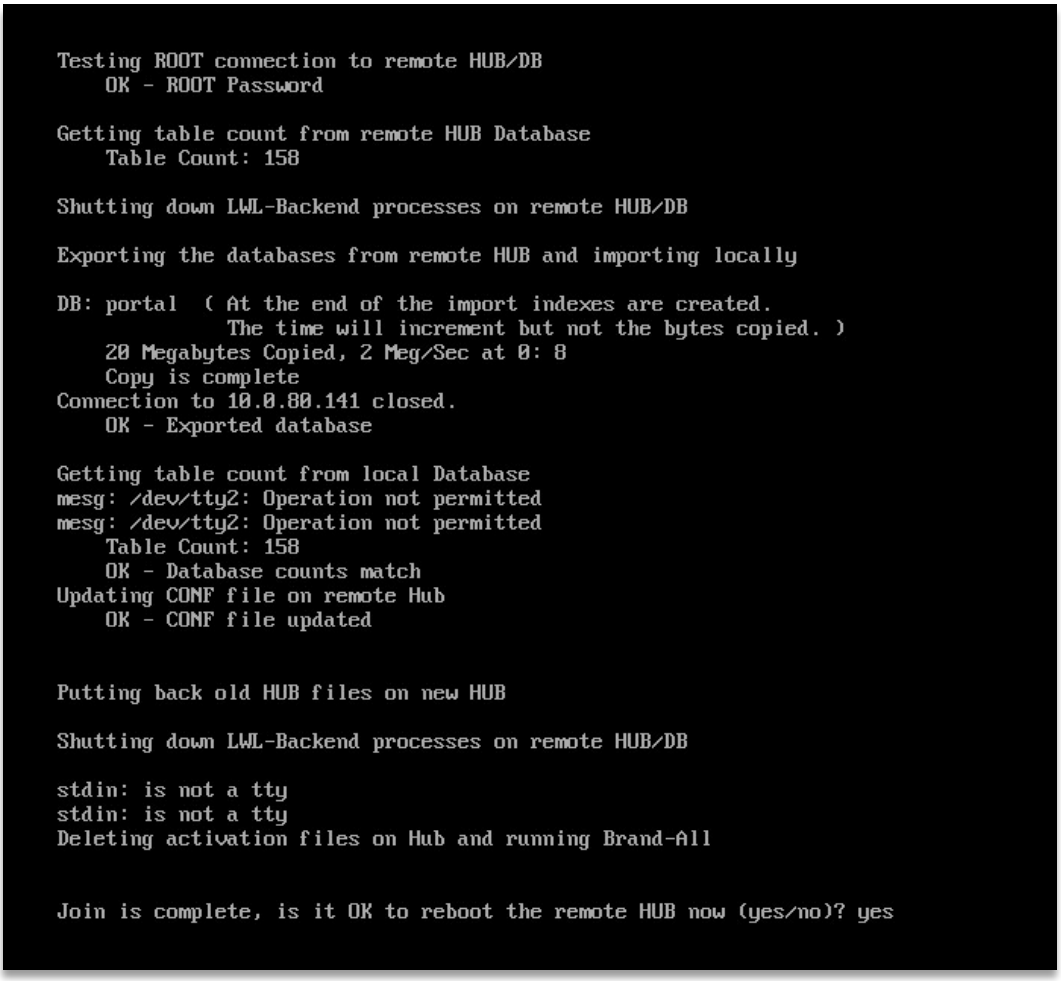
6. Type **yes** to begin the copy of the Database.



7. Then confirm the IP address of the Hub.



8. Type **yes** and then press **Enter** to allow the remote Hub to reboot.

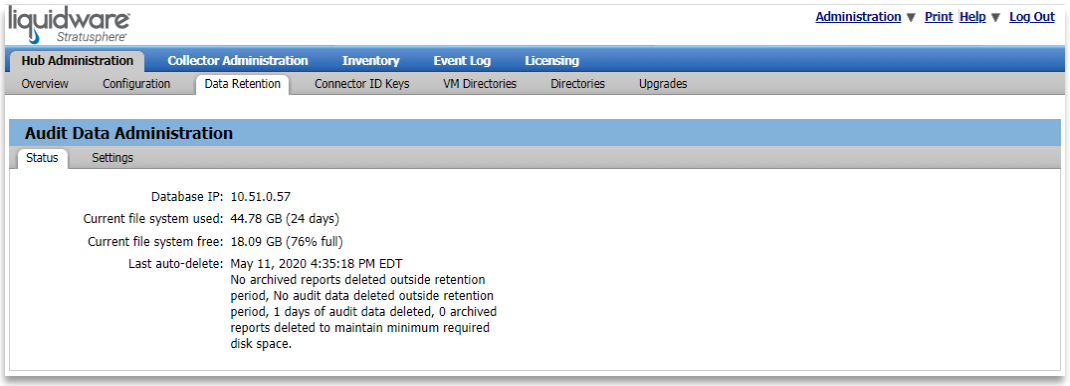


9. The Stratusphere Hub appliance will reboot. On the Stratusphere Database appliance, you may press **Enter** to complete the connection.

Verifying the Configuration

The Stratusphere Database appliance is now configured and connected to the Stratusphere Hub. Please verify the configuration by following these steps:

1. Once the Stratusphere Hub appliance has completed rebooting, you may log in to the Hub web interface to continue the configuration process using the Hub IP address and the following credentials:
    a. user name = **ssadmin**
    b. password = **sspassword** (Note: For AWS, use your VM Instance ID for the password.)
2. Navigate to the **Hub Administration > Data Retention > Status** tab and verify the Database IP and free space available matches the newly configured Stratusphere Database appliance.

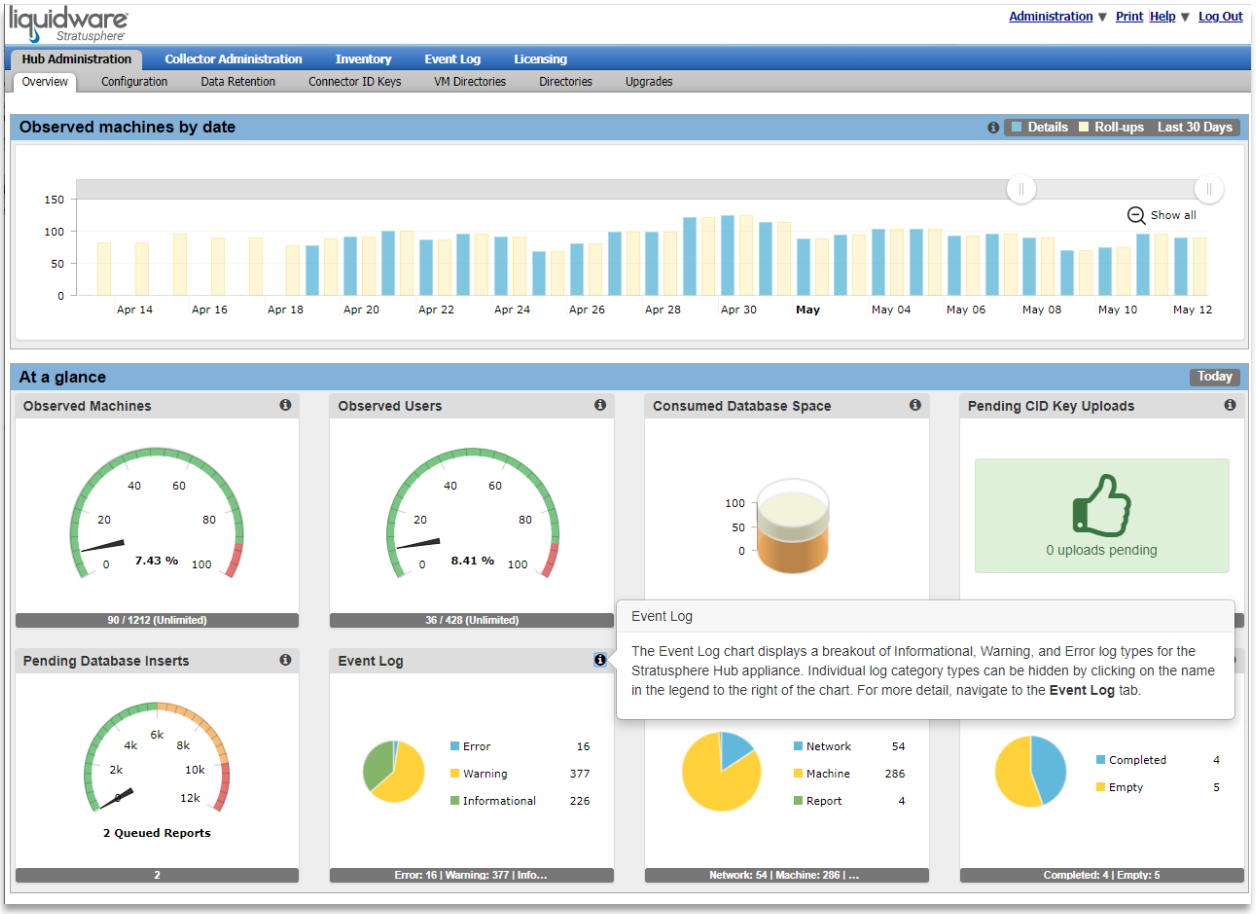


The database transfer and restore procedure is now complete. If you see any other messages or errors, please submit a request on the Liquidware Customer Support Portal to contact our Support Team.

> ***Note: If you are adding a Database appliance to an existing Stratusphere Hub installation where Collectors were deployed before the database was installed, you will need to re-register the Collector appliances to send data to the new Database instead of the Hub. Please see our KB article on re-registering Collectors.***

Reviewing Operations at a Glance with the Administration Overview

After logging in to the Stratusphere Hub Administration module, the display defaults to the **Overview** tab. The **Overview** tab displays several different dashboards that relay operational and communication information. Administrators can see at a glance how many machines and users are calling back to the Hub, how much space is remaining for the database, and monitor event logs and alerts. Clicking on the information icon in the upper right corner will give you a specific description for each dashboard.

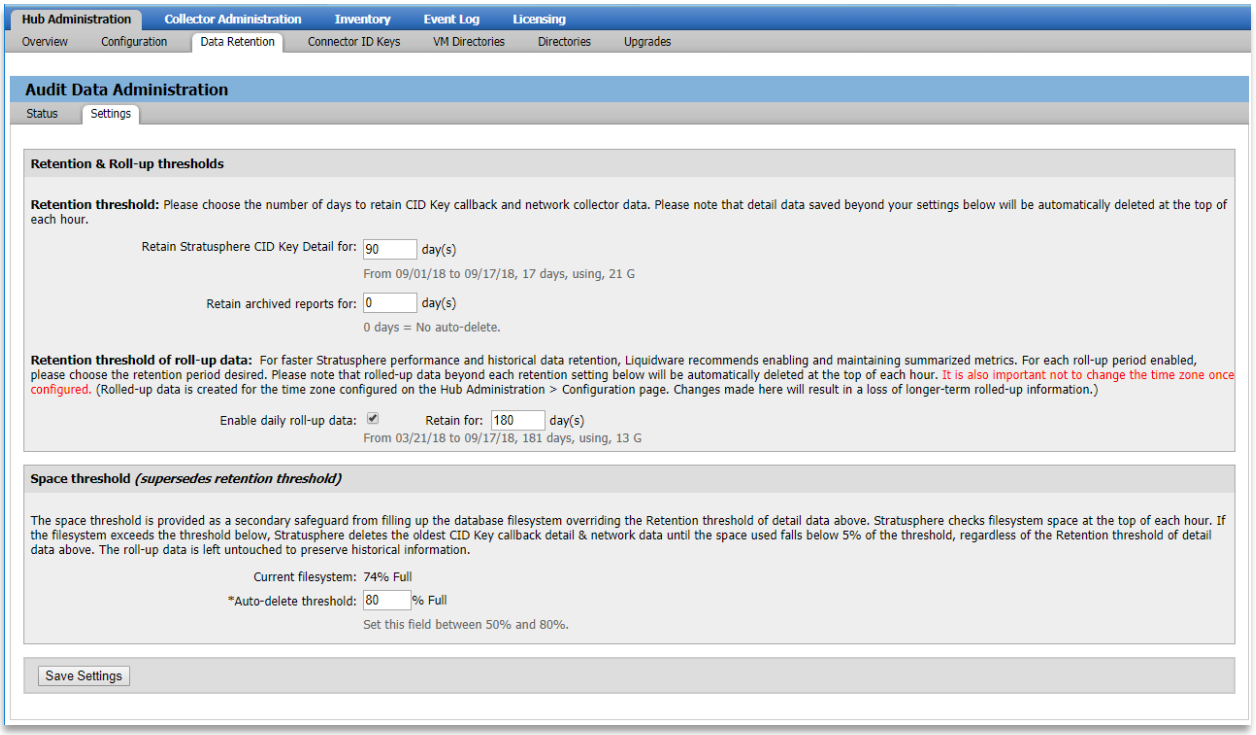


To start populating these dashboards for new Stratusphere installations, continue reading to learn how to configure Stratusphere to collect information on your environment.

Configuring Data Retention Settings

Administrators can setup policies to decide how much information from the environment to keep and how long to keep it. Earlier, if you opted to use the database appliance, you will remember that we used the **Hub Administration > Data Retention > Status** tab to verify that the Stratusphere Database appliance was connected to the Stratusphere Hub appliance.

Use the **Hub Administration > Data Retention > Settings** tab to customize your data retention policies. Additional help text to show the period and storage size of the data retained can be found below each threshold text box.

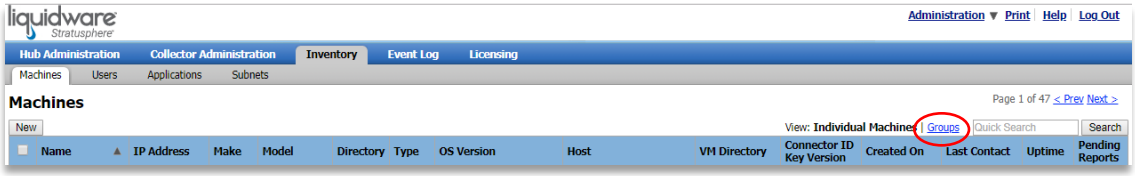


Setting Up Machine and User Groups

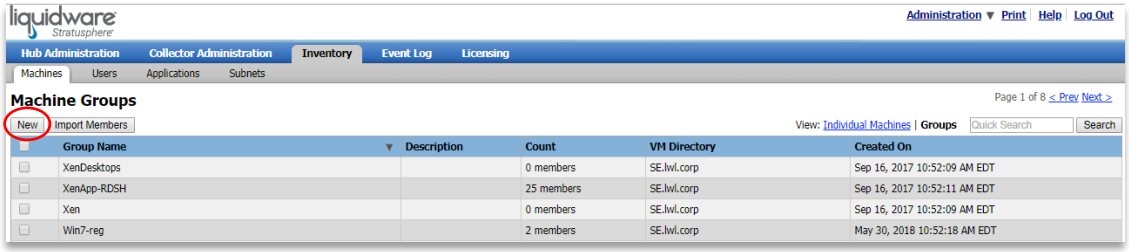
Now that you have completed the initial installation and settings for the Stratusphere Hub and are logged into the Hub Administration module, consider whether you want to define any user groups or machine groups. You may choose to setup groups if you have distinct sets of users or desktops that you want to analyze separately. These groups do not need to be setup initially. However, if you set them up from the beginning, 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 completely optional.

Machine groups can be used to group desktops for assessment, for example by location or by department. To define machine groups:

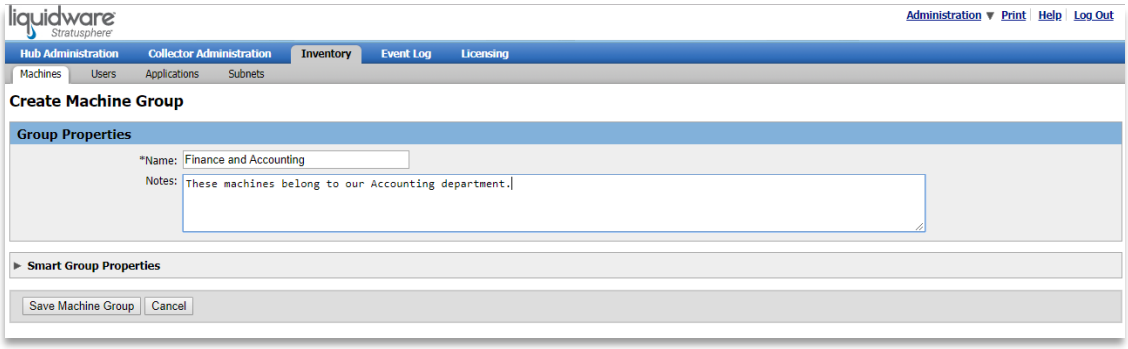
1. Go to **Inventory > Machines** and select **Groups.**



2. Click the **New** button.

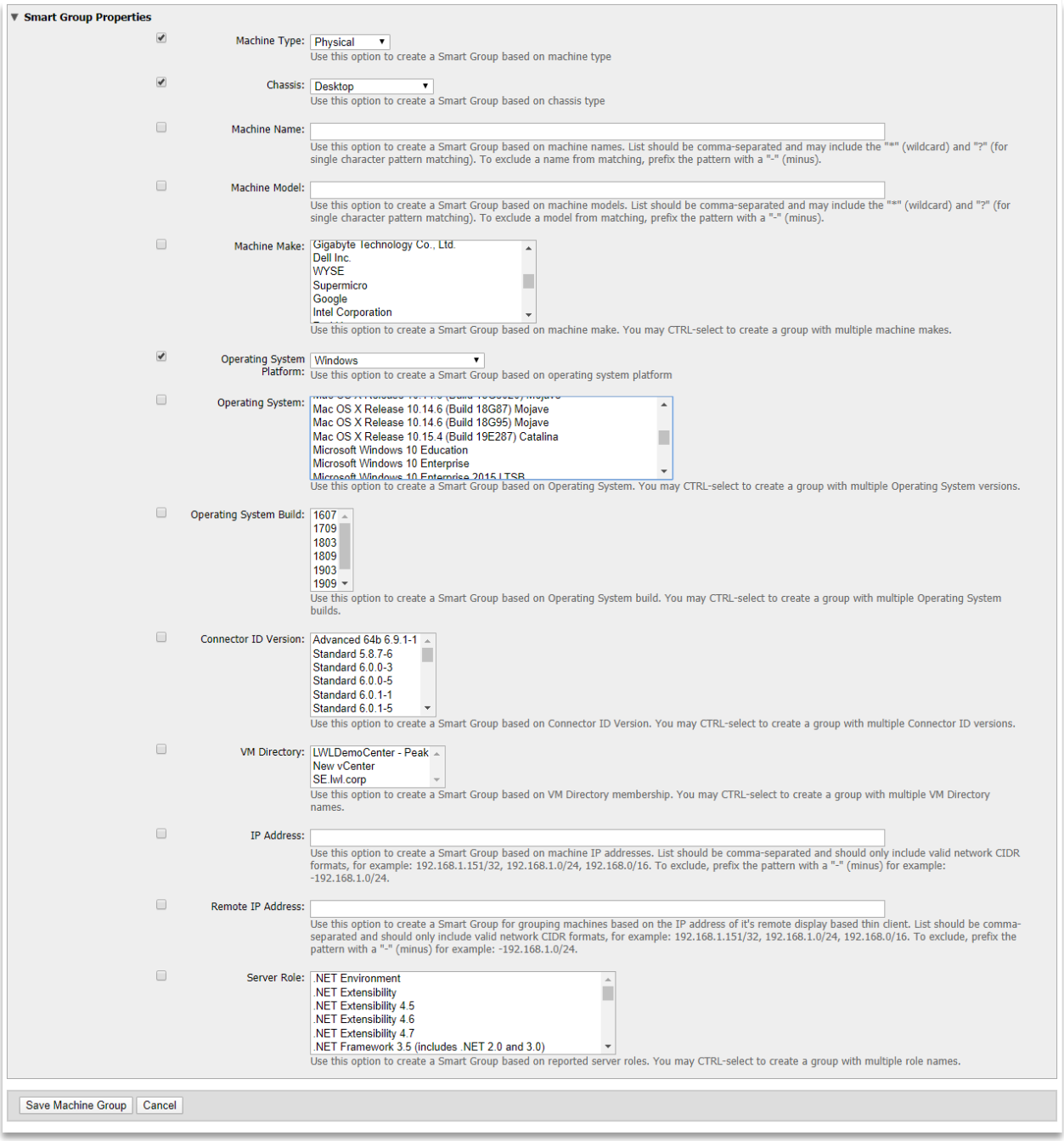


3. Enter your new machine group name and description.



4. As an optional step, expand the **Smart Group Properties** and choose the categories that apply to the new machine group. Stratusphere will populate groups for you based on the Smart Group properties chosen. For example, if the new machine group contains physical desktops running Windows, Stratusphere will automatically add that new machine group to a Physical Machines Smart Group, a Desktop Smart Group,

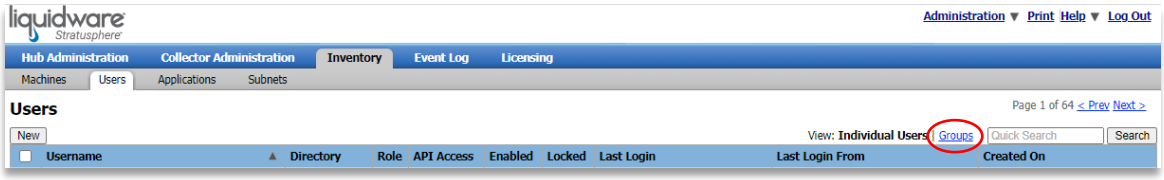
and a Windows Smart Group when it is created. Please note that drop-down options for each Smart Group Property is populated based on what CID Keys report back from the environment to the Hub.



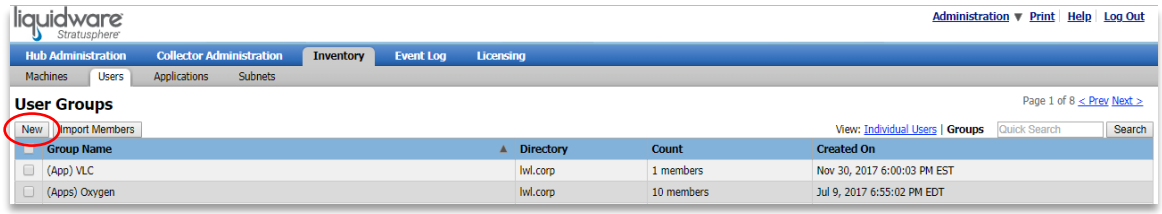
5. Click the **Save Machine Group** button to create the new machine group.

User groups can similarly be created by hand:

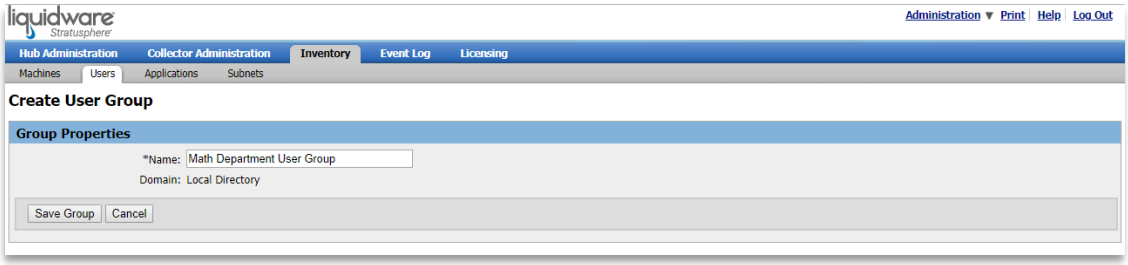
1. Go to **Inventory > Users** and select **Groups**.



2. Click on the **New** button.

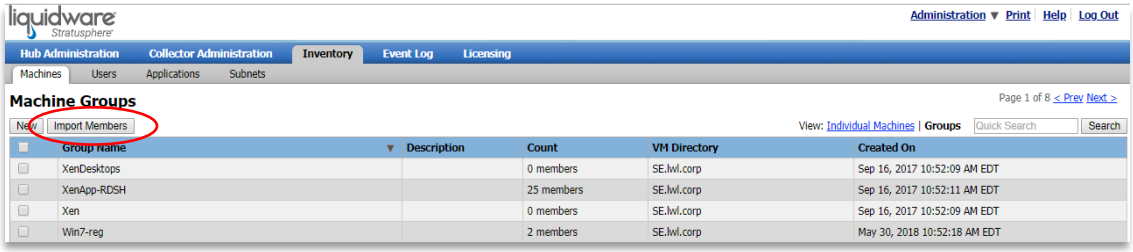


3. Enter your **ne**w user group name and click on **Save Group**.

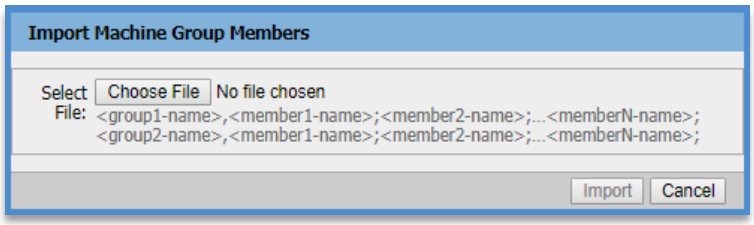


Instead of adding a new Machine or User Group one at a time, groups can also be imported. Group import files must have a CSV or TXT file extension. In addition, any machines or users listed under each group must already exist in the Stratusphere inventory in order to be organized into a group. If the machine or user has not previously been cataloged in the inventory, then it will not be added to the group. Creating groups can be done at any time, but adding members via import files should be done after the Stratusphere CID Keys are reporting data back to the Stratusphere Hub. To import groups:

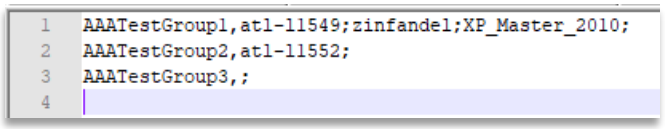
1. Go to **Inventory > Machines** or **Inventory > Users** and select **Groups**.
2. Click on the **Import Members** button instead of the **New** button.



3. Click on **Choose File** to select the CSV or TXT file containing your machine or user groups.



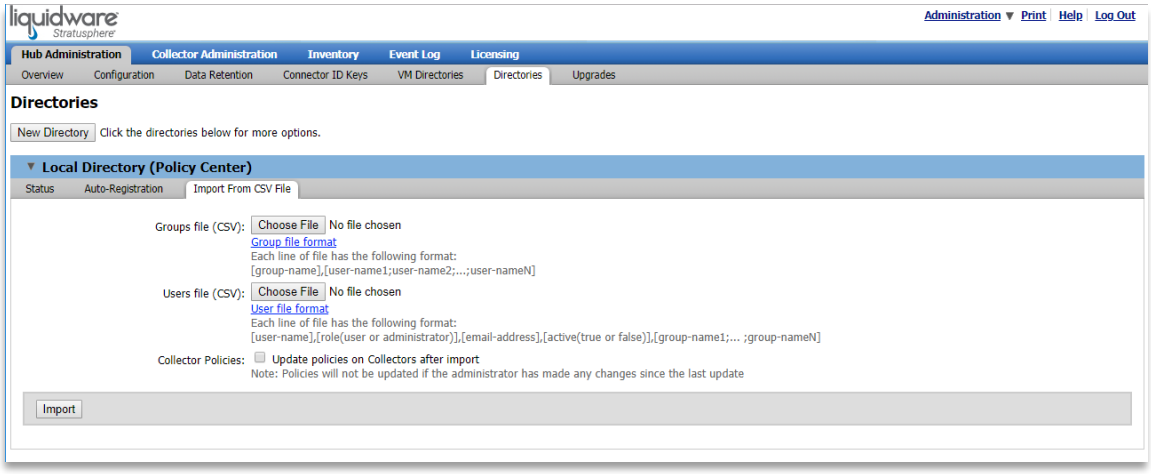
For example, here is a sample import file with groups that have multiple, one, or no machines:



4. Click on the **Import** button.

With user groups, you also have the choice to import groups from your Active Directory using LDAP or from a file. To import user groups from a file:

1. Go to **Hub Administration > Directories** and select the **Import From CSV File** tab from under the Local Directory (Policy Center). Information on the file formats for user groups and users can be found there.
2. Click on **Choose File** next to Groups to select the CSV file containing your user groups.
3. Click the **Import** button.



Using Stratusphere Collectors with UX (Recommended)

In Stratusphere 6.0, Liquidware introduced Stratusphere Collector appliances – a rebranded, and enhanced version of the older Stratusphere Network Stations. In addition to the existing functionality of the Stratusphere Network Stations of monitoring network connection traffic, the Stratusphere Collector appliances now also serve as a collection point for CID Key data. Previously, this functionality was only available within the Stratusphere Hub, but now has been extended to the Collector appliances as well. The Collector appliances serve in the following roles:

1. **CID Key Collector:** In this role, the Collector appliances are configured to serve as collection points for the CID Key to upload its metrics every callback interval. When the CID Keys register with the Stratusphere Hub, and if CID Key Collectors are available, the Stratusphere Hub gives a list of CID Key Collectors for the CID Key to upload its data every callback. The CID Key randomly chooses one CID Key Collector from this list to start, and then round robins its way through the entire list. The Collectors thus provide a highly available, and scalable architecture for data collection. When the CID Key Collectors receive data from a CID Key, they sanity check it for errors, and then save it to their internal disk-based queue. The Collector then removes the data from the queue, processes it, validates it, and then directly inserts it into the Stratusphere Database. It bypasses the Hub completely thus relieving the load on the Hub to basically do UI, Reports, and API handling. The current architecture supports up to 10 Stratusphere CID Key Collectors directly inserting data into the Database.
2. **Network Collector:** In this role, the Collector appliances are configured, like erstwhile Network Stations, to capture details on network traffic, bandwidth, latency, and server response times for your virtual desktops. To monitor or sniff network traffic of virtual desktops and servers, Network Collectors are deployed on each individual hypervisor hosts. They must be connected to a promiscuous port group (mirror port) on the host virtual switch. One Network Collector can monitor all the network traffic on an individual virtual switch on a single host. Once a Network Collector is installed and configured, it will automatically register with the Stratusphere Hub. The Network Collectors do not have their own browser user interface; however, they are configured via the console and the details of what traffic is to be monitored are set within the Stratusphere Hub Web UI's Administration section, under the Collector Administration tab. The Network Collector still monitors network traffic on a virtual switch and uploads this data to the Stratusphere Hub, which in turn inserts it into the Stratusphere Database. Since the Network Collector still uploads data collected to the Stratusphere Hub, more than 10 Network Collectors can be deployed with no change in settings.
3. **Dual CID Key & Network Collector:** In this role, the Collector appliances are configured to perform dual role of a CID Key & Network Collector in a single appliance. The CID Key data collected is directly inserted into the database whereas the Network data collected is uploaded to the Hub which in turn is inserted into the database.

> ***Note: Network Collectors are meant to be used with Stratusphere UX and not Stratusphere FIT.***

Host Configuration Changes for CID Collectors

The Stratusphere CID Key Collector appliances can be deployed right out of the box with no configuration changes required on the hypervisor hosts.

Host Configuration Changes for Network Collectors

The Stratusphere Network Collector needs some configuration changes on the host to monitor or sniff network traffic. The Network Collector requires 2 NICs. 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 or on a Cisco Nexus 1000v switch. The steps to configure a Network Collector are similar to the Stratusphere Hub. However, during the configuration, the Network Collector will prompt the user for information regarding the Stratusphere Hub's address and administrative credentials.

The summary of steps to install a Network Collector is:

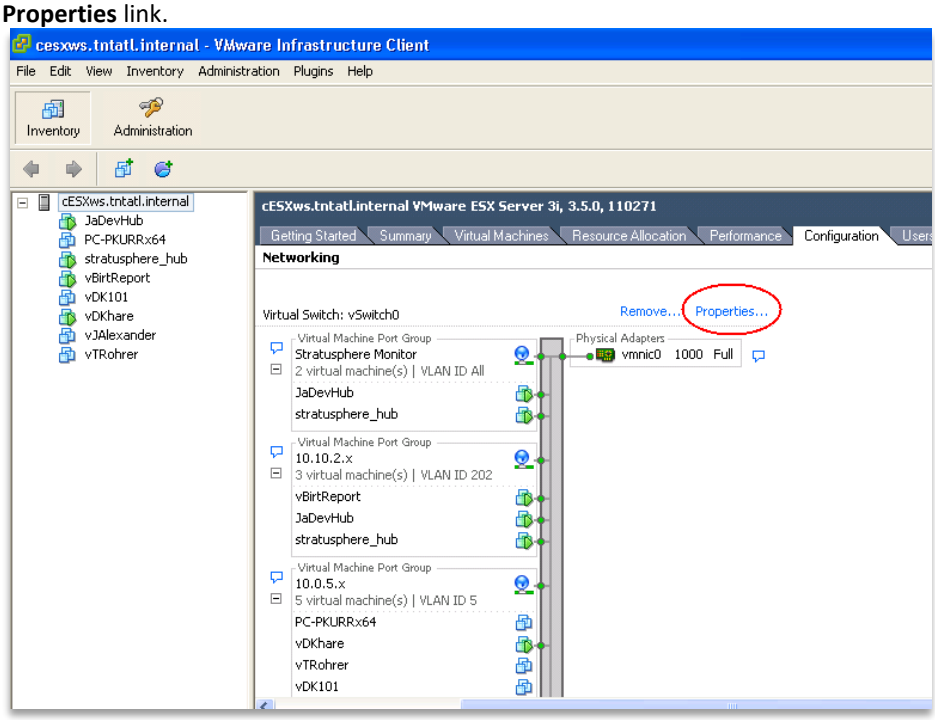
- Configure a promiscuous port on the target virtual host(s) as described below
- Import the OVF or XVA (Download from Liquidware)
- Connect the second port of the Network Collector to the promiscuous port
- Power on the Network Collector
- Click into the console, specifying the Collector's network connection information and specifying the connection information to connect to the Stratusphere Hub

To enable detailed network performance monitoring, the Network Collector 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. Configuring the Collector's second network connection for promiscuous mode will not affect any other VMs on the Host. Please follow the instructions that apply for your environment.

Configuring Network Monitoring on a VMware Standard Virtual Switch

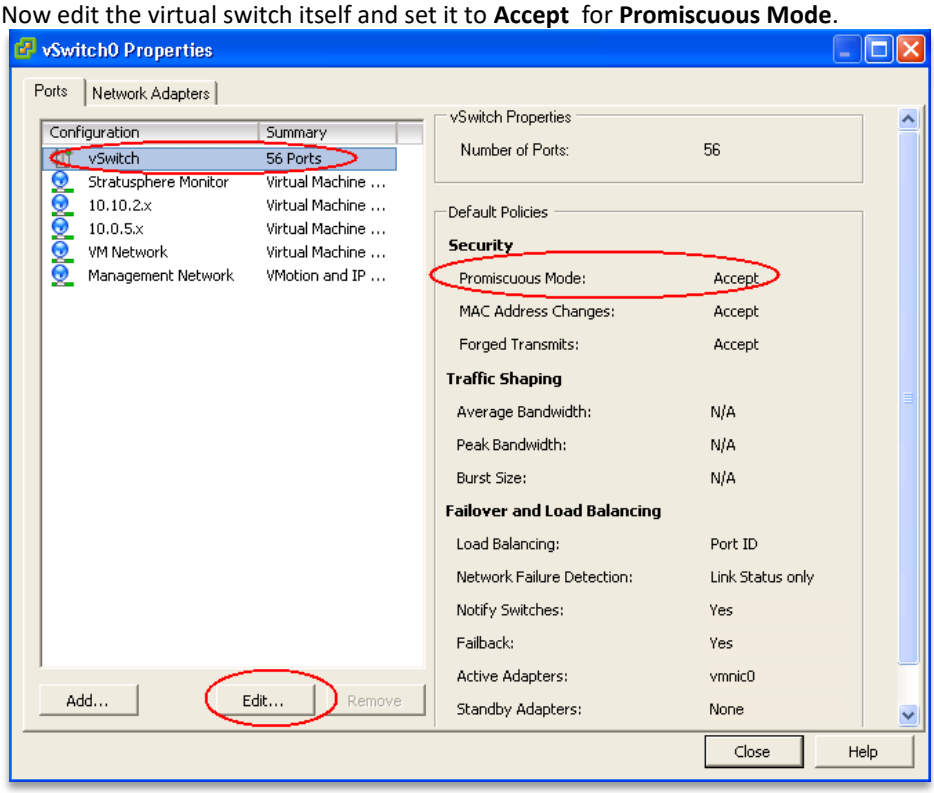
Here are the steps to configure a VMware standard virtual switch:

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 on the **Properties** link.

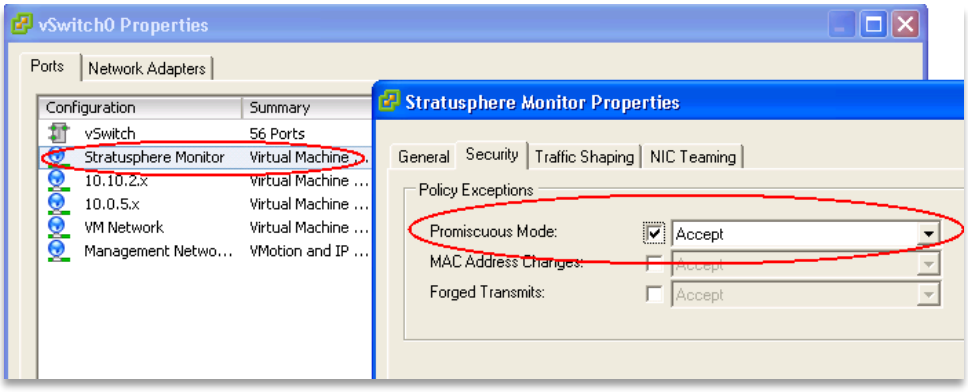


2. Set all existing production port groups on the virtual switch to **Reject** for **Promiscuous Mode**.

3. Now edit the virtual switch itself and set it to **Accept** for **Promiscuous Mode**.



4. Now add a new Port Group and it will inherit the **Accept** for **Promiscuous Mode** from the virtual switch. If there are multiple VLANs on this switch and you want to monitor only one, 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.

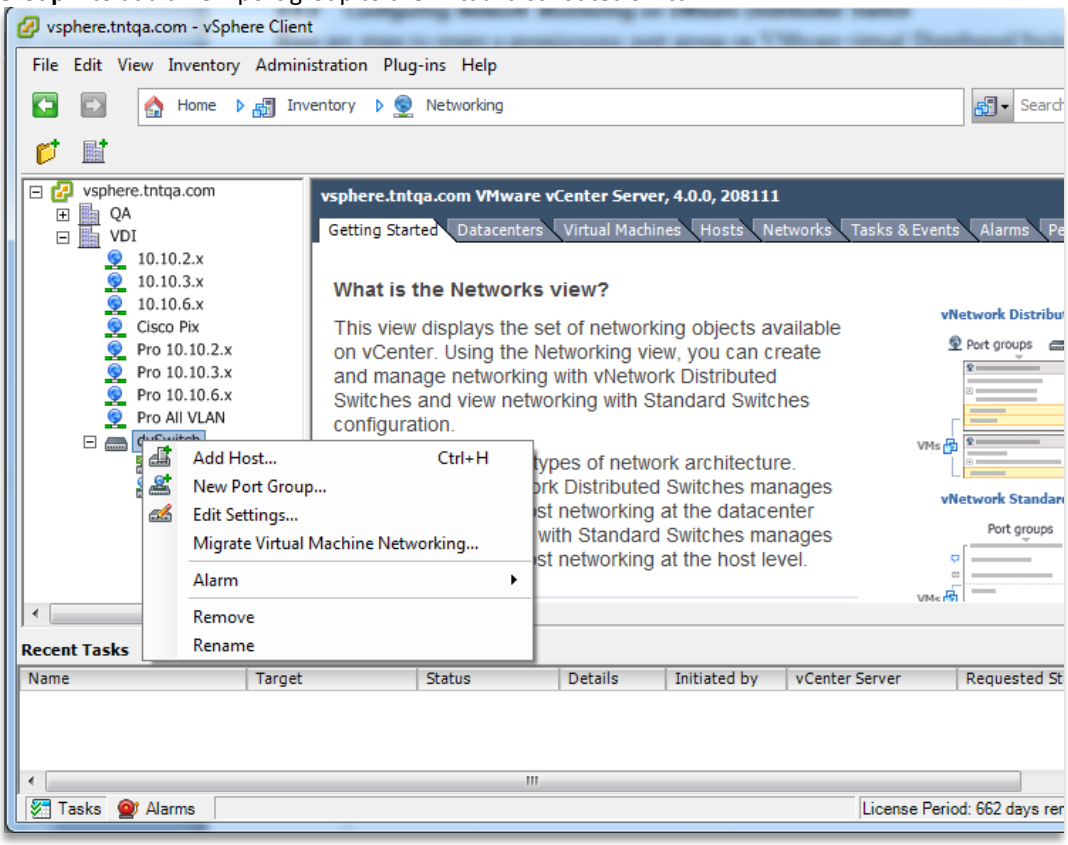


Once your virtual switch is configured, you are ready to download and install the Network Collector Virtual appliance onto your VMware host.

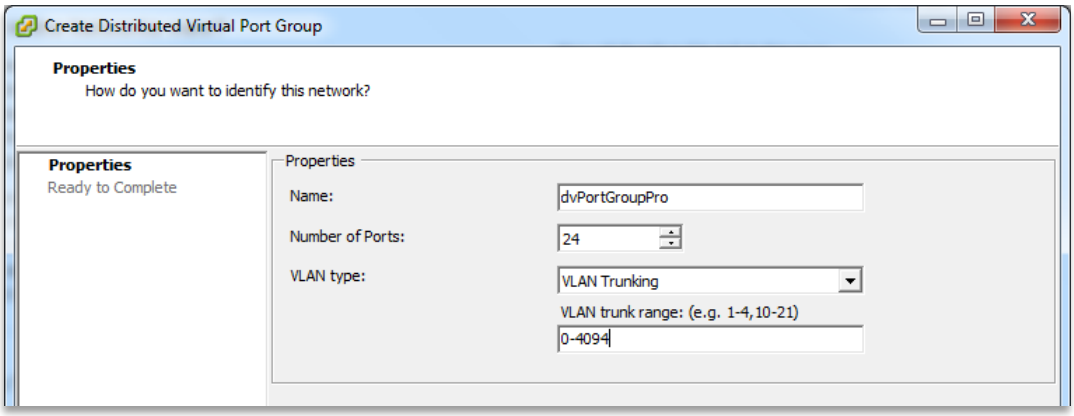
Configuring Network Monitoring on a VMware Distributed Switch

Here are steps to create a promiscuous port group on VMware Virtual Distributed Switch:

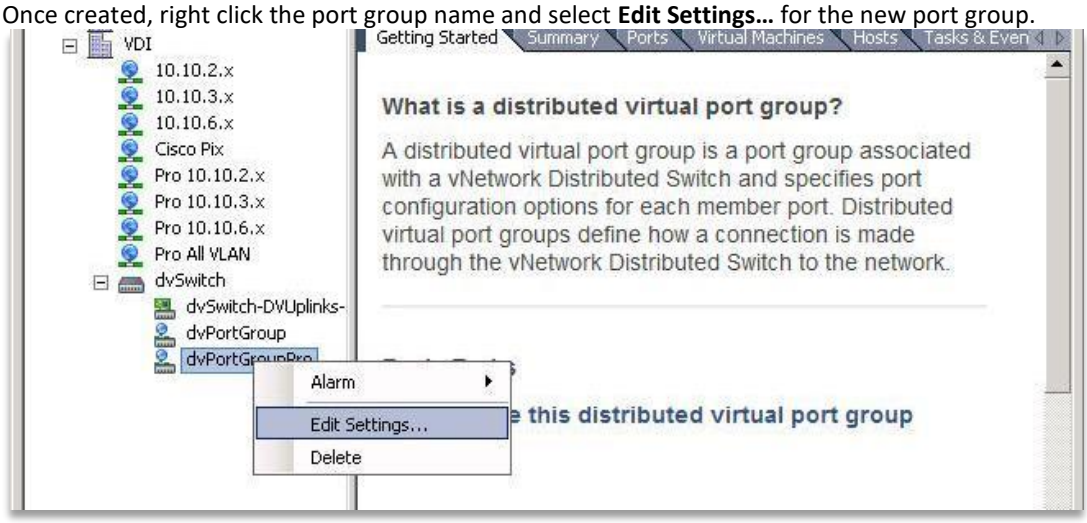
1. Inside the vSphere Client, right click on the name of your distributed switch and select **New Port Group…** to add a new port group to the virtual distributed switch.



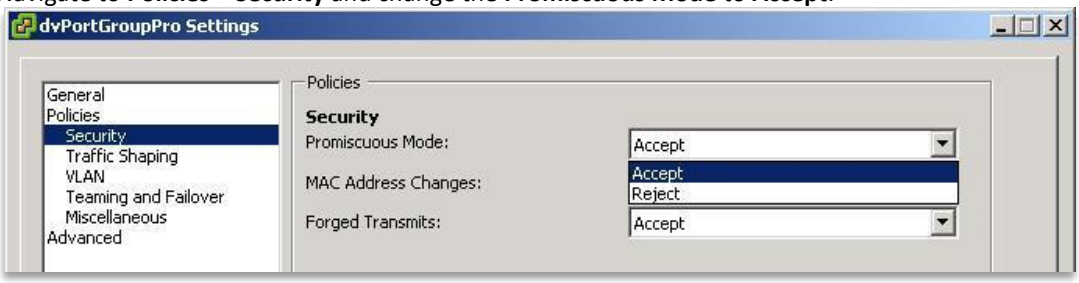
2. Give the port group an appropriate name such as “Monitor” or “dvPortGroupPro”. You can leave the default **Number of Ports** at 128 or reduce it to the number of hosts you have this distributed switch on in the cluster. Select the **VLAN Trunking** option for **VLAN Type** and enter **0-4094** for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



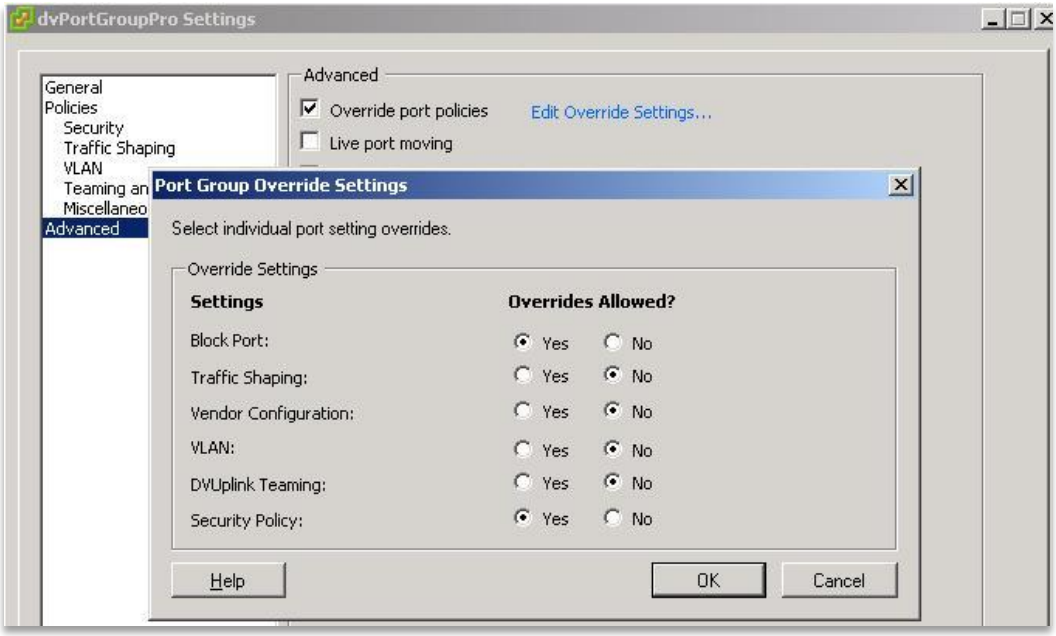
3. Once created, right click the port group name and select **Edit Settings…** for the new port group.



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



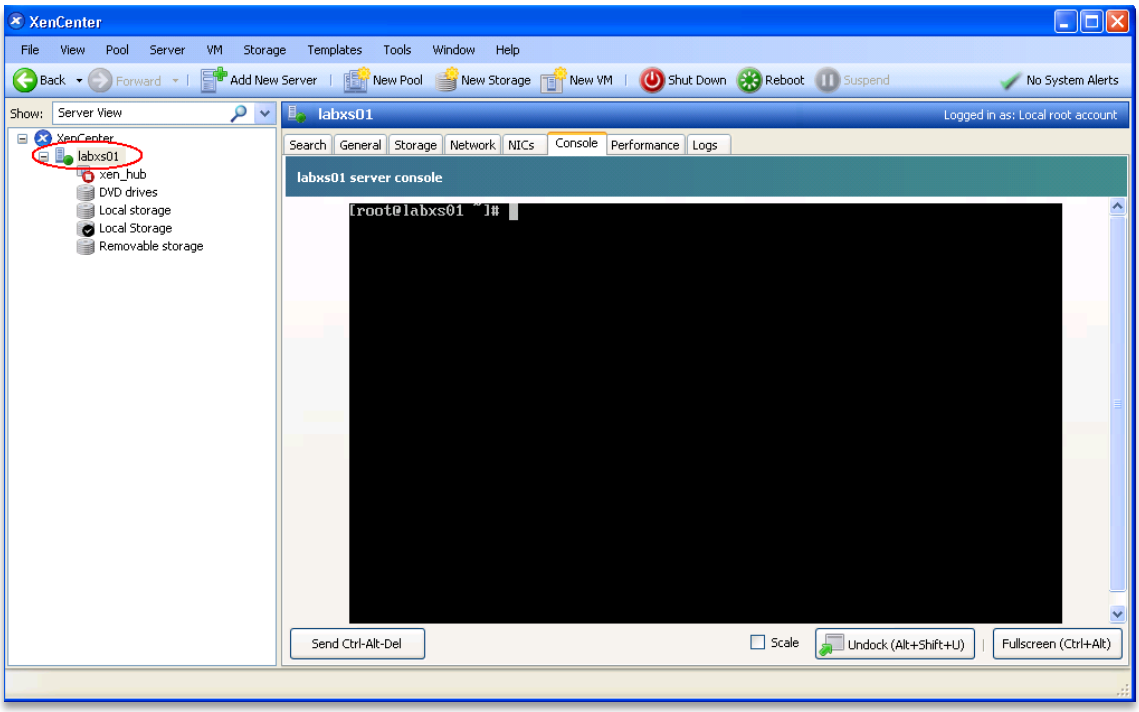
5. Now Navigate to **Advanced** and click on **Edit Override Settings…** Click on **Yes** to allow overrides for **Block Port** and **Security Policy**.



6. The promiscuous port group will now be available on each host that has this virtual distributed switch. Configure a Network Collector 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.

Configuring Network Monitoring on Citrix XenServer

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 press the **Tab** key.

At the console command line, perform the following steps:

1. Modify the promiscuous setting for the virtual host:

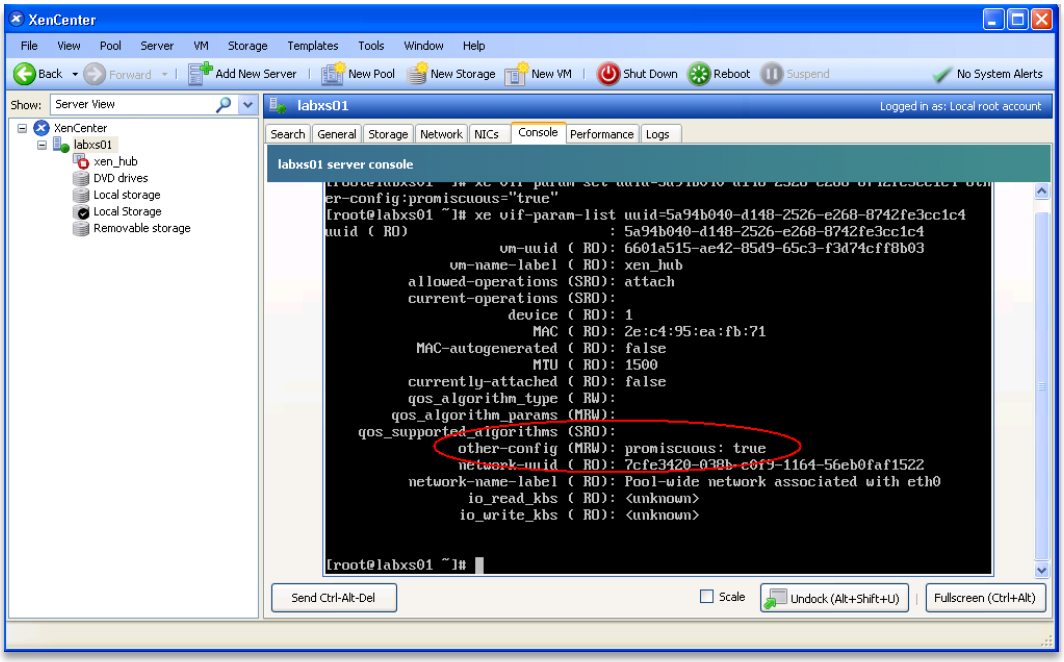
```
xe vif-list vm-name-label=station_monitor

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:

```
xe pif-list network-name-label=eth1

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:

```
xe network-list name-label=Pool-wide network associated
with eth1

xe network-param-set uuid=<uuid-of-network> other-
config:promiscuous="true"

xe network-param-list uuid=<uuid-of-network>
```



The Network Collector virtual appliance is now ready to be configured.

Configuring Network Monitoring on a Cisco Nexus 1000v Switch

Before making any changes, make a backup of the current configuration of the Cisco Nexus 1000v switch. Then, using administrative credentials, log into the Nexus 1000v console. Enter the following commands to configure the switch to sniff traffic in promiscuous mode. VLAN numbers are fictional in these instructions and should be substituted with actual VLAN numbers that host VDI traffic to be sniffed.

1. Create a new dummy VLAN to span traffic to:

```
nexus_switch(config)# vlan 3333
nexus_switch(config-vlan)# name MONITOR
```

2. Create new Port Profile that leverages the new dummy MONITOR VLAN

```
nexus_switch(config)# port-profile type vethernet VM-MONITOR-VLAN3333
nexus_switch(config-port-prof)# vmware port-group
nexus_switch(config-port-prof)# switchport mode access
nexus_switch(config-port-prof)# switchport access vlan 3333
nexus_switch(config-port-prof)# no shut
nexus_switch(config-port-prof)# state enabled
```

3. Setup Monitor Session. Within this monitor session, we will assign the source VLAN that contains all the VDI network traffic to be monitored and provide the MONITOR port profile as the destination to where it should be sent. The Stratusphere Network Collector will be connected to the Monitor port profile to sniff this traffic.

```
nexus_switch(config)# monitor session 10
```

4. Provide the source VLAN that contains the VDI network traffic to be monitored. In this example, we are using a fictional VLAN 3244 as the source VLAN that contains VDI traffic. The **rx** is the receive source specified to forward traffic that enters this VLAN. Use **tx** for transmit source for traffic leaving the VLAN.

```
nexus_switch(config-monitor)# source vlan 3244 rx
```

5. Send this collected traffic to the MONITOR port profile

```
nexus_switch(config-monitor)# destination port-profile VM-MONITOR-VLAN3333
```

6. Configure the monitor session so that it is running persistently

```
nexus_switch(config-monitor)# no shut
```

7. Save this configuration on the Nexus 1000v switch so that it persists beyond reboots. For any additional details please refer to Cisco's website for configuration and troubleshooting the Nexus 1000v switch.
8. Download the Stratusphere Network Collector as usual. The Network Collector has 2 NICs. NIC 1 is the management port that communicates with the Stratusphere Hub and requires a static IP address. NIC 2 is used for sniffing network traffic and it needs to be connected to newly created MONITOR VLAN port profile on the Nexus 1000v.

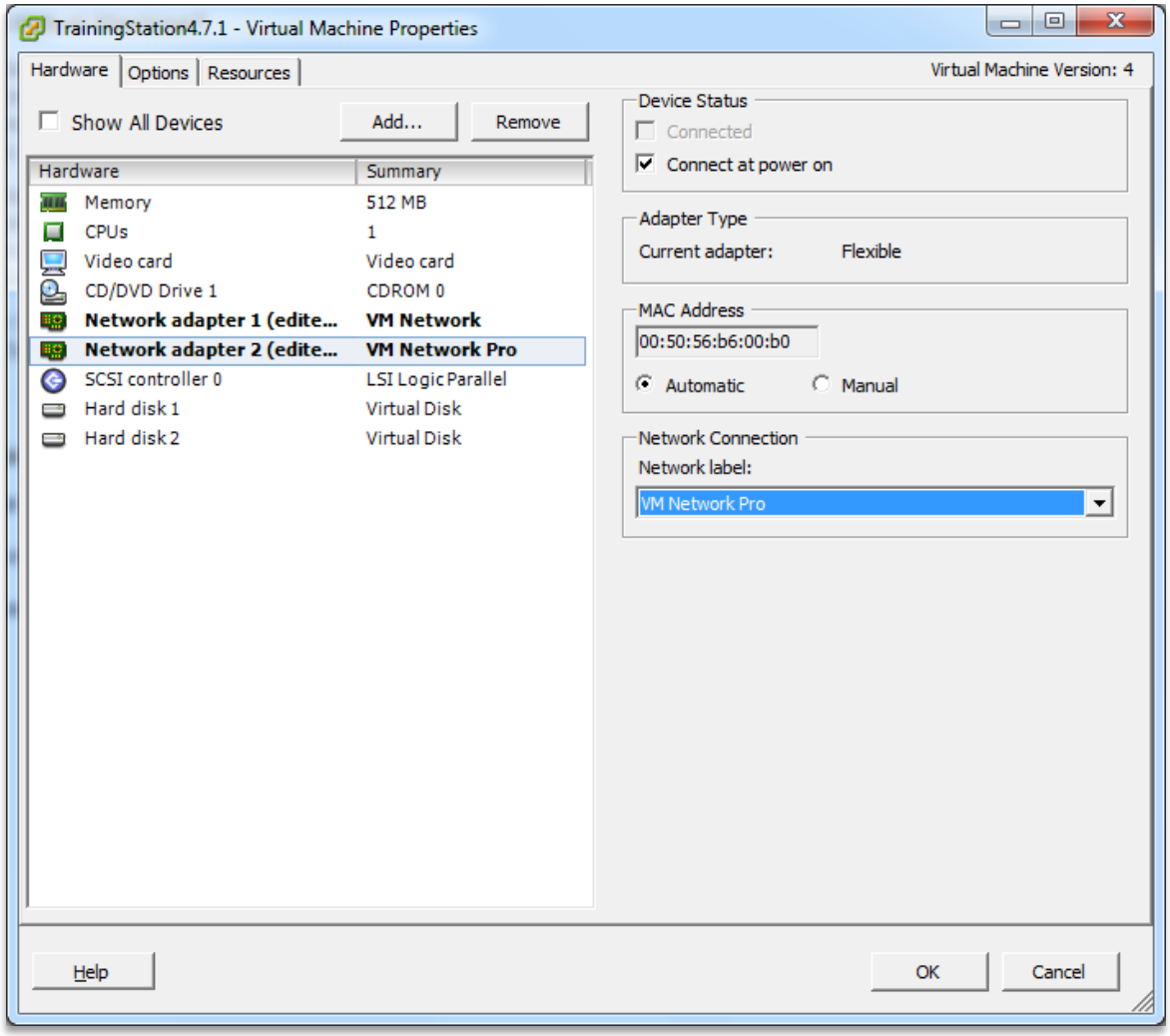
Installing a CID, Network, or Dual Role Collector

Please follow the instructions given in the beginning for **Installing the Stratusphere Appliances** in your virtual environment to assist you in installing a Stratusphere Collector appliance. The installation process is the same for CID, Network, and Dual Role Collectors.

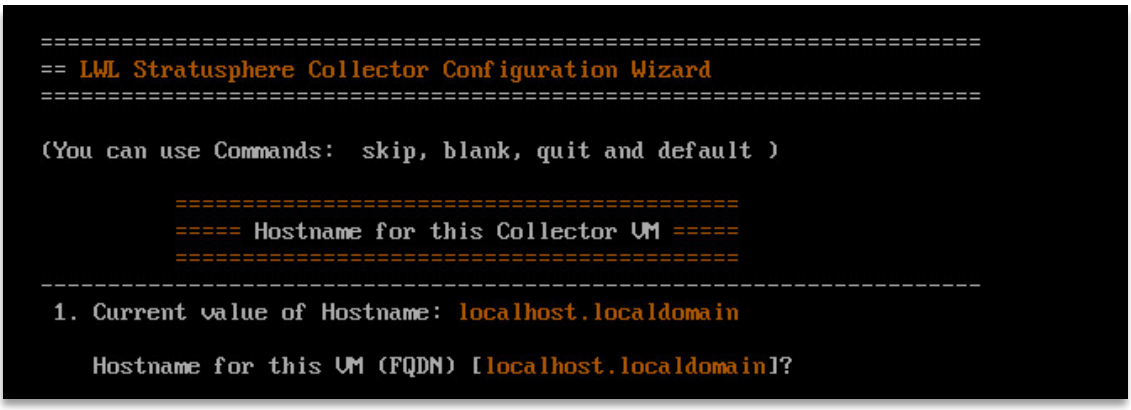
Configure a Stratusphere Collector using the Console

The Stratusphere Collector 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 sections above. It sniffs the traffic of this NIC and sends the data to the Stratusphere Hub over the management port. Once the Network Collector is downloaded from the Liquidware site, to configure these NICs, right click on the Network Collector appliance and select **Edit Settings**. Select the appropriate **Network Connection** labels and assign them to each NIC.

If installing a **CID Key Collector**, ignore or disregard the Network adapter 2 as it will not be used. If installing a **Network Collector or Dual Role Collector**, the second network adapter is required.



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.



The user needs to have the following ready items ready to configure the Collector:

1. Hostname: Please enter a DNS resolvable fully qualified host name. The Hub should be able to resolve this fully qualified host name to the IP Address. Also, if this is a CID Key Collector, CID Keys need to be able to resolve this DNS host name as well.
2. Static IP Address
3. Network Mask
4. Default Gateway IP Address
5. DNS Servers
6. NTP Enable and Servers
7. Stratusphere Hub's IP Address
8. Administrative credentials on the Stratusphere Hub: **ssadmin/sspassword**
9. Data Collected [cid/network/both]: Type cid for CID Key only, network for Network only, or both
10. Collector Inline [yes/no]: Type no
11. Enforcement or Monitor [enforce/monitor]: Type monitor

```
------------------------------------------------------------------------
 8. Current value of Enable NTP: Yes

    Enable the NTP Time Server Service [Yes]?

------------------------------------------------------------------------
 9. Current value of NTP SERVER: 0.centos.pool.ntp.org

    What NTP Time Server do you want to use [0.centos.pool.ntp.org]?


                ============================
                ===== Stratusphere Link =====
                ============================
------------------------------------------------------------------------
10. Current value of HUB Address:

    Use which Stratusphere HUB [ ]? 10.0.80.150

------------------------------------------------------------------------
11. Current value of HUB User:

    HUB admin account []? ssadmin

------------------------------------------------------------------------
12. Current value of HUB Pass:

    HUB admin password []? sspassword


           ======================================
           ===== Collector Monitoring Options =====
           ======================================
------------------------------------------------------------------------
13. Current value of Data Collected: network

    Type of data collected (network/cid/both) [network]? cid_
```

```
========================================================================
== LWL Stratusphere Collector Pending Configuration
========================================================================

* 1) Hostname              : scc600-01.se.lwl.corp

* 2) IP Address            : 10.0.80.152
  3) Netmask               : 255.255.255.0
* 4) Gateway               : 10.0.80.1

* 5) DNS Server 1          : 10.0.20.20
* 6) DNS Server 2          : 10.0.20.25
  7) DNS Server 3          :

  8) Enable NTP            : Yes
  9) NTP SERVER            : 0.centos.pool.ntp.org

*10) HUB Address           : 10.0.80.150
*11) HUB User              : ssadmin
*12) HUB Pass              : sspassword

*13) Data Collected        : cid
 14) Collector Inline      : No
 15) Enforcement or Monitor : monitor

Do you want to save this configuration (Write/Edit/Abort/Quit/No/#) ?
```

Once the user is satisfied with the configuration and types **W** and saves the configuration above, the Collector 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. The Collector will now show up under the

Stratusphere Hub's Web UI Administration product under the **Collector Administration** tab. It can be managed from the Hub's Web UI from that point forward.

Collector Administration

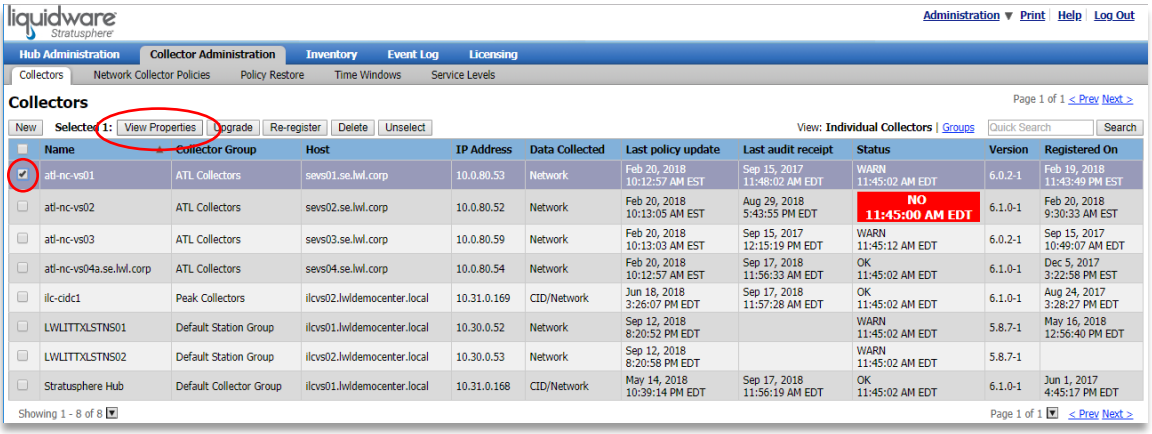
The **Collector Administration > Collectors** tab provides a list of all Collectors in the installation. It includes the Stratusphere Hub that has a Network Data Collector and CID Key Callback Data Collector embedded by default. Standalone Collectors can be configured to collect following data types:

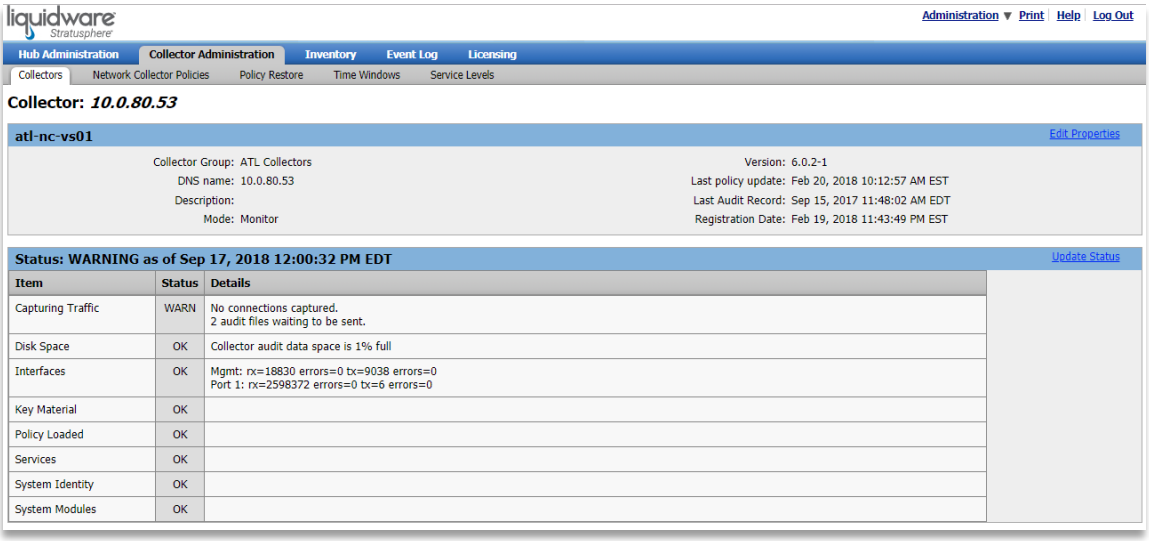
1. CID Key Callback data
2. Network data based on policies
3. Both types of information.

The Collectors tab is used to display and manage each Collector's properties and status. Collectors can be added to different Collector Groups, upgraded from the UI, and can also be selected to re-register themselves in certain cases.

Viewing Collector Status and Properties

Go to the **Collector Administration** tab to see the list of deployed collectors and perform management functions. From the list screen you can view status. To view details, select a collector and click on the **View Properties** button above.



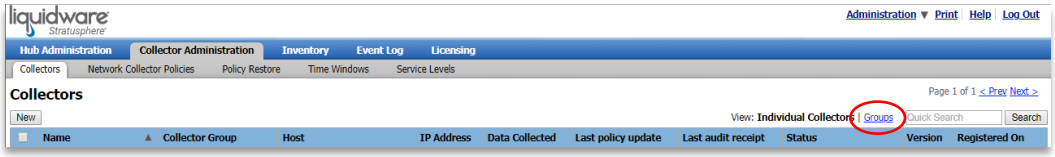


Setting Up Collector Groups

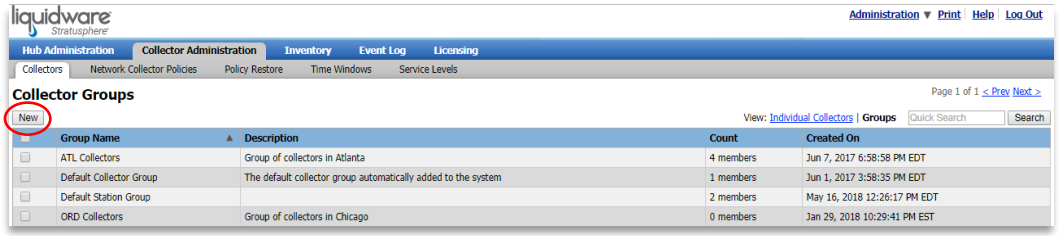
Individual collectors can be grouped together. Each group can have its own policy rules and can be filtered separately in diagnostic reports. Within the groups view, you can add, delete or change the existing groups.

To create collector groups:

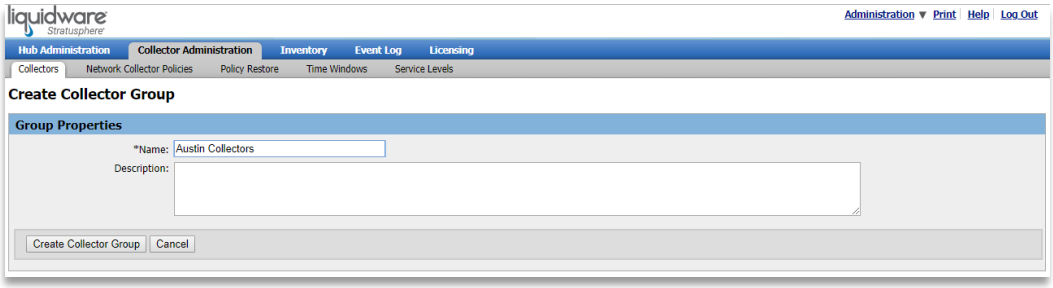
1. Go to **Collector Administration > Collectors** and select **Groups.**



2. Click the **New** button.



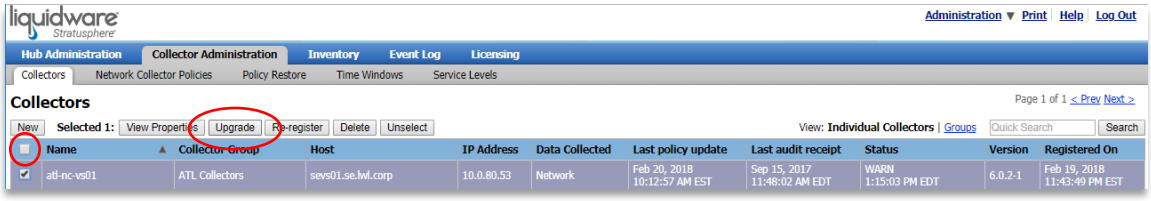
3. Enter your new group name and description.



4. Click the **Create Collector Group** button to create the new collector group.
5. To add individual collectors to this new group, select individual collectors from the Collectors tab and click on the **View Properties** button. Then click on the **Edit Properties** link at the top right. Select the **Collector Group** from the drop-down list.

Upgrading Collectors

To upgrade one or more collectors, select the collectors from the list and click the **Upgrade** button above. After a period of time, the upgraded collectors should display the new version in the list. If this doesn't happen, select the collectors and press the **Re-Register** button above, then the updated version number should show up.



Note: If you are adding a Database appliance to an existing Stratusphere Hub installation where Collectors were deployed before the database was installed, you will need to re-register the Collector appliances to send data to the new Database instead of the Hub. Please see our KB article on re-registering Collectors.

Capturing Metrics from the Environment

While the Stratusphere Hub serves as the central command center where all the data from your infrastructure can be reviewed, the data is coming from the Stratusphere Connector ID (CID) Keys that are distributed to all the devices you want to monitor in your environment. The Standard CID Key is a lightweight software agent that is responsible for gathering configuration information and collecting detailed performance data on user and application activity. The Advanced CID Key adds information on network packets to allow tracking of network latency, response times and bandwidth for individual users, machines and applications.

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

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

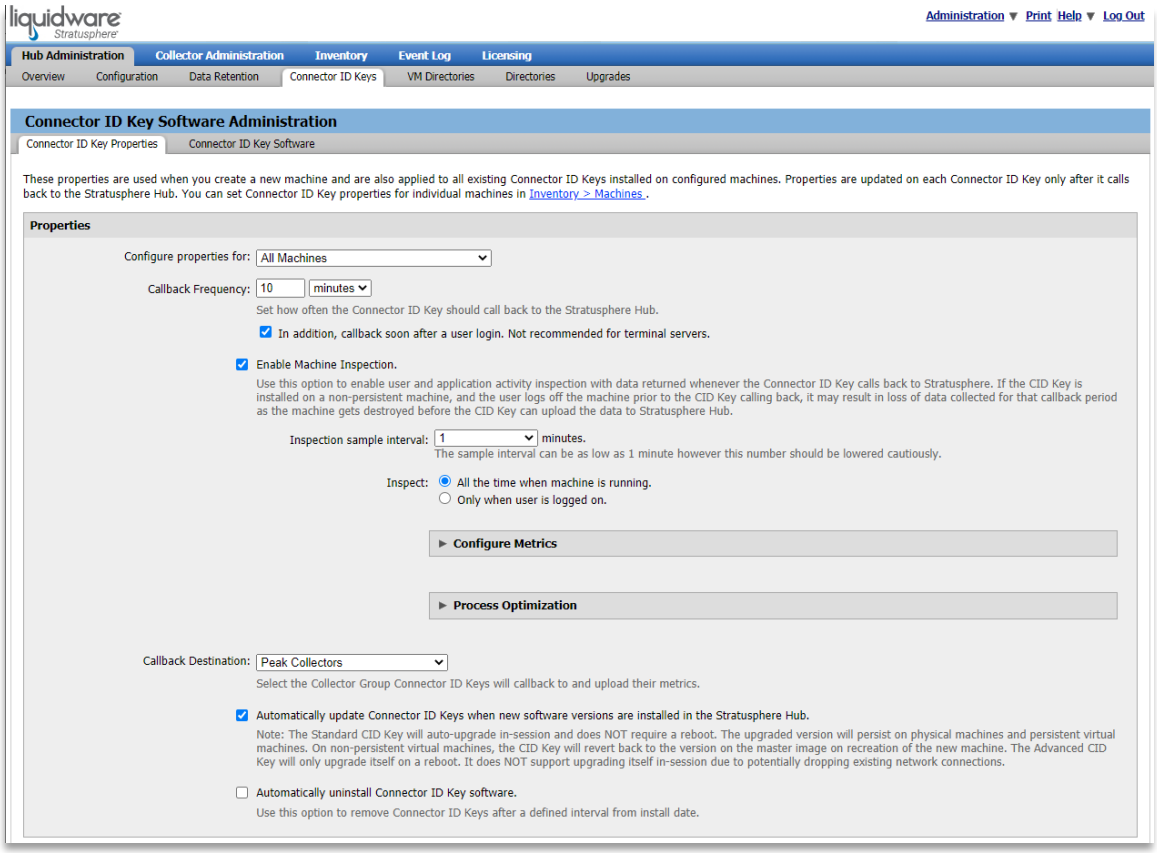
- **Machine configuration and age**—devices, CPU, memory, drives, and age
- **Application inventory**—versions and patch information for OS and used applications
- **User Logon Times and Duration**—the length of time to complete each user logon
- **User Types**—detect administrator privileges for individual users
- **Application Load Time**—the time it takes an application to fully initialize
- **User and Application Resource consumption**—CPU, memory, disk, network
- **Non-responding Applications**—detect when applications are not responding
- **Graphics Intensity of each application**—tracking the level of graphics for each process
- **Resource Utilization of each user, machine and application**
- **Performance Numbers of each user, machine, and application**
- **Login Process Breakdown information with details of events, processes, etc.**
- **Display protocol information for PCoIP, ICA, RDP, and VMware BLAST**
- **Browser Metrics for Google Chrome and Microsoft Internet Explorer**

The Connector ID Key is not designed to collect passwords or personal information. It also does not keep track of the files or documents accessed or opened.

Reviewing Data Collection Settings

The next step in the configuration process is to review your data collection settings. While logged in to the Hub Administration module, click on **Hub Administration > Connector ID Keys**. The first thing you will see is a set of **Connector ID Key Properties** that control the data collection functions. The suggested default settings are shown in the pictures below followed by a brief description of each setting.

Connector ID Key Properties



Configure Properties For:
Configure Connector ID Key settings for all machines in the environment or based on different machine groups.

Callback Frequency:
Specifies the frequency that the devices in your environment with Connector ID Key software agents will send collected data back to the Hub. Each callback to the Hub increases the network traffic by about 30K while storing the data takes up additional disk space. In environments where a single Hub is monitoring more than 500 desktops, you will want to be careful about setting the frequency too low to avoid network performance degradation. The **Callback Frequency** can be set as low as every 5 minutes; however, the default is once per hour. Please use our Stratusphere Sizing Guide for more specific recommendations.

In addition, callback soon after login. Not recommended for terminal servers.
The CID Key will send data to the Hub at each interval set by the **Callback Frequency**. If checked, this option allows the CID Key to make an extra call to the Hub shortly after a login rather than waiting the duration of

the **Callback Frequency** before the next callback occurs. Subsequent callbacks will be made using the **Callback Frequency** setting.

Enable Machine Inspection:
Indicates that configuration and usage data should be gathered from user desktops. If disabled, the CID Key will not collect any metrics from the machine but will continue calling back to Stratusphere Hub to check if its settings have changed.

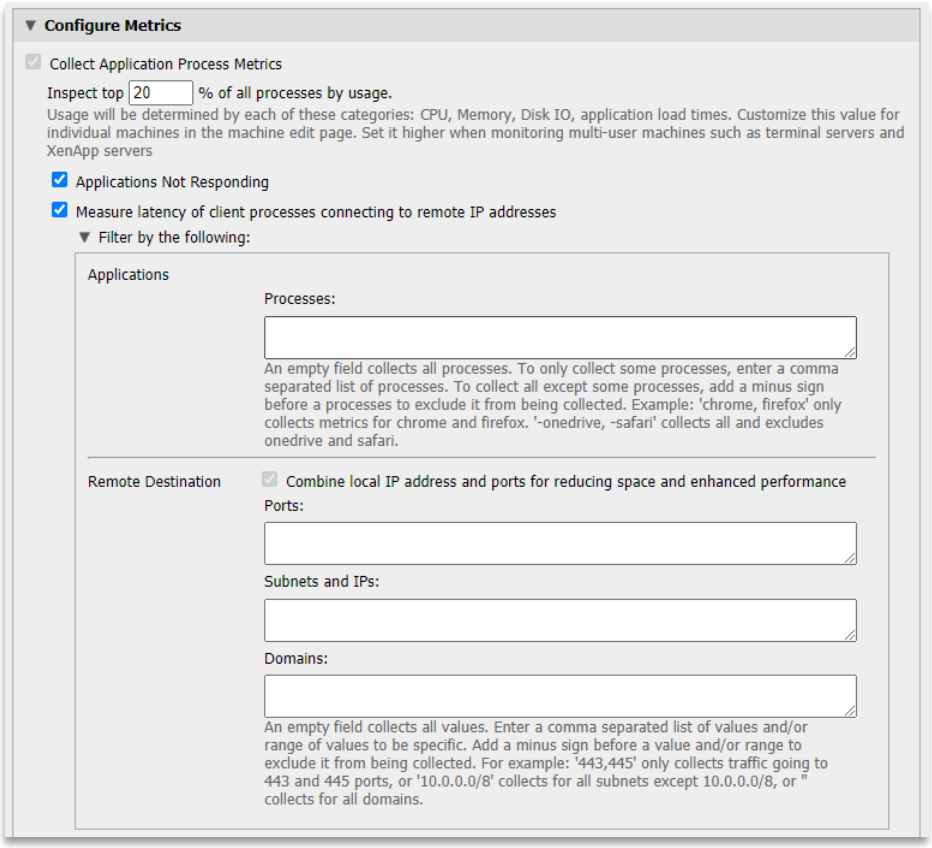
> **Inspection Sample Interval:**
> Specifies the frequency at which the Connector ID Key software gathers data on application and user activity and resource consumption on the user desktop. If the **Callback Frequency** is 15 minutes or less, then it is recommended that you set the sample interval to 1 or 2 minutes. If the **Callback Frequency** is greater than 15 minutes, then setting the sample interval to 5 minutes is recommended.
>
> **Inspect (All the time when machine is running or Only when user is logged on):**
> Specifies whether application activity should be inspected all the time if the machine is running, or only when a user is logged on. Selecting **Only when user is logged on** allows you to focus strictly on user activity.

Callback Destination:
Select the Collector Group that the CID Keys will callback to and report their metrics.

Automatically update Connector ID Keys when new software versions are installed in the Stratusphere Hub:
Any CID Key software updates will be included with future Hub software updates. If this option is checked, deployed CID Keys can auto-update themselves when the Hub is updated. Once updated, this new version will persist on physical and persistent virtual machines. However, when recreating a new machine image on non-persistent virtual machines, the CID Key software will revert to the version supplied on the master image. Automatic updates of the Standard CID Key do not require a reboot. However, the Advanced CID Key will only update upon reboot to ensure that existing network connections are not dropped.

Automatically uninstall Connector ID Key software:
For Connector ID Keys that are installed locally on user desktops, this setting allows you to specify the number of days after which the software agents on user desktops should dissolve or automatically remove themselves. This setting takes effect as soon as the CID Keys download their settings at the next callback interval. This setting is useful for Stratusphere FIT Assessments. For example, after finishing a three-week assessment with data collection, this setting can automatically remove CID Keys from the physical desktops that were part of the assessment.

Configure Metrics



Collect Application Process Metrics:

Application process metrics are collected by default, but the following settings are available:

Processes: Inspect top __% of all processes by usage:

By default, machine usage will be determined by each of these categories: CPU, Memory, Disk IO, and application load times. This cannot be changed at a system level for all CIDs. Customize this value for individual machines in the machine edit page. Set it higher when monitoring multi-user machines such as terminal servers and XenApp servers.

Applications Not Responding:

When enabled, the CID Key will detect when an Application goes into the Not Responding state. This feature does take additional resources on the target machine. So, if resources need to be conserved, this option could be disabled.

Measure latency of client processes connecting to remote IP addresses:

When enabled, the CID Key can measure latencies and jitter of each process communicating on the network to its remote destination IP Address. To elaborate a little on this feature, the CID Key collects per process network metrics. It collects information regarding source (local) and destination (remote) ports, IP Addresses, and reverse DNS addresses as well. It also collects information about the amount of data sent and received. To truly provide user experience we need to measure latency to the remote destination. To do so, the CID Key uses native operating system socket based APIs to measure the latency and jitter in milliseconds to the remote destination IP Address every sampling period.

By default, network data is collected on all processes, ports, subnets, IPs, and domains. However, you can reduce the amount of data Stratusphere collects by using the following fields to filter network stats. The filters can be setup to be used either as an inclusion list or an exclusion list.

Applications

Processes:

To collect data only on specific processes, enter all process names separated by commas. For example, 'chrome, firefox' only collects metrics for chrome and firefox. To collect data on all processes except for a few, add a minus sign in front of the process name to exclude it. For example, '-onedrive, -safari' collects metrics on all processes except for onedrive and safari. To collect all network data for all processes, leave this field blank.

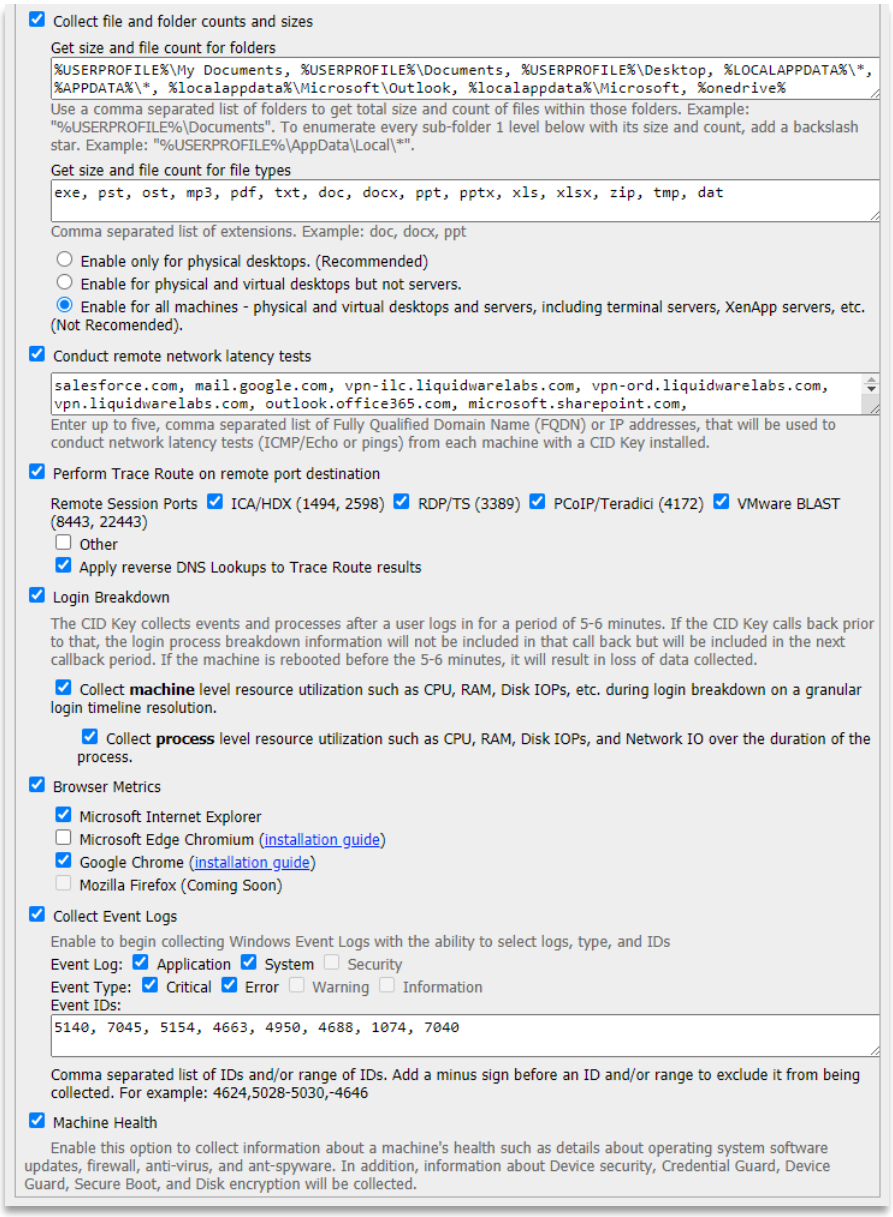
Remote Destination

Ports:

Subnets and IPs:

Domains:

To collect data only on specific values, enter all values and/or range of values separated by commas. For example, '443, 445' only collects traffic going to 443 and 445 ports. To collect data on all values except for a few, add a minus sign in front of the value to exclude it. For example, '-10.0.0.0/8' collects metrics for all subnets except 10.0.0.0/8. To collect all network data for all values, leave this field blank.



Collect file and folder counts and sizes:
When checked, the following settings are available:

Get size and file count for folders:

Get size and file count for file types:

Specifies which folders and document types on which the Connector ID Keys will gather data including the number of files and total file size for each folder or file type specified. Separate multiple folder names or file extensions with a comma. To get the number of files and total file size of any subfolders, add a backslash and star (*) to the folder name. To turn off folder statistics, leave this field empty.

This is used to determine the amount of disk space certain folders or file types are consuming on the hard disk. This data is very useful for capacity planning when trying to size the datastore during physical-to-virtual migrations using Stratusphere FIT.

For example, if you are planning to virtualize 50 desktops and you would like to know how much space is necessary on the datastore for storing the users' documents and profile, you will add the path to the profile and home directory in the **Get size and file count for folders** field.
If you further want to know within these two folders how many Word, Excel, PDF, and JPG files are there and their sizes, you will add these extensions to the **Get size and file count for file types** field.

If you leave these two settings empty, no data on size and counts will be collected. This feature scans the file system for file and folder content and does take up some CPU/RAM/Disk IOPs. If resources are needed to be conserved, then this feature can be disabled.

Here is an additional example of how to get subfolder information. For ProfileUnity migrations, it is important to understand what the sizes and file counts of each folder within the %USERPROFILE%\AppData\Local and %USERPROFILE%\AppData\Roaming folders. Using a backslash and star (*) and adding `%USERPROFILE%\AppData\*` to the **Get size and file count for folders** field will give you the information for each subfolder one level under the AppData folder.

Enable only for physical desktops. (Recommended)
Enable for physical and virtual desktops but not servers.
Enable for all machines – physical and virtual desktops and servers, including Terminal Servers, XenApp Servers, etc. (Not Recommended)
Determines which machine types will have file and folder information collected.

Conduct remote network latency tests:
If checked, enter up to 5 IP addresses, separated by commas, which will be used to perform network performance testing from each machine.

Perform Trace Route on remote port destinations:
The Stratusphere CID Keys can now be configured to automatically scan for the selected remote display sessions. To scan for any additional ports that are not part of the remote session ports, enable the "Other" check box, and add a comma separated list of remote destination ports for the CID Key to perform trace routes to. When enabled, if the CID Key observes a long running network connection to that remote port destination, it then runs trace routes to the destination IP address once every callback period. The CID Key keeps track of the number of visible hops, total number of hops, the latency of each hop, the IP address and DNS name of each hop as well. While the remote display session connection is still active, every sampling period, the CID Key also uses native operating system socket based API to measure the connection's latency and jitter to the destination IP address. These features require a CID Key to be installed on the remote client machine that initiates a connection to the destination machine using one of the selected protocols and port combination. NOTE: Due to standard network-based firewall rules, if the remote machine or network firewall is configured to not respond to the trace route requests, the CID Key will NOT be able to collect routes and will NOT be able to measure latencies nor calculate jitter.

Login Process Breakdown:
If checked the CID Keys will collect boot and login statistics that can be analyzed in the Advanced Inspectors **Login** tab. The feature allows a CID Key service to track all events and processes that are part of the user login process. It captures all the details of the login process, breaks it down into easy to understand steps, and provides details of all events, processes, errors, etc. that were encountered as part of the login process.

Collect machine level resource utilization
Collects resource utilization metrics such as CPU, RAM, Disk IOPs, etc. for each second during login. It provides a machine level overview of the resources used during logins.

Collect process level resource utilization
Collects resource utilization metrics such as CPU, RAM, Disk IOPs, and Network IO over the duration of the process. It provides the overall resources used over the entire duration of process during login and will help identify which process is consuming the most resources during login when allowing end users to compare machine and process level metrics during logins.

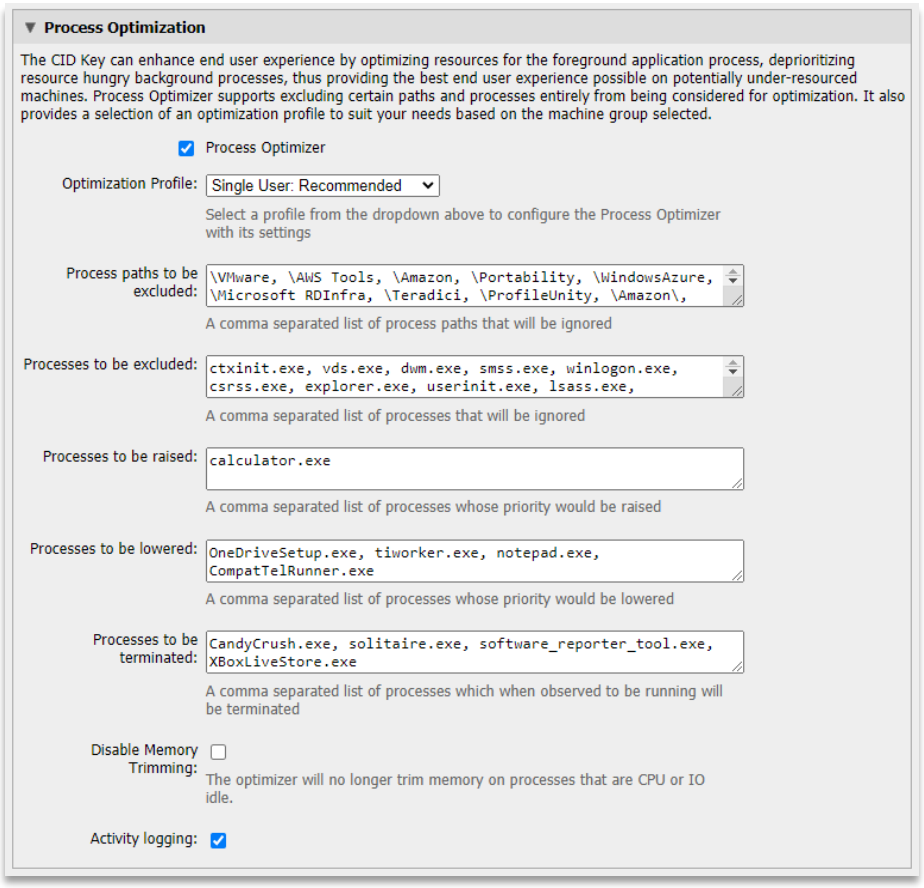
Browser Metrics:
If checked, choose which browser(s) should have stats collected. Choose from **Microsoft Internet Explorer, Microsoft Edge Chromium,** and **Google Chrome**. Support for Mozilla Firefox is coming soon. Note: Please see the **Capturing Browser Metrics from Desktops** section for additional instructions on collecting browser metrics from Google Chrome and Microsoft Edge Chromium.

Collect Event Logs:
If checked, choose whether to collect **Application**, **System** or **Security** Windows Event Logs. Choose from the following types of events: **Critical**, **Error**, **Warning**, and **Information**. You may specify certain event IDs to log or exclude from logging. To capture, type in a list of event IDs separated by commas. To exclude an event, type in the event ID preceded by a minus sign. Please note that event logs will take up a significant amount of space in the database if all logs and all event types are collected. This will also result in a significant increase in the amount of data uploaded to Stratusphere, increasing the upload bandwidth usage. To reduce the impact in your environment, customize the settings to enable only what you need.

Machine Health
When checked, this option collects information about a machine's health such as details about operating system software updates, firewall, anti-virus, and ant-spyware. In addition, information about Device security, Credential Guard, Device Guard, Secure Boot, and Disk encryption will be collected. This information is collected on startup of the CID Key and then on each login thereafter. This information is not updated with each CID Key callback.

Process Optimization

Enable Process Optimizer to allow the CID Key to enhance the end user experience by optimizing & boosting resources for the foreground application process and deprioritizing useless resource hungry background processes. This is especially useful on older or under-resourced machines.



Optimization Profile:
Select the optimization profile to best fit your needs. These profiles are optimized for Single User and Multi-user machines. Please make sure you select the appropriate profile for your machines you are configuring these properties for.

Process paths to be excluded:
Enter the list of paths, separated by a comma, that the process optimizer should ignore.

Processes to be excluded:
Enter the list of processes, separated by a comma, that the process optimizer should ignore.

Processes to be raised:
Enter the list of processes, separated by a comma, whose priority would be raised by the process optimizer.

Processes to be lowered:
Enter the list of processes, separated by a comma, whose priority would be lowered by the process optimizer.

Processes to be terminated:
Enter the list of processes, separated by a comma, that the process optimizer should terminate if or when they are observed to be running.

Disable Memory Trimming:
Memory trimming is enabled by default. Check this box to disable memory trimming processes that are CPU or IO idle.

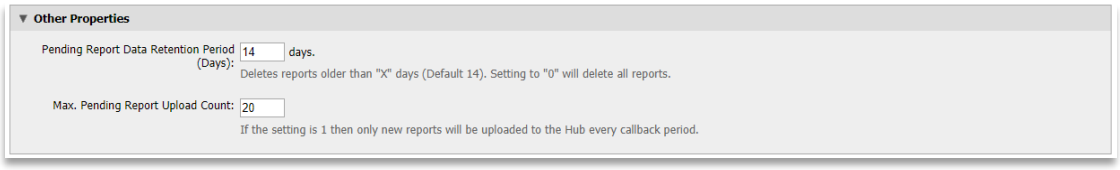
Activity logging:
The CID Key will log all optimizations made to any process by tracking the number of times it was raised, lowered, gained foreground focus, and terminated including how many times it trimmed memory. This information will then be visible within the **Advanced > Inspectors > Applications** and **Process Names** tabs under the **Summary | Optimizer Actions** Inspector View.

Properties that only apply to LEGACY versions

Enable Connector ID for TCP connections:
For Advanced versions of the CID Key software, this setting allows more accurate tracking of the network latency between the user desktop and the Hub during the assessment. The recommendation is to leave this checked.

Restrict To:
The Advanced CID Key embeds the identities of the user and machine that initiated the network connection into each network connection packet. Sometimes, these packets are not accepted by certain servers in some organizations. To ensure that the identities are embedded only within the user's organization, a network subnet or CIDR can be specified so that the CID Key will only embed the identities if the packet is being sent to IP addresses within the organizational CIDR or subnet and would leave packets that are leaving the organization subnet or CIDR as is.

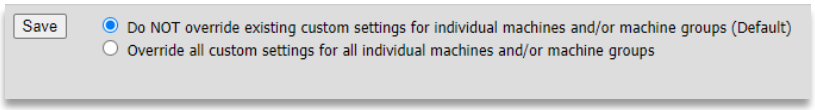
Other Properties



Pending Report Data Retention Period (Days):
Deletes reports older than the set number of days. The default is 14 days. Changing the setting to "0" will delete all reports.

Max. Pending Report Upload Count:
If the setting is 1 then only the latest call back period report will be uploaded to the Hub every callback period. If the count is set to 5, and the machine has pending reports then the CID Key will upload the current call back period report (1) and 4 pending reports starting with the latest pending reports first.

Save Options

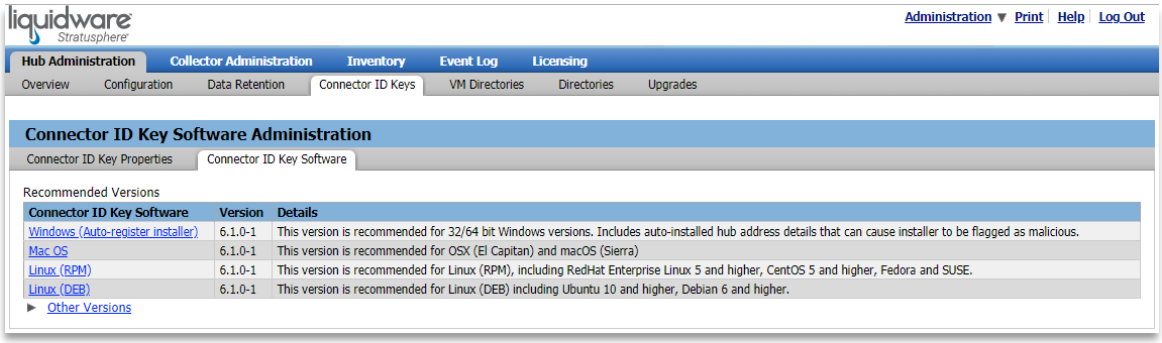


Do NOT override existing custom settings for individual machines and/or machine groups (default):
Select this option to just apply property changes to newly deployed CID Keys. This will not change the properties for CID Keys on existing devices.

Override all custom settings for all individual machines and/or machine groups:
Apply property changes to all deployed CID Keys.

Distributing 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. The Connector ID Agents will collect the information you specify for those devices and report the metrics back to the Stratusphere Hub periodically. You can find the software in the Hub Administration module by proceeding to **Hub Administration > Connector ID Keys** and clicking on the **Connector ID Key Software** tab. Recommended CID Key installers can be used interactively and distributed directly to your target desktops.



The recommended Standard Connector ID (CID) Keys have a small footprint (less than 10 MB) and run invisibly with minimal performance impact on end user desktops. By default, when using the Windows Standard version CID, the key will be installed in a folder named **Liquidware Labs\Connector ID** within the Program Files folder. The Windows Standard installer has information that allows it to call back to a Stratusphere Hub and register automatically. The CID Key will communicate securely with the Stratusphere Hub over TCP and UDP on port 443. Legacy versions of Stratusphere (versions 5.x and earlier) use port 5501 for communication between the CID Key and the Stratusphere Hub.

Note that while the CID Key agent is installed locally on machines (physical/virtual desktops/servers), these machines can be used remotely or be offline as long as there are certain times (including during the initial installation of the CID Key agent) when the machines are connected to the network and can reach the IP address (or DNS) of the Stratusphere Hub. Data collection will continue at the specified **Inspection sample interval** while the machines are offline. The next time the machine is connected to the network, the stored information can be sent to the Hub. Up to two weeks of information can be stored locally. If a machine is offline more than two weeks, only the latest two weeks of data will be kept. Older data will be deleted.

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-x_x_x-winStandard.exe /q
[HUBADDRESS="hub-ip-or-dns-name"] [MACHINEGROUP="machine-group-
name"] [USERGROUP="user-group-name"]
```

In the command above, "**x_x_x**" should be replaced with the version number of the CID Key you are installing. Other parameters within the […] are optional. The actual characters such as [and] are not to be used in the command and are provided merely for representational purposes. If using optional parameters,

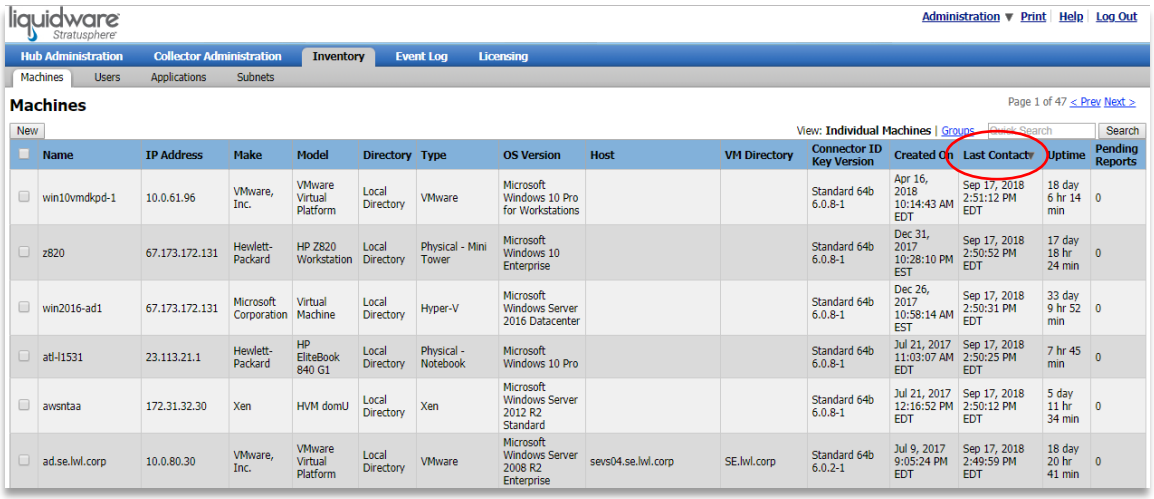
the quotes are required and the variables inside the quotes should be replaced with values specific to your environment.

> ***Please do NOT extract the MSI from the Windows Standard Version EXE. This will prevent the CID Key from calling back to the Stratusphere Hub.***

If you need to push out CID Keys using Active Directory Group Policy, you can also download the AD GPO version of the installer which is an MSI file along with the Group Policy template that can be used for software installation. More detailed instructions for deploying CID Keys using AD GPO or SMS can be found in **Appendix A** of this document.

If you are interested in using the 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. Please note that the Windows Advanced CID Key development has been paused.

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, check the following:

1. Review your installation steps.
2. Make sure the machine is connected to network for registration.
3. Ensure your machine can reach the Hub using TCP and UDP on port 443. For legacy versions of Stratusphere (versions 5.x and earlier), use TCP and UDP on port 5501.

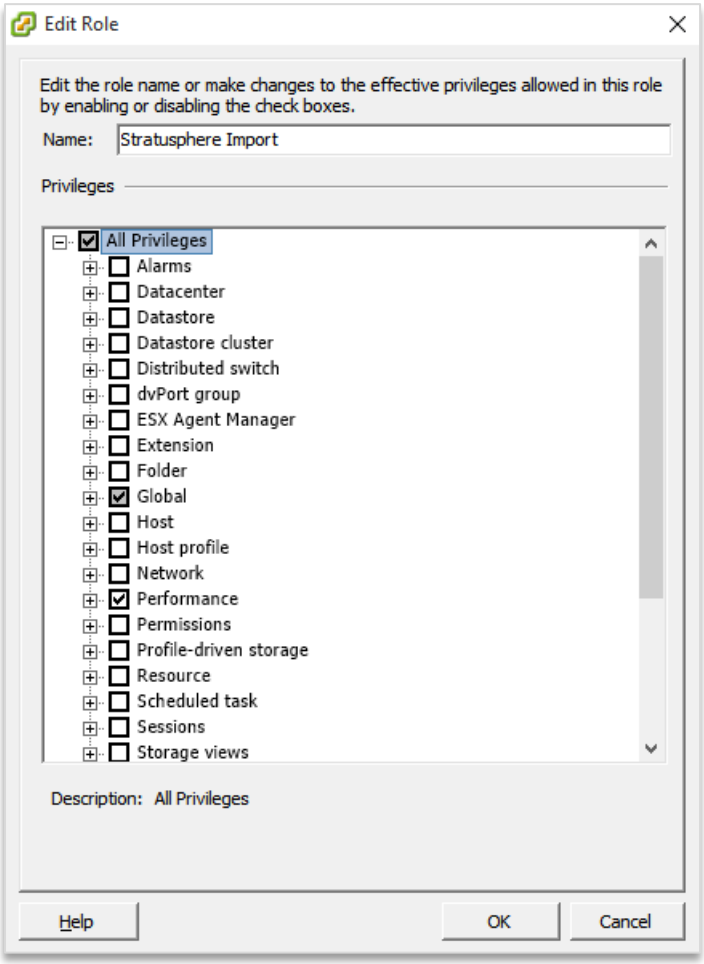
If you are still having trouble, please visit the Liquidware Customer Support Portal to log a support request.

Integrating with vCenter for Host Statistics (Optional)

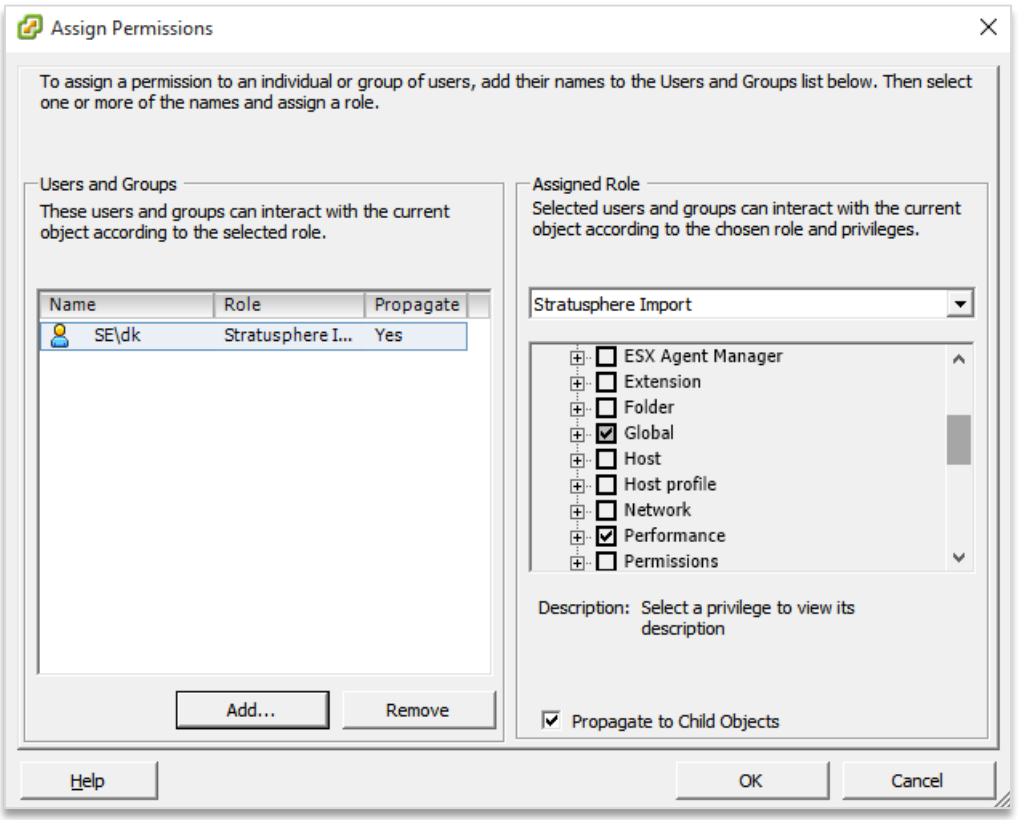
If you are using Stratusphere inside a VMware virtual environment, you can connect the Stratusphere Hub to your VMware vCenter Server (or multiple vCenter Servers) to import performance statistics on the virtual hosts, such as CPU Ready and Memory Swap Rate statistics. This capability is currently only available for VMware vCenter Server, however future versions will support XenServer and XenCenter as well.

Stratusphere needs a user account with a minimum level set of permissions to import vCenter performance statistics. Admins can use an existing user account with these permissions or create a user account reserved specifically for this purpose. To configure the user account settings:

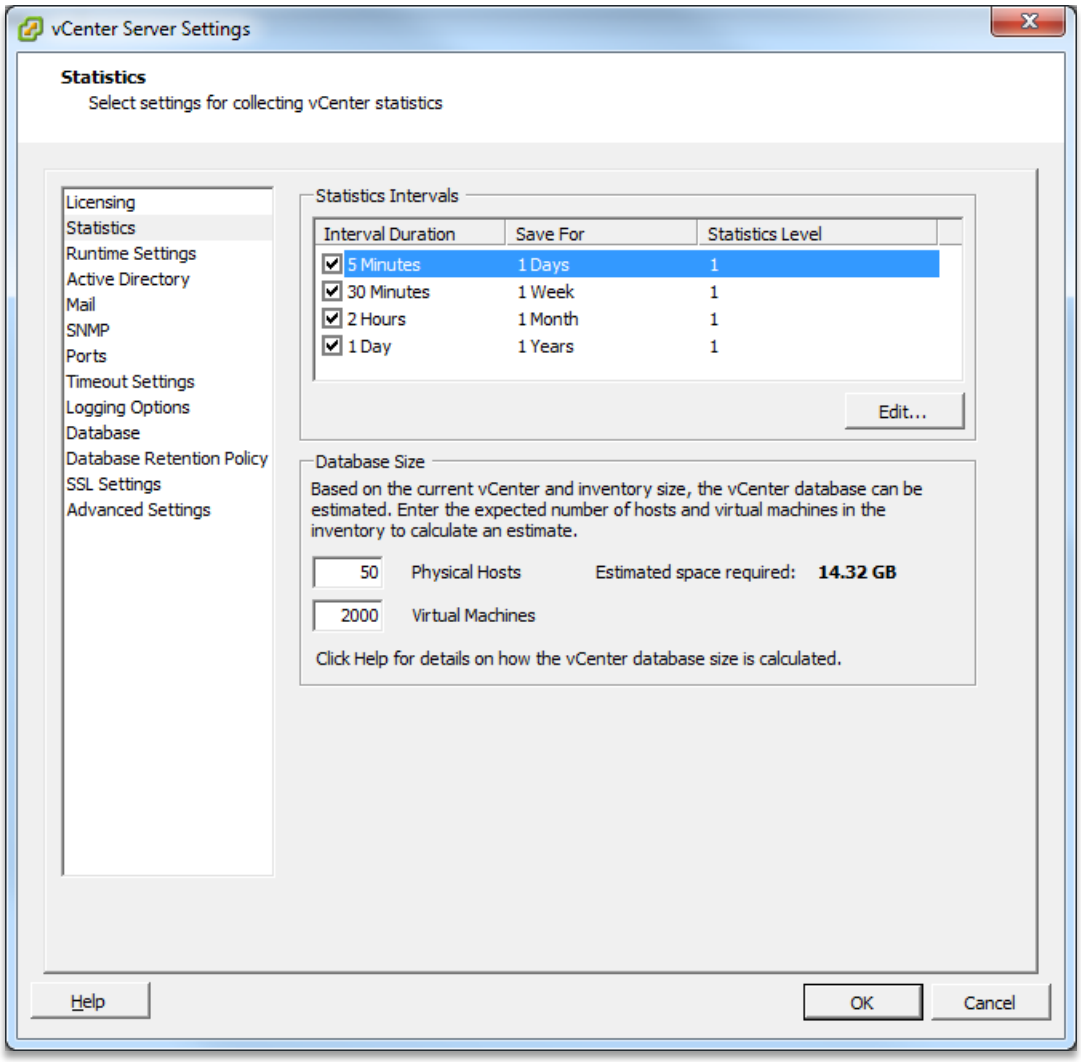
1. Create a user account “stratusphere” in Active Directory or the local vCenter Server.
2. Create a new Role:
    a. In vCenter, from the top-level menu options, select and navigate to **View > Administration > Roles**.
    b. Click **Add Role** and name it “Stratusphere Import”.
    c. Enable the following privileges:
        i. Global > Diagnostics
        ii. Global > Health
        iii. Performance > Modify intervals
    d. Click **OK**.



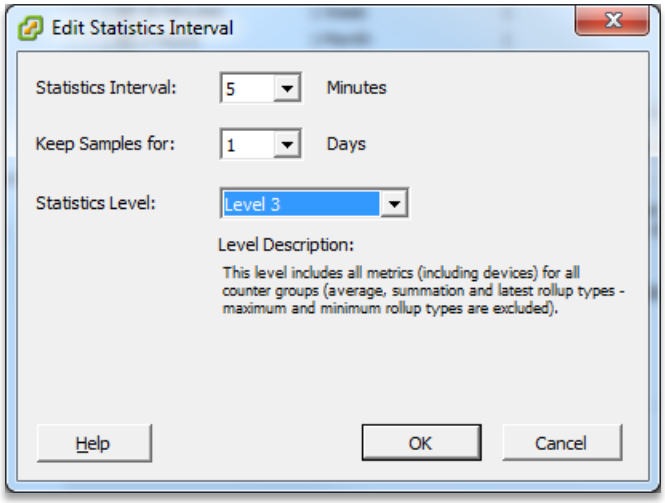
3. In vCenter, navigate to **Home > Inventory > Hosts and Clusters**.
    a. On the left tree, select the top level vCenter or the cluster you want to import within Stratusphere.
    b. On the right pane, select the **Permission** tab.
    c. Right-click and select **Add Permissions** option.
    d. Under the Users and Groups section on the left, click on the **Add** button to select the appropriate user account from the local vCenter Server or Active Directory.
    e. Under the Assigned Role section on the right, select the 'Stratusphere Import' option from the drop down.
    f. Click **OK**.



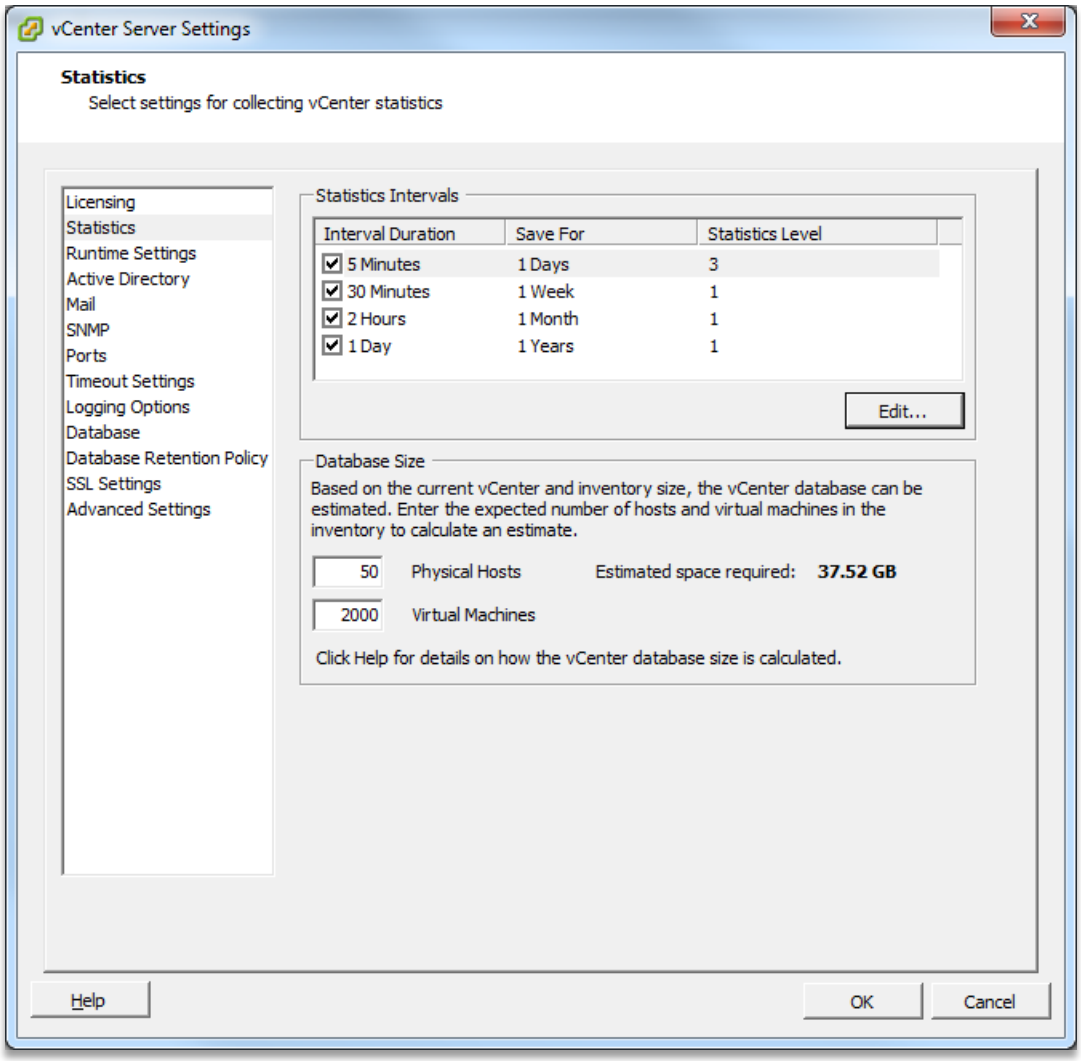
4. In the Stratusphere Web UI, you can now use this user account to import inventory and stats from vCenter.
5. The Stratusphere Hub imports detailed stats from vCenter. To configure these settings within your vCenter Client, navigate to **Administration > vCenter Server Settings** menu option. Select **Statistics** from the left-hand menu options. Then select the **5-minute** statistics interval from the list and click on the **Edit** button.



6. Change the Statistics Level to **Level 3**. Click **OK**.

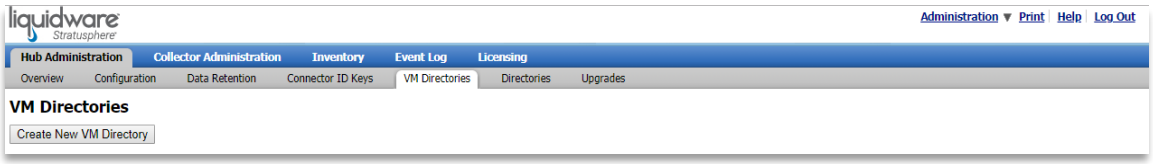


7. Verify the change was accepted and click **OK** again.

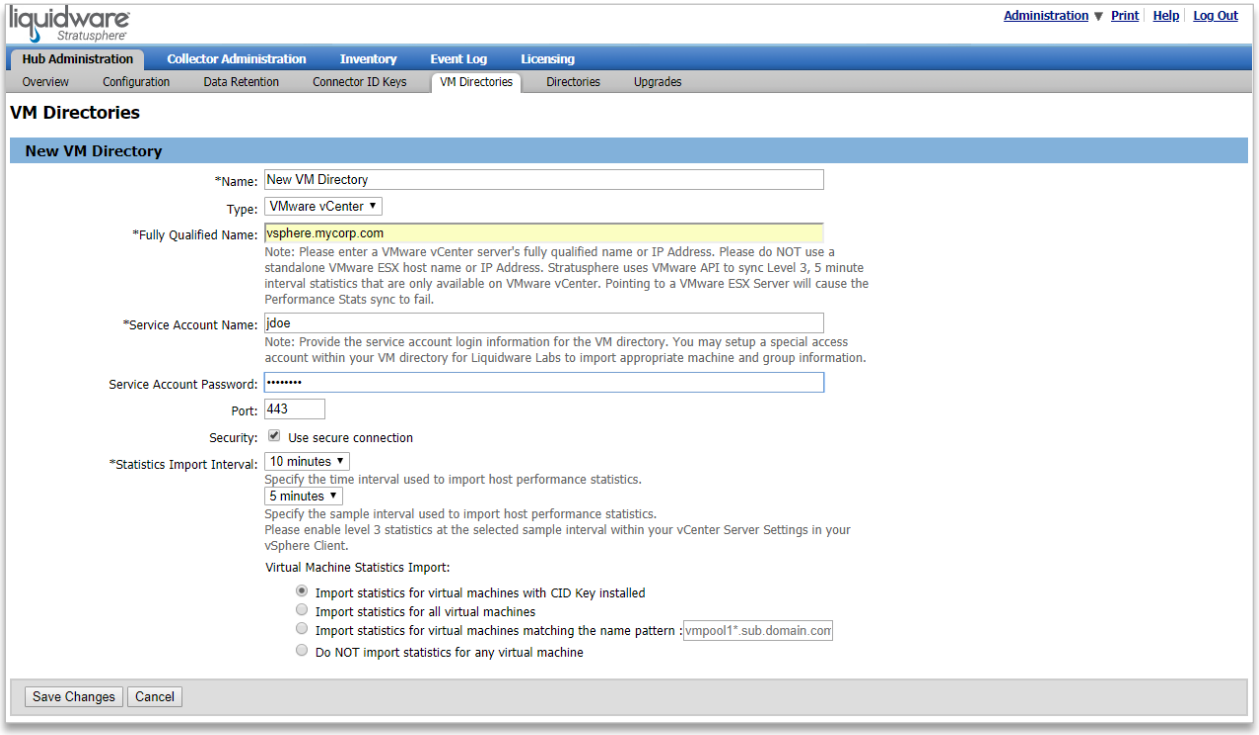


To configure the vCenter connection with the Stratusphere Hub:

1. Login to the Administration section of your Stratusphere Hub using an account with the proper permissions to import vCenter stats.
2. Go to **Hub Administration > VM Directories**.
3. Click on the **Create New VM Directory** button.



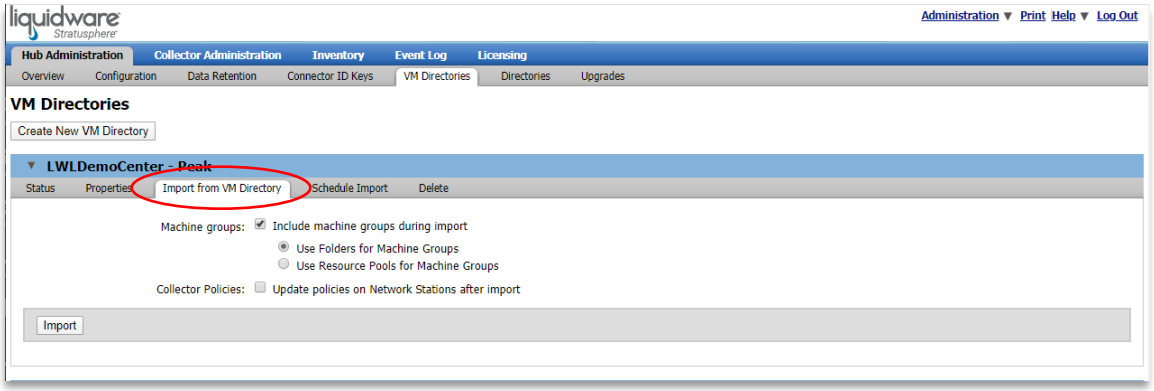
4. Specify the connection information.



Note: Please enter a VMware vCenter Server's fully qualified name or IP address. Please do NOT use a standalone VMware ESX host name or IP address. Stratusphere uses the VMware API to sync Level 3, 5-minute interval statistics that are only available on VMware vCenter. Pointing to a VMware ESX Server will cause the Performance Stats sync to fail.

5. Select the interval to import performance stats and choose which stats to import before clicking **Save Changes**. The **Virtual Machine Statistics Import** options allow you to save resources by importing statistics for only the virtual machines you need. Previously, all metrics were imported for all virtual machines. Therefore, for all upgraded installations of Stratusphere, **Import statistics for all virtual machines will be set as the default** to follow the prior operation. Starting with version 5.8.1, the default for new Stratusphere installations is **Import statistics for virtual machines with CID Key installed**. You may edit this setting at any time from the **Properties** tab of the chosen VM Directory.

6. To allow Stratusphere to initialize the information for your hosts, you also need to do an Import. Switch to the **Import from VM Directory** tab and click the **Import** button. Stratusphere will import the Host definitions and the information about the VMs assigned to each virtual host.



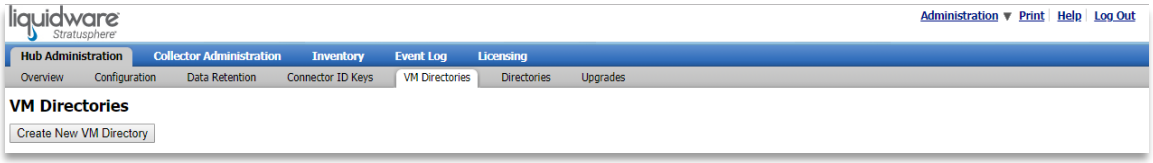
7. If you have more than one vCenter connection to configure, go back to Step #3 and repeat these instructions for each vCenter Server.

Integrating with Nutanix Prism for Host Statistics (Optional)

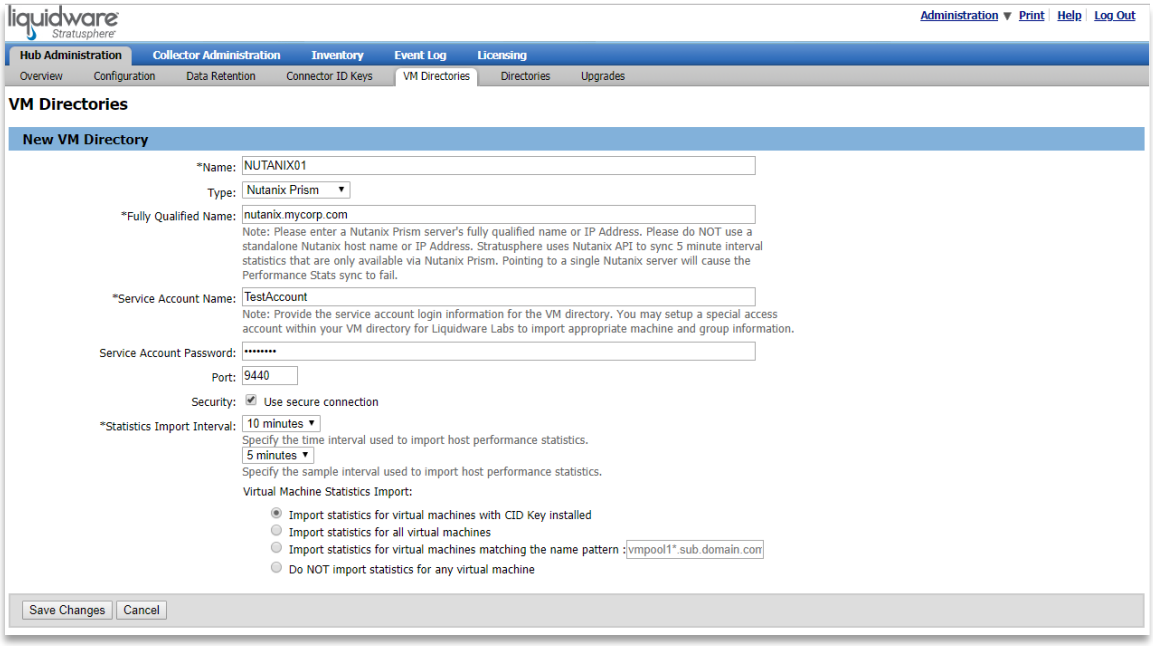
If you are using Stratusphere inside a Nutanix Acropolis virtual environment, you can connect the Stratusphere Hub to your Nutanix Prism Server (or multiple Prism Servers) to import performance statistics on the virtual hosts, such as CPU and Memory statistics.

Stratusphere needs an account with a minimum level set of permissions to import Prism-based performance statistics. Admins can use an existing account or create a user account reserved specifically for this purpose. Here is how to configure the Stratusphere Hub to connect to Nutanix Prism:

1. Log into the Stratusphere Web UI **Administration** product using your administrator credentials.
2. Navigate to the **Hub Administration > VM Directories** tab.
3. Click on the **Create New VM Directory** button to get started.



4. Specify connection information to connect to Nutanix Prism.



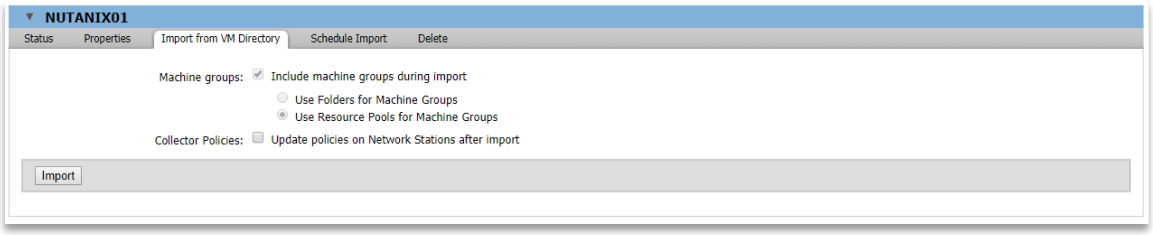
   a. **Name**: Enter a short easy name for the Name of the VM Directory.
   b. **Type**: Select ***Nutanix Prism*** from the drop down.
   c. **Fully Qualified Name**: Enter the Nutanix Prism machine's fully qualified host name or IP address.
   d. **Service Account Name/Password**: Use your existing account credentials or enter credentials created specifically for Stratusphere into the Service Account Name and Service Account Password fields.
   e. **Port**: The Port field defaults to *9440* since Nutanix Prism listens to that port by default. Please modify it if you have customized it to listen on a different port.
   f. **Security**: Leave the Security checkbox enabled.

g. **Statistics Import Interval**: Select the Statistics Import Interval that you want the Stratusphere Hub to connect to Prism and import statistics. Then select the sample interval to query Prism for statistics – values between 1 and 5 minutes are available.

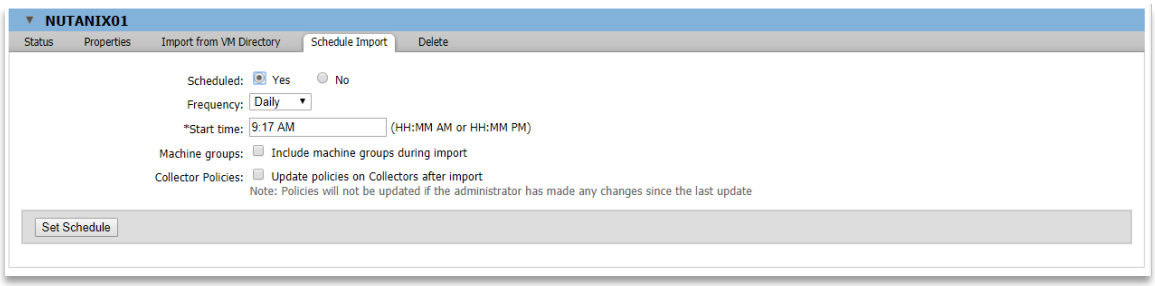
h. **Virtual Machine Statistics Import:** This option allows you to specify importing statistics for all virtual machines, only the ones with a CID Key installed, only the ones that match a specific naming pattern, or none.

i. Click **Save Changes** to complete the configuration.

5. To allow Stratusphere to initialize the information for your hosts, you also need to do an Import. Switch to the **Import from VM Directory** tab and click the **Import** button. Once clicked, Stratusphere will import the Host definitions and the information about the VMs assigned to each virtual host and display its progress. Check the Event Log tab for any details of any errors that may be encountered.



6. To allow Stratusphere to import inventory & statistics from Nutanix Prism on an ongoing, automated basis, you need to schedule an import. Navigate to the **Schedule Import** tab under the newly created Nutanix Prism VM Directory.



a. **Scheduled**: Select Yes.

b. **Frequency**: Pick the frequency to import inventory from Prism. Options are Daily, Weekly, Monthly.

c. **Start Time**: Pick a time to initiate the import.

d. Click on **Set Schedule** to save and set the schedule. Repeat steps for each Prism machine.

Capturing Browser Metrics from Desktops

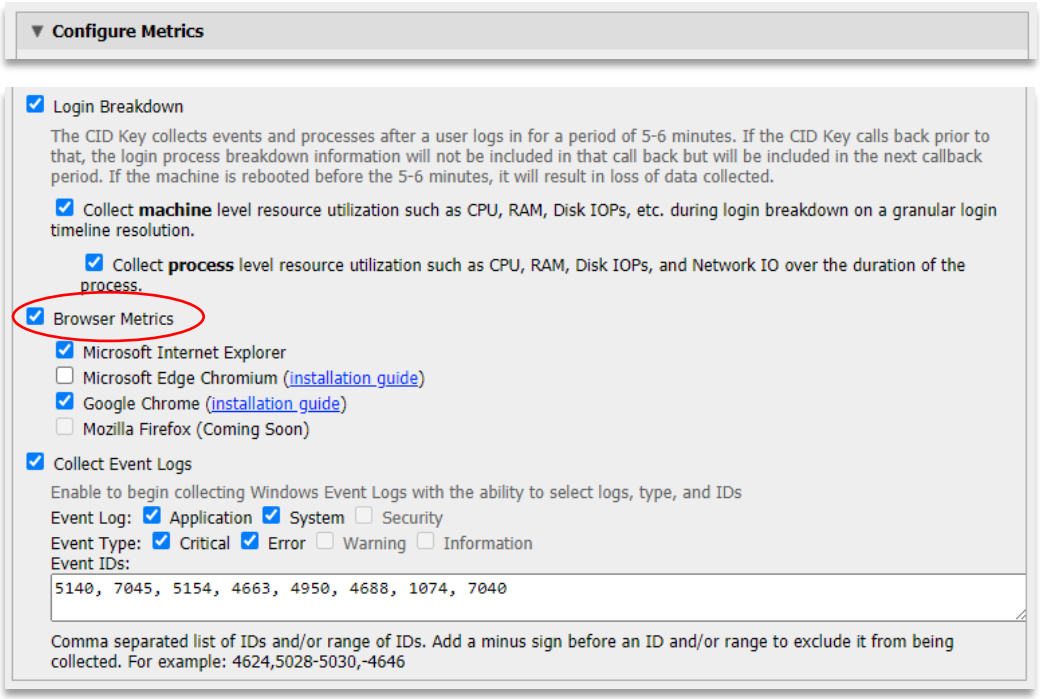
Starting with version 5.7, Stratusphere's Advanced Inspectors now include browser-level metrics that provide visibility into your internet traffic. Stratusphere tracks metrics including domain/URL, page-level details, and date and time of activity to give a clearer picture of peaks in internet traffic and usage of cloud applications.

Currently, Stratusphere collects metrics from Microsoft Internet Explorer (versions 9.x and higher) and two Chrome (versions 35 and higher) based browsers – Google Chrome and Microsoft Edge Chromium. Support for additional browsers is planned for future releases.

The Liquidware Chrome extension can be used in both Google Chrome and Microsoft Edge Chromium. With older versions of Stratusphere, all Chrome-related browser activity will display as "Chrome". Starting in Stratusphere 6.1.5, stats are differentiated so that browser activity using Google Chrome is labeled as "Chrome" and browser activity using Edge Chromium is labeled as "Edge". View your browser statistics in the Advanced Inspectors **Browser** tab.

Configuring the CID Key to Collect Browser Metrics

1. Make sure that the Connector ID Key has already been installed on the machine you are monitoring. If you have not already done so, download a CID Key installer from the Stratusphere Hub. Install it on a machine that has either Chrome or Internet Explorer installed. Refer to the section on **Capturing Metrics from the Environment** for additional information on installing the CID Key.
2. Login to the Hub Administration module and go to the **Hub Administration > Connector ID Keys > Connector ID Key Properties** tab and expand the **Configure Metrics** section.



3. Check the **Browser Metrics** checkbox. Then select which browser information to collect.
4. Click **Save** to change the settings.

Browser Metrics for Chrome-based Browsers

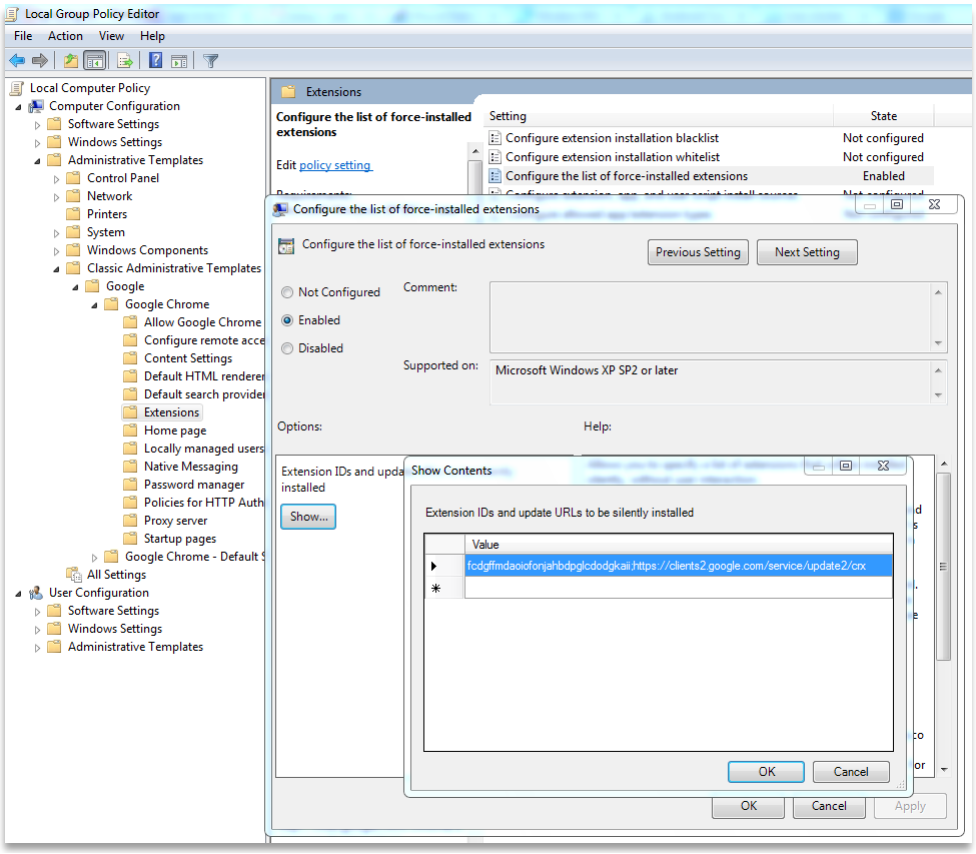
Liquidware has developed a Chrome Extension that is available within the Chrome Web Store to be installed within the Chrome-based browsers. This extension works in conjunction with the CID Key installed on the machine and collects detailed metrics which are then packaged and uploaded by the CID Key up to the Stratusphere Database. The same Chrome extension works on Google Chrome and Microsoft Edge Chromium.

Enabling Browser Metrics in Google Chrome

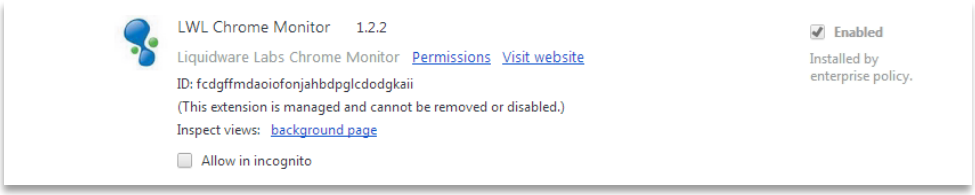
Collecting browser metrics requires a few more steps, including configuring some GPO settings and installing the Liquidware Chrome Extension in Google Chrome. In addition to the above steps, please follow these steps to capture Chrome metrics:

1. Download and unzip the following policy templates zip file:
   http://download.liquidwarelabs.com/stratusphere/tools/policy_templates.zip
2. Set Local Group Policy.
   a. Open **`gpedit.msc`** and navigate to **Computer Configuration > Administrative Templates**.
   b. Right click on **Administrative Templates** on the left tree view and click on **Add/Remove templates** option.
   c. On the new window, click the **Add** button. Browse to where you unzipped the ZIP file and select **`windows/adm/en-US/chrome.adm`**.
   d. Go to **Computer Configuration > Administrative Templates > Classic Administrative Templates > Google > Google Chrome > Extension,** and double click on **Configure the list of force-installed extensions**. Then check on **Enable** and click the **Show** button.
   e. Copy the following string in red and paste it into first row. Save it and exit out of the Local Group Policy editor.
      `fcdgffmdaoiofonjahbdpglcdodgkaii;https://clients2.google.com/service/update2/crx`

f. Here is a screen shot of all the combined screens you can expect to see:



3. Launch Google Chrome.
   a. In the address bar navigate to **`chrome://extensions/`** to verify if our extension **LWL Chrome Monitor** is listed there. To verify here is your screen shot:



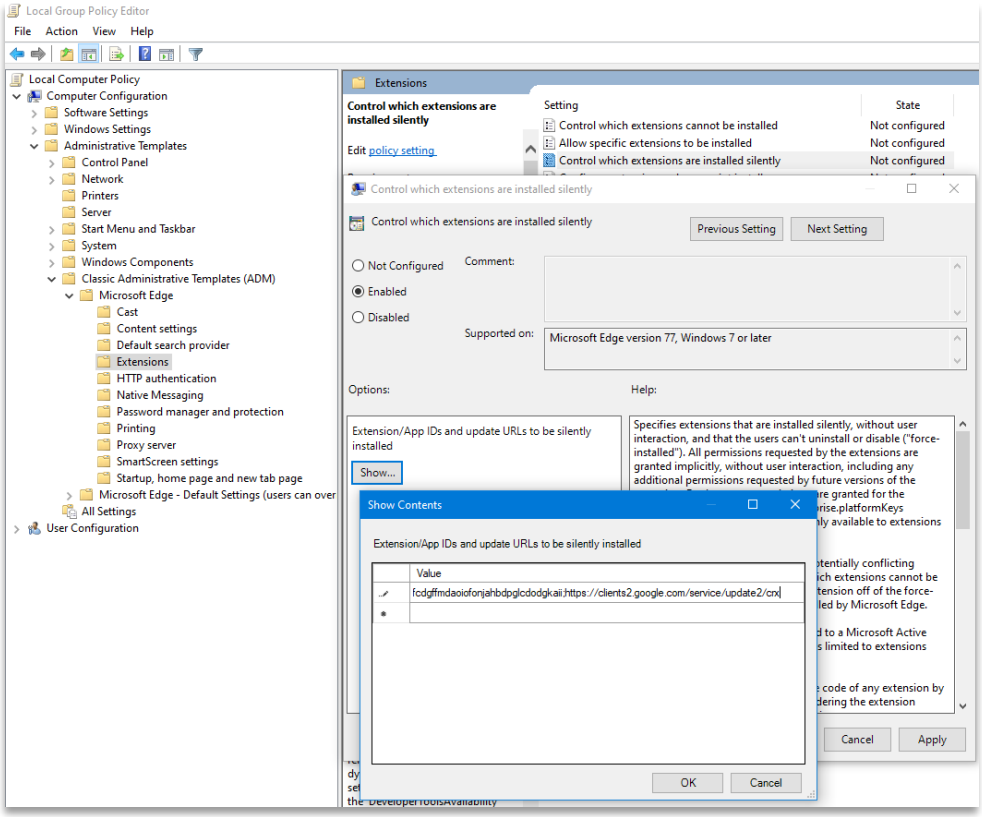
   b. To verify if you are collecting Browser Stats, look out for a **`stats.txt`** file in the **Connector ID** folder. Please note that it may take up to 5 minutes for this file to show up. Double Click it and search for **'browserStats'**. If you find a hit, we are collecting Chrome stats. If you do not find a hit, please contact Liquidware Support.

Enabling Browser Metrics in Microsoft Edge Chromium

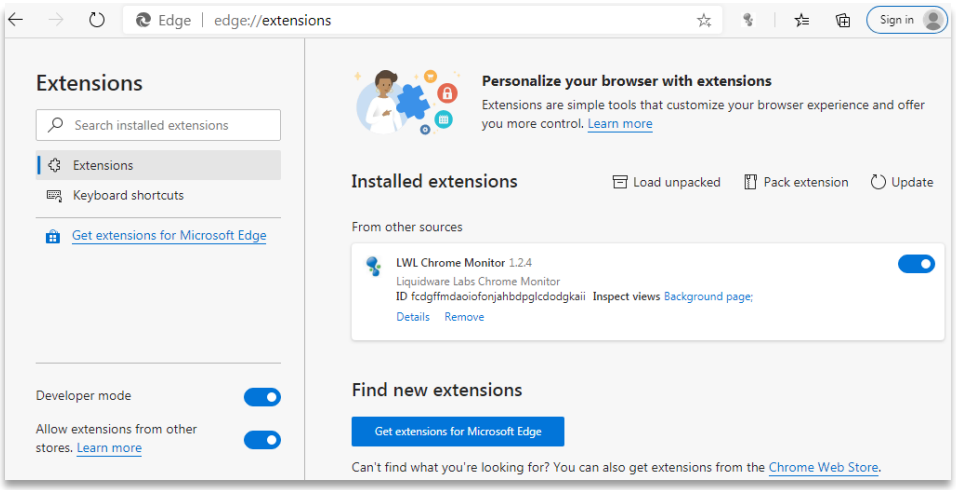
Collecting browser metrics requires a few more steps, including configuring some GPO settings and installing the Liquidware Chrome Extension in Microsoft Edge Chromium. In addition to the steps in the subsection above, please follow these steps to capture Chrome metrics:

1. Download and unzip the following policy templates zip file:
   http://download.liquidwarelabs.com/stratusphere/tools/MSEdgeTemplates.zip

2. Set Local Group Policy.
    a. Open **`gpedit.msc`** and navigate to **Computer Configuration > Administrative Templates**.
    b. Right click on **Administrative Templates** on the left tree view and click on **Add/Remove templates** option.
    c. On the new window, click the **Add** button. Browse to where you unzipped the ZIP file and select **`windows/adm/en-US/msedge.adm`**.
    d. Go to **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Microsoft Edge > Extensions,** and double click on **Control which extensions are installed silently**. Then check on **Enable** and click the **Show** button.
    e. Copy the following string in red and paste it into first row. Save it and exit out of the Local Group Policy editor.
    `fcdgffmdaoiofonjahbdpglcdodgkaii;https://clients2.google.com/service/update2/crx`
    f. Here is a screen shot of all the combined screens you can expect to see:



3. Launch Microsoft Edge Chromium.
    a. In the address bar navigate to **`edge://extensions`** to verify if our extension **LWL Chrome Monitor** is listed there. To verify here is your screen shot:

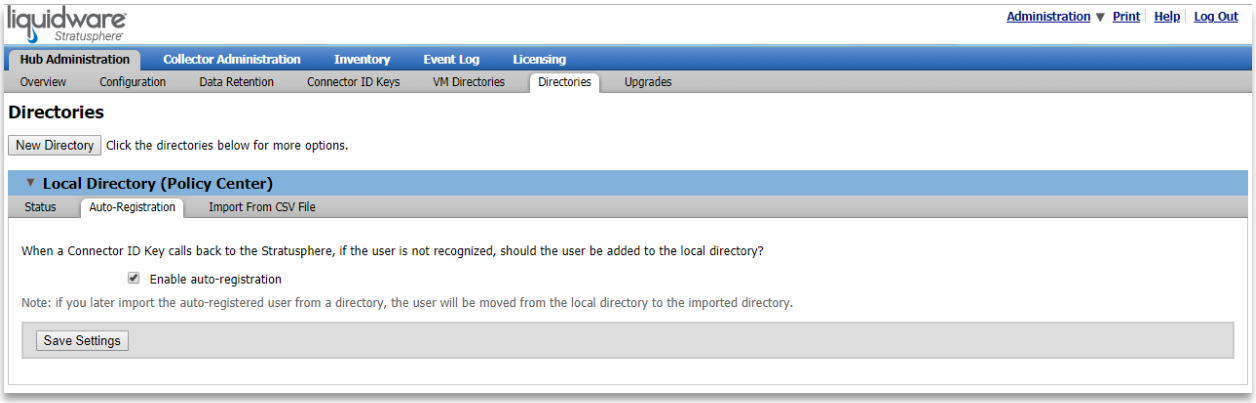


    b. To verify if you are collecting Browser Stats, look out for a **`stats.txt`** file in the **Connector ID** folder. Please note that it may take up to 5 minutes (Default sampling frequency) for this file to show up. Double Click it and search for **'browserStats'**. If you find a hit, we are collecting Chrome stats. If you do not find a hit, please contact Liquidware Support.

Hub Administration Directories

Under **Hub Administration > Directories**, you can manage the Local Directory that is used for Stratusphere user accounts, and you can integrate with Active Directory or LDAP directory servers. For the Local Directory, you can import users from a CSV file by going to the import tab.

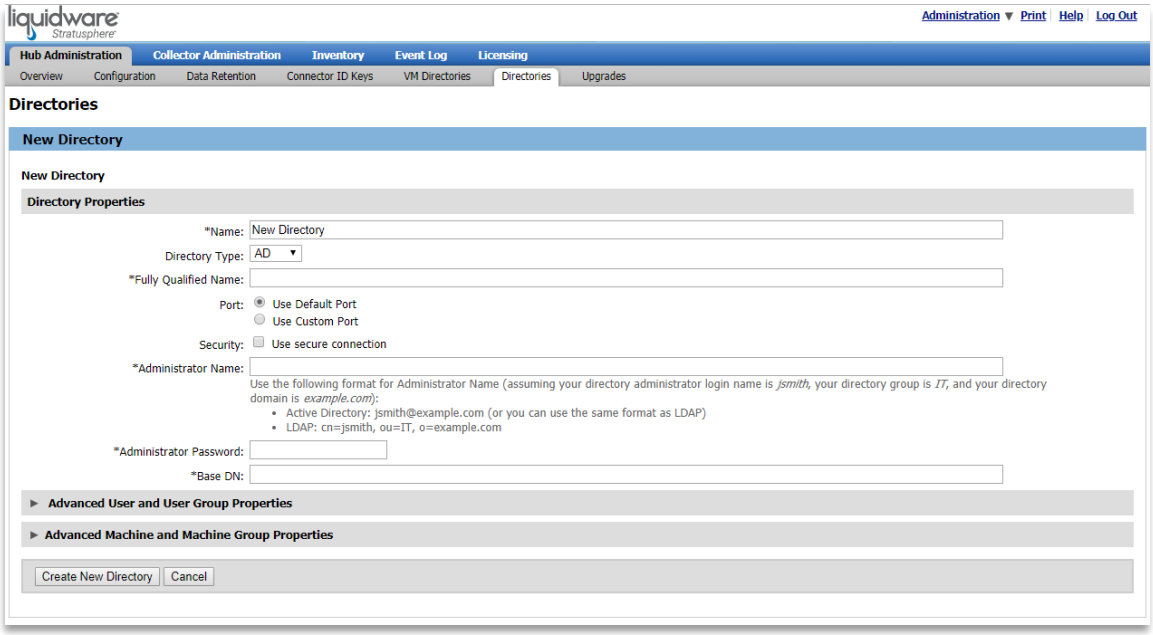
You can also choose whether auto-registration is enabled. When this is enabled, as Connector ID Keys detect logged on users, the users will automatically be registered and tracked in Stratusphere. It is recommended that you leave this setting on.



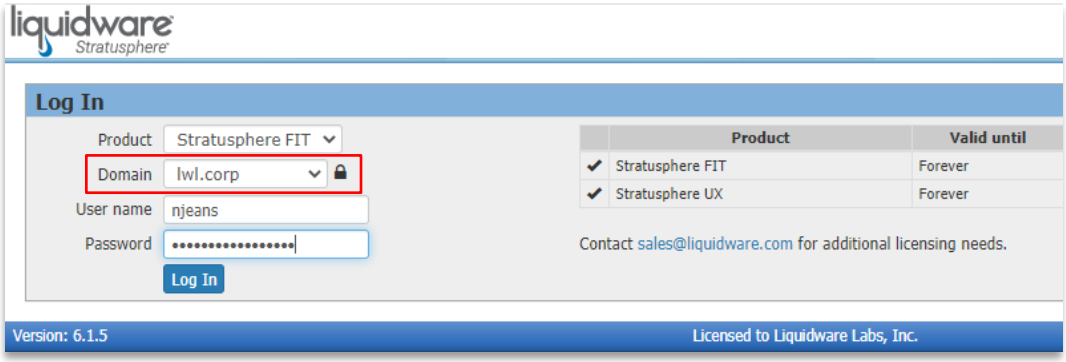
To setup integration with Active Directory or LDAP:

1. Go to the **Hub Administration > Directories** tab and click on the **New Directory** button.

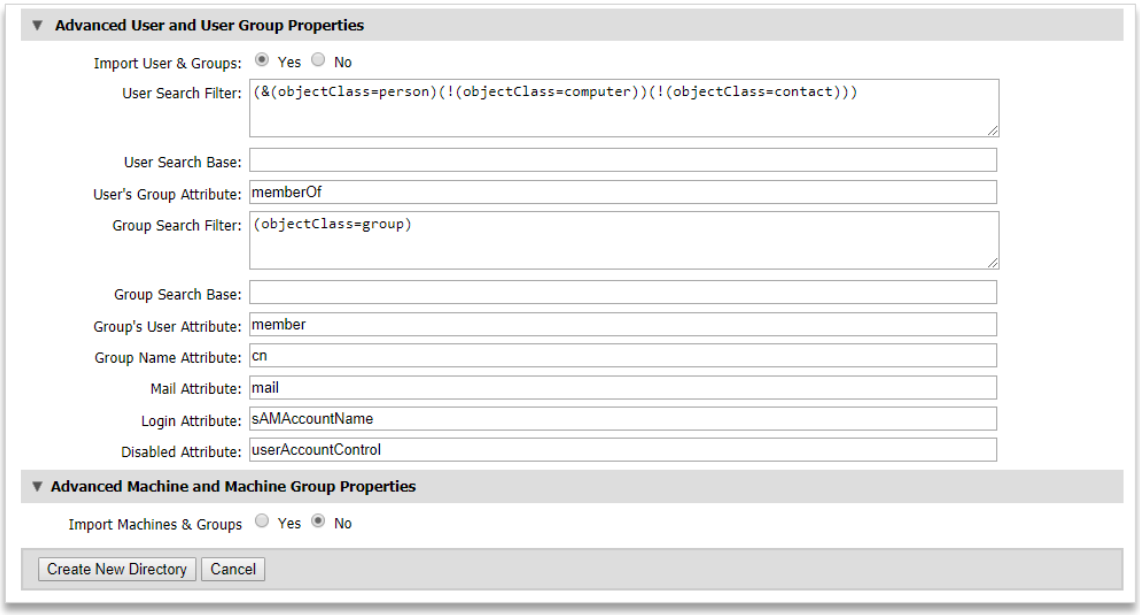
2. Enter the directory properties:



a. Security – When the "**Use secure connection**" option is checked, a closed lock icon will display next to the Domain name on the Login page on the Stratusphere web user interface. If this option is not checked, an unlocked icon will be displayed next to the Domain name. Liquidware recommends using a secure connection when configuring Active Directory or LDAP directories.

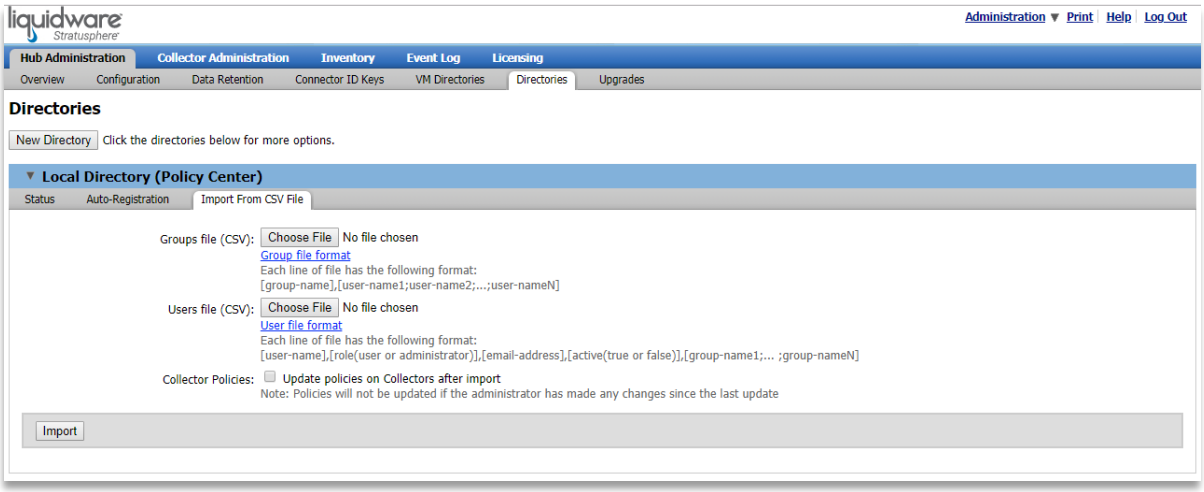


3. You can also choose to set advanced parameters to limit integration to specific portions of information from the directory server.



4. Click on the **Create New Directory** button when done.

Once you have defined the user directory within Stratusphere, you can perform manual import, or you can setup a scheduled import. You can perform an import from the directory or a file, or setup a scheduled import. An import will bring in user and group information. This information will be automatically synchronized with data already in the Hub. In the case of group memberships, the user directory server is always the "authority". To setup a scheduled import, you will need to select the frequency Daily, Weekly, or Monthly, and set the appropriate schedule times.



Hub Administration Upgrades

Software updates are available to all customers who have an active support plan. Depending on whether your Stratusphere appliances have direct access to the Internet or not, Liquidware Labs provides two options:

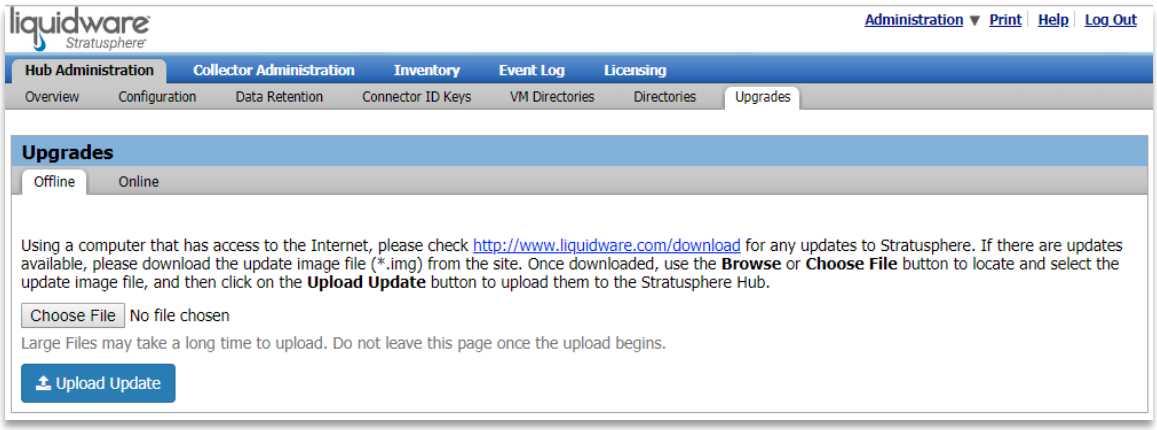
1. Online Upgrades: for appliances that have direct access to the Internet
2. Offline Upgrades: for appliances is in a secure, air-gapped environment with no direct access to the Internet. From another computer that does have access to the Internet, you will need to download a single upgrade image file first, then upload it to the Stratusphere Hub appliance using the Web UI within the Administration section under the **Hub Administration > Upgrades** tab.

Please refer to the ***Stratusphere Release Notes*** found in the Documentation section on the Liquidware Support Portal for more information. Depending on the version you are upgrading from, you may be redirected to a separate upgrade guide available on our Support Portal.

It is very important to follow the instructions given for upgrading your software. The order in which appliances need to be upgraded is particularly critical.

Offline Upgrades

Upgrades images downloaded using another computer can be uploaded into the Stratusphere interface under the **Hub Administration > Upgrades > Offline** tab. For more details, refer to your upgrade instructions.



Online Upgrades

Navigate to the **Hub Administration > Upgrades > Online** tab. If software updates are available, this tab will display a message that a new version is available for download. A button will be made available to download the upgrade image from within the Hub. Depending on your internet connection, it may take some time for the file to finish downloading. You may install the upgrade image by clicking on the **Install Update** button. However, if the default passwords (sspassword) for the friend or root users have been changed on the Database Appliance, you will need to complete some manual steps using the Database Appliance console. Please read the Release Notes and Upgrade Guides before performing any upgrades.

Inventory

The Inventory tab provides a grouping of all items discovered by Stratusphere such as Users, Machines, Desktop Applications, Network Applications, and Network Subnets in their own individual tabs. Each individual tab provides the ability to manage and group items together for usage and reporting purposes.

Machines

Machine inventory information is automatically populated into the Hub as you deploy CID Keys. Machine groups can be manually created, and machines can be assigned to groups for ease of policy and report filtering. Additional VM information and groups can also be imported via integration with a VM Directory such as VMware vCenter and Nutanix Prism.

Users

User inventory information will be automatically populated into the Stratusphere Hub as you deploy Connector ID Keys. User groups can be created, and users can be assigned to groups for ease of policy and report filtering. Additional user group information can also be imported through integration with Active Directory or any LDAP-compliant user directory system. User Groups are useful for policy and report filters. You can create and populate them manually or import defined groups from AD or an LDAP-compliant directory.

Applications

Application inventory information covers both Desktop and Network applications. Desktop applications will be automatically populated into the Stratusphere Hub as you deploy Connector ID Keys. Network applications come pre-populated in the Hub based on typical ports and protocols but can be edited. Use quick search to find specific applications.

Subnets

Subnets inventory information is manually added into the Stratusphere Hub for use in policy and report filtering. You can define a single subnet, or a group (list) of subnets under a single name.

Enabling Privacy – Anonymizing User and Machine Names

Liquidware understands and respects privacy related issues and concerns of its users across the world. Whether it may be due to government regulations or some organizations ensuring privacy of its users, there are legitimate requirements for enabling the option to anonymize end user names and machine names within Stratusphere.

Liquidware offers the ability to totally anonymize end user names and machine names within Stratusphere. It must be noted that once this privacy mode is enabled, **each newly registered user name and machine within the Stratusphere Database will be anonymized in a single one-way hash. The conversion is permanent and cannot be undone**. U**ser names and machines that existed prior to turning on privacy mode will still be stored in plain text.** Privacy mode can be disabled. However, the user and machine names already anonymized stay anonymized permanently. Any user name and machine name registration received after disabling privacy mode will be stored in plain text and will not be hashed.

Any user and machine that registered prior to enabling privacy mode will remain visible in plain text. Enabling privacy mode only works for users and machines that register from that point forward and does NOT work to hash user and machine names registered before enabling privacy mode.

Using the privacy mode may make Stratusphere reporting harder to read and follow since instead of user names and machines names, the end user will only see randomized pieces of text representing users and machines.

> ***Once Privacy mode is enabled the user and machine names already anonymized stay anonymized permanently even if Privacy mode is disabled later.***

Here are the instructions to enable Privacy mode:

1. Using an SSH client like PuTTY, log into the Stratusphere Hub console using credentials for the **friend** user. Then use credentials for the **root** user to switch to the root using the 'su -' command. Unless changed, the default password for both users is '`sspassword`'.
2. Execute the following command to invoke a limited shell prompt:
   ```
   > /opt/tnt/bin/mgrconfig
   ```
3. On the new shell prompt, execute the following commands to anonymize user and/or machine names within the Stratusphere Database:
   ```
   > set system user privacy on
   > set system machine privacy on
   ```
4. To save and quit enter the following commands:
   ```
   > write
   > quit
   ```
5. Enter **CTRL+D** twice to log out of root and friend SSH sessions and quit the SSH PuTTY client.

Please provide some time for Stratusphere to begin its anonymizing process. Once completed, please log into the Administration section of the Stratusphere Web UI and navigate to **Inventory > Machines** and **Inventory > Users** tabs to verify if the names have been anonymized.

Here are the instructions to disable Privacy mode:

1. Using an SSH client like PuTTY, log into the Stratusphere Hub console using credentials for the **friend** user. Then use credentials for the **root** user to switch to the root using the 'su -' command. Unless changed, the default password for both users is '`sspassword`'.
2. Execute the following command to invoke a limited shell prompt:
   ```
   > /opt/tnt/bin/mgrconfig
   ```
3. On the new shell prompt, execute the following commands to anonymize user and/or machine names within the Stratusphere Database:
   ```
   > set system user privacy off
   > set system machine privacy off
   ```
4. To save and quit enter the following commands:
   ```
   > write
   > quit
   ```
5. Enter **CTRL+D** twice to log out of root and friend SSH sessions and quit the SSH PuTTY client.

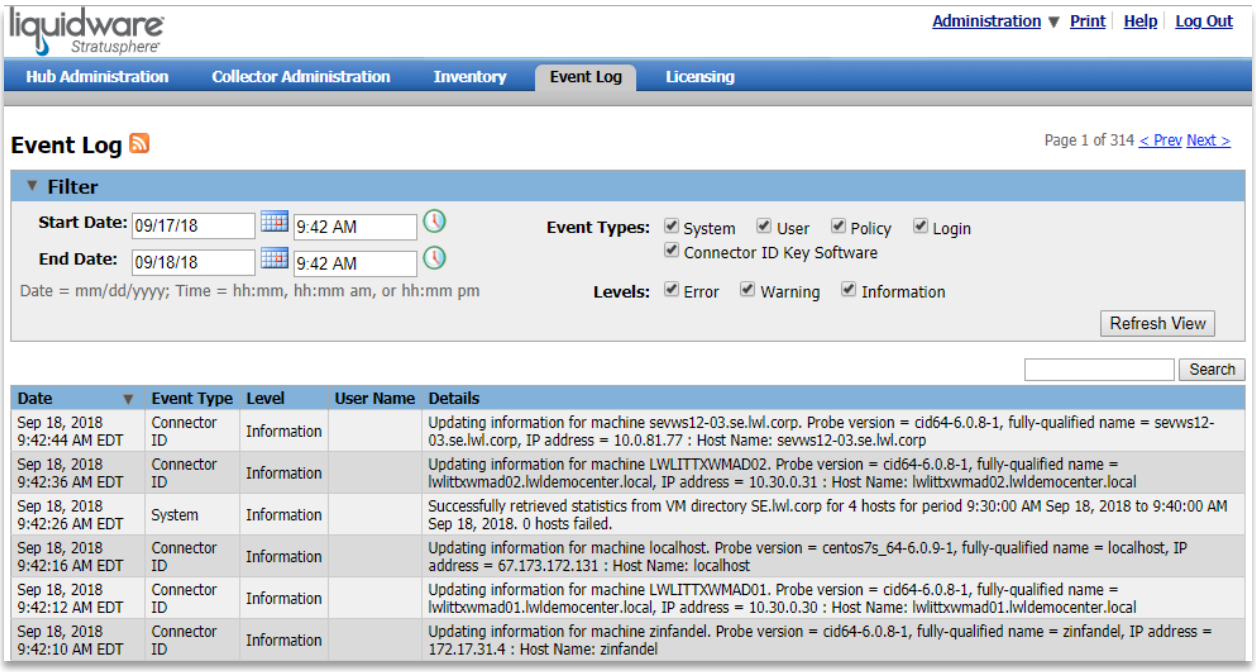
All users and machines registering for the first time since disabling privacy mode will now show up as plain text and will not be hashed. Users and machines that were previously anonymized under Privacy mode will remain anonymized.

Monitoring the Event Log

The event log is where error, warning and information messages are stored for the events that occur within the Stratusphere Hub. This includes administrative logins and actions, such as policy rule changes, CID Key registrations, and scheduled actions such as imports from directory systems and execution of scheduled and manually executed reports.

To view the event log, navigate to the **Event Log** tab. You can select the time range of events to view, and select the type of events to view, or perform a Quick Search for specific event data. You can also enable and disable various checkboxes to observe only a particular type of Event and/or a particular Event Level.

The secure RSS feed can be used to integrate all or select event log messages into other applications.



Event Types

System:
System events are ones that are logged when the Stratusphere back-end services perform some functions, or certain jobs or event begin and end. It includes items such as syncing with VMware vCenter or Microsoft Active Directory, or execution of certain scheduled or manually run reports. In 6.0, it will also include messages that show when a certain number of detail records are rolled up into a higher period time frame.

User:
User events are ones that are initiated by a user to update certain configuration items such as Connector ID Key properties for a machine or machine group, changing roles of a user, configuring parameters for syncing with Active Directory or vCenter, etc.

Policy:
Policy events are ones that are logged when a user adds/updates/deletes network policies on a Network Collector and then pushes the updated policies to the group of Network Collectors. This helps

administrators keep track of which user, at what time, updated network monitoring policies on which network Collectors.

Login:
Login events are ones that capture a login attempt, whether it was successful or not, what were the credentials (username) offered including domain credentials or Local Directory, along with the exact time and IP Address from which it occurred.

Connector ID Key Software:
Connector ID events are ones that capture when a CID Key agent sent registration information to the Stratusphere Hub and what were some of the main items that were observed as part of this registration information. If the machine already was registered before and has the same hardware signature as before, it will also state that it allowed a reactivation of the certificate given to each machine.

Event Levels

Error:
The Error Level event provides a listing of all errors, failures or critical events observed on the Stratusphere system regardless of the Event Type. If a vCenter sync failed, or a Network Collector policy push failed for some reason, then it would be classified as an Error Level event and logged as such. Unless there is a known reason, you should not see major number of error level events.

Warning:
The Warning Level event provides a listing of all warnings or non-critical events observed on the Stratusphere system regardless of the Event Type. Warnings are lower impacts than errors but are logged nonetheless to record events such as failed user logins into Stratusphere, or network communication problems between the Hub and a Collector or similar.

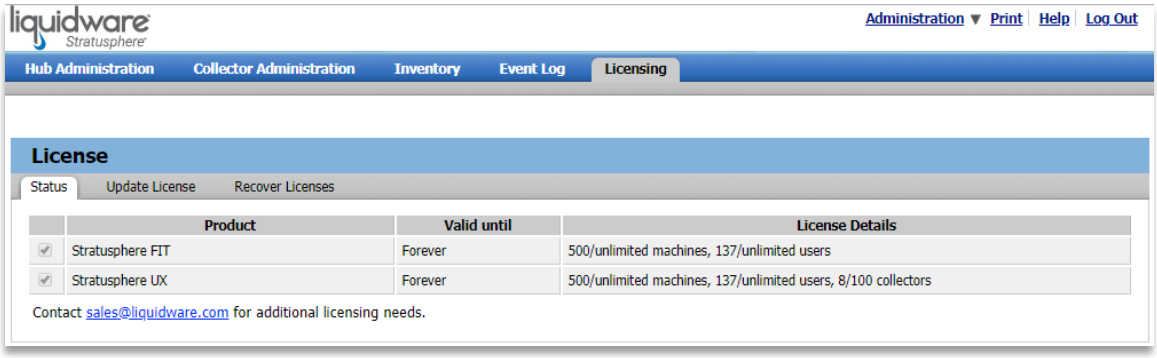
Information:
The Information Level event provides a more verbose level of logging. These are not associated with any critical errors or conditions, but merely to provide information updates on successful conclusion of certain tasks to log when it began and with it concluded successfully.

Working with Licenses

As your environment grows and changes, so might your Stratusphere needs. Stratusphere is licensed on a per user and/or per machine basis. You can view your current Licensing details in the Hub Administration module under the **Licensing** tab.

Viewing Your Current License Status

The **Licensing > Status** tab tells you which Stratusphere products your organization is licensed for, when product support for each license expires, and how many licenses are in use versus the total amount available for use. Please contact your sales representative at sales@liquidware.com to renew product support or to purchase additional licenses.

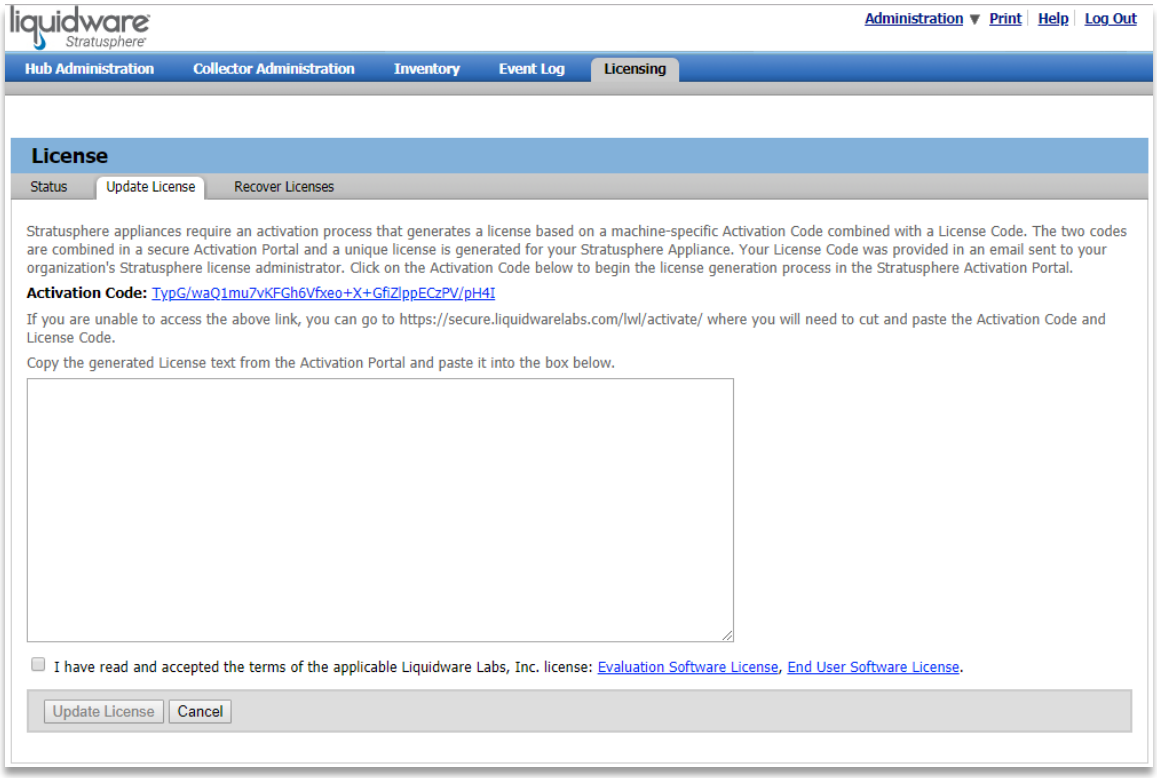


With the purchase of a Standard Support contract, customers receive the following elements of service:

- Unlimited access to Liquidware Support web site
- Downloads of the latest releases, patches, corrections, enhancements, and upgrades for Liquidware products as they are made generally available
- Access to the latest product
- Maintain case logging regarding operational/technical aspects of Liquidware software
- Access to Liquidware product documentation

How to Update a License Registration

When you extend product support or purchase additional licenses, you will need to update your license file. To generate and update a new license file:

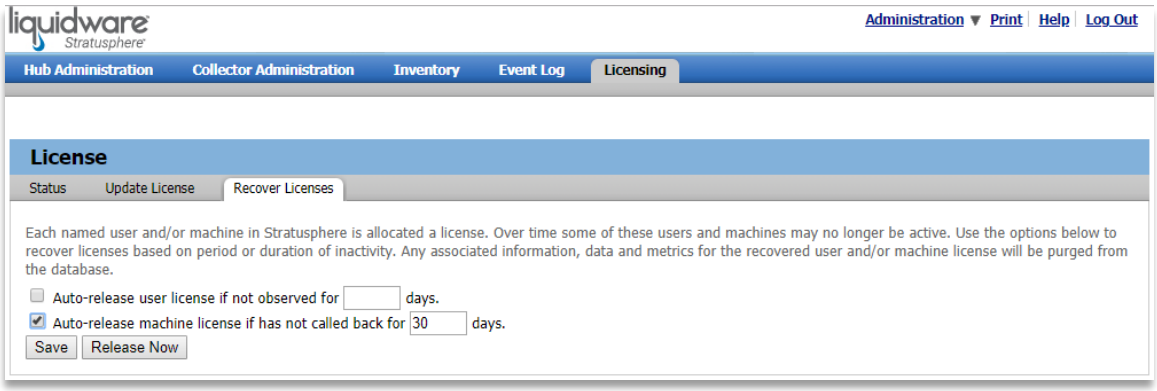


1. While logged in to the Hub Administration module, click on the **Licensing** tab and go to **Update License**.
2. Click on the **Activation Code** link. This **Activation Code** is unique, and the link will take you to the Liquidware Stratusphere License Activation Portal where your Activation Code will be prefilled for you.

3. Enter your unique **License Code** that was sent to you by email from Liquidware and click **Proceed**.
4. Copy the generated License text from the Activation Portal and paste it into the box on the **Update License** tab in the Hub Administration module.
5. Once you have reviewed and agree with the license agreements, click the checkbox below the License text.
6. Click **Update License** to finish.

How to Recover Unused Licenses

Over time you may have users who are no longer with the company or machines which were being monitored that are no longer in service. If so, those Stratusphere licenses that were issued to those users and/or machines can be reclaimed and added back to your pool of available licenses. To recover those unused licenses:



1. While logged in to the Hub Administration module, click on **Licensing** and then go to the **Recover Licenses** tab.
2. Set the number of days Stratusphere should wait before releasing a user who has not been reporting back to the Hub or a machine that has not been calling back to the Hub.
3. Check the checkbox next to each setting to activate it.

4. If you wish to go ahead and release user or machine licenses without waiting for Stratusphere's configuration settings to kick in, click **Release Now**.
5. Click on **Save** to keep your configuration changes.

Please be aware that all metrics collected for inactive users and machines whose licenses have been reclaimed, will be permanently deleted from the Stratusphere database and cannot be recovered.

Getting Help Installing Stratusphere

If you have questions or run into issues while using Stratusphere, Liquidware is here to help. Our goal is to provide you with the knowledge, tools, and support you need to be productive.

Using Online Resources

Liquidware maintains various kinds of helpful resources on our Customer Support Portal. If you have questions about your product, please use these online resources to your full advantage. The Support Portal includes product forums, a searchable Knowledge Base, documentation, and best practices among other items. You can visit our website at https://www.liquidware.com.

Contacting Support

If you wish to contact our Support staff for technical assistance, please either log a request on the Liquidware Customer Support Portal or give us a call. Prior to Logging a Case you may want to review these helpful tips:

- Check the Product Documentation included with your Liquidware Product.
- Try to see if the problem is reproducible.
- Check to see if the problem is isolated to one machine or more.
- Note any recent changes to your system and environment.
- Note the version of your Liquidware product and environment details such as operating system, virtualization platform version, etc.

To speak directly with Support, please use the following numbers:

Main Line: 1-678-397-0460

Toll Free in US & Canada: 1-866-914-9665

Europe/Middle East/Africa: +44 800 014 8097

Toll Free in Europe

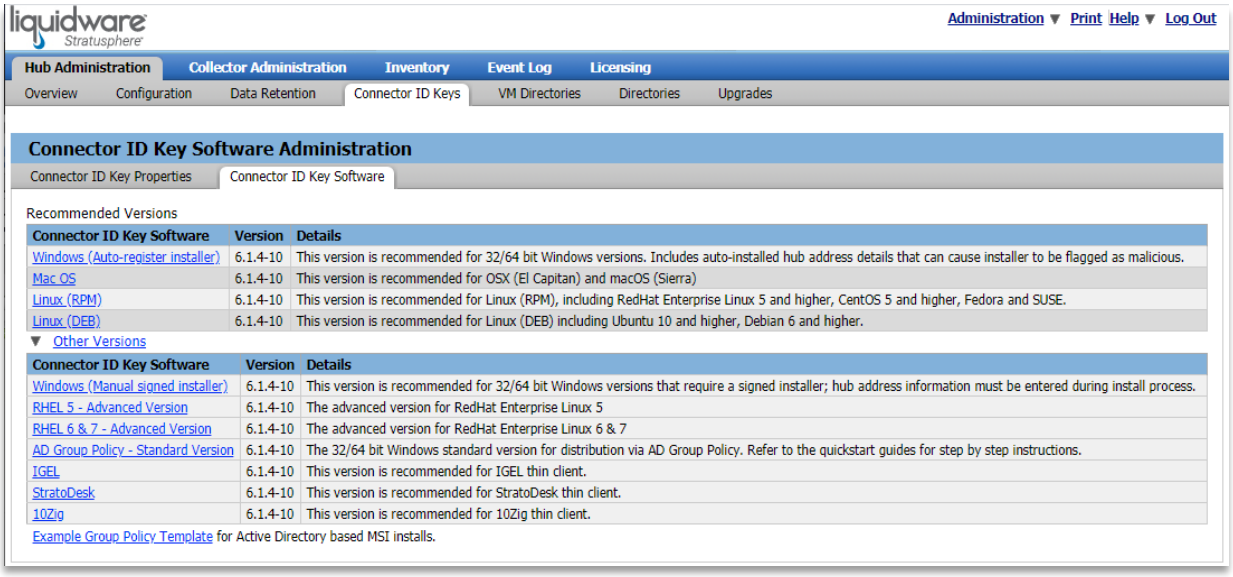
UK: 0800 014 8097

Netherlands: 0800 022 5973

Switzerland: 0800 561 271

Appendix A: Deploying Standard Connector ID Keys with AD GPO or SMS

As previously discussed, 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 in the Hub Administration module by proceeding to **Hub Administration > Connector ID Keys** and clicking on the **Connector ID Key Software** tab.



For evaluation, you can manually install the EXE on test desktops (see the earlier section on **Distributing Connector ID Keys to Target Desktops**), but this section provides further details if you wish to distribute Connector ID Keys using Microsoft's Active Directory (AD) Group Policy Object (GPO) or Systems Management Server (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", or auto-delete, themselves after a specified number of days.

If you have problems or questions regarding the steps described here, please submit a request for more information on the Liquidware Support Portal.

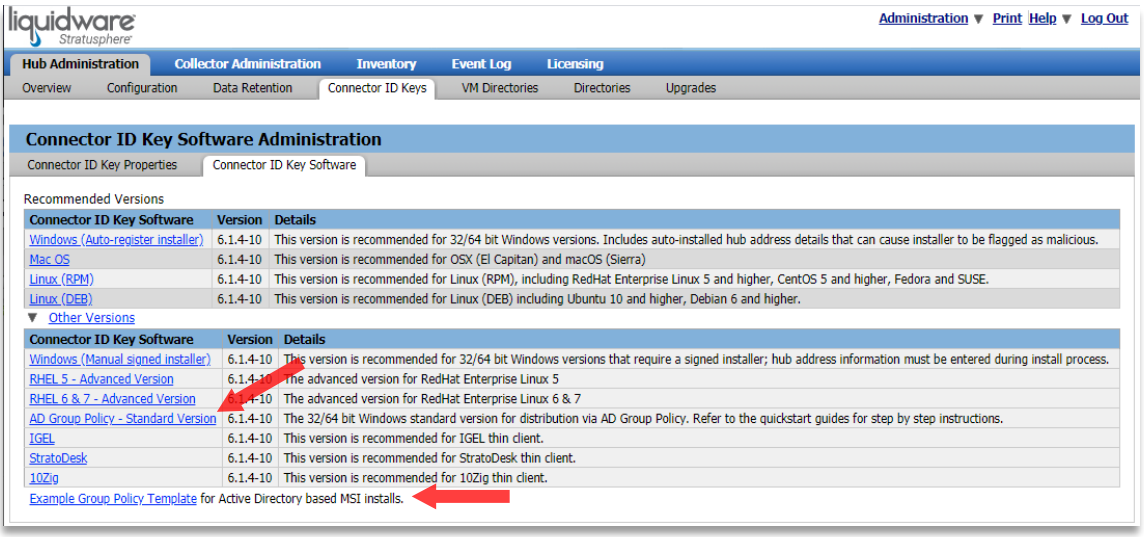
Deploying the Standard Connector ID Keys with AD GPO

This section describes how to use Active Directory Group Policy to automatically distribute the "locally installed" Connector ID Keys to desktop machines or users. When distributing the Connector ID Keys using Group Policy, we suggest 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: Download the CID Key MSI and Example Group Policy Template

The Connector ID Key MSI and the template can be found by clicking on the **Connector ID Key Software** tab under **Hub Administration > Connector ID Keys**. You will need to download these files from the Hub.

> ***This MSI is to be distributed using AD Group Policy only. Do not attempt to use any other distribution mechanism.***



Step Two: Create a Distribution Point

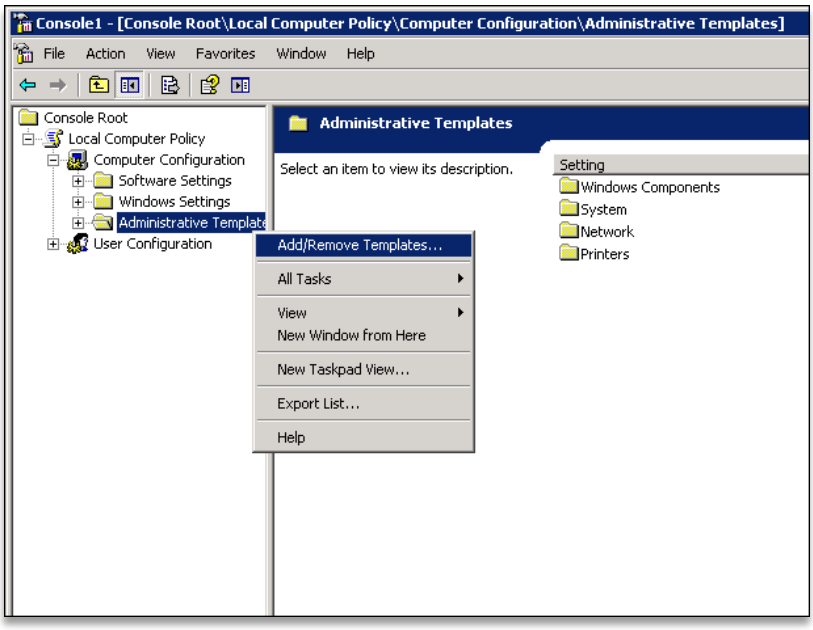
To assign the Connector ID Key MSI, you must create a distribution point on the publishing server:

1. Create a shared network 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 MSI file.
    a. Grant either “Authenticated Users” or “Everyone” read permission.

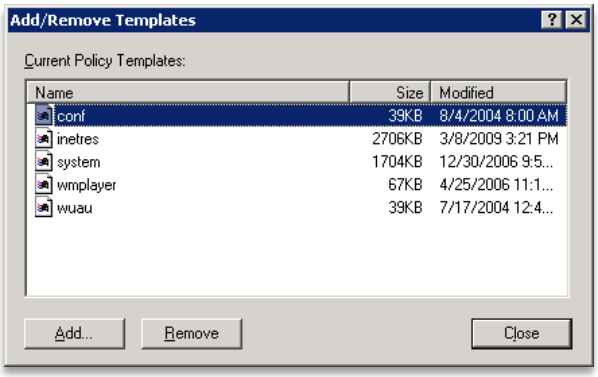
Step Three: Load Group Policy ADM Template

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

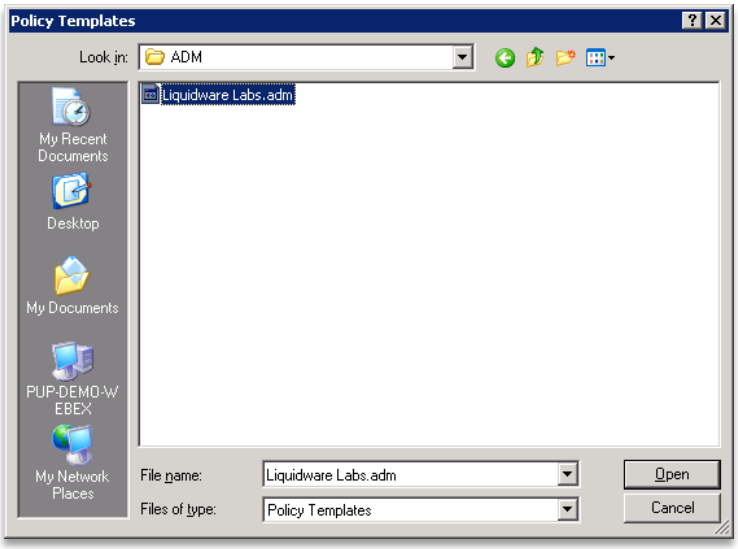
1. Right click **Administrative Templates** under **Computer Configuration** and select **Add/Remove Templates…**


Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates]
File
Action
View
Favorites
Window
Help
Console Root
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
User Configuration
Administrative Templates
Select an item to view its description.
Setting
Windows Components
System
Network
Printers
Add/Remove Templates...
All Tasks
View
New Window from Here
New Taskpad View...
Export List...
Help

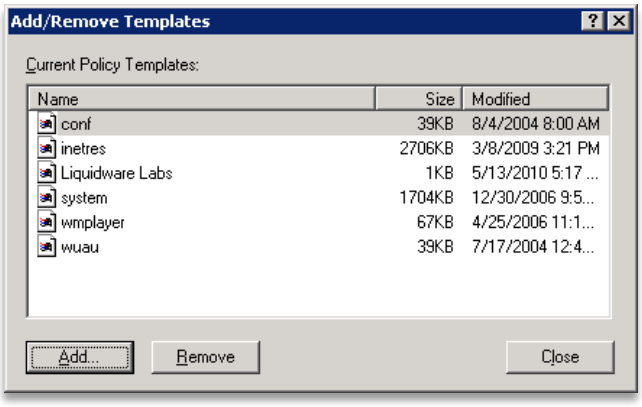
2. Select **Add…** to load the Liquidware Labs template.



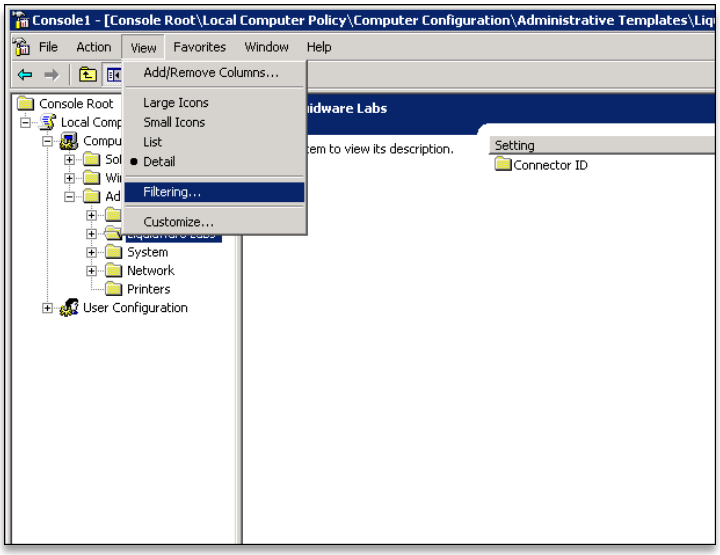
3. Browse to the location where Liquidware Labs template you previously downloaded is located.



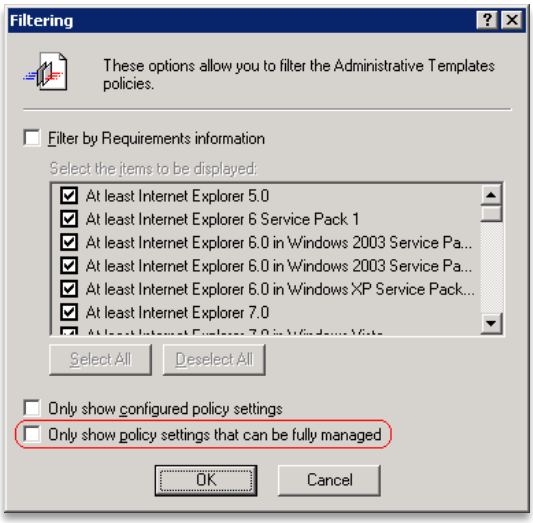
4. Once the template has been loaded, **Close** the dialog box.



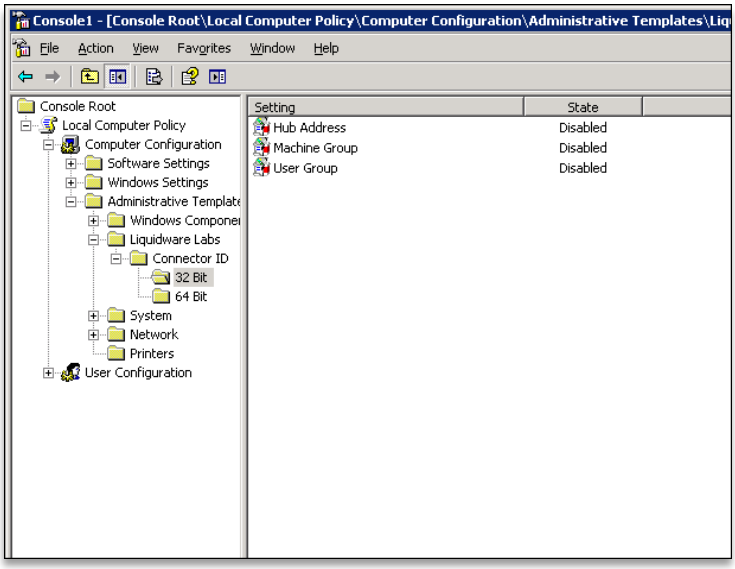
5. From the **View** menu, select **Filtering…**

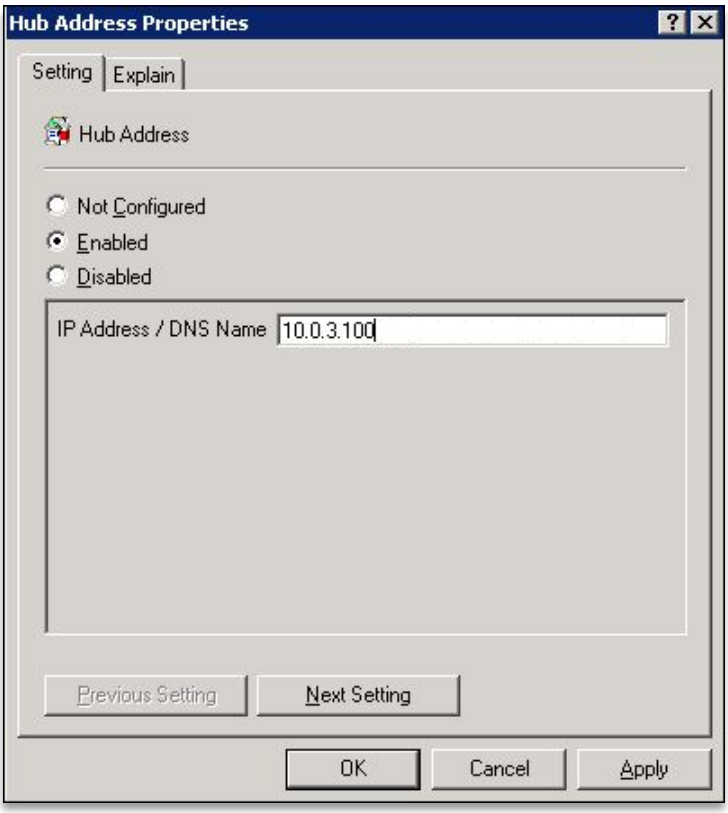


6. Disable, or uncheck, **Only show policy settings that can be fully managed**.



7. Specify Connector ID Options including the Hub Address for your environment.

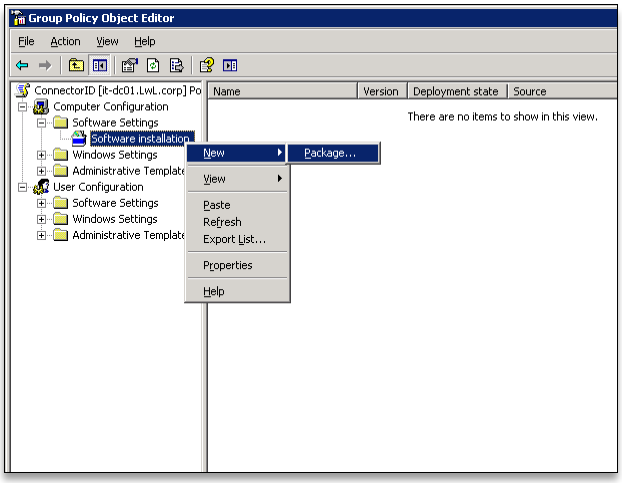




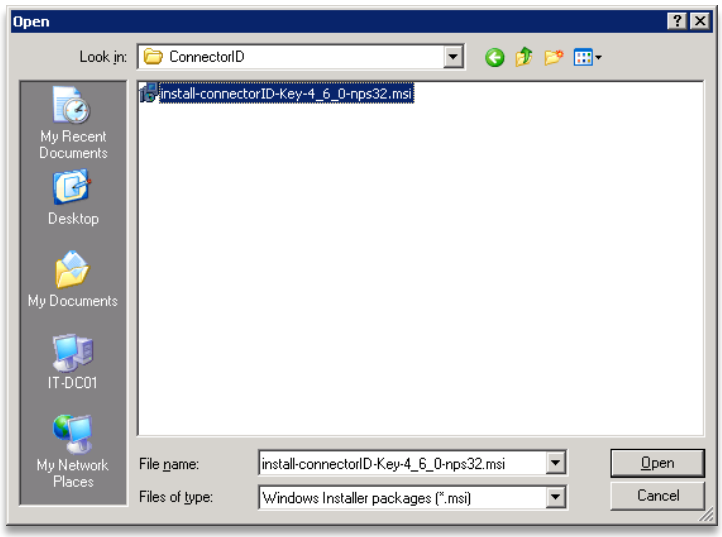
Step Four: Deploy the CID Key Agent

Create a Group Policy that deploys the Connector ID MSI package. Please reference the figures below for further assistance.

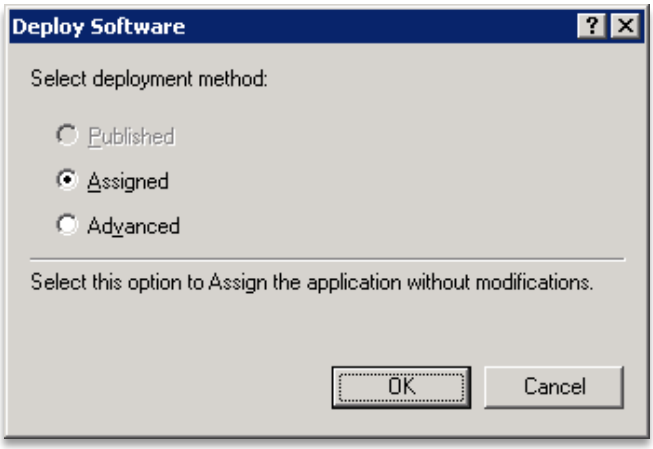
1. Right click the **Software installation** option under **Computer Configuration** and select **New** then **Package…**



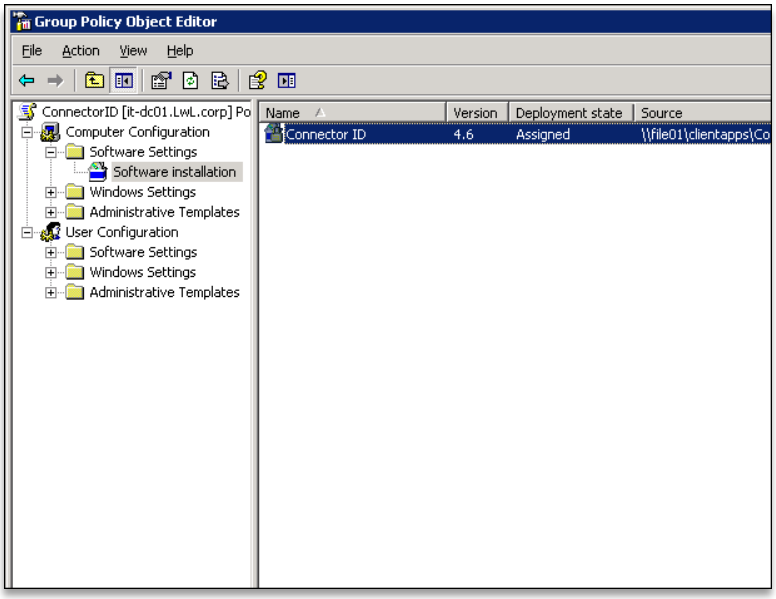
2. Browse to the location the where the Connector ID MSI is located. This path should be the UNC path created in Step 1.



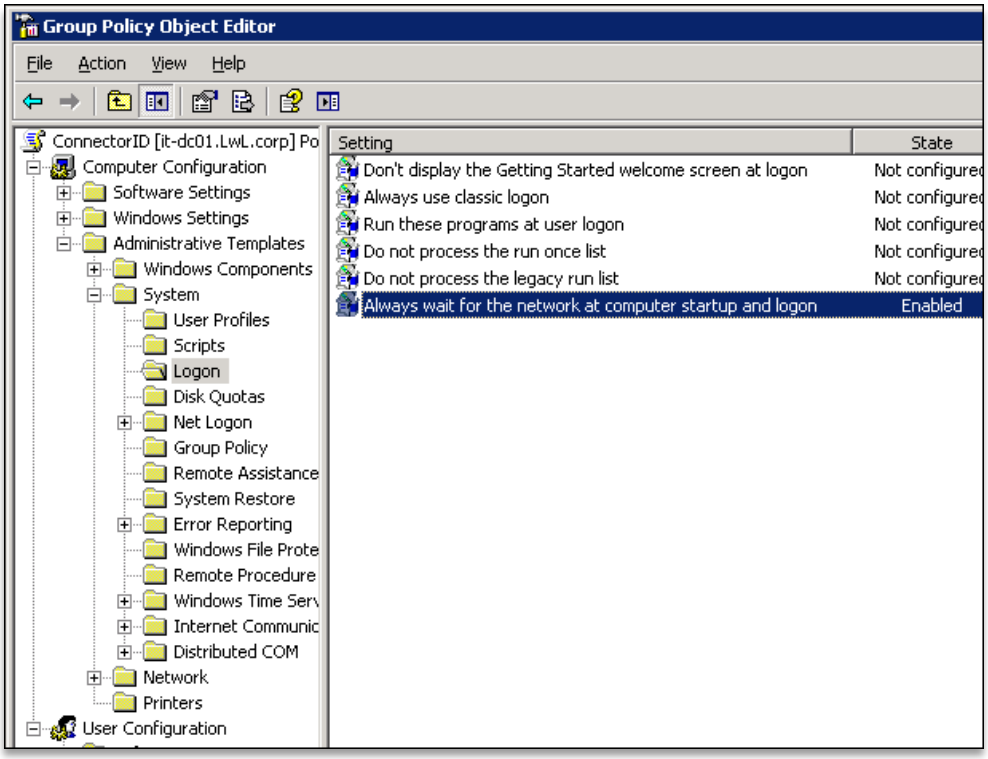
3. Select **Assigned** and then choose **OK**.



4. Double Click the Connector ID package to open the Properties dialog box.



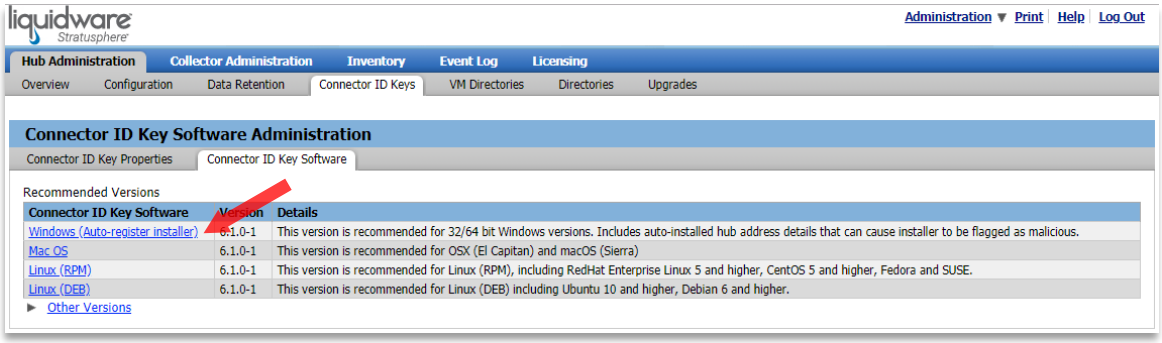
5. Enable the **Always wait for the network at computer startup and logon** setting.



Deploying the Standard Connector ID Keys with SMS

This section describes how to deploy the Connector ID Keys in your environment by using SMS. In this example, we will use the example folder named \InstallerCache\CID presumed on the SMS host machine named SMS01. However, you will need to change these to the actual names in your environment.

The Windows - Standard Version Connector ID Key can be found by clicking on the **Connector ID Key Software** tab under **Hub Administration > Connector ID Keys**. You will need to download this file from the Hub to the folder you created on your SMS host machine.



To distribute the CID Keys using SMS:

1. Start the SMS Administrative Console and create a new package with the following attributes:
    a. **Name:** Connector ID Keys
    b. **Version:** 6.x.x (specify the actual version to be deployed)
    c. **Publisher**: Liquidware Labs, Inc.
    d. **This package contains source files:** True (checked)
    e. **Source directory:** \\SMS01\InstallerCache\CID
2. Use the default or site-specific settings for all remaining attributes.
3. Create a Distribution Point for this newly created package according to your site needs.
4. Create a Program specifying the executable installer package:
    a. **Name:** Connector ID Keys
    b. **Command line:**

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

Note: The "x_x_x" in the command should be replaced with the version number of the CID Key you are installing. The last three parameters HUBADDRESS, MACHINEGROUP, and USERGROUP are optional. If you use them, do not use the actual bracket characters [and]. However, the quotes are required and the variables inside the quotes should be replaced with values specific to your environment. The EXE installer already has information regarding the address of the Stratusphere Hub it was downloaded from and must 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.

    c. **Run:** Normal

5. The following is necessary to complete Connector ID Keys installation and registration:
    a. **Estimated memory:** 512 MB RAM or higher
    b. **Maximum allowed run time:** 20 minutes
    c. **Program can run:** Whether or not a user is logged on (suggest scheduling install when users are not logged on)
    d. **Run mode/Run with Admin rights:** True (selected)
6. You are now ready to create a new Advertisement. Use the following attributes:
    a. **Package:** Connector ID Keys
    b. **Program:** Connector ID Keys Installer
    c. **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.
7. 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 the Stratusphere Hub under **Inventory > Machines**.

Appendix B: Embedding Connector ID Keys in VMware Horizon View Master Images

Another alternative way to deploying Stratusphere Connector ID Keys is to install the CID Key Agent on VMware View master images or templates. Remember, you must be an Administrator with full administrative credentials while installing the Connector ID Key on your base image.

Before deploying CID Keys in your VMware View master image, login to the Administration module of the Stratusphere Hub appliance and proceed to **Hub Administration > Connector ID Keys** and click on the **Connector ID Key Software** tab. Download the appropriate install package for your target environment.

> ***Note: If the Connector ID Key software is already installed and you need to simply upgrade the software, best practice is to uninstall the old software and then install the new software. From the Windows Control Panel, uninstall the Connector ID program from Liquidware Labs. Then follow the instructions below to install the new version of the Connector ID Key software.***

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 the following location and execute the batch file:

   On 32-bit Operating Systems:

   ```
   C:\Program Files\Liquidware Labs\Connector ID\admin scripts\
   VMwareView_MasterImagePrep.bat
   ```

   On 64-bit Operating Systems:

   ```
   C:\Program Files (x86)\Liquidware Labs\Connector ID\admin scripts\
   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. When configuring the resource pool in Horizon View Composer's Automated Desktop Pool, specify the following as Post Synchronization script:
   - **i.** For Linked Clones: On the QuickPrep Settings page use the following

     On 32-bit Operating Systems:

     ```
     C:\Program Files\Liquidware Labs\Connector ID\admin scripts\
     VMWareView_PostSyncScript.bat
     ```

     On 64-bit Operating Systems:

     ```
     C:\Program Files (x86)\Liquidware Labs\Connector ID\admin scripts\
     VMWareView_PostSyncScript.bat
     ```
   - **ii.** For Instant Clones: On the ClonePrep Settings page use the following

     On 32-bit Operating Systems:

     ```
     C:\Program Files\Liquidware Labs\Connector ID\admin scripts\
     VMWareInstantClones_PostSyncScript.bat
     ```

     On 64-bit Operating Systems:

     ```
     C:\Program Files (x86)\Liquidware Labs\Connector ID\admin scripts\
     VMWareInstantClones_PostSyncScript.bat
     ```

Appendix C: Installing Connector ID Keys in Citrix Provisioning Server Master Images

Another alternative way to deploying Stratusphere Connector ID Keys is to install the CID Key Agent on the master images that are deployed through Citrix Provisioning Server. Remember, you must be an Administrator with full administrative credentials while installing the Connector ID Key on your base image.

Before deploying CID Keys in your Citrix Provisioning Server master image, login to the Administration module of the Stratusphere Hub appliance and proceed to **Hub Administration > Connector ID Keys** and click on the **Connector ID Key Software** tab. Download the appropriate install package for your target environment.

> ***Note: If the Connector ID Key software is already installed and you need to simply upgrade the software, best practice is to uninstall the old software and then install the new software. From the Windows Control Panel, uninstall the Connector ID program from Liquidware Labs. Then follow the instructions below to install the new version of the Connector ID Key software.***

To install the Connector ID Key into your master image, do the following:

1. Power on and log into your XenDesktop master image.
2. Install the Connector ID Key manually. If there is an existing installation of Connector ID already on the master image, it will be updated to the latest version during the installation. The installer will automatically call back to the Stratusphere Hub and register with the default Hub address information embedded inside the installer. Chose the Custom option within the installer wizard to alter this default Hub information and specify a different Hub IP address or DNS address as well as specifying a Machine Group and User Group to register the machine and user into.
3. Once the installer completes, check to see if it registered with the Stratusphere Hub. You can do so by checking either one of two options below:
    a. Open your browser and log into the Stratusphere Management UI's "Administration" section using the **ssadmin/sspassword** credentials. (Note: For AWS use your VM Instance ID for the password.) Navigate to the **Inventory > Machines** tab. The master image machine name should exist in this list and verify its version number and call back times have been updated to the current date and time.
    b. Verify if the following file exists: **`C:\Program Files\Liquidware Labs\Connector ID\ca\cert.txt`** – If it exists then we have a successful installation, and now we need to prepare the master image for deployment through Provisioning Server.
4. To prepare the image for deployment, the initial registration cert.txt and other items must be cleared and reset. To do so on the base image open a command prompt as an Administrator and execute the following bat file:

    `C:\Program Files\Liquidware Labs\Connector Id\admin scripts\ProvisioningServer_MasterImagePrep.bat`
5. Shut down the base desktop virtual machine, you are now ready to deploy your desktop master image through Provisioning Server.

Appendix D: Working with Connector ID Keys on Linux

> ***Note: If the Connector ID Key software is already installed and you need to simply upgrade the software, best practice is to uninstall the old software and then install the new software. Instructions for both installing and uninstalling the Connector ID Key software are given below.***

Installation Instructions

Here are instructions to install the CID Key on your local Linux Desktop:

1. Log into your local Linux Desktop using administrative credentials.
2. Using your local browser, log into the Administration section of the Liquidware Stratusphere Hub Web Interface using the **ssadmin/sspassword** default credentials. (Note: For AWS use your VM Instance ID for the password.)
3. To download the Connector ID Key software, navigate to the **Hub Administration > Connector ID Keys > Connector ID Key Software** tab.
4. Click on the version that is the closest match for your Linux distribution.
5. After the download has finished, open an Xterm console on your Linux Desktop.
6. To install the CID Key, you must switch to the root user. To do so use any one of the following:
   ```
   $ su - root
   ```
   Or
   ```
   $ sudo /bin/bash
   ```
7. The installer needs to run from the root folder '/'. Copy or move your downloaded install binary to the root folder '/'. Assuming the browser saves all downloads into the 'Downloads' folder, please execute the following:
   ```
   $ cp ~/Downloads/install-connectorID-Key-x.x.x-x-<os>.bin /
   ```
8. Run the installer from the current directory
   ```
   $ sh ./install-connectorID-Key-x.x.x-x-<os>.bin
   ```

Creating a Linux Master Image with a CID Key

After completing the installation above, complete the steps below to convert the current installation into a Linux Master Image:

1. To prepare the Linux image as a master image, you must switch to the root user. To do so use any one of the following:
   ```
   $ su - root
   ```
   Or
   ```
   $ sudo /bin/bash
   ```
2. Stop the CID Key process by executing the following:
   ```
   $ /etc/init.d/vs-helper stop
   ```
3. Remove the following files:
   ```
   $ cd /opt/vdesktools/grd
   $ rm cert.txt stats.* stats/* uidcache key_material/certreq.tnt
   ```
4. Your image is now ready to be saved as the Linux Master Image.

Linux CID Key Commands & Files

1. Start the CID Key process by executing the following:
   $ sudo /etc/init.d/vs-helper start

2. Stop the CID Key process by executing the following:
   $ sudo /etc/init.d/vs-helper stop

3. Test if the CID Key process is running by executing the following:
   $ ps -ef | grep vs-helper

4. Remove or uninstall CID Key process by executing the following:
   $ sudo /opt/vdesktools/bin/idenq -R

5. Log file locations: **/var/log/grd.log**
6. Data Directory locations:
   a. **/opt/vdesktools/grd/cert.txt**
   b. **/opt/vdesktools/grd/imgrcomm.txt**
   c. **/opt/vdesktools/grd/key_material/public/mgrcert.pem**
7. Binary file locations: **/opt/vdesktools/bin/**

Uninstall Instructions

Here are instructions to uninstall the CID Key on your local Linux Desktop:

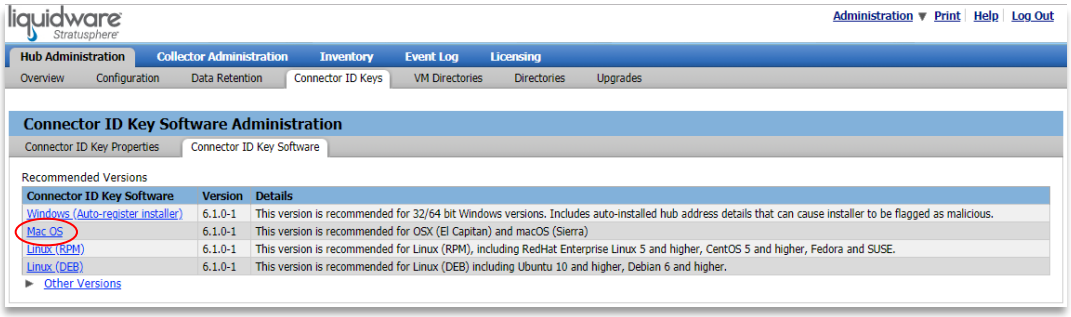
1. Log into your local Linux Desktop using administrative credentials.
2. Verify if you have the .bin file used for installing the CID Key. If you found it skip to item 8 below. If you do NOT have it, download it from the Stratusphere Hub Web UI. Using your local browser, log into the Administration section of the Liquidware Stratusphere Hub Web Interface using the **ssadmin**/**sspassword** default credentials. (Note: For AWS use your VM Instance ID for the password.)
3. To download the Connector ID Key software, navigate to the **Hub Administration > Connector ID Keys > Connector ID Key Software** tab.
4. Click on the version that is the closest match for your Linux distribution.
5. After the download has finished, open an Xterm console on your Linux Desktop.
6. To uninstall the CID Key, you must switch to the root user. To do so use any one of the following:
   $ su - root
   Or
   $ sudo /bin/bash
7. The uninstaller needs to run from the root folder '/'. Copy or move your downloaded install binary to the root folder '/'. Assuming the browser saves all downloads into the 'Downloads' folder, please execute the following:
   $ cp ~/Downloads/install-connectorID-Key-x.x.x-x-<os>.bin /
8. Run the uninstaller from the current directory
   $ sh ./install-connectorID-Key-x.x.x-x-<os>.bin remove

Appendix E: Working with Connector ID Keys on OS X & macOS

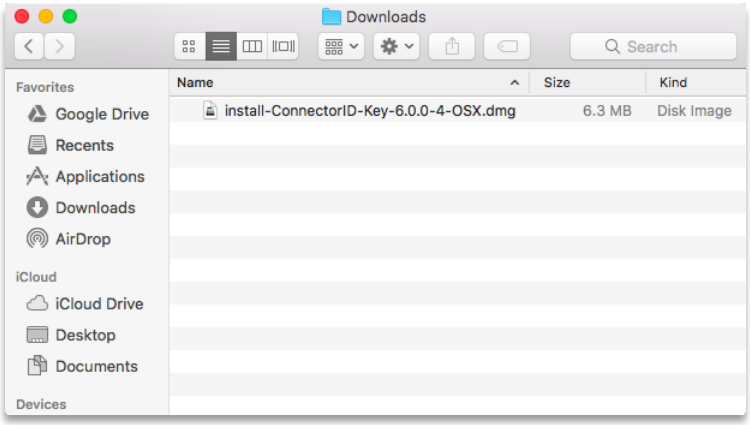
Installation Instructions

Here are instructions to install the CID Key on your local Apple Mac OS X or macOS Desktop:

1. Log into your local Apple Desktop using administrative credentials.
2. Using your local browser, log into the Administration section of the Liquidware Stratusphere Hub.
3. Navigate to the **Hub Administration > Connector ID Keys > Connector ID Key Software** tab and use the "MacOS" link to download the OS X/mac OS image from the Hub onto your Mac.



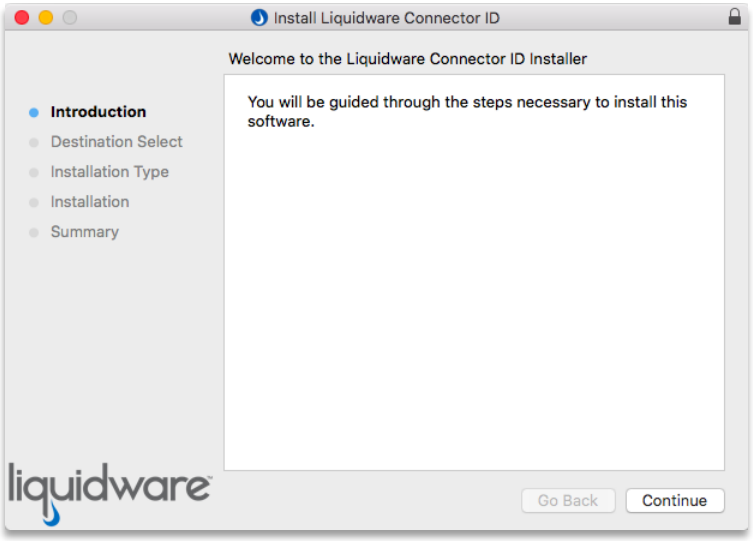
4. Once downloaded, navigate to the Downloads folder on your Mac and double click on the Connector ID Key installer DMG file to begin installation.

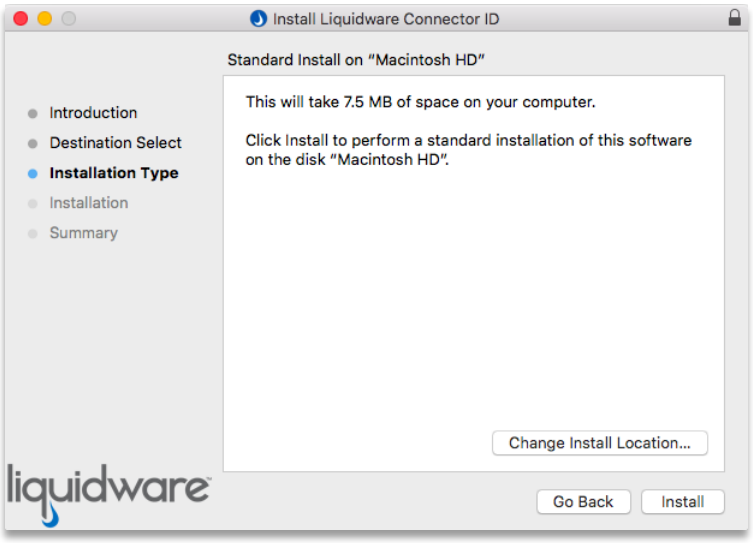


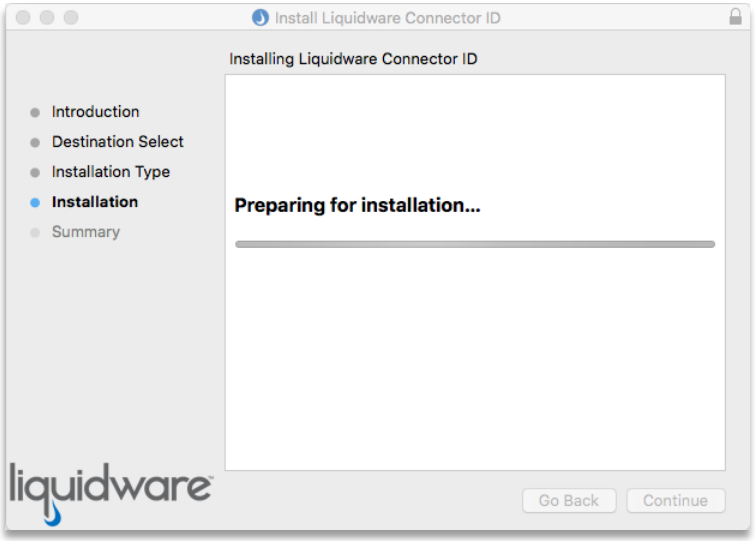
5. Double-clicking the DMG creates a ConnectorID device file, under Devices.
6. Open the ConnectorID Device file and it will reveal files; a ConnectorID.pkg which contains the OSX installer, and the mgrcert.pem which contains information how the CID Key will connect back to the Stratusphere Hub for registration.

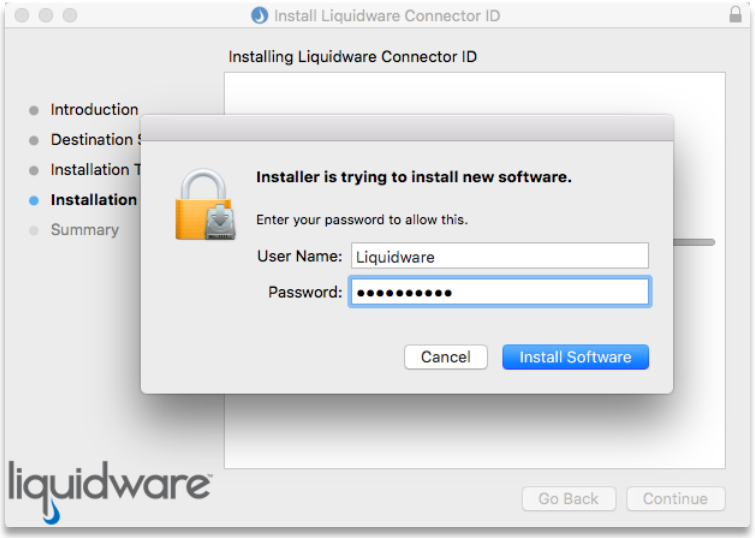
7. With the CTRL key pressed, double click on the Connector ID package file. A warning will be displayed stating the ConnectorID.pkg is from an unidentified developer. Click **Open** to ignore the warning and proceed with the installation.

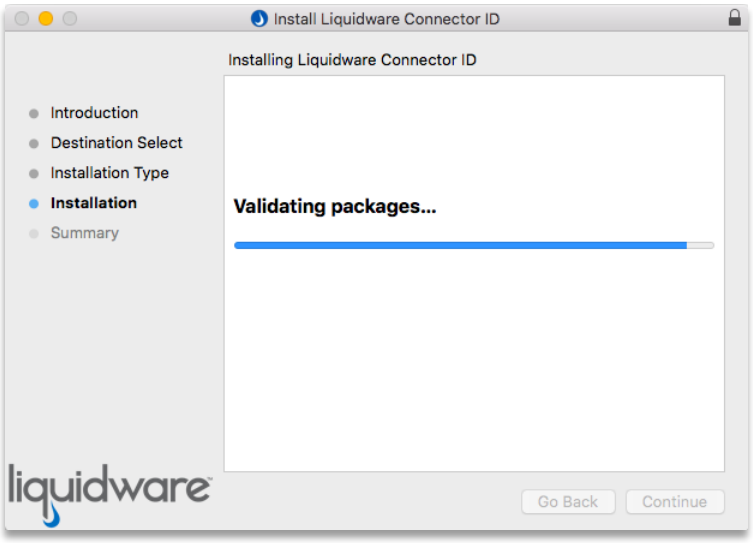
8. Follow the installation wizard to install the software on your local hard drive until it finishes.

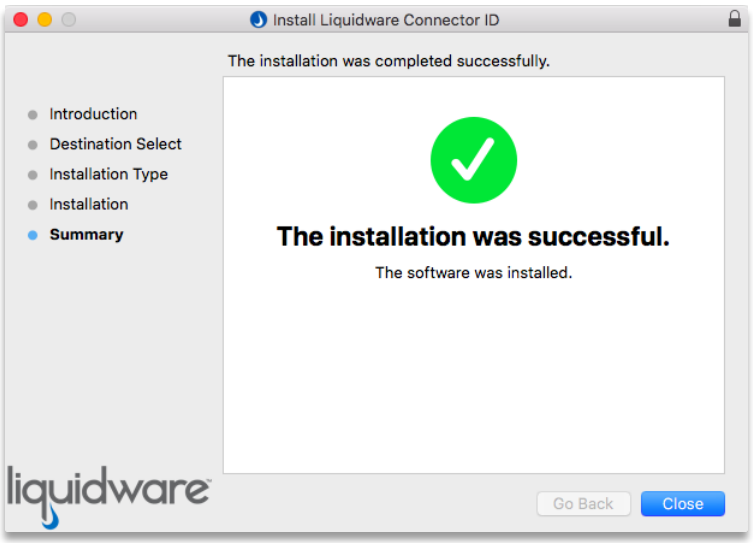



Install Liquidware Connector ID
Standard Install on "Macintosh HD"
Introduction
Destination Select
Installation Type
Installation
Summary
This will take 7.5 MB of space on your computer.
Click Install to perform a standard installation of this software on the disk "Macintosh HD".
Change Install Location...
Go Back
Install

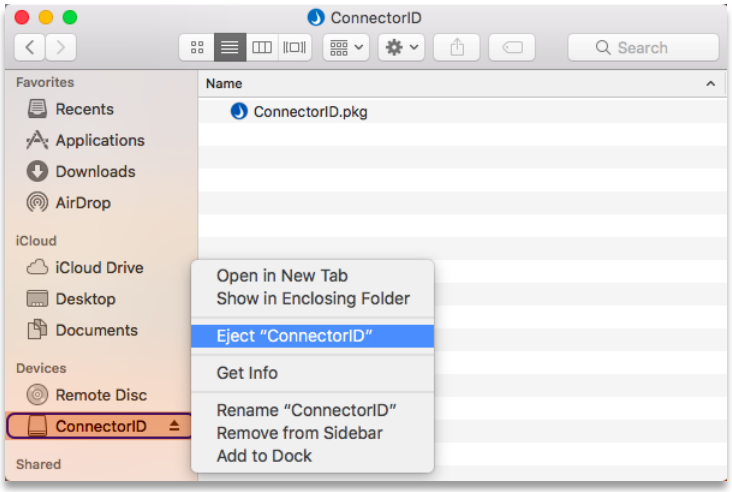

Install Liquidware Connector ID
Installing Liquidware Connector ID
Introduction
Destination Select
Installation Type
Installation
Summary
Preparing for installation...
Go Back
Continue


Install Liquidware Connector ID
Installing Liquidware Connector ID
Introduction
Installation
Summary
Installer is trying to install new software.
Enter your password to allow this.
User Name: Liquidware
Password:
Cancel
Install Software
Go Back
Continue





9. Once installed, please eject the ConnectorID Device from left pane by using the context menu **Eject "ConnectorID"** menu option.



MAC OS CID Key Commands & Files

1. Start the CID Key process by executing the following:
   $ /usr/bin/sudo /bin/launchctl load "/Library/LaunchDaemons/com.liquidwarelabs.connectorID.plist"

2. Stop the CID Key process by executing the following:
   $ /usr/bin/sudo /bin/launchctl unload "/Library/LaunchDaemons/com.liquidwarelabs.connectorID.plist"

3. Test if the CID Key process is running by executing the following:
   $ ps -ef | grep vs-helper

4. Remove or uninstall CID Key process by executing the following:
   $ sudo /Applications/Connector ID.app/Contents/MacOS/idenq -R

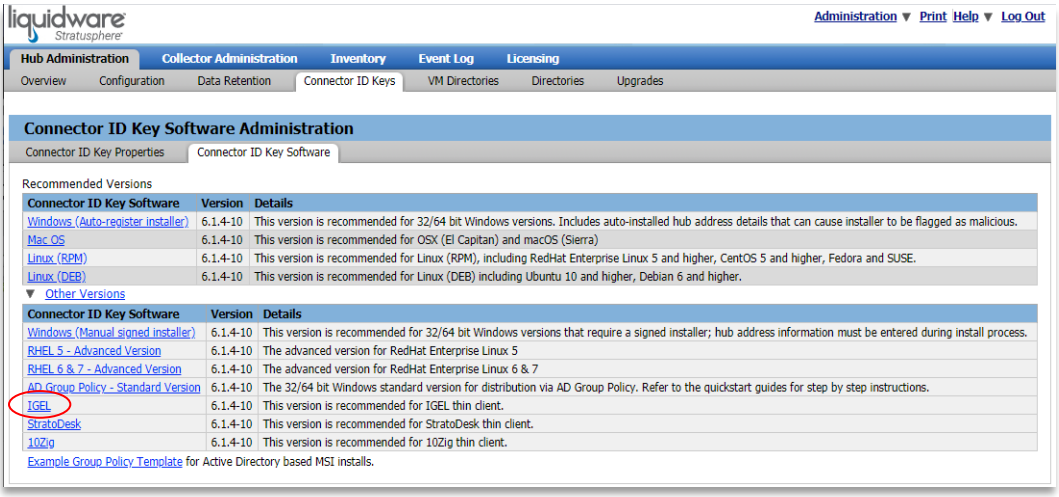
5. Log file locations: **/var/log/grd.log**
6. Data Directory locations:
   a. **/Library/Application Support/Connector ID.app/cert.txt**
   b. **/Library/Application Support/Connector ID.app/imgrcomm.txt**
   c. **/Library/Application Support/Connector ID.app/key_material/public/mgrcert.pem**
7. Binary file locations: **/Applications/Connector ID.app/Contents/MacOS/**

Appendix F: Working with Connector ID Keys on IGEL Thin Clients

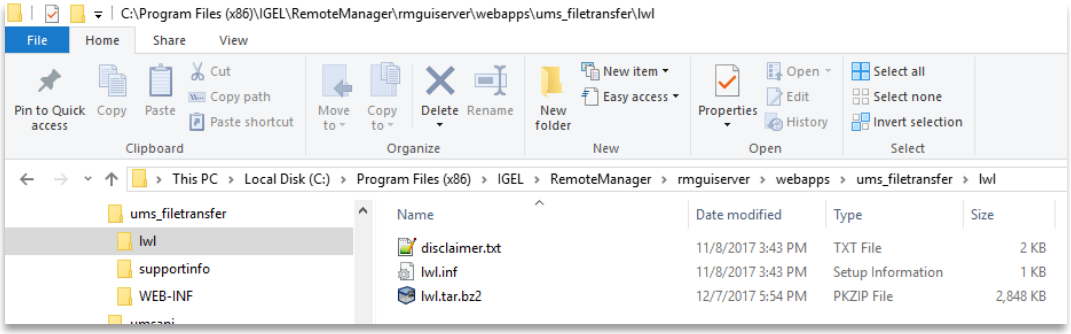
Installation Instructions

Here are instructions to install the CID Key on your IGEL Thin Clients using IGEL Universal Management Suite (UMS) Console:

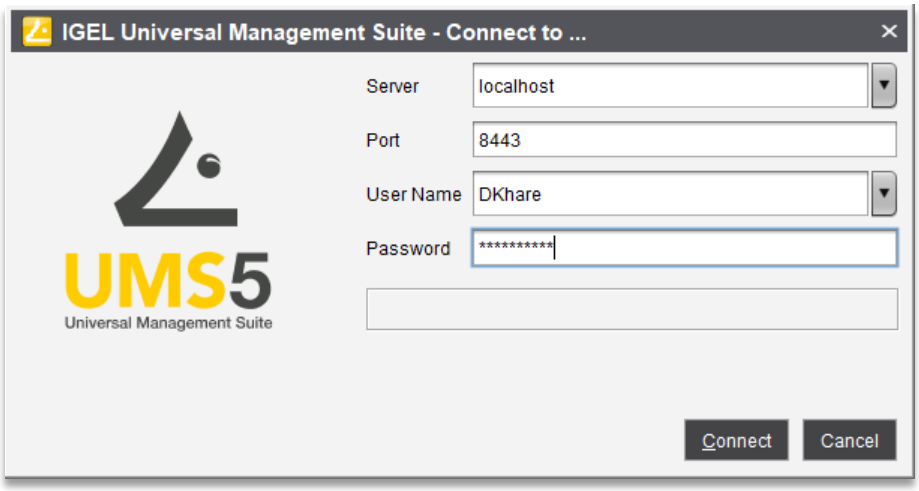
1. Log into your machine where you have the UMS Console as an administrator.
2. Using your local browser, log into the Administration section of the Liquidware Stratusphere Hub.
3. Navigate to the **Hub Administration > Connector ID Keys > Connector ID Key Software** tab and expand the **Other versions** section under the main download table. Use the "**IGEL**" link to download the IGEL ZIP from the Hub onto your local UMS machine.



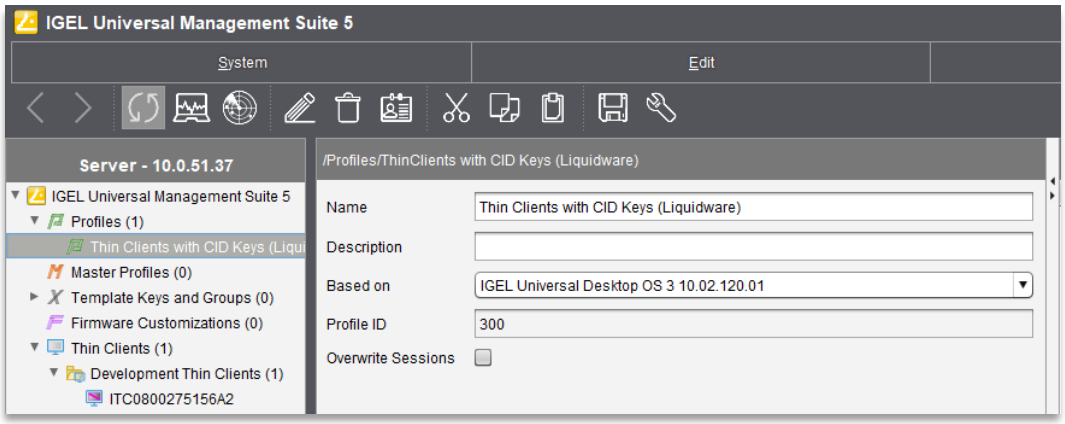
4. Navigate to the following folder to create a new folder **`lwl`** under `C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer\lwl`. Extract the contents of the ZIP file into this `lwl` folder. Once extracted, there should 3 files in this folder:



5. Check the accessibility of these files by opening the INF file in your favorite local browser using the following URL: http://[ums_server]:9080/ums_filetransfer/[name]/[name].inf – Keep this URL available as it will be needed in the step below.
6. Log into your UMS Console using your administrative credentials.

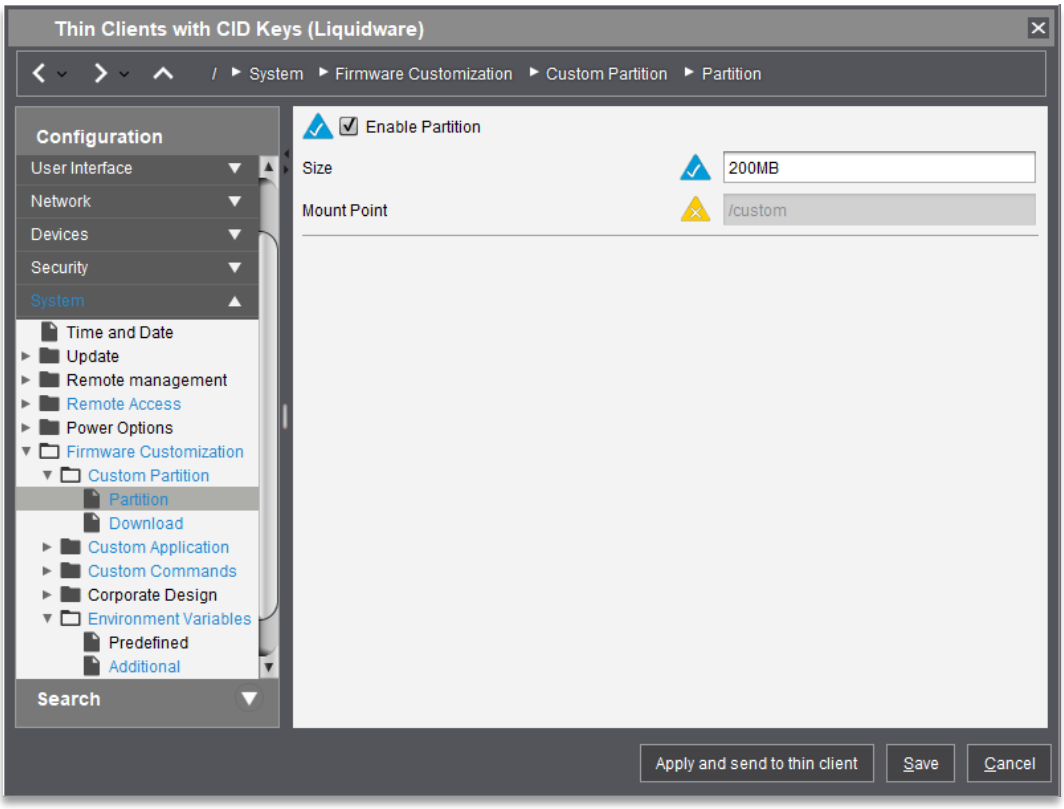


7. Once logged in to the UMS Console, within the left pane, navigate to your **Server - <IP Address>**, and expand **IGEL Universal Management Suite 5 > Profiles**.
8. Select an existing profile or make a copy of this existing profile to use as a starting point for installing the Stratusphere CID Key on your IGEL Thin Clients. For these instructions, we will call this profile **Thin Clients with CID Keys (Liquidware)**.

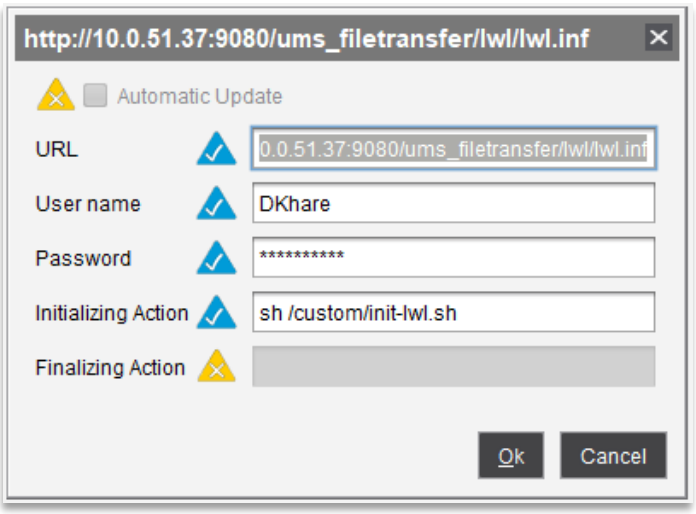


9. Right-click on **Thin Clients with CID Keys (Liquidware)** profile and select **Edit Configuration** menu option.
10. In the window that pops up, please expand the **Configuration > System > Firmware Customization** section on the left pane. Within this section, we are going to work with **Custom Partition**, **Custom Commands**, and **Environment Variables** sections to customize the CID Key installation.

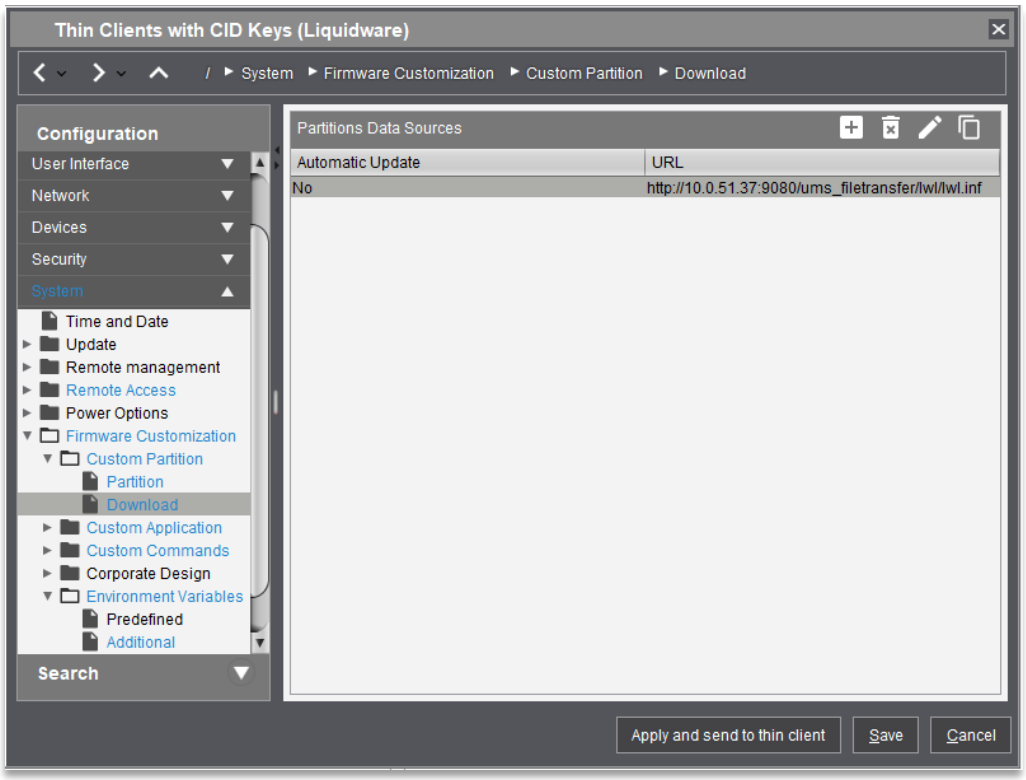
11. Expand the **Configuration > System > Firmware Customization > Custom Partition** section and click on **Partition**. On the right pane, check on **Enable Partition**, set **Size** to **200MB**, and use the default **Mount Point** which should be set to **/custom**. Click **Save**.



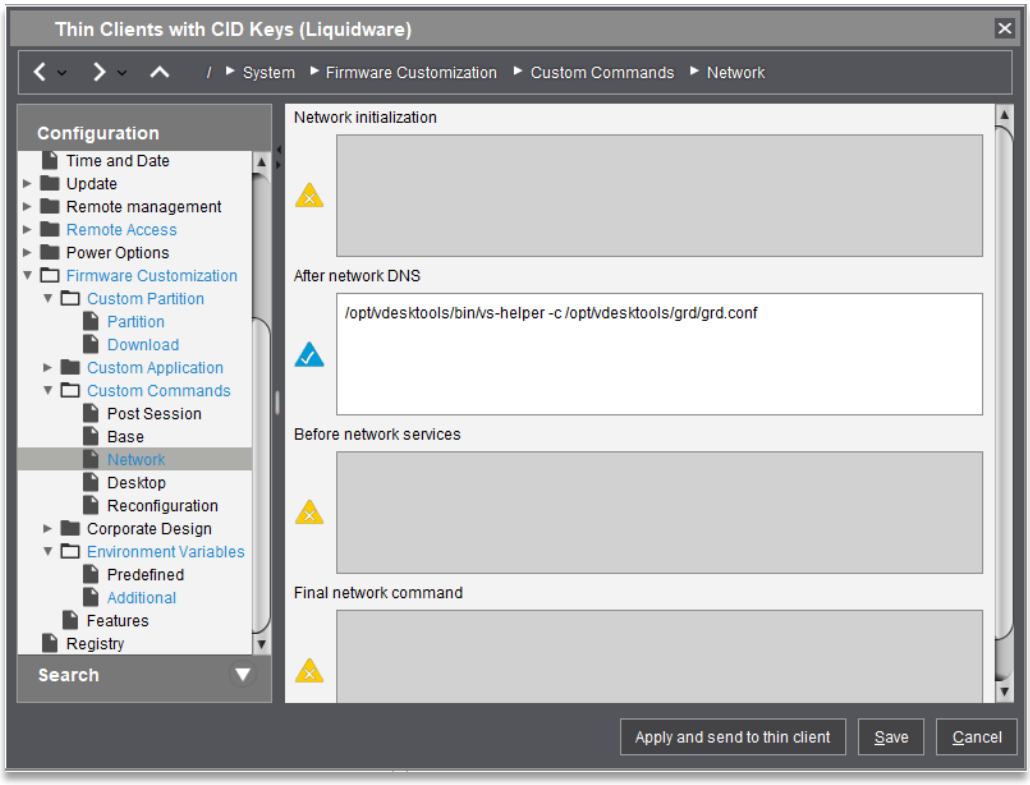
12. Now click on **Configuration > System > Firmware Customization > Custom Partition > Download** section. On the right pane, click on the **+** button to add a new Partitions Data Sources entry. For **URL**, copy and paste the URL tested in #5 above. Enter your credentials for **User Name** & **Password** to the UMS. Then enter the following for the **Initializing Action:** **`sh /custom/init-lwl.sh`** and the click **OK** to save it.



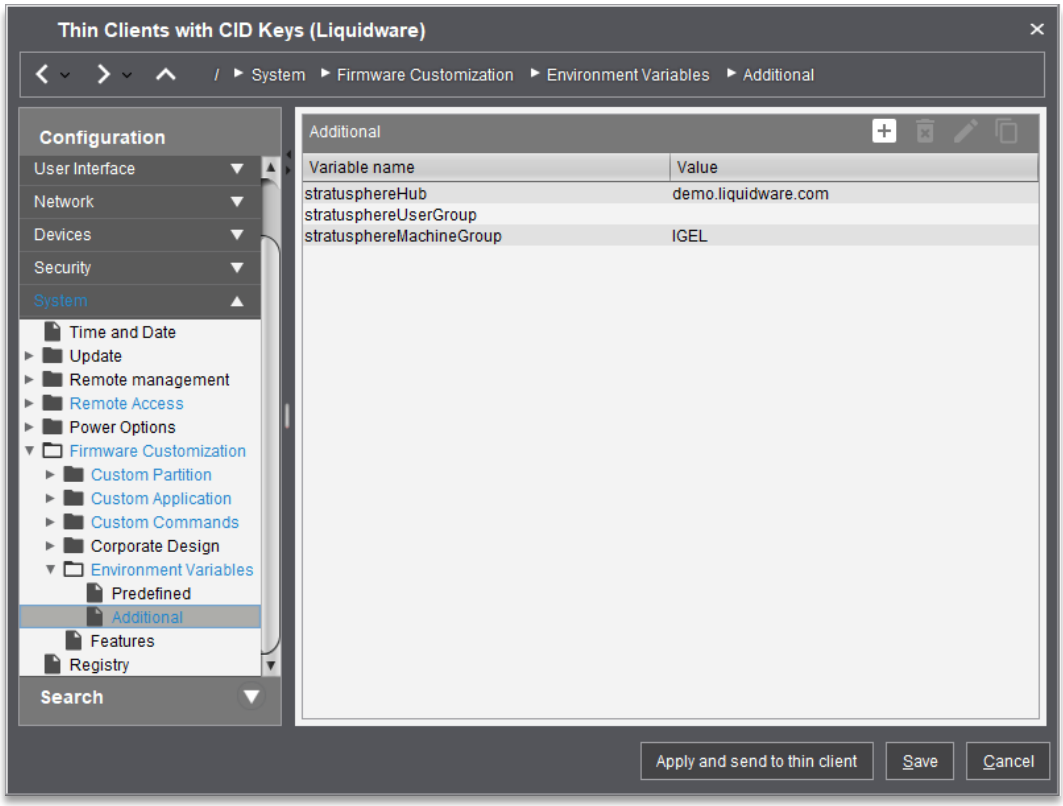
13. Now the new entry for Partitions Data Sources will be visible. Click **Save**.



14. Expand the **Configuration > System > Firmware Customization > Custom Commands** section and click on **Network.** On the right pane, enter the following in the **After network DNS** field box: **`/opt/vdesktools/bin/vs-helper -c /opt/vdesktools/grd/grd.conf`**
Click **Save**.



15. Expand the **Configuration > System > Firmware Customization > Environment Variables** section and click on **Additional.** On the right pane, use the + button to add three environment variables. The "**stratusphereHub**" variable name is a required variable that should contain the DNS name of the Stratusphere Hub (e.g. demo.liquidware.com) for the CID Key agent to register with the Stratusphere Hub. The "**stratusphereUserGroup**" and "**stratusphereMachineGroup**" variables are optional and should contain a text string to automatically register the user and machine into a pre-existing group within the Stratusphere Hub. Once you have entered the environment variable(s), click **Save**.



16. Now click **Apply and send to thin client** button to apply this profile to the thin clients within the selected Profile. You can also assign this profile to other thin clients. A reboot should now be required.
17. Log into any of the thin clients within the applied profile to verify whether the CID Key software is up and running by opening a terminal window and running the following command:

```
ps -ef | grep vs
```

```
root@ITC0800275156A2:/# ps -ef | grep vs
root     12946     1  0 Feb09 ?        00:13:09 /opt/vdesktools/bin/vs-helper -c /opt/vdesktools/grd/grd.conf
root     22978 22583  0 23:00 pts/0    00:00:00 grep --color=auto vs
```

The command lists all processes running on the machine, filtered by any process with '`vs`' in the process name. The screen shot of the output of this command is displayed above. It should display `/opt/vdesktools/bin/vs-helper` – this the CID Key process that is currently running, thus confirming that the CID Key is running.

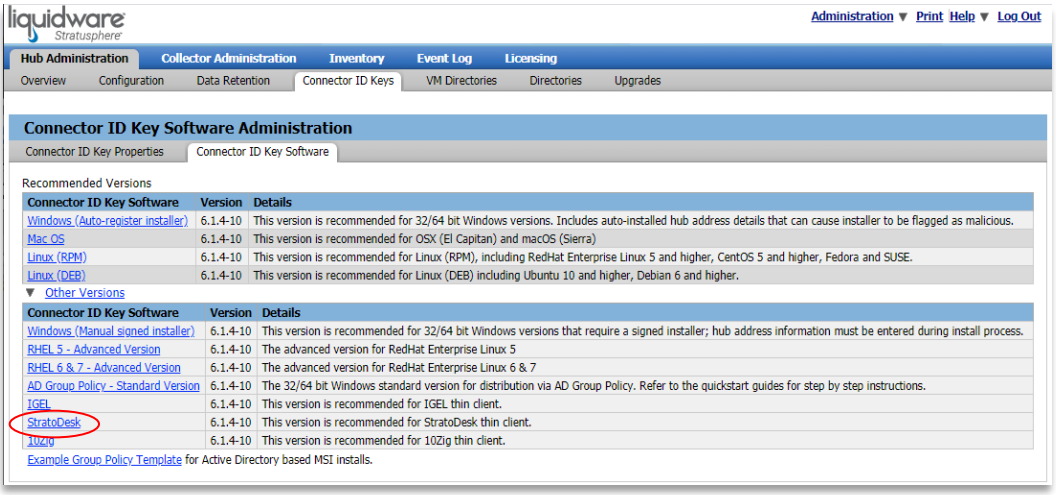
18. The CID Key is now installed and running on your IGEL Thin Clients.

Appendix G: Working with Connector ID Keys on Stratodesk NoTouch Thin Clients

Installation Instructions

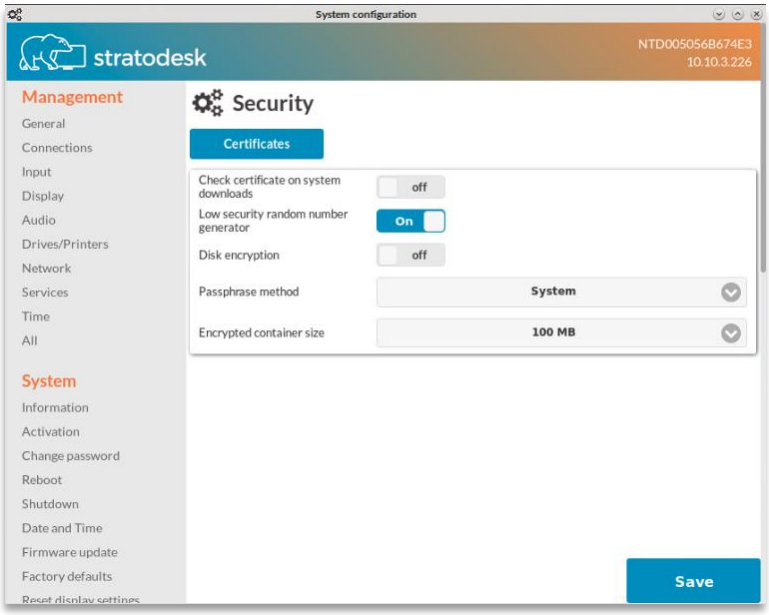
Here are instructions to install the CID Key on your Stratodesk NoTouch endpoints:

1. Using your local browser, log into the **Administration** section of the Liquidware Stratusphere Hub.
2. Navigate to the **Hub Administration > Connector ID Keys > Connector ID Key Software** tab and expand the **Other versions** section under the main download table. Look for the "**Stratodesk**" version of the Connector ID Key software.



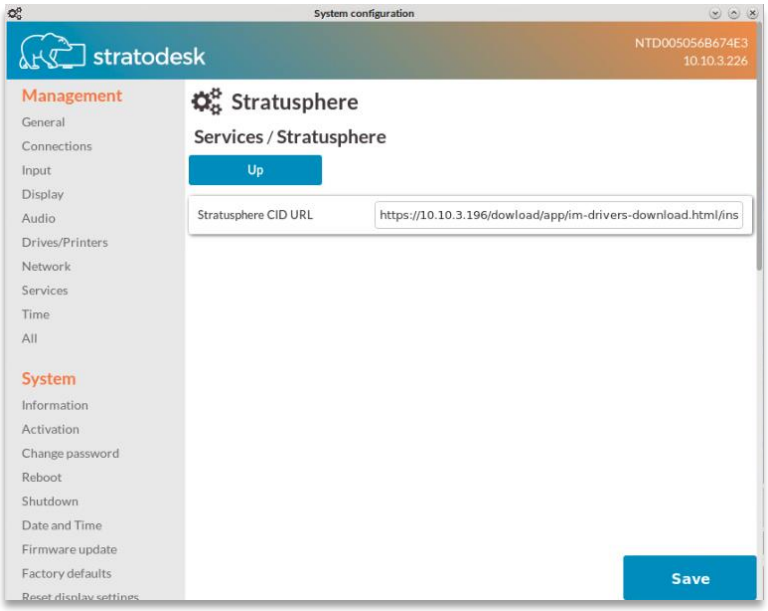
3. Login to your Stratodesk desktop as the root user.
4. Navigate to **Configuration**.

5. Go to **Management > All > Security**. Turn **"Check certificate on system downloads"** off and click the **Save** button.



6. Back at the main Configuration panel, go to **Management > Services > Stratusphere** and paste the following, using the IP/DNS address of your Stratusphere Hub and copying the Connector ID Key version number from the available Stratodesk version listed in the Hub:

   `https://<hub_address>/download/app/im-drivers-download.html/driverFile/install-connectorID-Key-6.x.x-x-stratodesk.zip`



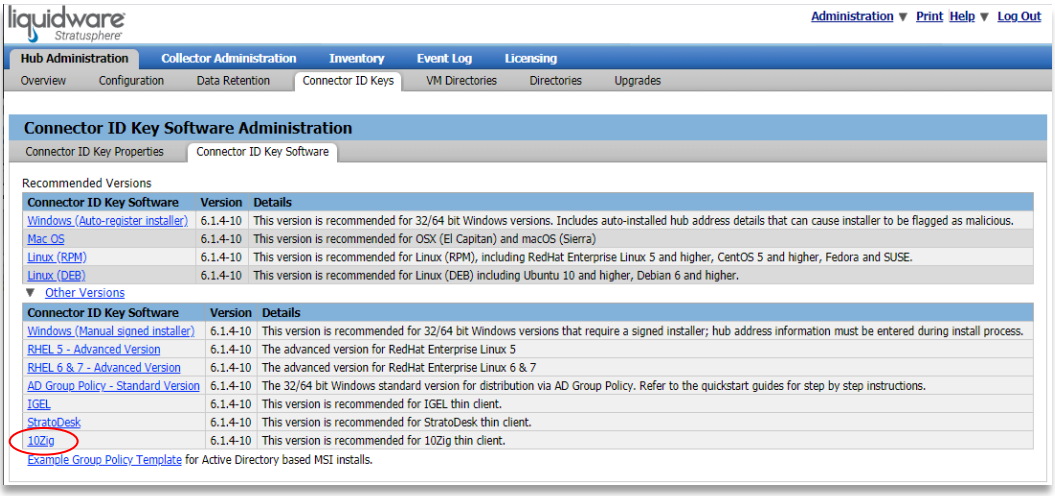
7. Click the **Save** button.
8. Back at the main Configuration panel, go to **System > Reboot** and confirm that you want to reboot the client.

Appendix H: Working with Connector ID Keys on 10ZiG Thin Clients

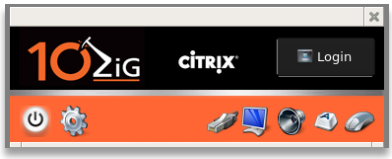
Installation Instructions

Here are instructions to install the CID Key on your 10Zig Thin Clients:

1. Using your local browser, log into the **Administration** section of the Liquidware Stratusphere Hub.
2. Navigate to the **Hub Administration > Connector ID Keys > Connector ID Key Software** tab and expand the **Other versions** section under the main download table. Look for the "**10Zig**" version of the Connector ID Key software.

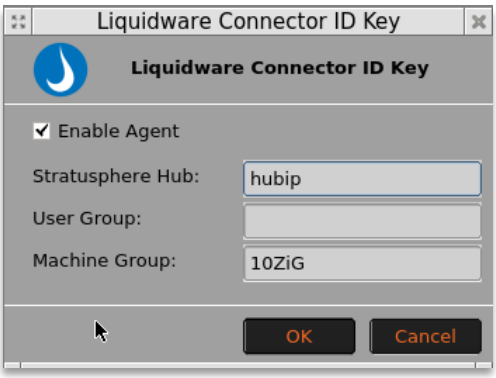


3. Login to your 10Zig Manager Console. Ensure you have updated your thin clients to the latest firmware.
4. On the Thin Client, navigate to the **Configuration Settings (cog)** icon.



5. Click on the **Liquidware CID Key** icon under the **System** category.

6. Click the checkbox to **Enable Agent**. Enter the IP or DNS address of your Stratusphere Hub appliance in the **Stratusphere Hub:** field. Enter the name of a pre-existing machine group into the **Machine Group:** field and click **OK** button to save changes.



7. The thin client will reboot and then register with the Stratusphere Hub appliance. After the configured call back period (default = 60 minutes) you should see data from the thin client being uploaded to the Stratusphere Hub.

Appendix I: Configuring WMI Performance Counters on Amazon WorkSpaces

Amazon WorkSpaces desktops are persistent virtual machines allocated to each user. The desktop comes with software installed based on options chosen and selected by your organization at the time of desktop configuration. Software can be installed on these desktops using standard or Amazon WorkSpaces based software distribution tools.

Depending on the type of desktop, sometimes the default install image does not come with the Teradici PCoIP Performance Counters installed and activated. In most cases, the performance counter DLLs are installed after making a request to WorkSpaces Support.

Liquidware cannot install these counters on AWS WorkSpaces instances. However, as part of the standard Liquidware Stratusphere Connector ID installation, we provide a script to find, register and activate the WMI Performance Counters DLLs, if they are present. This script is available under:

```
%PROGRAMFILES%\Liquidware Labs\Connector ID\admin
scripts\AmazonWorkSpacesTeradiciPCoIPCountersInstallPrep.bat.
```

Run this file once the DLLs are installed, and then from that point on PCoIP Performance Counters will be collected by the CID Key when users connect to their virtual desktops.