Visual Data Center

Administration Guide

Release 6.3.0

July 2020

Optimum Path Inc.

www.optimumpathinc.com
LEGAL NOTICE

Contact Optimum Path Inc Support

For your convenience, Optimum Path Inc provides one site where you can access the information that you need for our enterprise products. You can access the resources listed below by going to https://support.optimumpathinc.com.

- Online and telephone contact information for technical assistance and customer services
- Product and documentation downloads
- Other helpful resources appropriate for your product

OPTIMUM PATH INC.

Contents

1 Overview

The purpose of this document is to provide information on key tools and processed which help administer the Visual Data Center application. This document is not intended for end users, but rather is a tool to help support teams better manage and support implementation and support requests from end user customers.

Note, only experienced Linux System Administrators should execute the functions in this guide.

2 Versions and Patches

Each product release has 3 components in the release version: major, minor, patch-level. The standalone installs and the upgrade installers are responsible for establishing the major and minor versions. The patch installers (including cumulative, defect-fix or service pack) are responsible for setting the patch levels. Each patch installer has a patch-level number assigned to it. Patch installers must be applied in the exact numeric order of the patch level, for example 1.1.1, 1.1.2, 1.1.3, etc.

The version file, /opt/VDC/VERSION, is critical to the system. Every patch installer depends upon this file to determine if the pre-requisites are met before the patch can be installed. The version identifies the system version to the most granular level, which is needed for all support efforts. It is vital that this file in never modified manually. Use this file for read-only purposes.

```
cat /opt/VDC/VERSION
```

To find out the current release version on a deployed server, run: /opt/VDC/bin/vdcver. There are 3 components (separated by TABs) in the output: Product ID, Current Version and Base Version. The Base Version refers to the original product version when the product was first installed by the base installer. For example:

VDC 1 1 1 1 0 0

Most of the patch installers are released in an all-inclusive, cumulative format which includes all the required prerequisite patches required for the current patch. Although such patch installers are usually large in size, these installers provide a convenient way to automatically apply all the prerequisite patches to a system regardless of the current patch level of the system. For example, a cumulative v1.1.12 patch can be applied to a server running v1.1.3 or 1.1.9 and it will intelligently upgrade both systems to the 1.1.12 patch level.

Each patch installer is packaged as a bz2 compressed tar file format with extension of ".tar" or ".tar.bz2". Before the patch installer can be invoked on the command line, the patch package must be extracted under /opt/VDC/patch. The following 2 commands are standard for extracting and applying all patch packages:

1) `tar -C /opt/VDC -xvf /tmp/PATCH_NAME.tar.bz2`
   - Substitute /tmp/PATCH_NAME.tar.bz2 with the current path and actual patch package name
   - The command will automatically extract to /opt/VDC/patch directory

2) `/opt/VDC/patch/PATCH_NAME/install`

   NOTE: See the release notes for the specific patch you are applying. There are additional switches (- letter options) for handling model updates and monitoring template updates documented with the specific patch or upgrade.

3 Licensing Model

The application is activated by placing a valid license key into the /opt/VDC/.vdc directory. This key will enable the permitted number of licenses to be consumed by users with use of the application. Licenses for the application are counted as follows:

- FMA – Each floor mount asset is counted for licensing purposes regardless of how it is used in the application. This includes standard items such Generator, PDU, UPS, CRAC Units, Switchgear, Racks, Cabinets 2 and 4 Post Racks, etc.
- Device Specific – Using this license mode users can create an ala carte method of counting devices based on specifc usage within the application. For example Floor Facility and Monitored Facility can be tracked differently and there are three types of Rack licenses which can be used as explained below:
    - Managed – Allows rack building and port mapping for devices in the racks.
    - Limited – Allows for temperature and Rack PDU devices to be monitored within the rack and includes all Managed features.
    - Full – Allows for full monitoring of all devices within the rack and includes all Limited features.

Users can run the License Compliance report in the System report category to understand which model is being used for the application and to get current purchased, used and remaining licenses.

Only one license key can be in the /opt/VDC/.vdc directory or unexpected behavior can be presented by the interface.

After placing the key in the license directory, the following commands will enable the license for the application:

/opt/VDC/bin/setperm

reboot

4 License Configuration Options

A valid license activation key must be used in order for the application to perform correctly. AN invalid activation license key will prevent access to the application for all users. There are two types of license configuration options:

Server Hardware License

A server hardware bound license embeds the following server hardware signature within the key itself. As long as these information elements do not change on a given application server, the license will remain valid. Changes to these elements will require the generation of a new license activation key.

- Motherboard information
- CPU information
- Hostname of the server running the application

To apply a valid license key to a server using this model the following steps can be taken:

- Install application on the server
- Generate license request: /opt/VDC/bin/vdckeyreq > /tmp/license.txt
- Send license.txt file in to the support team for generation of a license activation key
- Receive license activation key from support
- Place license activation key in the /opt/VDC/.vdc directory. Ensure there is only one license activation key in this directory.
- Update permissions for the files in the system by running /opt/VDC/bin/setperm
- Reboot the server with the reboot command

Real Time License Server License

The Real Time License Server license is useful when the application server must be rotated among VM Hosts by technologies such as vMotion. A Real Time License Server is a separate running server instance, which is in the same network as the application server. The Real Time License Server itself requires a server hardware bound license in order to function properly. The Real Time License Server is bound to a specific server instance using the elements defined in the section above for the server hardware license. When license keys are issued for an RTLS implementation they will be issued in a pair for the RTLS and the application server. Once the keys are issued, the IP Address and URL for the application servers cannot be changed without the need to secure updated license activation keys.

With a Real Time License Server running on the same network, the application server can be bound to a specific IP address instead of the server hardware. The application server will then use a dynamic license to authenticate against the Real Time License Server to enable operations on the server.

Real Time License Server Hardware Specifications

- CentOS or Red Hat 6.x 64 Bit
- 2GB Memory
- TCP Port 16166 and 16167

Note, the RTLS server can run on the same physical or VM server as other applications.

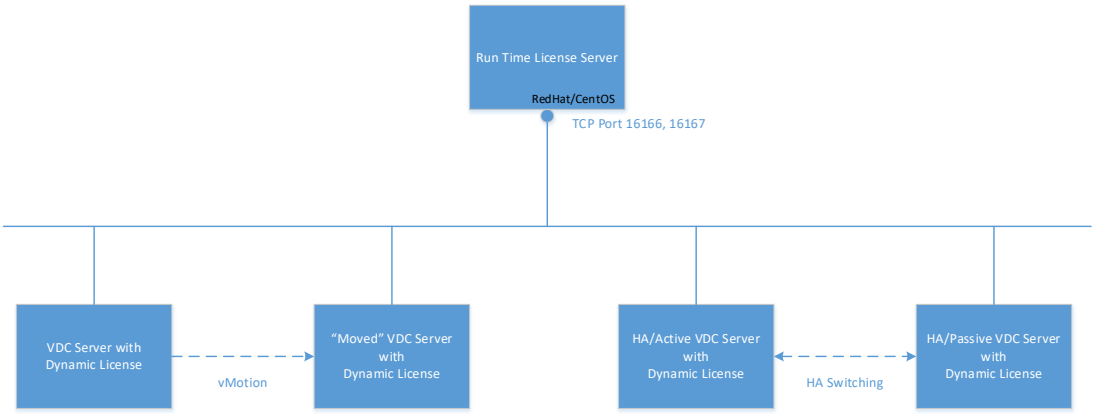


Figure 1.1 Run-Time-License-Server Model Illustration

RTLS Installation packages are created for each version of the application. Please ensure the correct version of the RTLS installation is used for your particular version and instance of the application. The following table provides guidance for the installation and configuration of an RTLS server and application instance. Note, update the file and folder references based on your version of the RTLS installation package.

#	Steps	Commands
1	Pick a Run-Time-License-Server to serve license for the VI server. The Run-Time-License-Server needs to: 1) Be a RedHat/CentOS 5.5/5.8 Server 2) Have at least 1GB FREE memory and 10GB Free disk space 3) Be on the SAME subnet as the application server	

	4) have the synchronized system clock with the application server (The time difference between the RTLS server and the application server can NOT exceed more than 30 minutes)	
2	Upload the RTLS installation package on to the RTLS server under /tmp directory	
3	Login RTLS server as the root user	
4	Extract the RTLS installation package	tar -C /opt -xvf /opt/RTLS-4.6-Installer.tar.bz2
5	Invoke the RTLS installer	/opt/RTLS-4.6-Installer/install
6	If the RTLS server has not been named yet, the user will see the hostname prompt to set the hostname. The RTLS server will be rebooted automatically when the hostname is set. Login as the root user again after the server is up and invoke the installer again: /opt/RTLS-4.6-Installer/install If the RTLS server is already named, this step is skipped.	* * * RTLS Installation(RTLS-4.6) * * * Red Hat Enterprise Linux Server release 5.8 (Tikanga)(64-Bit) OS found This server's host name is not set. Please be aware that the host name is linked with the license key. If you change the host name later, it may void any existing license keys. After setting the hostname, /opt/RTLS-4.6-Installer/install will reboot this server automatically. Please re-run /opt/RTLS-4.6-Installer/install after the reboot. Continue?(yes/no): yes Enter the host name for this server: MyRTLS
7	Set the system clock if needed and let the install script to finish	# /opt/RTLS-4.6-Installer/install * * * RTLS Installation(RTLS-4.6) * * * Red Hat Enterprise Linux Server release 5.8 (Tikanga)(64-Bit) OS found ping: unknown host rtls119 Bypass ping hostname: Unknown host Turning SELINUX to "disabled" Saving firewall rules to /etc/sysconfig/iptables: [OK] Current Firewall Settings: Decompressing and validating the installation package content. This may take a while. Please wait... The time difference between the RTLS server clock and its client clock can NOT be greater than 30 minutes. The current server clock shows Mon May 27 19:18:11 EDT 2013. Do you want to adjust it?(yes/no):yes Enter Year(between 11 and 99):13 Enter Month(between 1 and 12):5 Enter Day(between 1 and 31):27 Enter Hour(between 0 and 23):11 Enter Minute(between 0 and 59):14 Set year=13/month=05/day=27 hour=11:minute=14, correct?(yes/no):yes Mon May 27 11:14:00 EDT 2013 System clock is now set at Mon May 27 11:14:00 EDT 2013 bin/

		bin/rtlskeyreq bin/rtls RTLS is install correctly. Please install your RTLS license and run the reboot command as root user to reboot the server.
8	Generate a RTLS License Key Request	/opt/RTLS/bin/rtlskeyreq > /tmp/rtls.req
9	Send the following information elements to the support team: 1) RTLS license key request file: rtls.req 2) The current application server license 3) The application Server IP address from which the application Server will be connecting to the RTLS server.	
10	When the RTLS License Server key is delivered, copy it to /opt/RTLS/.vdc directory and restart the RTLS server.	/etc/init.d/rtls stop /etc/init.d/rtls start
11	Verify the rtls is started successfully by browsing file /var/log/messages and check to see if the following message is present: MM DD HH:MM:SS HOST rtls[..]: [YYYY:M:D HH:MM:SS]HC:953:16166	

Once the licensing needs have been addressed on both the Real Time License Server and the application server there is a configuration option which needs to be made on the application server to activate the Real Time License mechanism. The following table provides instructions on how to complete the application server configuration to fully enable the RTLS configurations.

#	Steps	Commands
1	Login to the application Server as the vdc user	
2	Invoke vdctools	/opt/VDC/bin/vdctools
3	Enter the menu item ID for “Enable Run Time License Mode”. Note that the menu item ID may be different according to the actual version of the application being used.	# /opt/VDC/bin/vdctools *** VDCTools *** 1) Session Timeout 2) Link with DCM 3) Configure Alarm Notification SMTP Server 4) Configure Report SMTP Server 5) Enable Active Directory 6) Disable Active Directory 7) Configure CA ITPAM Workflow 8) Configure Workflow SMTP Server 9) Test Gateway URL

		10) Configure Device Attribute 11) Reset User Password 12) Unlock a Locked User 13) Enable Run Time License Mode 14) Disable Run Time License Mode x) Exit
4	Enter the correct RTLS Server IP. Hit Enter when done.	Enter Your Selection: 13 Please ensure that the Run Time License Server is installed and is already running with the correct license. Do you still want to proceed to switch the license mode for the current server to Run Time License and restart all processes?(yes/no): yes Please enter the Run Time License Server IP: 10.10.10.192 Run Time License Mode is enabled. Please restart all processes or reboot the server. Press Enter to Continue...
5	Enter 'x' to exit VDCTools.	

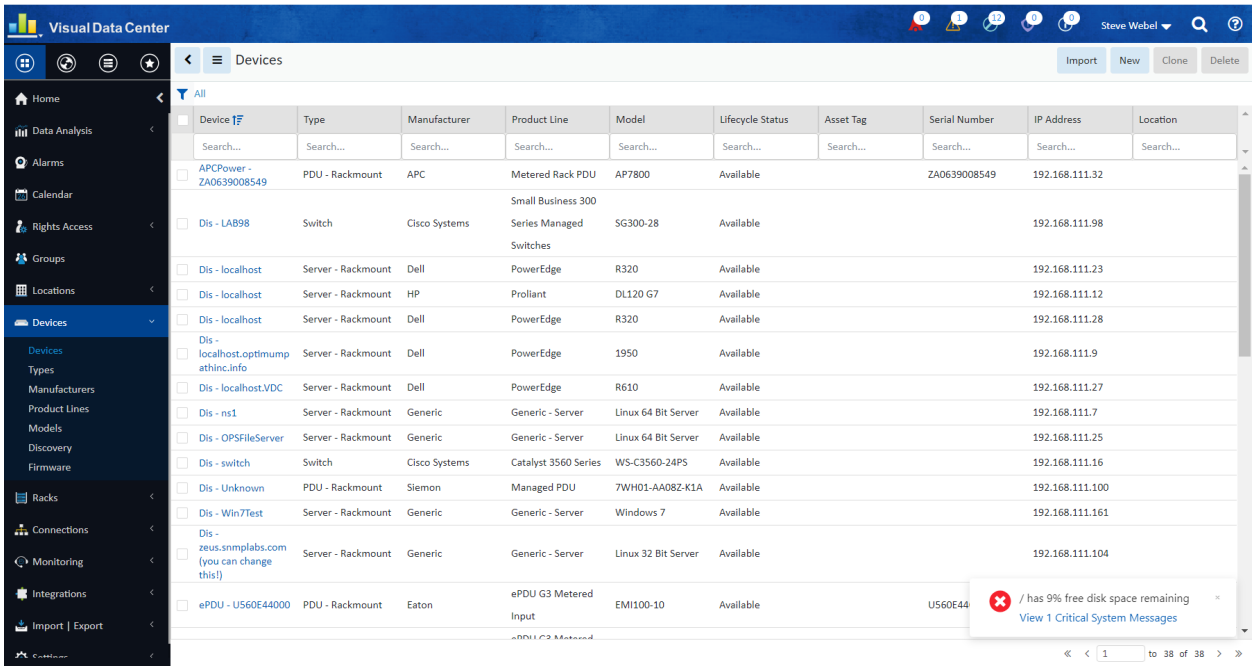
5 System Messages and License Grace Period

A System Messages mechanism delivers critical and warning notices. Messages displayed are related to the state of the application license and disk space warnings.

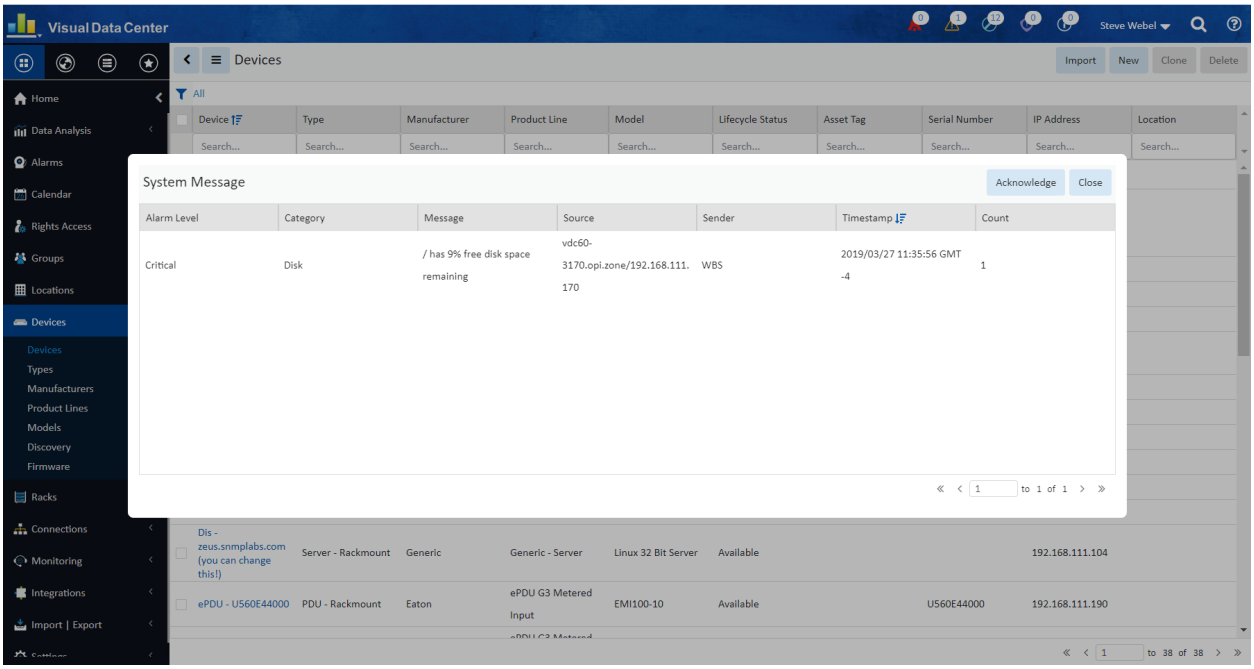
A grace period exists for production licenses. The grace period of 3 working days is activated if a license expires or the VM moves to a new server. Users receive critical and warnings messages so there is time to address the issues before access to the application is terminated.

Critical and Warning Messages

When a critical system message is triggered the system will present a red popup window in the lower right corner of the browser window with details about the nature of the message and a link to the System Messages window. The popup window will appear on the bottom right of the web pages indicating a user alert and provides a link for the user to click to access the System Messages list.



Clicking the link to view the system messages, the user will see the full list of current system messages related to the server and application instance. Users may click on an entry in the message table and Acknowledge the message. This will remove the message from the list.

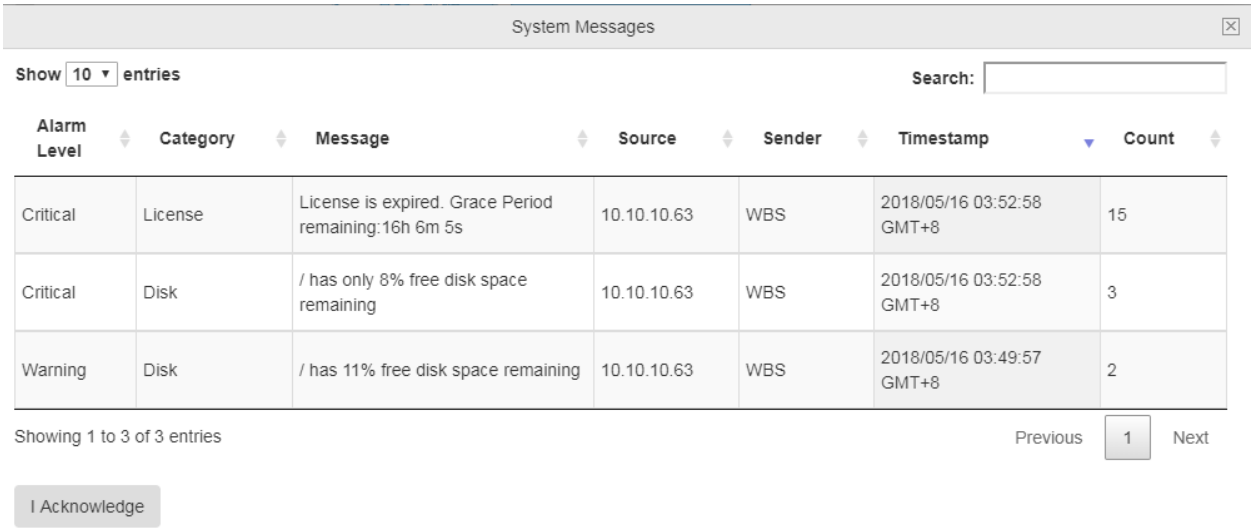


System Messages Window

The System Messages window displays the critical and warning messages. To open the System Messages window the user can click on the link in the red popup window or click on the red, yellow or green message indicator icons at the bottom of the screen.

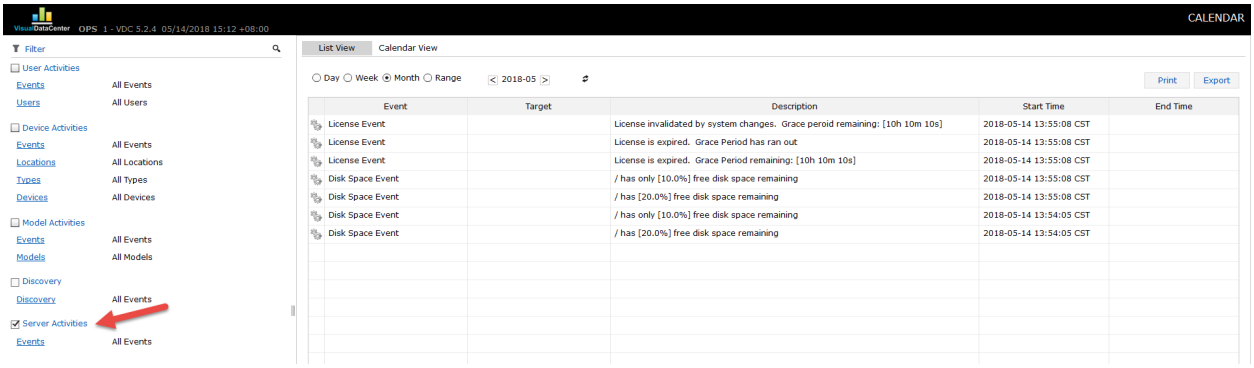
Use the Search field to filter the displayed messages.

The I Acknowledge button clears all the existing messages and resets the counters on message indicator icons to zero.



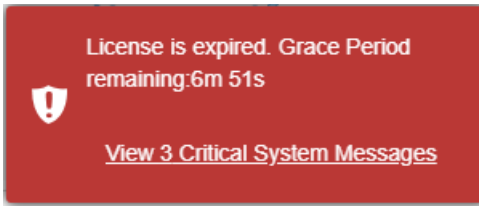
System Messages Added to Calendar

The system messages are also added as Server Activity events in the Calendar.



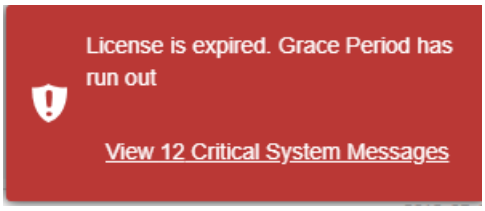
Grace Period is Activated when License Expires

When the application license expires due to date or a VM move, a grace period of 3 working days is activated. During the grace period users can access the application and a red critical message popup window will appear on the bottom right corner of the screen. The message displays the time remaining in the grace period and a link to view critical system messages. The red critical message popup window appears on all web interface tabs except Reports.



Grace Period Expiration

When the grace period is finished a red popup reports “License is expired. Grace Period has run out” and the user is terminated from the application.



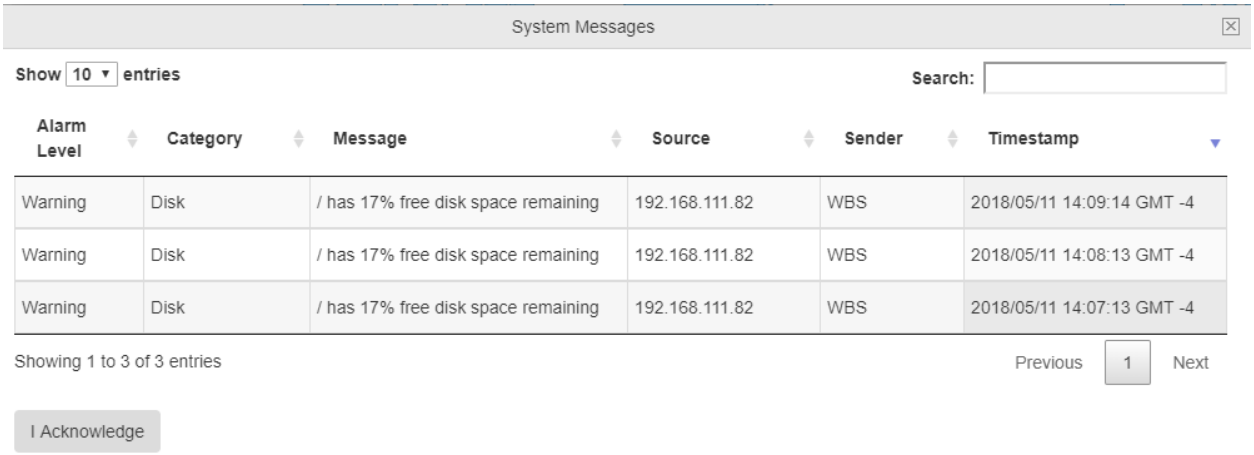
Login Message when Grace Period is Expired

If a user attempts to login to the application server after the grace period has expired an Error Message window will report: “The current application license key has expired or has an invalid

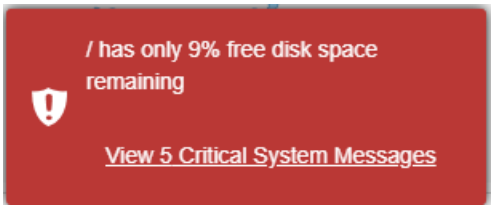
server hardware reference. Please access the Server Admin Tool to generate a new license request and submit to the support team." There will also be a link to the Server Admin Tool.

Additional Warnings and Critical System Messages

- **Remaining Disk Space between 10% and 20% -** triggers warning messages. These messages will not popup on the screen. The yellow icon will indicate that there are some number of warnings. Click on the yellow icon to see the warnings.

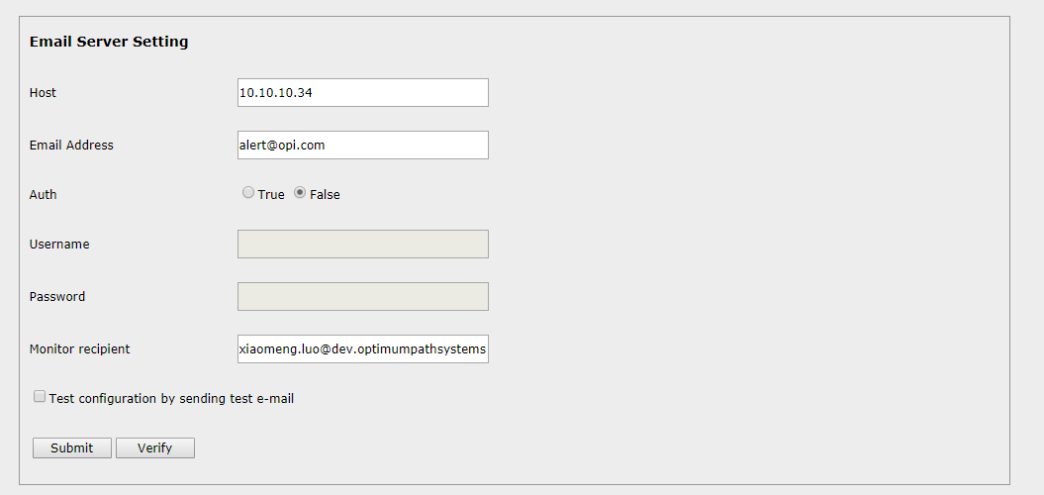


- **Remaining Disk Space less than 10% -** triggers a critical message. Critical messages will popup on the screen in the lower right.

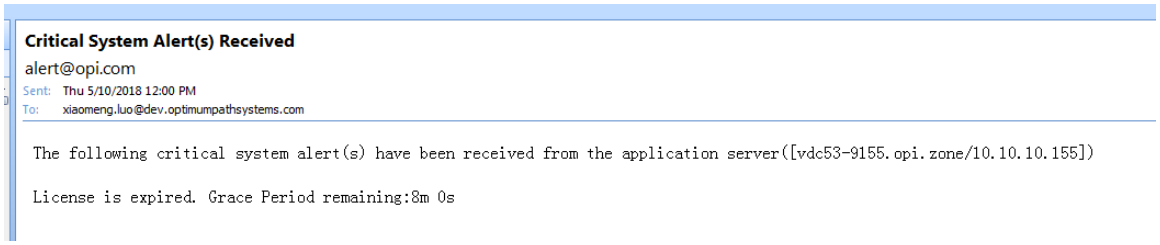


Critical System Message Emails

Critical system messages will be sent to the email address designated as the Monitor recipient in Server Admin Tool Email Server Setting configuration. See the Server Admin Tool section for configuration instructions.



When the license is expired, the recipient will receive the following email.



6 VM Conversion Process

The product's VM image can be distributed in either ESXi OVF format or VMWorkstation VMDK format. The following steps illustrate how to import ESXi OVF image and configure the image to work properly in the target network environment.

1) Import into ESXi

Login the VMWare vSphere client, select File->Deploy OVF Template… and browse to select the .ovf file in the downloaded OVF files on your local Windows PC. Click on the Next… button to move forward. You can change your VM guest instance name, pick storage options, etc. Please always select Thick Provision Lazy Zeroed as the Disk Format option. Click on the Finish button to start importing. Do not check the Power on after deployment checkbox.

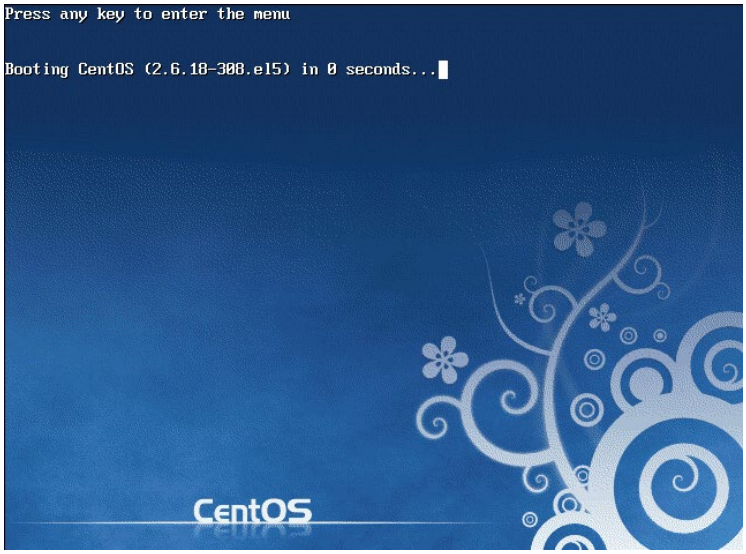
2) Allocate server resources

After the import is finished successfully, right click on the VM guest instance which was just created from the import process, and select Edit Settings…. Please make sure that at least 4 CPU cores and 8GB memory are allocated to this VM guest instance. For precise sizing requirements, please refer to the Excel Product Sizing Tool or consult a support engineer for assistance on the proper sizing based on intended production use of the application.

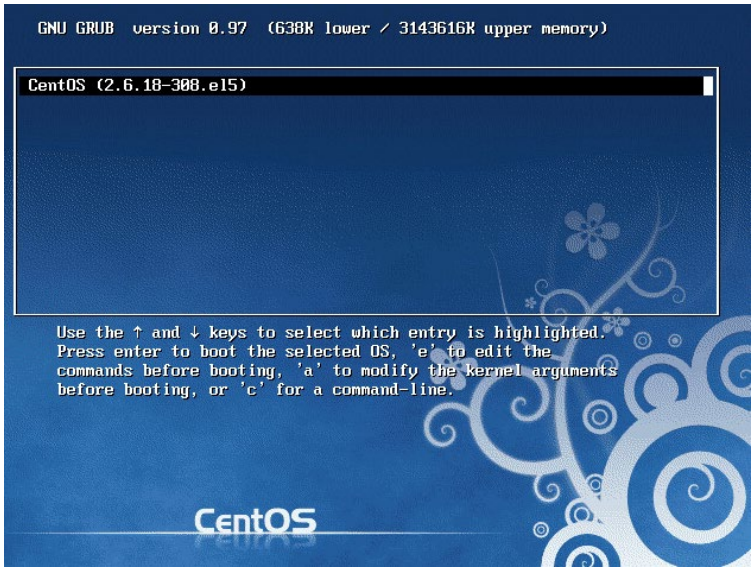
3) Boot up and set root password

Right click on the VM guest in the left VM Inventory List on the left hand side, select Power and then Power On to startup the VM guest. Click on the Console tab on the right to view the console. Although the default OVF root user password is usually Monit@r#1, it could change prior to the creation of the OVF image. If the default root password does not seem to work, please follow these steps to reset the root user password:

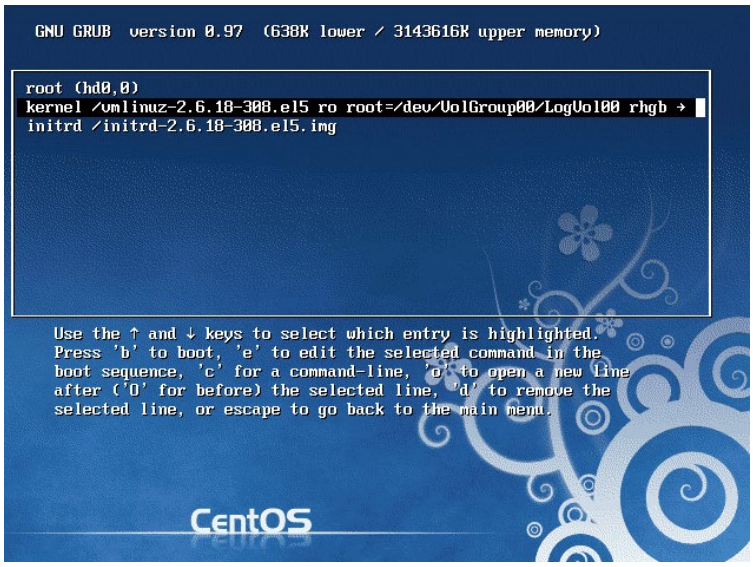
a) Right click on the VM guest in the left VM Inventory List on the left hand side, select Power->Reset. Watch the console closely. When the following boot screen pops up, hit the e key to interrupt the automatic booting process.



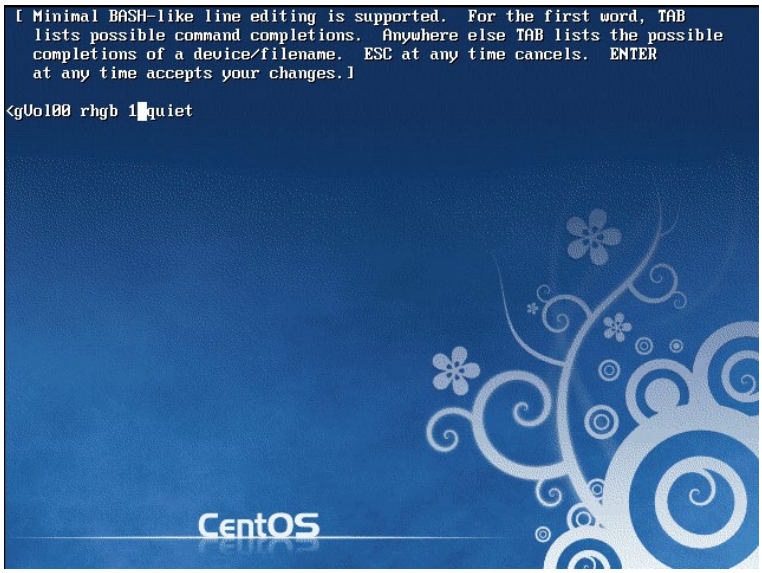
b) Click the e key on the following screen.



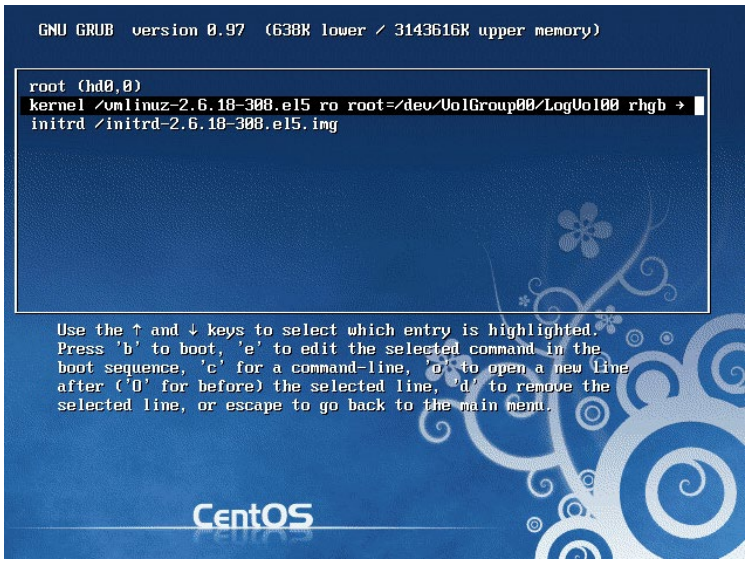
c) Use the arrow key to move to the row which has rhgb string and click the e key again.



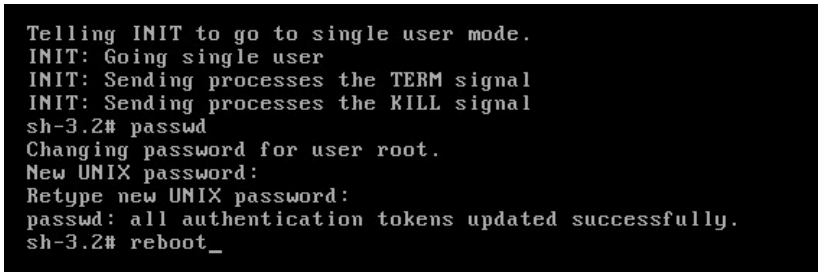
d) Add number 1 after rhgb by using the arrow key. Make sure there is a space before and after it. Hit the Enter key.



e) Click the b key to continue the booting process at the following screen:



f) At the following command prompt, enter passwd to reset the password for the root user. Enter reboot to restart the VM guest.



4) Setup IP address and host name

Login to the console with the root user password. Set up the correct IP address and hostname for the VM guest. Please make sure that both new IP address and hostname are shown correctly in the /etc/hosts file.

5) Change application IP settings

Use the following command to find out the previous IP address for the application. This is the IP address which was configured when the OVF files were created:

grep vdchost-server /etc/hosts

Run /opt/VDC/bin/newip OLD_IP NEW_IP to change the IP address to the new IP address in use for the target network environment. For example, if the previous IP is 199.59.80.20 and the new IP is 192.169.117.16, then run /opt/VDC/bin/newip 199.59.80.20 192.169.117.16.

6) Change application URL settings

Use the following command to find out the previous URL of the application. This is the access URL for the application which was configured when the OVF files were created:

grep VDCURLHOST@tomcat /opt/VDC/.conf

Run /opt/VDC/bin/newurl OLD_URL NEW_URL to change the URL. For example, if the previous URL is demo.hostname.com and the new URL is myapp.com, then run /opt/VDC/bin/newurl demo.hostname.com myapp.com.

7) Generate a License Request

Since the hardware profile of the server has been changed to the new VM host, the new VM instance will need an updated license to start its applications. Please run /opt/VDC/bin/vdckeyreq > /tmp/license.txt to generate a license request and email the license.txt file to the support team for the new license activation key.

8) Install the License

When the new license file is received, SCP the file into the /opt/VDC/.vdc on the VM guest without any modifications to the either its name or content.

Run /opt/VDC/bin/setperm after the license file is installed as root user.

9) Reboot

Run reboot as the root user. Depending upon the specific platform configuration it may take up to 10 minutes for the OS and application to start up completely.

10) Change Application Admin User Password

When you are at the application's login page the default access combination is user=admin and password=Monit@r#1. If this default combination does not work, then ssh into the server as the root user and run /opt/VDC/bin/vdctools and choose the Reset User Password option.

7 System Components

The installed application consists of the following functional modules:

1) Master database instance
2) Master Server
3) Probe database instance
4) Probe Server

When the above modules are running within a single physical/virtual server, it is referred to as the all-in-one architecture. Since the all-in-one architecture is much simpler to deploy and maintain, it is the preferred architecture for many customers. Introducing a distributed server architecture complicates the installation as well as the network and server readiness tasks which need to be completed by the customers. Unless needed due to scale or special technical requirements we should always recommend and install the all-in-one solution.

Within the master database there can be hundreds of Postgres database processes running against the vdc_repos database instance. All of these processes are owned by the postgres user. Do not attempt to interfere any of these postgres user processes manually from the command line.

The main process which runs inside the Master Server is the Tomcat server, which runs as two separate jsvc processes. One jsvc process is owned by the root user and the other one is owned by the vdc user. Both processes can be discovered by running the following command:

ps -ef|grep jsvc|grep -v grep

The probe database only runs a couple dozen or less Postgres processes accessing the vdc_sdb instance. These processes are responsible analyzing and storing real-time device monitoring data. Do not attempt to disrupt these processes from command line to avoid possible data loss.

There are 2 main processes running with the Probe Server:

1) The vms process which is responsible for all discovery, monitoring and control activities. The specific vms process information can be discovered by running this command:
   ps -ef|grep vms|grep -v grep

2) The database replication subsystem is responsible for synchronizing the individual probe database with the master database. It runs as a pair of vdc owned Java processes, which can be discovered by running this command:
ps -ef|grep -i replication|grep -v grep

8 Database

Postgres database 9.4.5 is used as the main database engine for the application. The Postgres 9.4 manual is available https://www.postgresql.org/docs/9.4/static/index.html for reference and details on the database solution.

There are two types of database instances in the application. One database is related to the master server and the other database is related to the probe server. One database instance is used for each probe server deployed in the solution.

The master database instance serves the master server and is the complete application data repository. This database may or may not reside on the actual master server. For scalability, this master database can be moved to a dedicated server. Note, this document does not cover details of distributed server solutions. Please consult a support consultant for more details on architectural options for the implementation of the application processes when multiple physical or virtual servers are required.

The probe database instance serves a given probe server and it typically resides on the same probe server. The probe database only stores the necessary information to support a specific probe server's operation. Each probe database is responsible for synchronizing with the master database server for the data elements that it requires.

The application is a database driven system and it is very important to ensure the integrity of database with the following measures:

1) Ensure the /usr/local/pgsql/ file system has at least 20GB FREE disk space at any given time. This is due to the background database maintenance activities which often require a large amount of temporary database table space to be created. If the database server runs out of space during these activities, there is a high likelihood for data corruption to occur.
2) Always shutdown the Postgres database gracefully as the postgres user with the command /usr/local/pgsql/bin/pg_ctl -D /usr/local/pgsql/data stop -m i whenever a database shutdown is needed. Never use the kill -9 command to terminate any Postgres process or shut down the server ungracefully (without going through the proper shutdown sequence for the specific run-level).
3) The application database schemas for the master database or probe database are designed for internal access by this application only. Do not attempt to read the application database tables directly for integration purposes. The database schema can

change between patch levels. The application provides specific API calls for 3rd party integration. Use the proper API set for required integration instead.

4) Access to the database is well encapsulated by all application tools and patches. There is no need to issue SQL commands via the SQL console for application system administrators.
5) Both the disk I/O throughput and physical memory size impact the database performance significantly. On any production server, 300MB/second or above disk I/O is recommended. Although 16GB physical memory size is suggested for production instances of the application, 24GB or 32GB physical memory size may be required for servers to efficiently handle thousands of active device monitoring or more. For specific details regarding scalability and suggested specifications for a larger deployment, please consult a support consultant who can analyze implementation requirements with an architecture sizing spreadsheet.

9 Server Ports

The application operates on multiple network ports to establish and maintain communication between server components and monitored devices. Customers must enable these ports during the setup of the server architecture in order for the system to operate as expected. The following summarizes the required ports in the application architecture.

From 3D Client to Master Server

#	Port Type	Port	Port Usage
1	TCP	80/443	Web Services
2	TCP	12002	Smart Panel Services
3	TCP	12003	License Services
4	TCP	12006	Alarm Services

From Web Client to Master Server

#	Port Type	Port	Port Usage
1	TCP	80/443	Web Server

From Master Server to Probe Server (Distributed Setup)

#	Port Type	Port	Port Usage
1	TCP	22	Remote Execution
2	TCP	5432	DB Access
3	TCP	80/12001	Remote Messaging

From Probe Server to Master Server (Distributed Setup)

#	Port Type	Port	Port Usage
1	TCP	5432	DB Access
2	TCP	12006	Alarm Services

From Master DB to and from all servers (Distributed Setup)

#	Port Type	Port	Port Usage
1	TCP	22	Remote Execution
2	TCP	5432	DB Access

From Probe Server to SNMP Monitored Devices

#	Port Type	Port	Port Usage
1	UDP	161	SNMP Query

From SNMP Monitored Devices to Probe Server

#	Port Type	Port	Port Usage
1	UDP	162	SNMP Traps

From Probe Server to Modbus Monitored Devices

#	Port Type	Port	Port Usage
1	TCP	502	Modbus Query

From Probe Server to Bacnet Monitored Devices

#	Port Type	Port	Port Usage
1	TCP	47808	Bacnet Query

From Bacnet Monitored Devices to Probe Server

#	Port Type	Port	Port Usage
1	TCP	47808	Bacnet Query

Internal Monitoring Ports on the Server

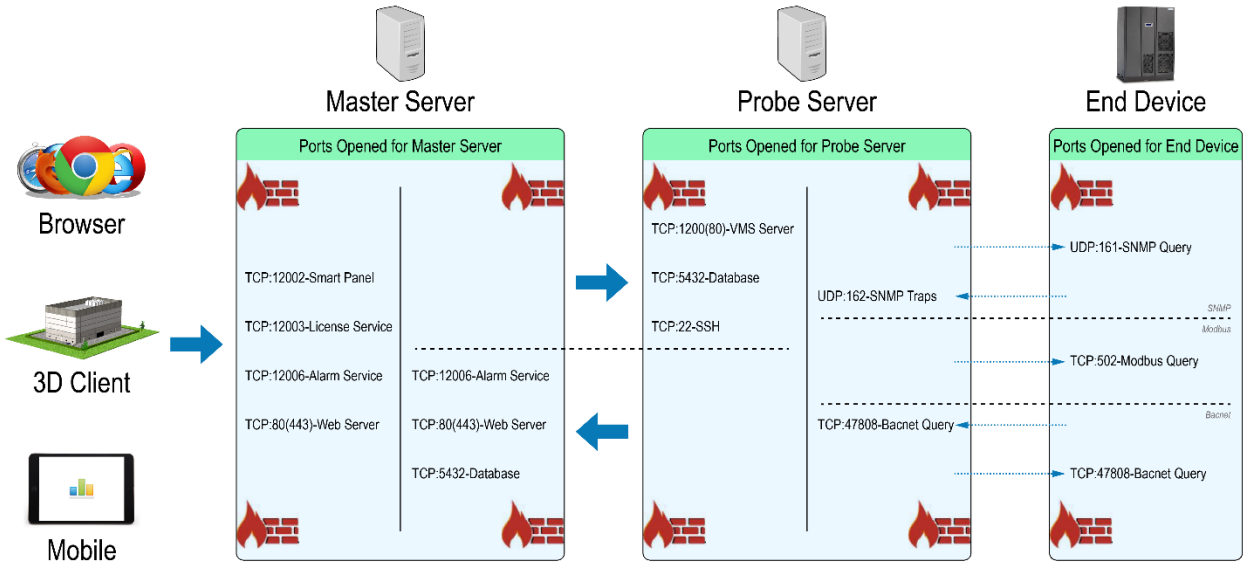
#	Port Type	Port	Port Usage
1	TCP	8015	Default VMS/probe port*
2	TCP	7015	Alternate VM/probe port*
3	TCP	9200	Elasticsearch
4	TCP	12008	VDC Core Server

* After Installation, if the probe log shows port 8015 is occupied by another application, then switch to the alternate VMS/probe port 7015. To make this change, use vi to edit the /opt/VDC/monitor/vms/conf/server.xml file and change the port to the alternate port. Following this change, the application services must be restarted to accept this change to the configuration file with the following commands:

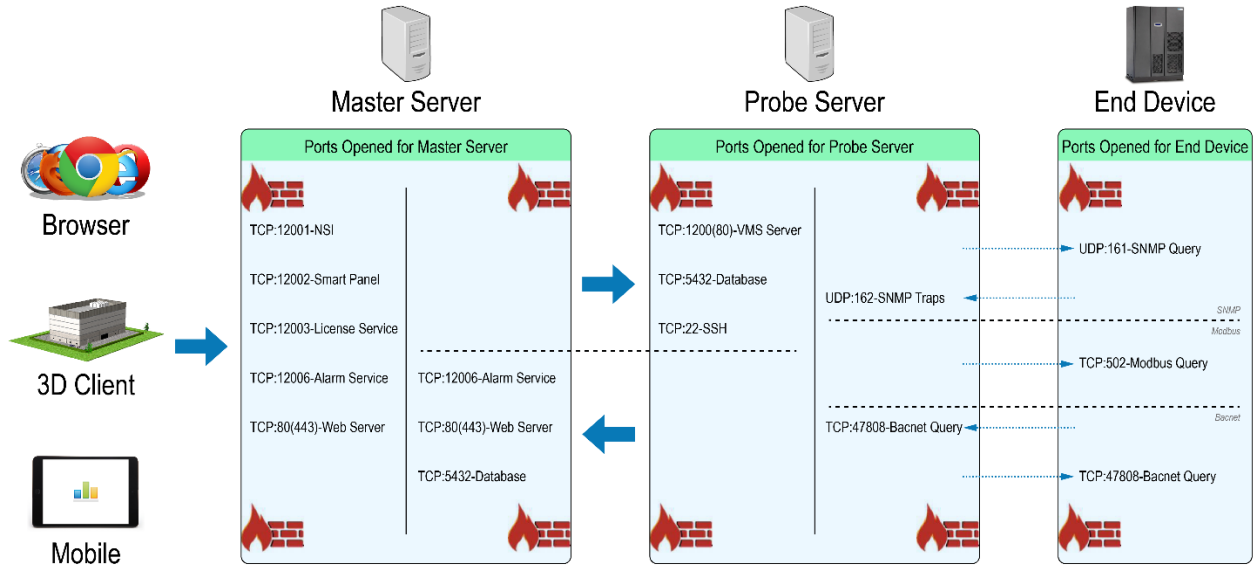
/etc/init.d/vdc stop

/etc/init.d/vdc start

VDC Ports Diagram (version 4.12 and above)



VDC Ports Diagram (prior to version 4.12)



Open Ports on Application Server

Follow the below steps to open ports on the application server (Redhat/CentOS 6.x servers only):

#	Description	Commands
1	Open the configuration file using the vi edit	vi /etc/sysconfig/iptables

2	You should see the following script (or something similar)
	
	`# Firewall configuration written by system-config-securitylevel`
	`# Manual customization of this file is not recommended.`
	`*filter`
	`:INPUT ACCEPT [0:0]`
	`:FORWARD ACCEPT [0:0]`
	`:OUTPUT ACCEPT [0:0]`
	`:RH-Firewall-1-INPUT - [0:0]`
	`-A INPUT -j RH-Firewall-1-INPUT`
	`-A FORWARD -j RH-Firewall-1-INPUT`
	`-A RH-Firewall-1-INPUT -i lo -j ACCEPT`
	`-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT`
	`-A RH-Firewall-1-INPUT -p 50 -j ACCEPT`
	`-A RH-Firewall-1-INPUT -p 51 -j ACCEPT`
	`-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT`
	`-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT`
	`-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT`
	`-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`
	`-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited`
	`COMMIT`
	
	Now add the necessary ports.
		–A RH-Firewall-1-INPUT –p tcp –m tcp --dport *'port number'* –j ACCEPT

3	Save the file in vi, and restart your firewall	service iptables restart

10 System User Accounts

The Visual Data Center application utilizes three primary Linux user accounts to manage all processes and functions within the operating system: root, vdc, postgres. Each of these users has specific roles and functions it performs within the application. Information on each account is provided below. The purpose of three users is to divide up responsibilities for quality control purposes.

root User

Root user is the default user when logging into the application server. The majority of administrative functions will be performed while logged in as the root user.

vdc User

The vdc user must stop and start all application processes and has some cron functions which operate under this user login. To become the vdc user enter “su – vdc” at the command prompt when logged in as root. To return to your original user status enter “exit” at the command prompt.

postgres User

The postgres user is used to gain access to the PostGres SQL database which is used in the application. To become the postgres user enter “su – postgres” at the command prompt when logged in as root. To return to your original user status enter “exit” at the command prompt.

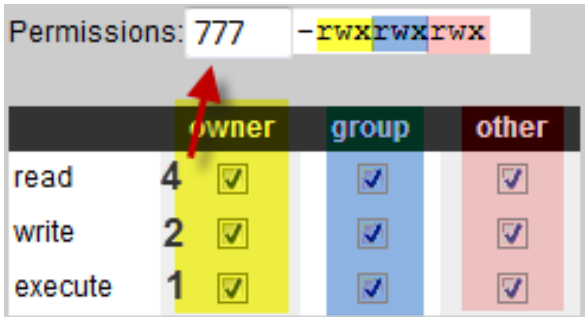
*****Do not run processes that are assigned to different users*****

User Control

chmod

http://ss64.com/bash/chmod.html

"change mode" – changes the permissions of each file according to mode, where mode describes the permissions to modify. Mode can be specified with octal numbers or with letters. Using letters is easier to understand by most people.



For every file there are three security settings: owner, group, permissions (read/write/exec)

- rwx:
    - r – read - 4
    - w – write – 2
    - x – execute – 1

chown

http://ss64.com/bash/chown.html

"change owner" – change the user and/or group ownership of each File to a new Owner.

Use this command if a process is run by the wrong user. Running a process with the wrong user, permissions are rewritten which can cause major problems within the application.

11 File System Structure

The application is installed onto a server with one of the Linux operating systems and all application files are contained within the standard Linux file management system. The following information provides high level detail on the key file/folder locations used in the operation of the software platform.

By default, the application files will be installed on the Linux file system in the /opt/VDC folder. The majority of all application files and functions are performed within this directory. The /opt/VDC folder has several sub-folders which provide core functions to the application. The following is a brief description of the key folders in this structure of the /opt/VDC system.

- bin – Many of the key functions in the application are controlled with scripts located in this directory. These scripts are called in cron jobs and the system start/stop scripts. Do not use these scripts if not familiar with the function they perform. Contact a support member for information on the function or process if needed.
- db – Contains scripts, logs and configuration files related to the database of the application.
- filedepot – Contains a series of folders where the files uploaded to the File Depot are stored. Please be aware this folder contains a bucketized set of folders to ensure the number of files in a given folder is distributed thru the file system.
- ibuilder – The ibuilder folder manages the search function and indexing of the database in the application.
- monitor – This folder contains the files necessary for the application's core monitoring function. SNMP, IPMI and MODBUS probes and dispatchers, log files and configuration files are kept in this folder.
    - monitor/share/spool – This folder within the monitor directory contains files that the trend charts will use to show the historical trending data.
- tomcat – The tomcat folder is where the web server files are located and managed.
- vdcmon – "VDCMON" reports process errors to an email. If one of the core application processes (probes, dispatcher, tomcat, etc) goes down then a notification email is sent

to an email address as a means of notification. This folder contains the files necessary for this feature to function properly.

- The /usr/local/pgsql folder contains the sql database information.
- The startup/shutdown script is located in the /etc/init.d directory and is a script called vdc.

12 Starting & Stopping Processes

A common action used while troubleshooting an application installation is to stop and start one or all of the processes running on a given server. The following instructions provides users an understanding of how to complete each of these actions.

Key processes running for this application include the following:

- Database processes (postgres)
- Replication service (replication)
- Monitoring service (vms)
- Core application server process (jsvc)

Start/Stop All Processes

A script to start/stop all Visual Data Center processes is located in the /etc/init.d directory and is called "vdc". The possible options to run this script are as follows:

Run this command as the root user ONLY!

- ./etc/init.d/vdc start – This will start all application processes including the web server, database and application.
- ./etc/init.d/vdc stop – This will stop all application processes including the web server, database and application.

By default, this script is invoked to start all processes when the server hardware is started. This ensures the application is started whenever a server restarts. Note, it may take several minutes after the server reboot for the full set of application processes to be running and available for users to log in.

Start/Stop Specific Processes

When a specific process needs to be stopped or started, follow the instructions for the relevant service below. In some cases, more than one process needs to be stopped or started for a service to be fully restarted.

All processes must be started as the vdc user with the exception of the Postgres process.

Monitoring Process

This command will start/stop application monitoring protocols, the Trap Manager process which manages SNMP traps being received from other devices and the alarm notification process.

/opt/VDC/monitor/vms/bin/vms [start|stop]

Postgres Database Process

The Postgres process controls the function of the database which contains all data related to the application. The database is required to be started for the application to operate normally. The following commands are used to start/stop the postgres process:

Run this process as postgres user ONLY!

To start the process:

su - postgres

/usr/local/pgsql/bin/pg_ctl -D /usr/local/pgsql/data start

To stop the process:

su - postgres

/usr/local/pgsql/bin/pg_ctl -D /usr/local/pgsql/data stop -m immediate

Web Server Process

The Web Server allows users to access the application interface via a supported internet browser such as Chrome, Internet Explorer or Firefox. This process is required to be running for normal application functions to be performed and is located in the /opt/VDC/tomcat/bin directory. This process will be listed as a jsvc process in the process list for the server. Use the following commands to start/stop the web server process.

To start the process:

su - vdc

nohup /opt/VDC/bin/vdc start &

To stop the process:

su - vdc

nohup /opt/VDC/bin/vdc stop &

Replication Process

The replication process is designed to keep key information located in the master and probe databases in synch. These separate database sources rely on this replication process to present accurate and up to date information to users in various parts of the application.

/opt/VDC/bin/replication start | stop

Automatic Start/Stop Processes During Server Startup/Shutdown

The application installer sets up an automatic process startup/shutdown script which is used during the server start/shutdown for OS run-level: 3, 4 and 5. If an application server boots under these run-levels, then all of the processes will be started automatically with the /etc/init.d/vdc script which is called during the server startup process.

13 Log File Management

Due to the number of features and activities occurring with this application there is a need to maintain detailed history of data, actions, etc for troubleshooting purposes. The following table provides an overview of the different locations and purposes of the main log files which are maintained with the application.

Log File Directory	Description
/opt/VDC/tomcat/logs	Web server log files
/opt/VDC/monitor/vms/logs	Monitoring process log files
/opt/VDC/vdcmon/logs	Log files for the vdcmon toll which checks self health of the application server

cleanlogs Script

Log files generated from the application can be archived using the cleanlogs cron job which is located in the /opt/VDC/bin directory. By default, the cleanlogs script is executed in the cron schedule at 4AM server time nightly. This script purges and rotates the log files automatically. As long as the server has enough free disk space to meet the disk space requirements set by the cleanlogs retention policy then no manual intervention should be needed to manage the log files. The key configuration items in the cron task are the number of days to archive the logs (DAYS_MIN), which logs to archive and the destination location for the archived files. The minimum recommended setting for DAYS_MIN is 2. If disk space allows, then the recommended setting for DAYS_MIN is 7 which allows a week long window of reference logs for possible troubleshooting needs.

By default, the following logs/directories are managed by the cleanlogs cron script. Note, this script can be edited to manage other logs if needed:

- /opt/VDC/tomcat/logs
- /opt/VDC/monitor/logs
- /opt/VDC/monitor/vms/logs
- /opt/VDC/db/logs
- /opt/VDC/ibuilder/logs
- /opt/VDC/3DService/Nsi/logs
- /opt/VDC/vdcmon/logs
- /opt/VDC/tools/logs
- /opt/VDC/VDCMPCollect/logs

- /opt/VDC/monitor/shared/autodiscovery/cmdb/logs
- /opt/VDC/monitor/shared/autodiscovery/unknowmibs

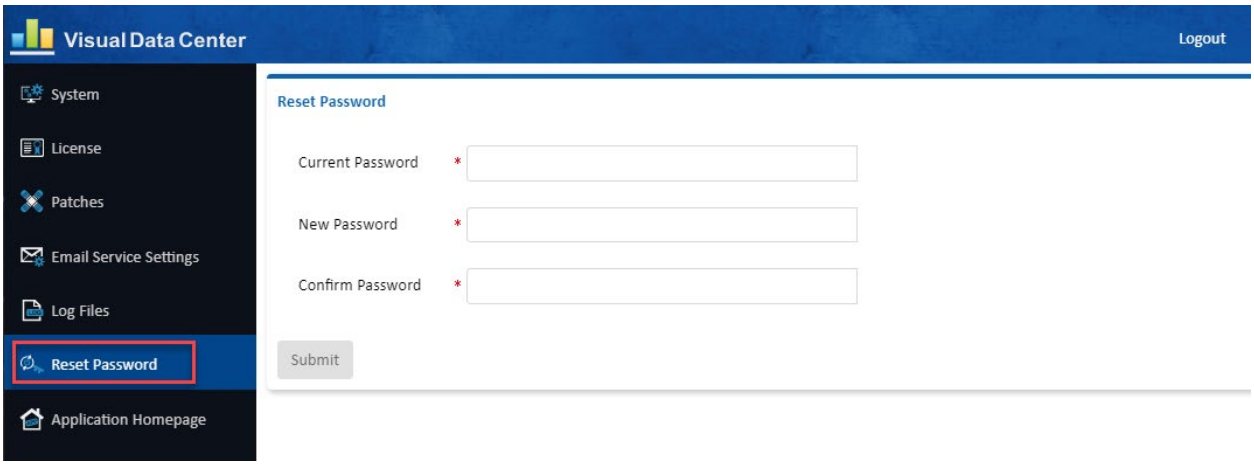
14 Server Admin Tool

The Server Admin Tool is a built-in Web-based administrative tool to allow administrators to perform the following tasks without interacting with the command line console. This can help bypass the command line requirements for customers who may have issues with security of command line access or customers who lack basic command line skills. This tool runs independently from the main application, so it does not need a valid license activation key to be applied to the application server prior to running this tool.

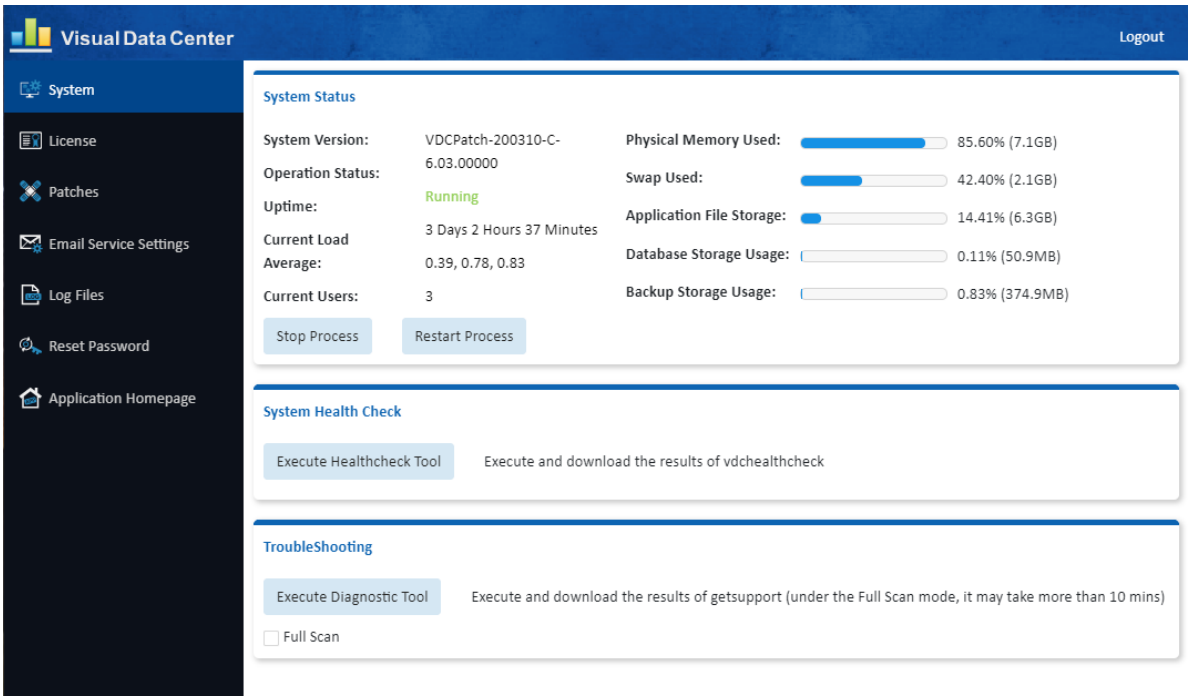
Accessing the Server Admin Tool and Reset Password Page

By default, the server admin tool is installed with the standard installation script and can be accessed in a web browser at http://Server-URL/ServerAdmin where Server-URL refers to the URL used for accessing the application. This URL is supplied during installation of the application by the installer. Note, if the URL used to access the application is https:// then please use https:// for accessing the ServerAdmin tool as well.

The default password to access the server admin tool is admin/Monit@r#1 . Use the Reset Password function to change the default admin password as soon as the tool is installed.



Server Admin Interface



The Server Admin interface has a navigation panel on the left with the following menu items:

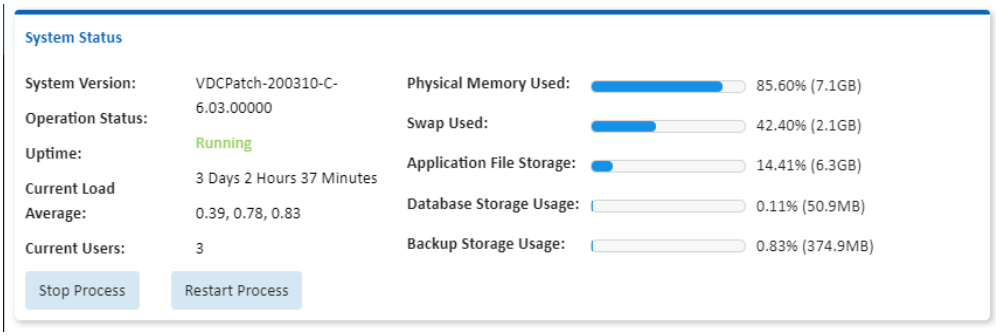
Menu Item	Definition
System	Provides status of the Master server and access to health and diagnostic tools.
License	Provides information on the currently applied license and functions to request a new license and upload a license to the server.
Patches	Lists the full patch history and allows users to apply a new patch to the server.
Email Service Settings	Shows information related to the Email settings for delivering key information from the server to recipients and allows changes to be made to these settings.
Log Files	Provides functions to download specific application log files for support or review.
Reset Password	Function to update the password for the ServerAdmin “admin” user.
Application Homepage	Link to the home page of the application.

System Menu Item

Displays System Status, System Helath Check and Troubleshooting areas where relevant information and tools are available.

System Status

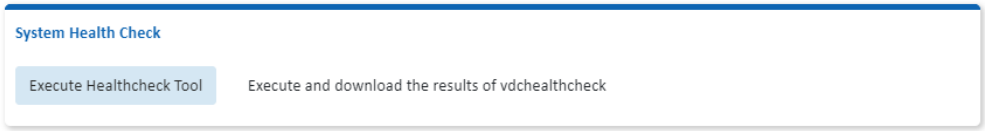
Key application and server information is displayed in the various metrics reported.



Attribute	Definition
System Version	Current version of the Product instance
Operating Status	Operating status of the current instance based on number of processes
Uptime	Amount of time the since the server was last rebooted
Current Load Average	Load Average on the server
Current Users	Number of users logged onto the server
Physical Memory Used	Amount of physical memory used
Swap Used	Amount of swap spaced used
Application File Storage	Percentage and Size of the /opt/VDC directory
Database File Storage	Percentage Size of the Database
Backup Storage Usage	Percentage Size of the /opt/VDC.BACKUP directory

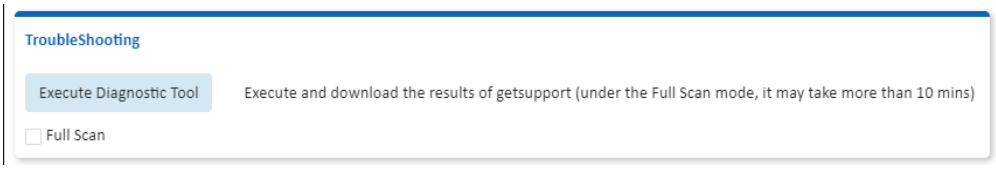
Button	Definition
Stop Processes	Will stop all application related process on the server. This replicates the /etc/init.d/vdc stop command on the server.
Restart Processes	Will start any processes which are not running or stop and then start any processes which are currently running. This replicates the /etc/init.d/vdc start command on the server.
Upload License	Uploads an activation license key to the server

System Health Check



Button	Definition
Execute Healthcheck Tool	Executes a specific diagnostic health check designed for the server admin interface. The output is downloaded to the user device for review and submission to support.

TroubleShooting

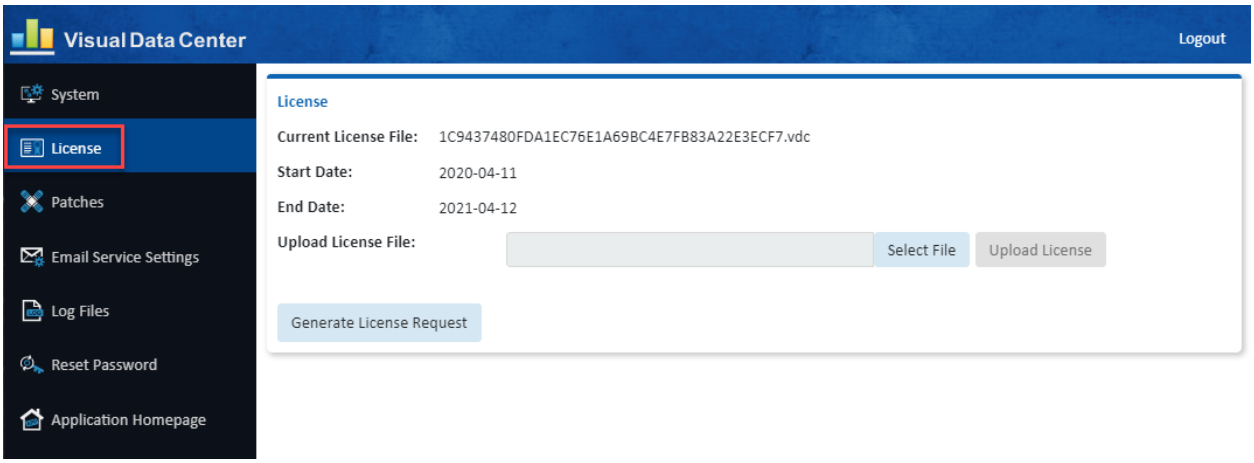


Button	Definition
Execute Diagnostic Tool	Execute Diagnostic Tool button - Runs the /opt/VDC/bin/getsupportinfo command. • No option checked runs getsupportinfo with the -q for quick option • Full Scan option runs getsupportinfo with no arguments and will take 10 minutes or more • Output is sent to local downloads folder • Logfile getsupportinfo.log.bz2 is a compressed file and must be uncompressed to open.

Note: The full scan logs is approximately 45MB when uncompressed, the regular log is approximately 25MB. The getsupportinfo tool can also be run at the command line. See the gestsupport Tool chapter for details and other options.

License

Users can generate a license request and apply a new license.

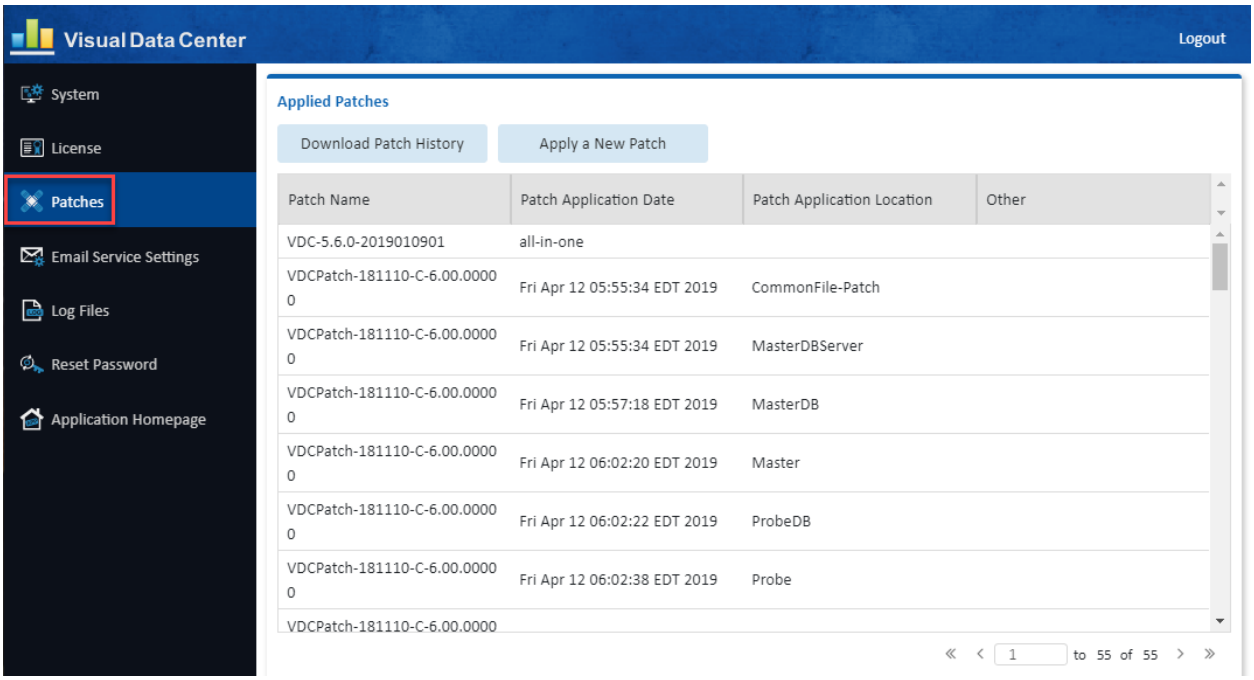


Attribute	Definition
Current License File	Filename of the current activation license key on the server
Start Date	Start date for the use of the activation license key
End Date	End date for the activation license key
FMA Total/FMA Allowed	Number of licenses used compared to the number of licenses enabled in the license activation key

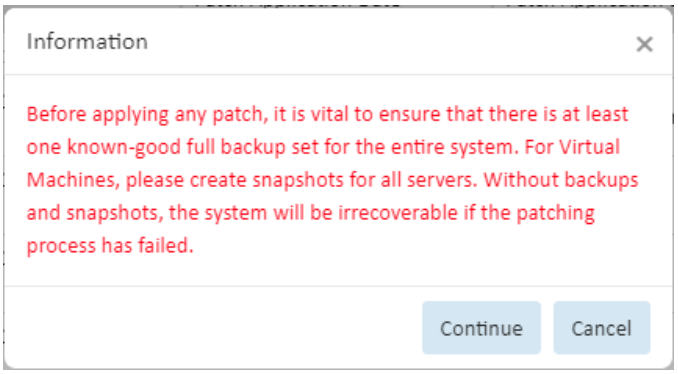
Button	Definition
Generate License Request	Produces and downloads a license request to the user's computer so users can request an activation key for the application. The file keyreq.req is delivered to the downloads folder. This function replicates the /opt/VDC/bin/vdckeyreq command on the server.
Select File	Used to navigate to the new license activation file (.lic).
Upload License	Uploads an activation license key to the server

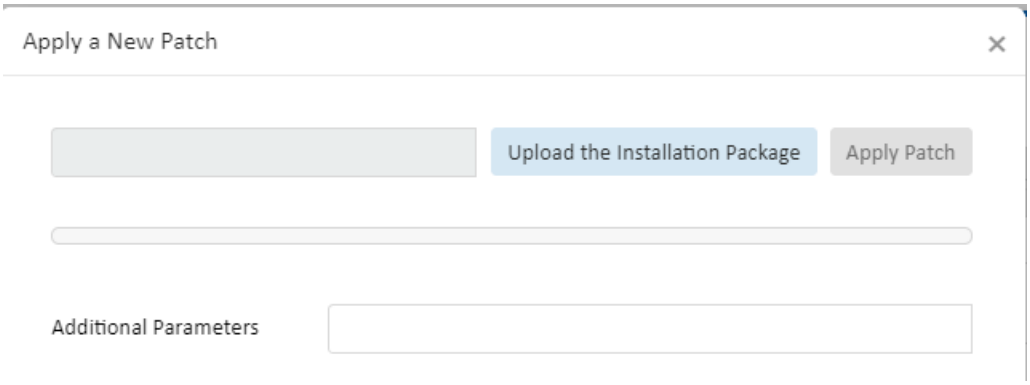
Patches

Displays the patch and version history in a table which is maintained in the /opt/VDC/VERSION file.



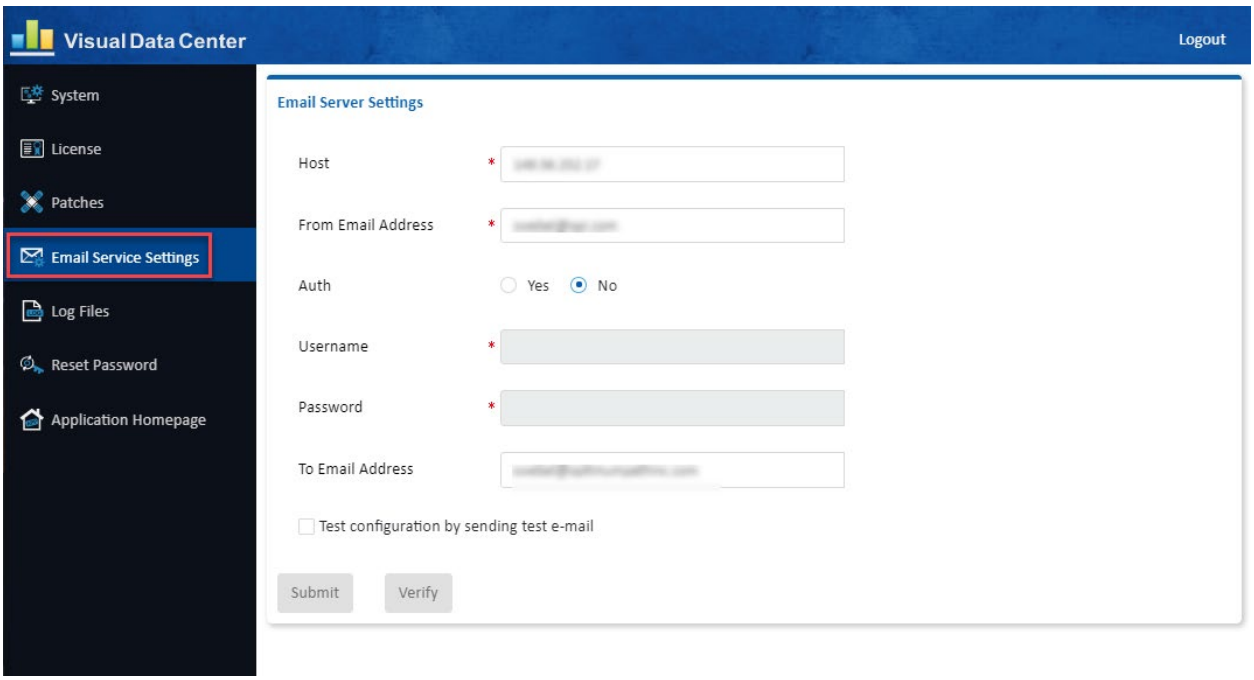
Button	Definition
Download Patch History	Downloads the patch history onto the user's computer
Applied a New Patch	Launches a warning window and then a browse window to upload and apply a patch to the server.





Email Server Settings

This function allows users to manage the mail delivery settings for the application. There are multiple email delivery functions in the application which will utilize these settings. If there are reasons to manage each of these mail delivery features with separate mail settings then please use the vdctools feature to configure them individually.

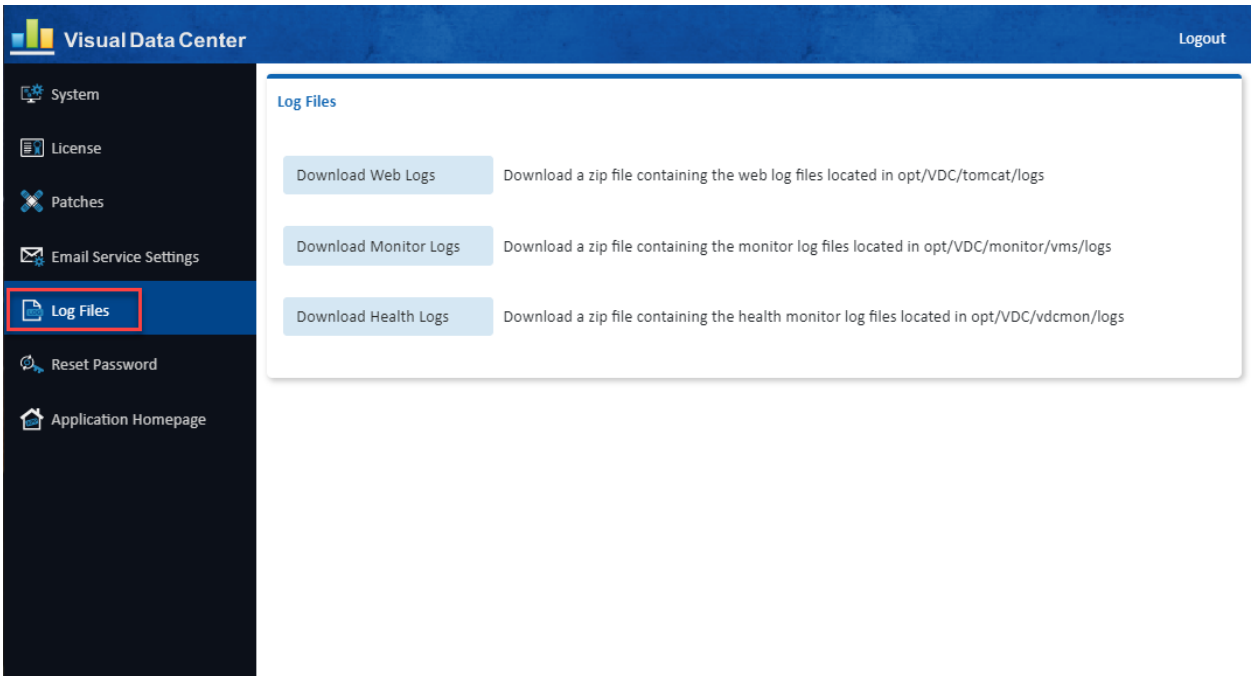


Note: Configurations defined on this page are implemented without the need to restart processes or reboot the server. The page shows the current email server settings.

Field	Definition
Host	IP Address or hostname of the SMTP mail delivery server.
From Email Address	The From address to be used for delivery of all messages to end users.
Auth	SMTP Authorization setting for the use of the SMTP server.
Username and Password	If SMTP Authorization is required, then provide the user and password needed to connect to the SMTP server to deliver the messages.
To Email Address	Destination address for all internal server admin messages logged by the vdcmon process which will monitor health of the application servers. Only one recipient or distribution address can be configured in this setting.
Test Configuration	Test configuration option allows users to verify the settings are working by providing a test recipient for the test email to be delivered. Choose the Verify button after the recipient is defined to test the mail delivery.
Verify Button	Check Test Configuration before clicking the Verify Button.
Submit Button	Saves changes to the mail settings. No restart of processes or reboot of server is required to enable these settings for all mail delivery features in the application.

Log Files

Three separate log file archives are created for submission to a support team for troubleshooting purposes.



Button	Definition
Download Web Logs	Downloads a zip file containing the web log files located in /opt/VDC/tomcat/logs
Download Monitor Logs	Downloads a zip file containing the monitor log files located in /opt/VDC/monitor/vms/logs
Download Health Logs	Downloads a zip file containing the health monitor log files located in /opt/VDC/vdcmon/logs

15 Application Removal from Server

If a customer has a failed installation attempt or for other reasons needs to perform a full reinstall of the application, it is recommended that the existing server be purged of the application files prior to initiating the installation again.

Option 1 - Snapshot

Ideally there is a virtual snapshot or equivalent which will allow users to quickly revert to a server image which has not yet been installed, but the following steps can be followed to purge an existing installation from a server.

Option 2 – Full Server Install

If a snapshot image is not available, then the safest option for customers is to perform a full reinstall of the operating system and application to the server. This guarantees there are no corrupt or partial files remaining from the aborted or problematic install which was performed on the server previously.

Option 3 – Remove Application Files & Reinstall Application Only

The final option available to a customer is to purge the application files and reinstall the application on the server. To complete this option perform the steps listed in the table below.

#	Description	Commands
1	Login to the application server as the root user.	
2	Remove the application startup scripts.	rm /etc/init.d/vdc rm /etc/rc5.d/S99vdc
3	Remove cronjobs for root user.	crontab -e Use vi and execute the dd command to delete ALL lines in the file.

		When all the lines are deleted, run :wq command to save the change.
4	Remove cronjob for vdc user.	su - vdc crontab -e Use vi and execute the dd command to delete ALL lines in the file. When all the lines are deleted, run :wq command to save the change.
5	Reboot the application server.	reboot
6	Login to the application server as the root user.	
7	Delete the Postgres database.	rm -rf /usr/local/pgsql
8	Delete application core file directory.	rm -rf /opt/VDC
9	Reinstall the application and apply an updated license key.	

16 Backup & Recovery

To properly guard against system outages, both the application files and the application database should be backed up. This is the only way to guarantee a full restore of the application is possible. The application contains a native backup script which can be used to create backups for all of these key components.

For best practice, installations should follow these rules to efficiently manage the backup process:

- Maintain seven days of backup images to safeguard against issues which are not found within a few days of use.
- The backup file system should utilize mount points using disks other than those used by the primary application and database files. To avoid a single point of failure with disk issues, this is an important aspect of backup configurations.
- Never mount the /opt/VDC.BACKUP directory under the /opt/VDC directory. This will result in the backup job creating backups of backups which will consume resources to process backups and large amounts of disk space to manage the backup file images.
- If you are using the Real Time License Server, you may need to stop and restart after the restore process is completed.
- If you are using https, you may need to reconfigure.

Backup Script Overview

The following details the basic operation of this backup script:

- The backup script, *bkpvdc*, is located under /opt/VDC/bin. It must be run by the "*root*" user on the server.

- The bkpvdc backup script has the following running modes:

    - –a - Daily with 7-day retention policy, which not only performs the backup, but also removes any previous backups which are older than 7 days. This is the default operation mode of the script. This option will back up the application files and the database files.
    - –d - Daily, which only does new backup and does not remove any old backups for the number of days specified. Administrators must remove the old backups manually if no number is provided. The "-d" option turns this mode on.
    - –q - This option turns on "quiet" mode which suppresses debug messages.

- By default, bkpvdc is run by a cronjob entry under the root user. For example, the following crontab entry backs up the database and application files to the /opt/VDC.BACKUP directory at 2AM daily. Users can edit the root cronjob to change the timing, frequency and location for the backup processes to take place.
    - 0 2 * * * /opt/VDC/bin/bkpvdc -d -a -q /opt/VDC.BACKUP
- There are four components of the backup routine which will be backed up during the scheduled cron job activity. These sets of files will be compressed and stored separately to enable easy restore to other instances of the application as needed.
    - vdcdb – Master database.
    - sdb – Probe database.
    - vdc – Application files on /opt/VDC directory.
    - spool – Trend chart data stored with the rrd function.
    - site-packages -
- All application and backup images will follow a day/time naming convention as described later in this section of the document.

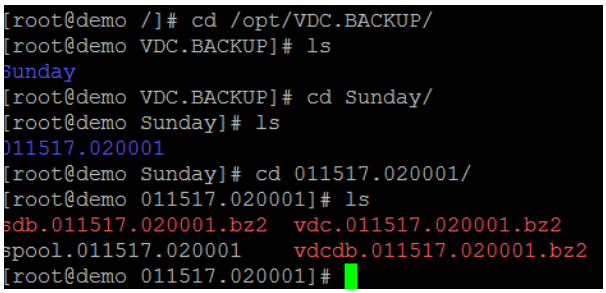
Daily Backup Naming Convention

When the backup job is executed the files will be compressed and stored in an organized folder tree to help retrieve needed backup images easily.

- The seven day rotation is managed with top level folders using the name of the day the backup job was executed. If a server is configured to store seven days of backup images then there will be seven folders under /opt/VDC.BACKUP with each having a name of the day.
- Under the day folder a directory will be created with the MMDDYY.HHMMSS naming convention which contains the backup files for that particular backup event. This will help differentiate backup images if more than seven days are retained in the backup configuration.
- Under each date folder there will be a set of files created by the backup function. Each of these files contains the compressed set of backed up files for the particular function of the application.
    - vdcdb – Master database.
    - sdb – Probe database.
    - vdc – Application files on /opt/VDC directory.

- spool – Trend chart data stored with the rrd function.

An example of the directories and files is contained in the image below:



Backup Configurations

The backup job has two levels of configuration which can be managed by the system administrator. The frequency and location of the backup files can be managed with the crontab entry while the retention policy can be managed within the backup script directly.

Crontab Updates

By default, the backup script will run nightly at 2AM server time and place the backup images in the /opt/VDC.BACKUP directory. The frequency of the backup can be managed with the time settings on the cronjob itself so that it runs less frequently. For example, this option below will only run on Sunday.

0 2 * * 7 /opt/VDC/bin/bkpvdc -d -a -q /opt/VDC.BACKUP

The folder reference at the end of the cron job will indicate to the bkpvdc script where to deposit the backup images. If a separate reference is needed then update the cron job. Please ensure this directory is not under the /opt/VDC folder and is using separate disks for backup storage.

Retention Policy

Within the backup script there is a parameter num_of_days which indicates the number of days to retain images on the backup server. As part of the backup script execution, new backups are created and backup images which are beyond the retention policy limit will be purged.

All-in-One Application Server Recovery

In this use case there is only one server.

- All-in-One server - runs the Master, Master DB and Probe application processes.

Overview All-in-One Recovery on Same Server

If customer administrators have issues with the integrity of the application or database, the following instructions can be followed to recover a backed-up copy into the same server production instance.

High-level overview of the steps:

- Start log
- Copy and decompress the backup images into the /opt/Install directory
- Shut down the application services on the server instance
- Re-initialize the database so an import of the backup data can be performed
- Import the database data for the master and probe database components
- Remove the application files from the server instance
- Restore the application files from the backup data set
- Restore trend data
- Enable start scripts, cron jobs, etc for a fully functioning application instance
- Restore python libraries
- Exit log
- Reboot the server
- Verify system web login, 3D client login and monitoring

Steps for All-in-One Recovery on Same Server

Note: Commands are in **bold** and can be copied and pasted to the server command line.
Do NOT copy the prompt indicators (#, $ or prompt text) preceding the commands.

The detailed step by step instructions for restoring a backup image to the same server are listed below:

1. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of disk space depending on the size of the database. Ensure that you have enough room.

2. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS). Make note of the path to the desired backup.

3. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.**
   When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

4. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process.
   # **script /tmp/backup.log**

5. Create the /opt/Install directory if it doesn't already exist.
   # **mkdir /opt/Install**

6. Navigate to the day/date directory that contains the last known good backup files.
   # **cd /opt/VDC.BACKUP/day/MMDDYY.HHMMSS**
   Copy all of the files to /opt/Install.
   # **cp ./* /opt/Install**

   There should be the following files:
   vdc.MMDDYY.HHMMSS.bz2
   vdcdb.MMDDYY.HHMMSS.bz2

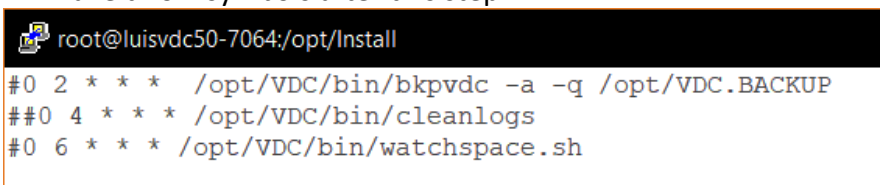
sdb.MMDDYY.HHMMSS.bz2
spool.MMDDYY.HHMMSS
site-packages.tar (optional)

Note: site-packages.tar is not always present, if it process it as directed in later steps. If it is not present, do not be concerned.

7. Decompress the backup data
   Note: You do not need to decompress the spool or the site-packages files.
   # **bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2**
   # **bzip2 -d /opt/Install/vdcdb.MMDDYY.HHMMSS.bz2**
   # **bzip2 -d /opt/Install/sdb.MMDDYY.HHMMSS.bz2**

8. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the "crontab -e" command.
   The crontab editor functions like the vi editor.
   You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

   This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



   For user root:
   # **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.
   esc
   :wq

   Switch to vdc user. Note: The su command has a space on either side of the dash (-).
   # su - vdc
   $ **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.

esc
:wq

9. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
   $ **exit**
   a. For 6.* OS:
      # **rm -rf /etc/rc5.d/S99vdc**
   b. For 7.* OS:
      # **systemctl disable vdc**
      You should see the following message if the command ran properly.

```
[root@vdc54-3073 ~]# systemctl disable vdc
Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
```

   c. Reboot the server.
      # **reboot**
      Wait 5 minutes for the server to come back online.

10. Login as root when the server is back up.

11. Restart the log file to capture the next batch commands for this backup activity**.**
    # **script -a /tmp/backup.log**

12. From root change to the postgres user.
    # **su - postgres**

13. Start the database.
    $ **/usr/local/pgsql/bin/pg_ctl -D data start**
    Hit enter until you see the prompt.
    Confirm the database is started.
    $ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

14. Drop vdc_repos
    The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

    /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
    UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_repos';
    ALTER DATABASE vdc_repos CONNECTION LIMIT 1;
    SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_repos';
    DROP DATABASE vdc_repos;
    __EOF__

15. Drop vdc_sdb.
    The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.
    /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
    UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_sdb';
    ALTER DATABASE vdc_sdb CONNECTION LIMIT 1;
    SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_sdb';
    DROP DATABASE vdc_sdb;
    __EOF__

16. Create the new Postgres database instance.
    $ **/usr/local/pgsql/bin/createdb -h vdchost-db -U root vdc_repos**
    $ **/usr/local/pgsql/bin/createdb -h vdchost-db -U root vdc_sdb**

17. Run the import command for vdc_repos to import the desired backup file "vdcdb.MMDDYY.HHMMSS"

    $ **/usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos < /opt/Install/vdcdb.MMDDYY.HHMMSS**

    Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

18. Run the import command for vdc_sdb to import the desired backup file "sdb.MMDDYY.HHMMSS"

    $ **/usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_sdb < /opt/Install/sdb.MMDDYY.HHMMSS**

Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

19. Exit postgres user, become vdc user and stop and start the replication between the master and slave database.
    $ **exit**
    # **su - vdc**
    $ **/opt/VDC/bin/replication stop**
    $ **/opt/VDC/bin/replication start**
    Hit enter until you see the prompt.

20. Exit vdc user, return to root and clear the current application directory.
    $ **exit**
    # **rm -rf /opt/VDC**

    Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
    # **rm -rf /opt/VDC/***
    # rm -rf /opt/VDC/*.*

21. Restore the application from the backup file vdc.MMDDYY.HHMMSS using tar extract.
    # **cd /opt/**
    # **tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS**

22. Restore trend data from the backup file spool/MMDDYY.HHMMSS using tar extract.
    # **cd /opt/**
    # **tar -xvf /opt/Install/spool.MMDDYY.HHMMSS**

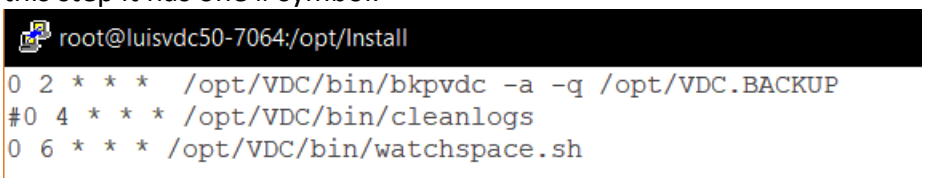
23. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
    a. For OS 6.*
       # **ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc**
    b. For OS 7.*
       # **systemctl enable vdc**
       You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

24. Enable cronjobs for root user and then for the vdc user.
    To edit the crontab use the “crontab -e” command.

The crontab editor functions like the vi editor.
You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.



For user root:
crontab -e
After deleting one # from each line, save and exit.
esc
:wq

Switch to vdc user.
su - vdc
$ **crontab -e**
After deleting one # from each line, save and exit.
esc
:wq

25. Exit vdc user
    $ **exit**

26. Restore python libraries.
    Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
    a. Stop any current running Python processes
       # **ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'**
    b. Remove the current Python libraries
       # **rm -rf /usr/local/lib/python3.5/site-packages/**
    c. Restore the Python libraries from the backup
       # **tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar**
    d. Set permission
       # **chmod -R 755 /usr/local/lib/python3.5/site-packages/**

27. End the script capture log file.
    # **exit**
    Output when successfully exiting the script:
    ```
    Script done, file is /tmp/backup.log
    ```

28. Reboot the server.
    # **reboot**

29. Wait 10 minutes.

30. The system is ready for use, test web and 3D Client connections and monitoring activity to confirm.

Overview All-in-One Recovery on a Different Server Overview

In some cases, an instance of the application must be restored to a new server. In this situation, there are more configuration items which need to be considered as part of the restore process.

- On the new server install VDC with the 5.X version that matches the server to be recovered.
- Get info from the new server
- Start log
- Place backup images on the new server
- Decompress the backup images into the /opt/Install directory
- Shut down the application services on the server instance
- Re-initialize the database so an import of the backup data can be performed
- Get info and update database configurations for the probe on the new server
- Import the database data for the master and probe database components
- Remove the application files from the server instance
- Restore the application files from the backup data set
- Restore the trend data
- Update configurations for IP and URL changes for the system on the new server
- Enable start scripts, cron jobs, etc for a fully functioning application instance
- Restore python libraries
- Exit log
- Reboot the server
- Verify system web login, 3D client login and monitoring

Prerequisites for All-in-One Recovery on a Different Server

- On the new server do a full install of VDC at the 5.X version that matches the server to be recovered.
- Request and install license and confirm that your new instance is working.
    - Save the license file as you will need to place it back on the server after the restore.
- **HTTPS - if your server is configured for HTTPS contact support for additional instructions before continuing with the restore.**

Steps for All-in-One Recovery on a Different Server

Note: Commands are in **bold** and can be copied and pasted to the server command line.
Do NOT copy the prompt indicators (#, $ or prompt text) preceding the commands.

The detailed step by step instructions for restoring a backup image to a new server are listed below:

1. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.**
   When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

2. Before starting the migration from the old server to the new server you will need to gather information from the new server. Once the data is transferred over to the new server, the needed information is overwritten by the old server data. Below is a list of items that need to be collected on the new server as well as the commands to get the information. The results of these commands correspond to variables for the values that are referenced on subsequent recovery steps. Where you see $SDBName and $ProbeName in later commands you will use your values.

    a. Retrieve **$SDBName**
    # cat /opt/VDC/bin/sdbinit.sh | grep -i "NAME" | sed -n 3p | awk -F'=' '{print $2}'
    Example: sdb192.168.111.60
    Copy the SDBName to a text file for use in subsequent commands.
    This will be the $New_SDBName.

b. Retrieve **$ProbeName**
 # cat /opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties | grep -i "agent.name" | awk -F'=' '{print $2}'
Example: SP192.168.111.60
Copy the ProbeName to a text file for use in subsequent commands.
This will be the $New_ProbeName.

3. Check disk space on the application server.
 # df -h
Copying the backup files and decompressing them can take up significant amounts of disk space depending on the size of the database. Ensure that you have enough room.

4. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process.
 # script /tmp/backup.log

5. Create the /opt/Install directory if it doesn't already exist.
 # mkdir /opt/Install

6. Move the desired backup date files from the old server's backup directory and place them on the new server within the /opt/Install directory. There should be the following files:
vdc.MMDDYY.HHMMSS.bz2
vdcdb.MMDDYY.HHMMSS.bz2
sdb.MMDDYY.HHMMSS.bz2
spool.MMDDYY.HHMMSS
site-packages.tar (optional)

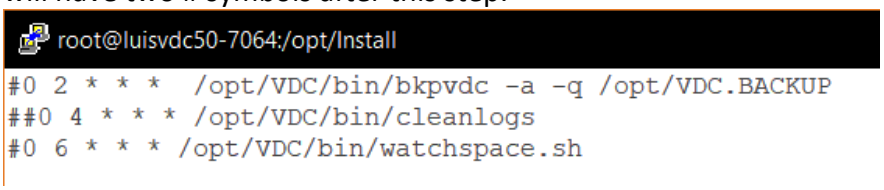
Note: site-packages.tar is not always present, if it is move it to the new server and process it as directed in later steps. If it is not present, do not be concerned.

7. Decompress the backup data
NOTE: You do not need to decompress the spool or the site-packages files.
 # bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2
 # bzip2 -d /opt/Install/vdcdb.MMDDYY.HHMMSS.bz2
 # bzip2 -d /opt/Install/sdb.MMDDYY.HHMMSS.bz2

8. Disable cronjobs for root user and then for the vdc user.
To edit the crontab use the "crontab -e" command.
The crontab editor functions like the vi editor.
You will be inserting a # symbol at the beginning of each and every line, including those

that already have a # symbol.

This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



For user root:
crontab -e
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

Switch to vdc user. **Note:** The su command has a space on either side of the dash (-).
su - vdc
$ crontab -e
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

9. Become root user and disable the Auto-start. **Note:** The command is different depending on the Operating System version.
   $ **exit**
   a. For 6.* OS:
      # **rm -rf /etc/rc5.d/S99vdc**
   b. For 7.* OS:
      # **systemctl disable vdc**
      You should see the following message if the command ran properly.

```
[root@vdc54-3073 ~]# systemctl disable vdc
Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
```

   c. Reboot the server.
      # **reboot**

Wait 5 minutes for the server to come back online.

10. Login as root when the server is back up.

11. Restart the log file to capture the next batch commands for this backup activity**.**
    # script -a /tmp/backup.log

12. From root change to the postgres user.
    # su - postgres

13. Start the database.
    $ **/usr/local/pgsql/bin/pg_ctl -D data start**
    Hit enter until you see the prompt.
    Confirm the database is started.
    $ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

14. Drop vdc_repos
    The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

    /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
    UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_repos';
    ALTER DATABASE vdc_repos CONNECTION LIMIT 1;
    SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_repos';
    DROP DATABASE vdc_repos;
    __EOF__

15. Drop vdc_sdb.
    The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

    /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
    UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_sdb';
    ALTER DATABASE vdc_sdb CONNECTION LIMIT 1;
    SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_sdb';
    DROP DATABASE vdc_sdb;
    __EOF__

16. Create the new Postgres database instances.
    $ **/usr/local/pgsql/bin/createdb -h vdchost-db -U root vdc_repos**
    $ **/usr/local/pgsql/bin/createdb -h vdchost-db -U root vdc_sdb**

17. Run the import command for vdc_repos to import the desired backup file "vdcdb.MMDDYY.HHMMSS"

    $ **/usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos < /opt/Install/vdcdb.MMDDYY.HHMMSS**

    Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

18. From postgres user exit to root.
    $ exit

19. Log in to vdc_repos.
    # **/usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos**
    The prompt changes to vdc_repos=#.

20. Update registered Probe process info in the repos database.
    a. Retrieve the Probe ID
    vdc_repos=# **select name,id from server.process_info where type_id = 1;**

```
[root@vdc54-3060 ~]# /usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos -c "select name,id from server.process_info where type_id = 1;"
Welcome To VDC PSQL
        name        |                  id
--------------------+--------------------------------------
 SP192.168.111.64 | 5695dc32-1d58-11e8-8fbf-000c2980a499
(1 row)
```

    Copy the Probe ID to a text file for use in subsequent commands.

    b. Update the Probe IP address.
    Note: The three lines below are one long command. When you copy, drag to select all three lines and it will paste as one line.
    vdc_repos=# **update server.process_info set name = '$New_ProbeName',option = format('<opt serviceType="1" url="rmi://$New_Probe_IP:12004/RmiService"/>')::xml where id = '$ProbeID';**

    Example:
    vdc_repos=# update server.process_info set name = '**SP192.168.111.60**',option = format('<opt serviceType="1" url="rmi://**192.168.111.60**:12004/RmiService"/>')::xml where id = '**5695dc32-1d58-11e8-8fbf-000c2980a499**';

21. Update registered SDB in the repos database.
    a. Retrieve the SDB ID
    vdc_repos=# **select name,id from mac.sdb;**

```
vdc_repos=# select name,id from mac.sdb;
        name         |                  id
---------------------+--------------------------------------
 sdb192.168.111.64 | 5695afb4-1d58-11e8-988b-000c2980a499
(1 row)
```

    Copy the SDB ID to a text file for use in subsequent command.
    Note: The SDB ID is a similar but different number than Probe ID above. Please

copy and save as requested. You will need both IDs in subsequent commands

b. Update the SDB IP address
vdc_repos=# **update mac.sdb set name = '$New_SDBName' where id = '$SDBID';**

Example:
vdc_repos=# update mac.sdb set name = '**sdb192.168.111.60**' where id = '**5695afb4-1d58-11e8-988b-000c2980a499**';

22. Quit from the vdc_repos database to return to root.
vdc_repos=# **\q**

23. From root change to the postgres user and run the import command for vdc_sdb to import the desired backup file "sdb.MMDDYY.HHMMSS"
    a. # **su - postgres**

    b. $ **/usr/local/pgsql/bin/psql -h vdchost-probe -U root vdc_sdb < /opt/Install/sdb.MMDDYY.HHMMSS**

    Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

24. From postgres user exit to root.
$ **exit**

25. Login to the sdb database.
 # /usr/local/pgsql/bin/psql -h vdchost-probe -U root vdc_sdb
prompt changes to vdc_sdb=#

26. Update the IP address in rc.sdb_info. You will use the $SDBID you retrieved earlier.
vdc_sdb=# **update rc.sdb_info set name = '$New_SDBName' where id = '$SDBID';**

Example:
vdc_sdb=# update rc.sdb_info set name = '**sdb192.168.111.60**' where id = '**5695afb4-1d58-11e8-988b-000c2980a499**';

27. Quit from the vdc_repos database to return to root.
vdc_sdb=# **\q**

28. Clear the current application directory.
    # rm -rf /opt/VDC

    Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
    # rm -rf /opt/VDC/*
    # rm -rf /opt/VDC/*.*

29. Restore the application from the backup file vdc.MMDDYY.HHMMSS using tar extract.
    # cd /opt/
    # tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS

30. Restore trend data from the backup file spool/MMDDYY.HHMMSS using tar extract.
    # cd /opt/
    # tar -xvf /opt/Install/spool.MMDDYY.HHMMSS

31. Run the newip command to update some of the entries.
    # /opt/VDC/bin/newip OLD_IP NEW_IP
    Example: *# /opt/VDC/bin/newip 192.168.111.64 192.168.111.60*
    Note: Ensure that you are only entering actual IP addresses. If your OLD IP address is 127.0.0.1 contact support for additional instructions.

32. In the .conf file replace any instances of the old IP address with new IP address.
    a. Change to the /opt/VDC directory
       # cd /opt/VDC
    b. Backup the existing .conf file.
       # cp .conf conf-backup
    c. Run the following command to make the changes to the .conf file.
       # sed -i -e 's/OLD_IP/NEW_IP/g' /opt/VDC/.conf
    d. Verify the changes were made.
       # grep NEW_IP .conf

       You should see these 7 lines from the file with the new IP address.

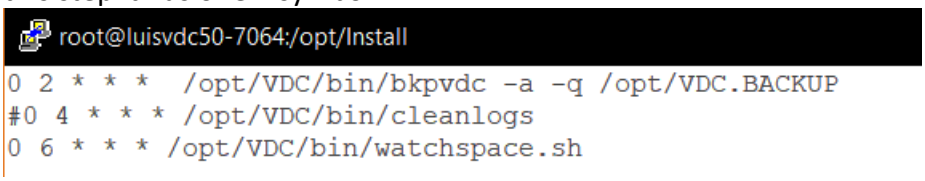
```
VDCIP@/opt/VDC/vdcmon/conf/content=192.168.111.121
SDBNAME@/opt/VDC/bin/sdbinit.sh=sdb192.168.111.121
AGENTTRAPIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties=192.168.111.121
AGENTNAME@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties=SP192.168.111.121
AGENTRMISERVICEIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties=192.168.111.121
DISCOVERYMASTERHOST@/opt/VDC/monitor/vms/webapps/discovery/WEB-INF/classes/master.properties=192.168.111.121
EMPSERVERIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Probe.properties=192.168.111.121
```

33. Run /opt/VDC/bin/vdcconf to push values from the .conf file to all the appropriate locations.

/opt/VDC/bin/vdcconf

34. Enable cronjobs for root user and then for the vdc user.
    To edit the crontab use the “crontab -e” command.
    The crontab editor functions like the vi editor.
    You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

    This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.



    For user root:
    # **crontab -e**
    After deleting one # from each line, save and exit.
    esc
    :wq

    Switch to vdc user.
    # **su - vdc**
    $ **crontab -e**
    After deleting one # from each line, save and exit.
    esc
    :wq

35. Exit vdc user
    $ **exit**

36. Update the URL.
    # **/opt/VDC/bin/newurl OLD_URL NEW_URL**

    Example: *# /opt/VDC/bin/newurl luisvdc50-7064 vdc54-3060.opi.zone*

37. Remove the old license file.
    # **rm -rf /opt/VDC/.vdc/*.vdc**

38. Place the new license file from the prerequisite stage in /opt/VDC/.vdc.

39. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
    a. For OS 6.*
       # ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc
    b. For OS 7.*
       # systemctl enable vdc
       You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

40. Reset permissions.
    # /opt/VDC/bin/setperm

41. Restore python libraries.
    Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
    a. Stop any current running Python processes
       # ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'
    b. Remove the current Python libraries
       # rm -rf /usr/local/lib/python3.5/site-packages/
    c. Restore the Python libraries from the backup
       # tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar
    d. Set permission
       # chmod -R 755 /usr/local/lib/python3.5/site-packages/

42. This step is only required if you're new server is CentOS/RedHat 7.* and the old server was CentOS/RedHat 6*. There are 2 commands that need to be run.
    a. **# cp /opt/VDC/tomcat/conf/server.xml /opt/VDC/tomcat/conf/server.xml.back**

    b. The lines that follow are one line, copy and paste into the command line.
       # sed -i -e 's/Connector address="vdchost-server" port="80" protocol="org.apache.coyote.http11.Http11NioProtocol/Connector address="localhost" port="12008" protocol="org.apache.coyote.http11.Http11NioProtocol/g' /opt/VDC/tomcat/conf/server.xml

43. End the script capture log file.
    # exit
    Output when successfully exiting the script:

```
Script done, file is /tmp/backup.log
```

44. Reboot the server.
    # **reboot**

    Note: The reboot can take up to 10 minutes.

45. The system is ready for use, test web and 3D Client connections and monitoring activity to confirm.

Multi-Server: Master & Probe Recovery

In this use case there are at least two servers.

- Master server - runs the Master and Master DB application processes
- Probe server - runs the Probe data collection and Probe database processes. There can be more than one Probe server.

Overview Multi-Server: Master & Probe Recovery on the Same Servers

If customer administrators have issues with the integrity of the application or database, the following instructions can be followed to recover backed-up copies onto the same server production instances.

When working in multi-server environments the recovery process is done in stages. Alternating between servers at each stage. The order is critical.

Note: Follow the step-by-step instructions in each stage for each server in the order presented below. **DO NOT skip ahead!**

High-level overview of each stage:

- **Stage 1 - On the Master Server:** start log, copy and decompress backups, stop automatic processes, reboot, restart log
- **Stage 2 - On the Probe Server(s):** start log, copy and decompress backups, stop automatic processes, reboot, restart log
- **Stage 3 - On the Master Server:** start db, drop vdc_repos, create new db, restore vdcdb, remove application directory contents, restore application directory contents from backup, restore python libraries, stop database
- **Stage 4 - On the Probe Server(s):** start db, drop vdc_sdb, create new db, restore sdb, remove application directory contents, restore application directory contents from backup, restore trend data, restore python libraries
- **Stage 5 - On the Master Server:** enable automatic processes, exit log script, reboot, verify server processes are running
- **Stage 6 - On the Probe Server(s):** enable automatic processes, exit log script, reboot, verify server processes are running, verify system web login, 3D client login and monitoring

Steps for Multi-Server: Master & Probe Recovery on the Same Servers

Note: Commands are in **bold** and can be copied and pasted to the server command line.
Do NOT copy the prompt indicators (#, $ or prompt text) preceding the commands.

Stage 1 - On the Master Server:

1. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of disk space depending on the size of the database. Ensure that you have enough room.

2. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS). Make note of the path to the desired backup.

3. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.**
   When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

4. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.
   # **script /tmp/backup_master.log**

5. Create the /opt/Install directory if it doesn't already exist.
   # **mkdir /opt/Install**

6. Navigate to the day/date directory that contains the last known good backup files.
   # cd /opt/VDC.BACKUP/day/MMDDYY.HHMMSS
   Copy all of the files to /opt/Install.
   # cp ./* /opt/Install

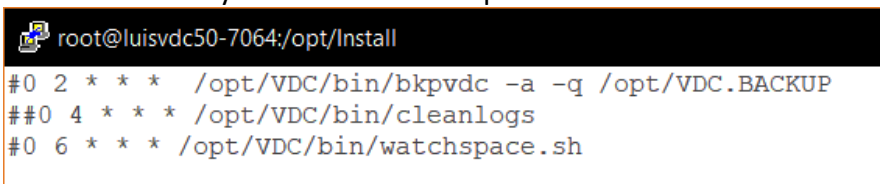
   There should be the following files:
   vdc.MMDDYY.HHMMSS.bz2
   vdcdb.MMDDYY.HHMMSS.bz2
   spool.MMDDYY.HHMMSS
   site-packages.tar (optional)

   Note: site-packages.tar is not always present, if it process it as directed in later steps. If it is not present, do not be concerned.

7. Decompress the backup data
   NOTE: You do not need to Decompress the spool or the site-packages files.
   # bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2
   # bzip2 -d /opt/Install/vdcdb.MMDDYY.HHMMSS.bz2

8. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

   This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



   For user root:
   # crontab -e
   Change to insert mode.
   i
   After adding one # to each line, save and exit.
   esc
   :wq

Switch to vdc user. Note: The su command has a space on either side of the dash (-).
su - vdc
$ **crontab -e**
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

9. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
   $ **exit**
   a. For 6.* OS:
      # **rm -rf /etc/rc5.d/S99vdc**
   b. For 7.* OS:
      # systemctl disable vdc
      You should see the following message if the command ran properly.
      ```
      [root@vdc54-3073 ~]# systemctl disable vdc
      Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
      ```
   c. Reboot the server.
      # reboot
      Wait 5 minutes for the server to come back online.

10. Login as root when the server is back up.

11. Restart the log file to capture the next batch commands for this backup activity**.**
    # **script -a /tmp/backup_master.log**

Stage 2: On the Probe Server(s):

1. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of disk space depending on the size of the database. Ensure that you have enough room.

2. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS). Make note of the path to the desired backup.

3. Login as “root” user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you’re logged in as root the command line prompt will end in the # symbol**.**
   When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

4. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.
   # **script /tmp/backup_probe.log**

   For example: script /tmp/backup_master.log

5. Create the /opt/Install directory if it doesn’t already exist.
   # **mkdir /opt/Install**

6. Navigate to the day/date directory that contains the last known good backup files.
   # **cd /opt/VDC.BACKUP/day/MMDDYY.HHMMSS**
   Copy all of the files to /opt/Install.
   # **cp ./* /opt/Install**

   There should be the following files:
   vdc.MMDDYY.HHMMSS.bz2
   sdb.MMDDYY.HHMMSS.bz2
   spool.MMDDYY.HHMMSS
   site-packages.tar (optional)

   Note: site-packages.tar is not always present, if it is move it to the new server and process it as directed in later steps. If it is not present, do not be concerned.

7. Decompress the backup data
   NOTE: You do not need to decompress the spool or the site-packages files.
   # **bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2**
   # **bzip2 -d /opt/Install/sdb.MMDDYY.HHMMSS.bz2**

8. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.

You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.

```
root@luisvdc50-7064:/opt/Install
#0 2 * * *  /opt/VDC/bin/bkpvdc -a -q /opt/VDC.BACKUP
##0 4 * * * /opt/VDC/bin/cleanlogs
#0 6 * * * /opt/VDC/bin/watchspace.sh
```

For user root:
crontab -e
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

Switch to vdc user. Note: The su command has a space on either side of the dash (-).
su - vdc
$ **crontab -e**
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

9. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
   $ **exit**
   a. For 6.* OS:
      # **rm -rf /etc/rc5.d/S99vdc**
   b. For 7.* OS:
      # systemctl disable vdc
      You should see the following message if the command ran properly.

```
[root@vdc54-3073 ~]# systemctl disable vdc
Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
```

   c. Reboot the server.
      # reboot

Wait 5 minutes for the server to come back online.

10. Login as root when the server is back up.

11. Restart the log file to capture the next batch commands for this backup activity**.**
    # script -a /tmp/backup_probe.log

Stage 3 - On the Master Server:

1. From root change to the postgres user.
   # su - postgres

2. Start the database.
   $ **/usr/local/pgsql/bin/pg_ctl -D data start**
   Hit enter until you see the prompt.
   Confirm the database is started.
   $ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

3. Drop vdc_repos
   The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

   /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
   UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_repos';
   ALTER DATABASE vdc_repos CONNECTION LIMIT 1;
   SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_repos';
   DROP DATABASE vdc_repos;
   __EOF__

4. Create the new Postgres database instance
   $ **/usr/local/pgsql/bin/createdb -h vdchost-db -U root vdc_repos**

5. Run the import command for vdc_repos to import the desired backup file "vdcdb.MMDDYY.HHMMSS"

   $ **/usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos < /opt/Install/vdcdb.MMDDYY.HHMMSS**

   Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

6. Exit postgres user
   $ **exit**

7. Clear the current application directory.
   # **rm -rf /opt/VDC**
   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # **rm -rf /opt/VDC/***
   # **rm -rf /opt/VDC/*.***

8. Restore the application directory from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # **cd /opt/**
   # **tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS**

9. Restore python libraries.
   Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
   a. Stop any current running Python processes
      # ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'
   b. Remove the current Python libraries
      # rm -rf /usr/local/lib/python3.5/site-packages/
   c. Restore the Python libraries from the backup
      # tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar
   d. Set permission
      # chmod -R 755 /usr/local/lib/python3.5/site-packages/

10. Stop the postgres processes
    # su - postgres -c "/usr/local/pgsql/bin/pg_ctl -D /usr/local/pgsql/data stop -m immediate"

Stage 4 - On the Probe Server(s):

1. From root change to the postgres user.
   # su - postgres

2. Start the database.
   $ **/usr/local/pgsql/bin/pg_ctl -D data start**
   Hit enter until you see the prompt.
   Confirm the database is started.
   $ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

3. Drop vdc_sdb.
   The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

   /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
   UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_sdb';
   ALTER DATABASE vdc_sdb CONNECTION LIMIT 1;
   SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_sdb';
   DROP DATABASE vdc_sdb;
   __EOF__

4. Create the new Postgres database instance.
   $ **/usr/local/pgsql/bin/createdb -h vdchost-probe -U root vdc_sdb**

5. Run the import command for vdc_sdb to import the desired backup file "sdb.MMDDYY.HHMMSS"

   $ **/usr/local/pgsql/bin/psql -h vdchost-probe -U root vdc_sdb < /opt/Install/sdb.MMDDYY.HHMMSS**

   Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

6. Exit postgres user
   $ **exit**

7. Clear the current application directory.
   # **rm -rf /opt/VDC**
   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # **rm -rf /opt/VDC/***
   # **rm -rf /opt/VDC/*.***

8. Restore the application directory from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # cd /opt/
   # tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS

9. Restore trend data from the backup file spool/MMDDYY.HHMMSS using tar extract.
   # tar -xvf /opt/Install/spool.MMDDYY.HHMMSS

10. Restore python libraries.
    Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
    a. Stop any current running Python processes
       # ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'
    b. Remove the current Python libraries
       # rm -rf /usr/local/lib/python3.5/site-packages/
    c. Restore the Python libraries from the backup
       # tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar
    d. Set permission
       # chmod -R 755 /usr/local/lib/python3.5/site-packages/

Stage 5 - On the Master Server:

1. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
   a. For OS 6.*
      # ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc
   b. For OS 7.*
      # systemctl enable vdc
      You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

2. Enable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

   This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.

```
root@luisvdc50-7064:/opt/Install
0 2 * * *  /opt/VDC/bin/bkpvdc -a -q /opt/VDC.BACKUP
#0 4 * * * /opt/VDC/bin/cleanlogs
0 6 * * * /opt/VDC/bin/watchspace.sh
```

   For user root:

 # crontab -e
After deleting one # from each line, save and exit.
esc
:wq

Switch to vdc user.
 # su - vdc
$ **crontab -e**
After deleting one # from each line, save and exit.
esc
:wq

3. Exit vdc user
   $ **exit**

4. End the script capture log file.
   # exit
   Output when successfully exiting the script:
   ```
   Script done, file is /tmp/backup.log
   ```

5. Reboot the server.
   # reboot

6. After the Master reboots wait at least 10 minutes for the server to completely boot up. Confirm the server is fully functional by checking for the jsvc and postgres processes.
   a. Confirm the database is started. Find the postgres line as highlighted below.
      # ps -ef | grep postgres

```
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

   b. Confirm that jsvc has started. There are two jsvc process, one run by root and one run by vdc.
      # ps -eaf | grep jsvc

7. The master is now completely restored.

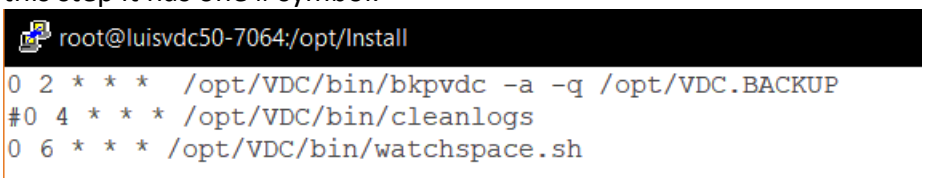
Stage 6 - On the Probe Server(s):

1. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
   a. For OS 6.*
      # ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc
   b. For OS 7.*
      # systemctl enable vdc
      You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

2. Enable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

   This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.



   For user root:

 # crontab -e
After deleting one # from each line, save and exit.
esc
:wq

Switch to vdc user.
 # su - vdc
$ **crontab -e**
After deleting one # from each line, save and exit.
esc
:wq

3. Exit vdc user
   $ **exit**

4. End the script capture log file.
   # exit
   Output when successfully exiting the script:
   ```
   Script done, file is /tmp/backup.log
   ```

5. Reboot the server.
   # reboot

6. After the Master reboots wait at least 10 minutes for the server to completely boot up. Confirm the server is fully functional by checking for the postgres and vms processes.
   a. Confirm the database is started. Find the postgres line as highlighted below.
      # ps -ef | grep postgres

```
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

   b. Confirm that vms has started.
      # ps -eaf | grep vms

7. The probe server is complete.

8. The system is ready for use, test web and 3D Client connections and monitoring activity to confirm.

Overview Multi-Server: Master & Probe Recovery on Different Servers

In some cases, an instance of the application must be restored to a new servers. In this situation, there are more configuration items which need to be considered as part of the restore process.

When working in multi-server environments the recovery process is done in stages. Alternating between servers at each stage. The order is critical.

Note: Follow the step-by-step instructions in each stage for each server in the order presented below. **DO NOT skip ahead!**

High-level overview of each stage:

- **Prerequisites -** Prepare the new servers as directed and save the licenses for use later
- **Stage 1 - On the Master Server:** start log, place and decompress backups, stop automatic processes, reboot, restart log
- **Stage 2 - On the Probe Server(s):** start log, retrieve data from new server, place and decompress backups, stop automatic processes, reboot, restart log
- **Stage 3 - On the Master Server:** start db, drop vdc_repos, create new db, restore vdcdb, remove application directory contents, restore application directory contents from backup, restore python libraries, get info from db and update, update IP address, update URL (if changed), remove old license, place new license, stop database
- **Stage 4 - On the Probe Server(s):** start db, drop vdc_sdb, create new db, restore sdb, remove application directory contents, restore application directory contents from backup, restore trend data, restore python libraries, update db with info retrieved earlier, update IP addresses, remove old license, place new license
- **Stage 5 - On the Master Server:** enable automatic processes, exit log script, reboot, verify server processes are running
- **Stage 6 - On the Probe Server(s):** enable automatic processes, exit log script, reboot, verify server processes are running, verify system web login, 3D client login and monitoring

Prerequisites for Mutli-Server: Master & Probe Recovery on Different Servers

- On the new servers install VDC following the same architecture type as your original servers with the 5.X version that matches the server to be recovered.

- Request and install licenses and confirm that your new instances are working.
    - Save the license files as you will need to place them back on the servers after the restore.
- **HTTPS - if your server is configured for HTTPS contact support for additional instructions before continuing with the restore**.

Steps for Multi-Server: Master & Probe Recovery on Different Servers

Note: Commands are in **bold** and can be copied and pasted to the server command line.
Do NOT copy the prompt indicators (#, $ or prompt text) preceding the commands.

Stage 1 - On the Master Server:

1. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS). Make note of the path to the desired backup.

2. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.** When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

3. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.
   # **script /tmp/backup_master.log**

4. Create the /opt/Install directory if it doesn't already exist.
   # **mkdir /opt/Install**

5. Place the desired backup date files from the old server's backup directory on the new server within the /opt/Install directory. Change directory to /opt/Install.
   # **cd /opt/Install**

   There should be the following files:

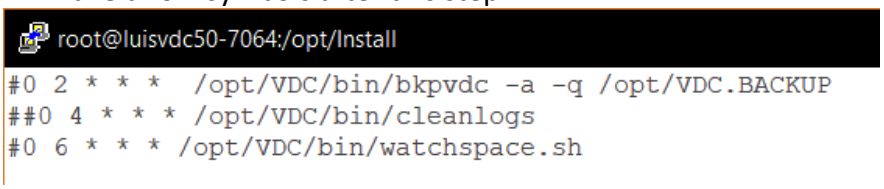
vdc.MMDDYY.HHMMSS.bz2
vdcdb.MMDDYY.HHMMSS.bz2
spool.MMDDYY.HHMMSS
site-packages.tar (optional)

Note: site-packages.tar is not always present, if it is process it as directed in later steps. If it is not present, do not be concerned.

6. Decompress the backup data
   NOTE: You do not need to decompress the spool or the site-packages files.
   # **bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2**
   # **bzip2 -d /opt/Install/vdcdb.MMDDYY.HHMMSS.bz2**

7. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the "crontab -e" command.
   The crontab editor functions like the vi editor.
   You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

   This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



   For user root:
   # **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.
   esc
   :wq

   Switch to vdc user. Note: The su command has a space on either side of the dash (-).
   # **su - vdc**
   $ **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.

esc
:wq

8. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
   $ **exit**
   a. For 6.* OS:
      # rm -rf /etc/rc5.d/S99vdc
   b. For 7.* OS:
      # systemctl disable vdc
      You should see the following message if the command ran properly.
      ```
      [root@vdc54-3073 ~]# systemctl disable vdc
      Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
      ```
   c. Reboot the server.
      # **reboot**
      Wait 5 minutes for the server to come back online.

9. Login as root when the server is back up.

10. Restart the log file to capture the next batch of commands for this backup activity**.**
    # **script -a /tmp/backup_master.log**

Stage 2 - On the Probe Server(s):

1. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of disk space depending on the size of the database. Ensure that you have enough room.

2. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS). Make note of the path to the desired backup.

3. Login as “root” user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you’re logged in as root the command line prompt will end in the # symbol**.**

When you su to another user the command line prompt will end in $ symbol**.**
Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

4. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.
   # **script /tmp/backup_probe.log**

5. Retrieve $SDBName and $ProbeName from the new server using the commands below, before starting the restore from the old server backup files.

   Note: If you have multiple probes the $SDBName and $ProbeName will be different. When you paste the information into a text file make note from which probe it was retrieved. The IP address imbedded in the name should be that of the current probe.

   a. Retrieve **$SDBName**
      # **cat /opt/VDC/bin/sdbinit.sh | grep -i "NAME" | sed -n 3p | awk -F'=' '{print $2}'**
      Example: sdb192.168.111.60
      Copy the SDBName to a text file for use in subsequent commands.
      This will be the $New_SDBName.

   b. Retrieve **$ProbeName**
      # **cat /opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties | grep -i "agent.name" | awk -F'=' '{print $2}'**
      Example: SP192.168.111.60
      Copy the ProbeName to a text file for use in subsequent commands.
      This will be the $New_ProbeName.

6. Create the /opt/Install directory if it doesn't already exist.
   # **mkdir /opt/Install**

7. Place the desired backup date files from the old server's backup directory on the new server within the /opt/Install directory.
   # **cd /opt/Install**

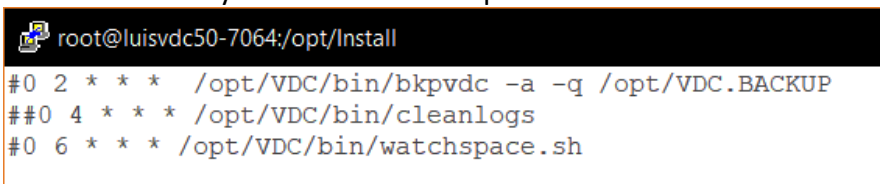
   There should be the following files:
   vdc.MMDDYY.HHMMSS.bz2
   sdb.MMDDYY.HHMMSS.bz2
   spool.MMDDYY.HHMMSS
   site-packages.tar (optional)

Note: site-packages.tar is not always present, if it is process it as directed in later steps. If it is not present, do not be concerned.

8. Decompress the backup data
   NOTE: You do not need to decompress the spool or the site-packages files.
   # **bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2**
   # **bzip2 -d /opt/Install/sdb.MMDDYY.HHMMSS.bz2**

9. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the "crontab -e" command.
   The crontab editor functions like the vi editor.
   You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

   This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



   For user root:
   # **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.
   esc
   :wq

   Switch to vdc user. Note: The su command has a space on either side of the dash (-).
   # **su - vdc**
   $ **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.
   esc

:wq

10. Become root user and disable the Auto-start.
    Note: The command is different depending on the Operating System version.
    $ **exit**
    a. For 6.* OS:
       # **rm -rf /etc/rc5.d/S99vdc**
    b. For 7.* OS:
       # **systemctl disable vdc**
       You should see the following message if the command ran properly.

```
[root@vdc54-3073 ~]# systemctl disable vdc
Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
```

    c. Reboot the server.
       # **reboot**
       Wait 5 minutes for the server to come back online.

11. Login as root when the server is back up.

12. Restart the log file to capture the next batch commands for this backup activity**.**
    # **script -a /tmp/backup_probe.log**

Stage 3 - On the Master Server:

1. From root change to the postgres user.
   # **su - postgres**

2. Start the database.
   $ **/usr/local/pgsql/bin/pg_ctl -D data start**
   Hit enter until you see the prompt.
   Confirm the database is started.
   $ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

3. Drop vdc_repos
   The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

   /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
   UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_repos';
   ALTER DATABASE vdc_repos CONNECTION LIMIT 1;
   SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_repos';
   DROP DATABASE vdc_repos;
   __EOF__

4. Create the new Postgres database instance
   $ **/usr/local/pgsql/bin/createdb -h vdchost-db -U root vdc_repos**

5. Run the import command for vdc_repos to import the desired backup file "vdcdb.MMDDYY.HHMMSS"

   $ **/usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos < /opt/Install/vdcdb.MMDDYY.HHMMSS**

   Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

6. Exit postgres user.
   $ **exit**

7. Clear the current application directory.
   # **rm -rf /opt/VDC**
   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # **rm -rf /opt/VDC/***
   # **rm -rf /opt/VDC/*.***

8. Restore the application from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # **cd /opt/**
   # **tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS**

9. Restore python libraries.
   Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.

a. Stop any current running Python processes
   # **ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'**
b. Remove the current Python libraries
   # **rm -rf /usr/local/lib/python3.5/site-packages/**
c. Restore the Python libraries from the backup
   # **tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar**
d. Set permission
   # **chmod -R 755 /usr/local/lib/python3.5/site-packages/**

10. This step is only required if you're new server is CentOS/RedHat 7.* and the old server was CentOS/RedHat 6*. There are 2 commands that need to be run.

    a. **# cp /opt/VDC/tomcat/conf/server.xml /opt/VDC/tomcat/conf/server.xml.back**

    b. The lines that follow are one line, copy and paste into the command line.
       # sed -i -e 's/Connector address="vdchost-server" port="80" protocol="org.apache.coyote.http11.Http11NioProtocol/Connector address="localhost" port="12008" protocol="org.apache.coyote.http11.Http11NioProtocol/g' /opt/VDC/tomcat/conf/server.xml

11. Log in to vdc_repos.
    # **/usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos**
    The prompt changes to vdc_repos=#.

12. Update registered Probe process info in the repos database.
    Note: If you have more than 1 probe you will have to make the updates for each probe entry.
    a. Retrieve the Probe ID
       vdc_repos=# **select name,id from server.process_info where type_id = 1;**

```
vdc_repos=# select name,id from server.process_info where type_id = 1;
       name       |                  id
------------------+--------------------------------------
 SP192.168.111.74 | 53969044-6a5b-11e8-9c51-000c29c6350b
(1 row)
```

       Copy the Probe ID(s) to a text file for use in subsequent commands.

    b. Update the Probe IP address. Run this command for each probe on your system.
       Note: The three lines below are one long command. When you copy, drag to select all three lines and it will paste as one line.

       vdc_repos=# **update server.process_info set name =**

'$New_ProbeName',option = format('<opt serviceType="1" url="rmi://$New_Probe_IP:12004/RmiService"/>')::xml where id = '$ProbeID';

Example:
vdc_repos=# update server.process_info set name = '**SP192.168.111.73**',option = format('<opt serviceType="1" url="rmi://**192.168.111.73**:12004/RmiService"/>')::xml where id = '**53969044-6a5b-11e8-9c51-000c29c6350b**';

13. Update registered SDB in the repos database. Run this command for each probe on your system.
    a. Retrieve the SDB ID
    vdc_repos=# **select name,id from mac.sdb;**

```
vdc_repos=# select id,name from mac.sdb;
                  id                  |        name
--------------------------------------+--------------------
 5395ee50-6a5b-11e8-a657-000c29c6350b | sdb192.168.111.74
(1 row)
```

    Copy the SDB ID to a text file for use in subsequent command.
    Note: The SDB ID is a similar but different number than Probe ID above. Please copy and save as requested. You will need both IDs in subsequent commands

    b. Update the SDB IP address. Run this for each probe on your system.
    vdc_repos=# **update mac.sdb set name = '$New_SDBName', jdbcurl = 'jdbc:postgresql://$New_Probe_IP:5432/vdc_sdb?sslmode=verify-ca&user=root&ApplicationName=sdb', host = '$New_Probe_IP' where id = '$SDBID';**

    Example:
    update mac.sdb set name = '**sdb192.168.111.73**', jdbcurl = 'jdbc:postgresql://**192.168.111.73**:5432/vdc_sdb?sslmode=verify-ca&user=root&ApplicationName=sdb', host = '**192.168.111.73**' where id = '**5395ee50-6a5b-11e8-a657-000c29c6350b**';

14. Exit repos database
    vdc_repos=# **\q**

15. Run the newip command to update some of the entries.
    # **/opt/VDC/bin/newip OLD_Master_IP NEW_Master_IP**

Example: *# /opt/VDC/bin/newip 192.168.111.64 192.168.111.60*
Note: Ensure that you are only entering actual IP addresses. If your OLD IP address is 127.0.0.1 contact support for additional instructions.

16. In the .conf file replace any instances of the old IP address with new IP address.
    a. Change to the /opt/VDC directory
       # cd /opt/VDC
    b. Backup the existing .conf file.
       # cp .conf conf-backup
    c. Run the following command to make the changes to the .conf file.
       # sed -i -e 's/OLD_Master_IP/NEW_Master_IP/g' /opt/VDC/.conf

17. Verify the changes were made.
    # grep NEW_Master_IP .conf

    You should see these 4 lines from the file with the new IP address.

```
[root@vdc54p-7074 061418.020002]# grep .73 /opt/VDC/.conf
VDCDBIP@ibuilder/conf/.ib.rc=192.168.111.73
VDCIP@/opt/VDC/vdcmon/conf/content=192.168.111.73
VDCDBIP@/opt/VDC/db/conf/30min.dbjobs.properties=192.168.111.73
VDCDBIP@/opt/VDC/VDCMPCollect/conf/rpt_collect.properties=192.168.111.73
```

18. Run /opt/VDC/bin/vdcconf to push values from the .conf file to all the appropriate locations.
    # /opt/VDC/bin/vdcconf

19. Update the URL.
    Note: If the URL has not been changed, you can skip this step.
    # /opt/VDC/bin/newurl OLD_URL NEW_URL

    Example: *# /opt/VDC/bin/newurl luisvdc50-7064 vdc54-3060.opi.zone*

20. Remove the old license file.
    # rm -rf /opt/VDC/.vdc/*.vdc

21. Place the new license file from the prerequisite stage in /opt/VDC/.vdc.

22. Reset permissions.
    # /opt/VDC/bin/setperm

23. Stop the postgres processes
    # su - postgres -c "/usr/local/pgsql/bin/pg_ctl -D /usr/local/pgsql/data stop -m immediate"

Stage 4 - On the Probe Server(s):

1. From root change to the postgres user.
   # su - postgres

2. Start the database.
   $ **/usr/local/pgsql/bin/pg_ctl -D data start**
   Hit enter until you see the prompt.
   Confirm the database is started.
   $ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

3. Drop vdc_sdb.
   The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

   /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
   UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_sdb';
   ALTER DATABASE vdc_sdb CONNECTION LIMIT 1;
   SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_sdb';
   DROP DATABASE vdc_sdb;
   __EOF__

4. Create the new Postgres database instance.
   $ **/usr/local/pgsql/bin/createdb -h vdchost-probe -U root vdc_sdb**

5. Run the import command for vdc_sdb to import the desired backup file "sdb.MMDDYY.HHMMSS"

$ **/usr/local/pgsql/bin/psql -h vdchost-probe -U root vdc_sdb < /opt/Install/sdb.MMDDYY.HHMMSS**

Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

6. Exit postgres user, return to root and clear the current application directory.
   $ **exit**
   # **rm -rf /opt/VDC**
   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # **rm -rf /opt/VDC/***
   # **rm -rf /opt/VDC/*.***

7. Restore the application from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # **cd /opt/**
   # **tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS**

8. Restore trend data from the backup file spool/MMDDYY.HHMMSS using tar extract.
   # **tar -xvf /opt/Install/spool.MMDDYY.HHMMSS**

9. Restore python libraries.
   Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
   a. Stop any current running Python processes
      # **ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'**
   b. Remove the current Python libraries
      # **rm -rf /usr/local/lib/python3.5/site-packages/**
   c. Restore the Python libraries from the backup
      # **tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar**
   d. Set permission
      # **chmod -R 755 /usr/local/lib/python3.5/site-packages/**

10. Login to the sdb database.
   # **/usr/local/pgsql/bin/psql -h vdchost-probe -U root vdc_sdb**
   prompt changes to vdc_sdb=#

11. Update the IP address in rc.sdb_info. You will use the $SDBID you retrieved earlier.
   NOTE: Ensure that you are using the $New_SDBName and $SDBID that corresponds to the current probe server.

vdc_sdb=# **update rc.sdb_info set name = '$New_SDBName' where id = '$SDBID';**

Example:
vdc_sdb=# update rc.sdb_info set name = '**sdb192.168.111.73**' where id = '**5395ee50-6a5b-11e8-a657-000c29c6350b**';

12. Quit from the vdc_repos database to return to root.
    vdc_sdb=# **\q**

13. Run the newip command to update some of the entries.
    NOTE: On the probe you will need to update the ip addresses for both the master and the current probe. You will run newip twice.

    a. # **/opt/VDC/bin/newip OLD_Probe_IP NEW_Probe_IP**
       Example: *# /opt/VDC/bin/newip 192.168.111.64 192.168.111.60*
       Note: Ensure that you are only entering actual IP addresses. If your OLD IP address is 127.0.0.1 contact support for additional instructions.

    b. # **/opt/VDC/bin/newip OLD_Master_IP NEW_Master_IP**
       Example: *# /opt/VDC/bin/newip 192.168.111.48 192.168.111.80*
       Note: Ensure that you are only entering actual IP addresses. If your OLD IP address is 127.0.0.1 contact support for additional instructions.

14. In the .conf file replace any instances of the old IP address with new IP address.
    NOTE: On the probe you will need to update the ip addresses for both the master and the current probe. You will run the sed command twice.

    a. Change to the /opt/VDC directory
       # **cd /opt/VDC**
    b. Backup the existing .conf file.
       # **bp .conf conf-backup**
    c. Run the following command to make the changes to the .conf file.
       # sed -i -e 's/OLD_Probe_IP/NEW_Probe_IP/g' /opt/VDC/.conf
    d. Run the following command to make the changes to the .conf file.
       # sed -i -e 's/OLD_Master_IP/NEW_Master_IP/g' /opt/VDC/.conf
    e. Verify the changes were made for NEW_Probe_IP.
       # grep NEW_Probe_IP .conf

You should see these 4 lines from the file with the new IP address.

```
[root@vdc54-3073 ~]# grep .73 /opt/VDC/.conf
SDBNAME@/opt/VDC/bin/sdbinit.sh=sdb192.168.111.73
AGENTTRAPIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties=192.168.111.73
AGENTNAME@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties=SP192.168.111.73
AGENTRMISERVICEIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties=192.168.111.73
```

f. Verify changes were made for NEW_Master_IP.
 # grep NEW_Master_IP .conf

You should see these 4 lines from the file with the new IP address.

```
[root@vdc54-3073 ~]# grep .74 /opt/VDC/.conf
DISCOVERYMASTERHOST@/opt/VDC/monitor/vms/webapps/discovery/WEB-INF/classes/master.properties=192.168.111.74
MDBIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/MDB.properties=192.168.111.74
EMPSERVERIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Probe.properties=192.168.111.74
VDCDBIP@/opt/VDC/tools/SNMPAgent/config/SAS.rc=192.168.111.74
[root@vdc54-3073 ~]#
```

15. Run /opt/VDC/bin/vdcconf to push values from the .conf file to all the appropriate locations.
/opt/VDC/bin/vdcconf

16. Remove the old license file.
rm -rf /opt/VDC/.vdc/*.vdc

17. Place the new license file from the prerequisite stage in /opt/VDC/.vdc.

18. Reset permissions.
/opt/VDC/bin/setperm

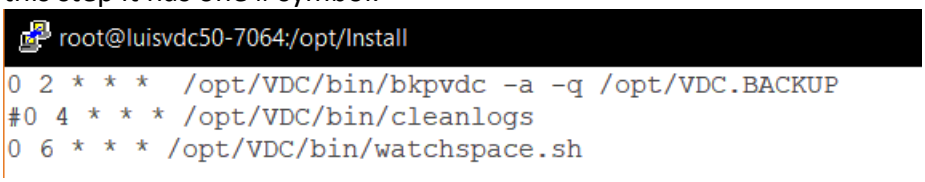
Stage 5 - On the Master Server:

1. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
   a. For OS 6.*
   # ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc
   b. For OS 7.*
   # **systemctl enable vdc**
   You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

2. Enable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.



For user root:
crontab -e
After deleting one # from each line, save and exit.
esc
:wq

Switch to vdc user.
su - vdc
$ **crontab -e**
After deleting one # from each line, save and exit.
esc
:wq

3. Exit vdc user.
   $ **exit**

4. End the script capture log file.
   # **exit**
   Output when successfully exiting the script:
   ```
   Script done, file is /tmp/backup.log
   ```

5. Reboot the server.
   # **reboot**

6. After the Master reboots wait at least 10 minutes for the server to completely start. Confirm the server is fully functional by checking for the postgress and jsvc processes.

   a. Confirm the database is started. Find the postgres line as highlighted below.
      # **ps -ef | grep postgres**

```
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

b. Confirm that jsvc has started. There are two jsvc process, one run by root and one run by vdc.
 # ps -eaf | grep jsvc

19. The master is now completely restored.

Stage 6 - On the Probe Server(s):

1. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
    a. For OS 6.*
    # ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc

b. For OS 7.*
 # systemctl enable vdc
You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

2. Enable cronjobs for root user and then for the vdc user.
   To edit the crontab use the "crontab -e" command.
   The crontab editor functions like the vi editor.
   You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

   This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.

```
root@luisvdc50-7064:/opt/Install
0 2 * * *  /opt/VDC/bin/bkpvdc -a -q /opt/VDC.BACKUP
#0 4 * * * /opt/VDC/bin/cleanlogs
0 6 * * * /opt/VDC/bin/watchspace.sh
```

   For user root:
   # **crontab -e**
   After deleting one # from each line, save and exit.
   esc
   :wq

   Switch to vdc user.
   # **su - vdc**
   $ **crontab -e**
   After deleting one # from each line, save and exit.
   esc
   :wq

3. Exit vdc user
   $ **exit**

4. End the script capture log file.
   # **exit**
   Output when successfully exiting the script:

```
Script done, file is /tmp/backup.log
```

5. Reboot the server.
   # **reboot**

6. After the Master reboots wait at least 10 minutes for the server to completely boot up. Confirm the server is fully functional by checking for the postgres and vms processes.
   a. Confirm the database is started. Find the postgres line as highlighted below.
      # **ps -ef | grep postgres**

```
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

   b. Confirm that vms has started.
      # **ps -eaf | grep vms**

```
[root@vdc54p-7074 ~]# ps -ef |grep vms
root      3977     1 60 15:48 ?        00:00:40 /opt/VDC/jdk/bin/java -Djava.util.log
ging.config.file=/opt/VDC/monitor/vms/conf/logging.properties -Djava.util.logging.man
ager=org.apache.juli.ClassLoaderLogManager -Djava.awt.headless=true -server -Xms800m
-Xmx2000m -XX:PermSize=512m -XX:MaxPermSize=256m -XX:MaxNewSize=128m -XX:-UseGCOverhe
adLimit -Duser.timezone=US/Eastern -Djava.endorsed.dirs=/opt/VDC/monitor/vms/endorsed
 -classpath /opt/VDC/monitor/vms/bin/bootstrap.jar:/opt/VDC/monitor/vms/bin/tomcat-ju
li.jar -Dcatalina.base=/opt/VDC/monitor/vms -Dcatalina.home=/opt/VDC/monitor/vms -Dja
va.io.tmpdir=/opt/VDC/monitor/vms/temp org.apache.catalina.startup.Bootstrap start
root      4239  3029  0 15:49 pts/0    00:00:00 grep --color=auto vms
[root@vdc54p-7074 ~]#
```

7. The probe server is complete.

8. The system is ready for use, test web and 3D Client connections and monitoring activity to confirm.

Multi-Server: Master DB, Master & Probe Recovery

In this use case there are at least three servers:

- Master DB server - runs the Master DB application processes
- Master server - runs the Master application processes
- Probe server - runs the Probe data collection and Probe database processes. There can be more than one Probe server.

Overview Multi-Server: Master DB, Master & Probe Recovery on the Same Servers

If customer administrators have issues with the integrity of the application or database, the following instructions can be followed to recover backed-up copies onto the same server production instances.

When working in multi-server environments the recovery process is done in stages. Alternating between servers at each stage. The order is critical.

Note: Follow the step-by-step instructions in each stage for each server in the order presented below. **DO NOT skip ahead!**

High-level overview of each stage:

- **Stage 1 - On the Master DB Server:** start log, copy and decompress backups, stop automatic processes, reboot, restart log
- **Stage 2 - On the Master Server:** start log, copy and decompress backups, stop automatic processes, reboot, restart log
- **Stage 3 - On the Probe Server(s):** start log, copy and decompress backups, stop automatic processes, reboot, restart log
- **Stage 4 - On the Master DB Server:** start db, drop vdc_repos, create new db, restore vdcdb, remove application directory contents, restore application directory contents from backup, restore python libraries, stop database
- **Stage 5 - On the Master Server:** remove application directory contents, restore application directory contents from backup, restore python libraries
- **Stage 6 - On the Probe Server(s):** start db, drop vdc_sdb, create new db, restore sdb, remove application directory contents, restore application directory contents from backup, restore trend data, restore python libraries

- **Stage 7 - On the Master DB Server:** enable automatic processes, exit log script, reboot, verify server processes are running
- **Stage 8 - On the Master Server:** enable automatic processes, exit log script, reboot, verify server processes are running
- **Stage 9 - On the Probe Server(s):** enable automatic processes, exit log script, reboot, verify server processes are running, verify system web login, 3D client login and monitoring

Steps for Multi-Server: Master DB, Master & Probe Recovery on the Same Servers

Stage 1 - On the Master DB Server:

1. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS).

2. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.** When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

3. Create the /opt/Install directory if it doesn't already exist.
   # **mkdir /opt/Install**

4. From the Master server retrieve the file /opt/VDC.BACKUP/vdcdb.MMDDYY.HHMMSS.bz2 and place it in the /opt/Install directory on the Master DB server.

5. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of disk space depending on the size of the database. Ensure that you have enough room.

6. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.

 # script /tmp/backup_masterdb.log

7. Navigate to the day/date directory on the Master DB server that contains the last known good backup files.
   # cd /opt/VDC.BACKUP/day/MMDDYY.HHMMSS
   Copy all of the files to /opt/Install.
   # cp ./* /opt/Install

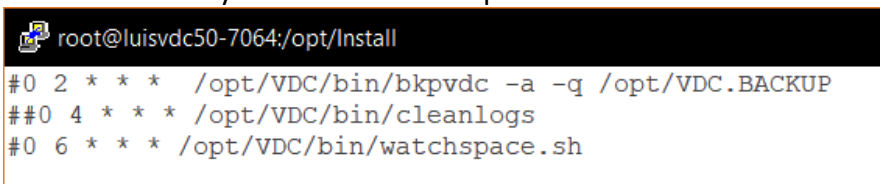
   There should be the following files:
   vdc.MMDDYY.HHMMSS.bz2
   vdcdb.MMDDYY.HHMMSS.bz2 (placed from the Master Server)
   spool.MMDDYY.HHMMSS
   site-packages.tar (optional)

   Note: site-packages.tar is not always present, if it is process it as directed in later steps. If it is not present, do not be concerned.

8. Decompress the backup data
   Note: You do not need to decompress the spool or the site-packages files.
   # bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2
   # bzip2 -d /opt/Install/vdcdb.MMDDYY.HHMMSS.bz2

9. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

   This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



   For user root:
   # crontab -e
   Change to insert mode.
   i
   After adding one # to each line, save and exit.

esc
:wq

Switch to vdc user. Note: The su command has a space on either side of the dash (-).
su - vdc
$ **crontab -e**
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

10. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
    $ **exit**
    a. For 6.* OS:
       # **rm -rf /etc/rc5.d/S99vdc**
    a. For 7.* OS:
       # **systemctl disable vdc**
       You should see the following message if the command ran properly.

```
[root@vdc54-3073 ~]# systemctl disable vdc
Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
```

    b. Reboot the server.
       # **reboot**
       Wait 5 minutes for the server to come back online.

11. Login as root when the server is back up.

12. Restart the log file to capture the next batch commands for this backup activity**.**
    # **script -a /tmp/backup_masterdb.log**

Stage 2 - On the Master Server:

1. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of disk space depending on the size of the database. Ensure that you have enough room.

2. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day

directory contains directories named for the date and time (MMDDYY.HHMMSS). Make note of the path to the desired backup.

3. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.**
   When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

4. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.
   # **script /tmp/backup_master.log**

5. Create the /opt/Install directory if it doesn't already exist.
   # **mkdir /opt/Install**

6. Navigate to the day/date directory that contains the last known good backup files.
   # **cd /opt/VDC.BACKUP/day/MMDDYY.HHMMSS**
   Copy all of the files to /opt/Install.
   # **cp ./* /opt/Install**

   There should be the following files:
   vdc.MMDDYY.HHMMSS.bz2
   vdcdb.MMDDYY.HHMMSS.bz2 (this file is not used on the Master Server)
   spool.MMDDYY.HHMMSS
   site-packages.tar (optional)

   Note: site-packages.tar is not always present, if it is process it as directed in later steps. If it is not present, do not be concerned.

7. Decompress the backup data
   NOTE: You do not need to decompress the spool or the site-packages files.
   # **bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2**

8. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the "crontab -e" command.
   The crontab editor functions like the vi editor.

You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.

```
root@luisvdc50-7064:/opt/Install
#0 2 * * *  /opt/VDC/bin/bkpvdc -a -q /opt/VDC.BACKUP
##0 4 * * * /opt/VDC/bin/cleanlogs
#0 6 * * * /opt/VDC/bin/watchspace.sh
```

For user root:
crontab -e
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

Switch to vdc user. Note: The su command has a space on either side of the dash (-).
su - vdc
$ crontab -e
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

9. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
   $ **exit**
   a. For 6.* OS:
      # **rm -rf /etc/rc5.d/S99vdc**
   b. For 7.* OS:
      # **systemctl disable vdc**
      You should see the following message if the command ran properly.

```
[root@vdc54-3073 ~]# systemctl disable vdc
Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
```

   b. Reboot the server.
      # **reboot**

Wait 5 minutes for the server to come back online.

10. Login as root when the server is back up.

11. Restart the log file to capture the next batch commands for this backup activity**.**
    # **script -a /tmp/backup_master.log**

Stage 3 - On the Probe Server(s):

2. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of disk space depending on the size of the database. Ensure that you have enough room.

3. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS). Make note of the path to the desired backup.

4. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.**
   When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

5. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.
   # **script /tmp/backup_probe.log**

   For example: script /tmp/backup_master.log

6. Create the /opt/Install directory if it doesn't already exist.
   # **mkdir /opt/Install**

7. Navigate to the day/date directory that contains the last known good backup files.
   # **cd /opt/VDC.BACKUP/day/MMDDYY.HHMMSS**
   Copy all of the files to /opt/Install.
   # **cp ./* /opt/Install**

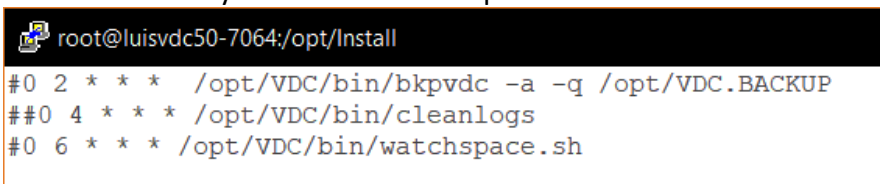
There should be the following files:
vdc.MMDDYY.HHMMSS.bz2
sdb.MMDDYY.HHMMSS.bz2
spool.MMDDYY.HHMMSS
site-packages.tar (optional)

Note: site-packages.tar is not always present, if it is process it as directed in later steps. If it is not present, do not be concerned.

8. Decompress the backup data
   NOTE: You do not need to decompress the spool or the site-packages files.
   # **bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2**
   # **bzip2 -d /opt/Install/sdb.MMDDYY.HHMMSS.bz2**

9. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the "crontab -e" command.
   The crontab editor functions like the vi editor.
   You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

   This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



   For user root:
   # **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.
   esc
   :wq

   Switch to vdc user. Note: The su command has a space on either side of the dash (-).
   # **su - vdc**
   $ **crontab -e**
   Change to insert mode.

i
After adding one # to each line, save and exit.
esc
:wq

10. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
    $ **exit**
    a. For 6.* OS:
       # **rm -rf /etc/rc5.d/S99vdc**
    b. For 7.* OS:
       # **systemctl disable vdc**
       You should see the following message if the command ran properly.

```
[root@vdc54-3073 ~]# systemctl disable vdc
Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
```

    c. Reboot the server.
       # **reboot**
       Wait 5 minutes for the server to come back online.

11. Login as root when the server is back up.

12. Restart the log file to capture the next batch commands for this backup activity**.**
    # **script -a /tmp/backup_probe.log**

Stage 4 - On the Master DB Server:

1. From root change to the postgres user.
   # **su - postgres**

2. Start the database.
   $ **/usr/local/pgsql/bin/pg_ctl -D data start**
   Hit enter until you see the prompt.
   Confirm the database is started.
   $ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

3. Drop vdc_repos
   The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

   /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
   UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_repos';
   ALTER DATABASE vdc_repos CONNECTION LIMIT 1;
   SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_repos';
   DROP DATABASE vdc_repos;
   __EOF__

4. Create the new Postgres database instance
   $ **/usr/local/pgsql/bin/createdb -h vdchost-db -U root vdc_repos**

5. Run the import command for vdc_repos to import the desired backup file "vdcdb.MMDDYY.HHMMSS"

   $ **/usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos < /opt/Install/vdcdb.MMDDYY.HHMMSS**

   Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

6. Exit postgres user
   $ **exit**

7. Clear the current application directory.
   # **rm -rf /opt/VDC**
   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # **rm -rf /opt/VDC/***

 # rm -rf /opt/VDC/*.*

8. Restore the application directory from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # cd /opt/
   # tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS

9. Restore python libraries.
   Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
   a. Stop any current running Python processes
      # ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'
   b. Remove the current Python libraries
      # rm -rf /usr/local/lib/python3.5/site-packages/
   c. Restore the Python libraries from the backup
      # tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar
   d. Set permission
      # chmod -R 755 /usr/local/lib/python3.5/site-packages/

10. Stop the postgres processes
    # su - postgres -c "/usr/local/pgsql/bin/pg_ctl -D /usr/local/pgsql/data stop -m immediate"

Stage 5 - On the Master Server:

1. Clear the current application directory.
   # rm -rf /opt/VDC
   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # rm -rf /opt/VDC/*
   # rm -rf /opt/VDC/*.*

2. Restore the application directory from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # cd /opt/
   # tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS

3. Restore python libraries.
   Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
   a. Stop any current running Python processes
      # ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'

b. Remove the current Python libraries
 # rm -rf /usr/local/lib/python3.5/site-packages/
c. Restore the Python libraries from the backup
 # tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar
d. Set permission
 # chmod -R 755 /usr/local/lib/python3.5/site-packages/

Stage 6 - On the Probe Server(s):

1. From root change to the postgres user.
 # su - postgres

2. Start the database.
$ **/usr/local/pgsql/bin/pg_ctl -D data start**
Hit enter until you see the prompt.
Confirm the database is started.
$ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

3. Drop vdc_sdb.
The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

/usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_sdb';
ALTER DATABASE vdc_sdb CONNECTION LIMIT 1;
SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_sdb';
DROP DATABASE vdc_sdb;
__EOF__

4. Create the new Postgres database instance.
$ **/usr/local/pgsql/bin/createdb -h vdchost-probe -U root vdc_sdb**

5. Run the import command for vdc_sdb to import the desired backup file "sdb.MMDDYY.HHMMSS"

   $ **/usr/local/pgsql/bin/psql -h vdchost-probe -U root vdc_sdb < /opt/Install/sdb.MMDDYY.HHMMSS**

   Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

6. Exit postgres user
   $ **exit**

7. Clear the current application directory.
   # **rm -rf /opt/VDC**
   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # **rm -rf /opt/VDC/***
   # **rm -rf /opt/VDC/*.***

8. Restore the application directory from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # **cd /opt/**
   # **tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS**

9. Restore trend data from the backup file spool/MMDDYY.HHMMSS using tar extract.
   # **tar -xvf /opt/Install/spool.MMDDYY.HHMMSS**

4. Restore python libraries.
   Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
   a. Stop any current running Python processes
      # **ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'**
   b. Remove the current Python libraries
      # **rm -rf /usr/local/lib/python3.5/site-packages/**
   c. Restore the Python libraries from the backup
      # **tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar**
   d. Set permission
      # **chmod -R 755 /usr/local/lib/python3.5/site-packages/**

Stage 7 - On the Master DB Server:

1. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
   a. For OS 6.*
      # **ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc**
   b. For OS 7.*
      # **systemctl enable vdc**
      You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

2. Enable cronjobs for root user and then for the vdc user.
   To edit the crontab use the "crontab -e" command.
   The crontab editor functions like the vi editor.
   You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

   This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.

```
root@luisvdc50-7064:/opt/Install
0 2 * * *  /opt/VDC/bin/bkpvdc -a -q /opt/VDC.BACKUP
#0 4 * * * /opt/VDC/bin/cleanlogs
0 6 * * * /opt/VDC/bin/watchspace.sh
```

   For user root:
   # **crontab -e**
   After deleting one # from each line, save and exit.
   esc
   :wq

   Switch to vdc user.
   # **su - vdc**
   $ **crontab -e**
   After deleting one # from each line, save and exit.
   esc
   :wq

3. Exit vdc user
   $ **exit**

4. End the script capture log file.
   # **exit**
   Output when successfully exiting the script:
   ```
   Script done, file is /tmp/backup.log
   ```

5. Reboot the server.
   # **reboot**

6. After the Master reboots wait at least 10 minutes for the server to completely boot up. Confirm the server is fully functional by checking for the postgres process. Find the postgres line as highlighted below.

   # **ps -ef | grep postgres**
   ```
   root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
   postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
   postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
   postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
   postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
   postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
   postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
   postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
   postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
   postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
   postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
   ```

7. The master db is now completely restored.

Stage 8 - On the Master Server:

1. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
   a. For OS 6.*
      # **ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc**
   b. For OS 7.*
      # **systemctl enable vdc**
      You should see the following message if the command ran properly.
      ```
      [root@vdc54mdb-3072 opt]# systemctl enable vdc
      Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
      ```

2. Enable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

   This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.

```
root@luisvdc50-7064:/opt/Install
0 2 * * *  /opt/VDC/bin/bkpvdc -a -q /opt/VDC.BACKUP
#0 4 * * * /opt/VDC/bin/cleanlogs
0 6 * * * /opt/VDC/bin/watchspace.sh
```

For user root:
crontab -e
After deleting one # from each line, save and exit.
esc
:wq

Switch to vdc user.
su - vdc
$ crontab -e
After deleting one # from each line, save and exit.
esc
:wq

3. Exit vdc user
   $ **exit**

4. End the script capture log file.
   # **exit**
   Output when successfully exiting the script:
   ```
   Script done, file is /tmp/backup.log
   ```

5. Reboot the server.
   # **reboot**

6. After the Master reboots wait at least 10 minutes for the server to completely boot up. Confirm the server is fully functional by checking for the jsvc processes. There are two jsvc process, one run by root and one run by vdc.
   # **ps -eaf | grep jsvc**

7. The master is now completely restored.

Stage 9 - On the Probe Server(s):

1. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
   a. For OS 6.*
      # ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc
   b. For OS 7.*
      # systemctl enable vdc
      You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

2. Enable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

   This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.

```
root@luisvdc50-7064:/opt/Install
0 2 * * *  /opt/VDC/bin/bkpvdc -a -q /opt/VDC.BACKUP
#0 4 * * * /opt/VDC/bin/cleanlogs
0 6 * * * /opt/VDC/bin/watchspace.sh
```

For user root:
crontab -e
After deleting one # from each line, save and exit.
esc
:wq

Switch to vdc user.
su - vdc
$ crontab -e
After deleting one # from each line, save and exit.
esc
:wq

3. Exit vdc user
   $ **exit**

4. End the script capture log file.
   # **exit**
   Output when successfully exiting the script:
   ```
   Script done, file is /tmp/backup.log
   ```

5. Reboot the server.
   # **reboot**

6. After the Master reboots wait at least 10 minutes for the server to completely boot up. Confirm the server is fully functional by checking for the postgres and vms processes.
   a. Confirm the database is started. Find the postgres line as highlighted below.
      # **ps -ef | grep postgres**

```
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

b. Confirm that vms has started.
 # ps -eaf | grep vms

7. The probe server is complete.

8. The system is ready for use, test web and 3D Client connections and monitoring activity to confirm.

Overview Multi-Server: Master DB, Master & Probe Recovery on Different Servers

In some cases, an instance of the application must be restored to a new servers. In this situation, there are more configuration items which need to be considered as part of the restore process.

When working in multi-server environments the recovery process is done in stages. Alternating between servers at each stage. The order is critical.

Note: Follow the step-by-step instructions in each stage for each server in the order presented below. **DO NOT skip ahead!**

High-level overview of each stage:

- **Prerequisites -** Prepare the new servers as directed and save the licenses for use later
- **Stage 1 - On the Master DB Server:** start log, place and decompress backups, stop automatic processes, reboot, restart log
- **Stage 2 - On the Master Server:** start log, place and decompress backups, stop automatic processes, reboot, restart log
- **Stage 3 - On the Probe Server(s):** start log, place and decompress backups, stop automatic processes, reboot, restart log
- **Stage 4 - On the Master DB Server:** start db, drop vdc_repos, create new db, restore vdcdb, remove application directory contents, restore application directory contents from backup, restore python libraries, get info from db and update, stop database
- **Stage 5 - On the Master Server:** remove application directory contents, restore application directory contents from backup, restore python libraries, update IP addresses, update URL (if changed), remove old license, place new license
- **Stage 6 - On the Probe Server(s):** start db, drop vdc_sdb, create new db, restore sdb, remove application directory contents, restore application directory contents from backup, restore trend data, restore python libraries, update db with info retrieved earlier, update IP addresses, remove old license, place new license
- **Stage 7 - On the Master DB Server:** enable automatic processes, exit log script, reboot, verify server processes are running
- **Stage 8 - On the Master Server:** enable automatic processes, exit log script, reboot, verify server processes are running
- **Stage 9 - On the Probe Server(s):** enable automatic processes, exit log script, reboot, verify server processes are running, verify system web login, 3D client login and monitoring

Prerequisites for Mutli-Server: Master DB, Master & Probe Recovery on a Different Servers

- On the new servers install VDC following the same architecture type as your original servers with the 5.X version that matches the server to be recovered.
- Request and install licenses and confirm that your new instances are working.
    - The Master and Probes will require licenses. The Master DB does not have a license.
    - Save the license files as you will need to place them back on the servers after the restore
- **HTTPS - if your server is configured for HTTPS contact support for additional instructions before continuing with the restore.**

Steps for Multi-Server: Master DB, Master & Probe Recovery on Different Servers

Stage 1 - On the Master DB Server:

1. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS).

2. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.**
   When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

3. Create the /opt/Install directory if it doesn't already exist.
   # **mkdir /opt/Install**

4. From the old Master server retrieve the file /opt/VDC.BACKUP/vdcdb.MMDDYY.HHMMSS.bz2 and place it in the /opt/Install directory on the new Master DB server.

5. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of

disk space depending on the size of the database. Ensure that you have enough room.

6. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.
   # **script /tmp/backup_masterdb.log**

7. Place the desired backup date files from the old server's backup directory on the new server within the /opt/Install directory. Change directory to /opt/Install.
   # **cd /opt/Install**

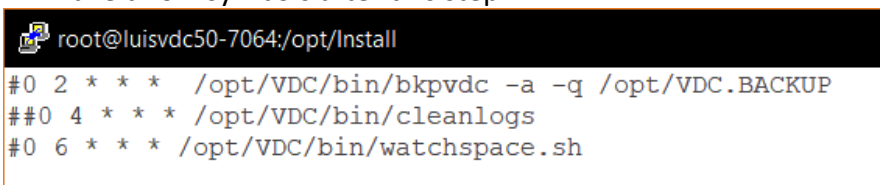
   There should be the following files:
   vdc.MMDDYY.HHMMSS.bz2
   vdcdb.MMDDYY.HHMMSS.bz2 (placed from the Master Server)
   spool.MMDDYY.HHMMSS
   site-packages.tar (optional)

   Note: site-packages.tar is not always present, if it is process it as directed in later steps. If it is not present, do not be concerned.

8. Decompress the backup data
   Note: You do not need to decompress the spool or the site-packages files.
   # **bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2**
   # **bzip2 -d /opt/Install/vdcdb.MMDDYY.HHMMSS.bz2**

9. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the "crontab -e" command.
   The crontab editor functions like the vi editor.
   You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

   This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



   For user root:
   # **crontab -e**

Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

Switch to vdc user. Note: The su command has a space on either side of the dash (-).
su - vdc
$ **crontab -e**
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

10. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
    $ **exit**
    a. For 6.* OS:
       # **rm -rf /etc/rc5.d/S99vdc**
    b. For 7.* OS:
       # **systemctl disable vdc**
       You should see the following message if the command ran properly.

```
[root@vdc54-3073 ~]# systemctl disable vdc
Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
```

    c. Reboot the server.
       # **reboot**
       Wait 5 minutes for the server to come back online.

11. Login as root when the server is back up.

12. Restart the log file to capture the next batch commands for this backup activity**.**
    # **script -a /tmp/backup_masterdb.log**

Stage 2 - On the Master Server:

1. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of

disk space depending on the size of the database. Ensure that you have enough room.

2. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS). Make note of the path to the desired backup.

3. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.** When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

4. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.
   # script /tmp/backup_master.log

5. Create the /opt/Install directory if it doesn't already exist.
   # mkdir /opt/Install

6. Place the desired backup date files from the old server's backup directory on the new server within the /opt/Install directory. Change directory to /opt/Install.
   # **cd /opt/Install**

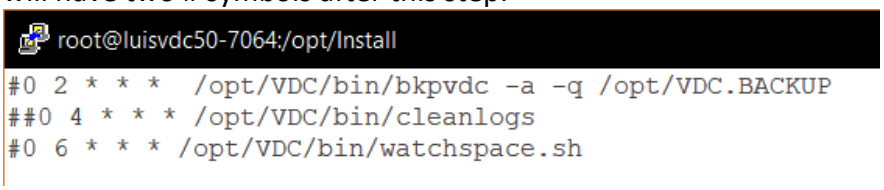
   There should be the following files:
   vdc.MMDDYY.HHMMSS.bz2
   vdcdb.MMDDYY.HHMMSS.bz2 (this file is not used on the Master Server)
   spool.MMDDYY.HHMMSS
   site-packages.tar (optional)

   Note: site-packages.tar is not always present, if it is process it as directed in later steps. If it is not present, do not be concerned.

7. Decompress the backup data
   Note: You do not need to decompress the spool or the site-packages files.
   # **bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2**

8. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

   This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



   For user root:
   # **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.
   esc
   :wq

   Switch to vdc user. Note: The su command has a space on either side of the dash (-).
   # **su - vdc**
   $ **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.
   esc
   :wq

9. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
   $ **exit**
   a. For 6.* OS:
      # **rm -rf /etc/rc5.d/S99vdc**
   b. For 7.* OS:
      # **systemctl disable vdc**
      You should see the following message if the command ran properly.

```
[root@vdc54-3073 ~]# systemctl disable vdc
Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
```

c. Reboot the server.
   # **reboot**
   Wait 5 minutes for the server to come back online.

10. Login as root when the server is back up.

11. Restart the log file to capture the next batch commands for this backup activity**.**
    # **script -a /tmp/backup_master.log**

Stage 3 - On the Probe Server(s):

1. Check disk space on the application server.
   # **df -h**
   Copying the backup files and decompressing them can take up significant amounts of disk space depending on the size of the database. Ensure that you have enough room.

2. Identify which backup you will use for the restore. The default backup directory is /opt/VDC.BACKUP. There you will find a directory for each day of the week. The day directory contains directories named for the date and time (MMDDYY.HHMMSS). Make note of the path to the desired backup.

3. Login as "root" user on the application server.
   Login as: **root**
   root@servername password: **rootpassword**
   #
   Note: When you're logged in as root the command line prompt will end in the # symbol**.** When you su to another user the command line prompt will end in $ symbol**.**
   Do not copy the *#, $* or *prompt text* at the beginning of the commands below.

4. Start a log file to capture all commands for this backup activity. This file is valuable for troubleshooting issues with the backup or recovery process. Name the backup log for the server you are working on.
   # **script /tmp/backup_probe.log**

   For example: script /tmp/backup_master.log

5. Create the /opt/Install directory if it doesn't already exist.
   # **mkdir /opt/Install**

6. Place the desired backup date files from the old server's backup directory on the new server within the /opt/Install directory. Change directory to /opt/Install.
   # **cd /opt/Install**

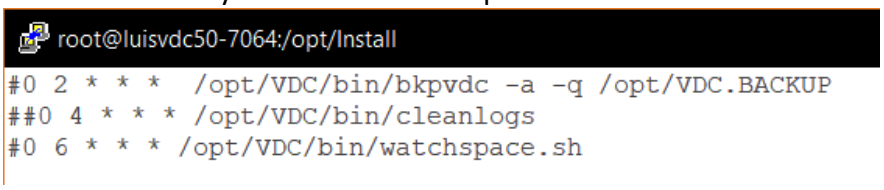
   There should be the following files:
   vdc.MMDDYY.HHMMSS.bz2
   sdb.MMDDYY.HHMMSS.bz2
   spool.MMDDYY.HHMMSS
   site-packages.tar (optional)

   Note: site-packages.tar is not always present, if it is process it as directed in later steps. If it is not present, do not be concerned.

7. Decompress the backup data
   Note: You do not need to decompress the spool or the site-packages files.
   # **bzip2 -d /opt/Install/vdc.MMDDYY.HHMMSS.bz2**
   # **bzip2 -d /opt/Install/sdb.MMDDYY.HHMMSS.bz2**

8. Disable cronjobs for root user and then for the vdc user.
   To edit the crontab use the "crontab -e" command.
   The crontab editor functions like the vi editor.
   You will be inserting a # symbol at the beginning of each and every line, including those that already have a # symbol.

   This example shows a crontab where the cleanlogs process was already disabled so it will have two # symbols after this step.



   For user root:
   # **crontab -e**
   Change to insert mode.
   i
   After adding one # to each line, save and exit.
   esc

:wq

Switch to vdc user. Note: The su command has a space on either side of the dash (-).
su - vdc
$ **crontab -e**
Change to insert mode.
i
After adding one # to each line, save and exit.
esc
:wq

9. Become root user and disable the Auto-start. Note: The command is different depending on the Operating System version.
   $ **exit**
   a. For 6.* OS:
      # **rm -rf /etc/rc5.d/S99vdc**
   b. For 7.* OS:
      # **systemctl disable vdc**
      You should see the following message if the command ran properly.
      ```
      [root@vdc54-3073 ~]# systemctl disable vdc
      Removed symlink /etc/systemd/system/multi-user.target.wants/vdc.service.
      ```
   c. Reboot the server.
      # **reboot**
      Wait 5 minutes for the server to come back online.

10. Login as root when the server is back up.

11. Restart the log file to capture the next batch commands for this backup activity**.**
    # **script -a /tmp/backup_probe.log**

Stage 4 - On the Master DB Server:

1. From root change to the postgres user.
   # **su - postgres**

2. Start the database.
   $ **/usr/local/pgsql/bin/pg_ctl -D data start**
   Hit enter until you see the prompt.
   Confirm the database is started.
   $ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

3. Drop vdc_repos
   The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

   /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
   UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_repos';
   ALTER DATABASE vdc_repos CONNECTION LIMIT 1;
   SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_repos';
   DROP DATABASE vdc_repos;
   __EOF__

4. Create the new Postgres database instance
   $ **/usr/local/pgsql/bin/createdb -h vdchost-db -U root vdc_repos**

5. Run the import command for vdc_repos to import the desired backup file "vdcdb.MMDDYY.HHMMSS"

   $ **/usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos < /opt/Install/vdcdb.MMDDYY.HHMMSS**

   Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

6. Exit postgres user, become vdc user and stop and start the replication between the master and slave database.
   $ **exit**
7. Clear the current application directory.
   # **rm -rf /opt/VDC**

   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # **rm -rf /opt/VDC/***

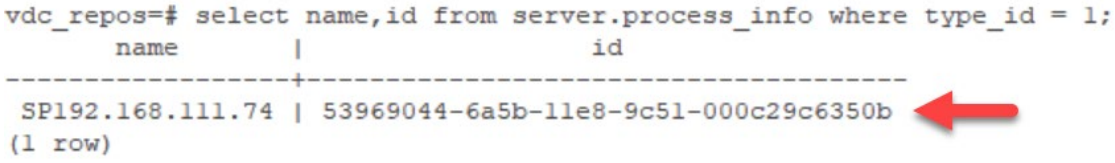
 # rm -rf /opt/VDC/*.*

8. Restore the application from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # cd /opt/
   # tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS

9. Restore python libraries.
   Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
   a. Stop any current running Python processes
      # ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'
   b. Remove the current Python libraries
      # rm -rf /usr/local/lib/python3.5/site-packages/
   c. Restore the Python libraries from the backup
      # tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar
   d. Set permission
      # chmod -R 755 /usr/local/lib/python3.5/site-packages/

10. Log in to vdc_repos.
    # /usr/local/pgsql/bin/psql -h vdchost-db -U root vdc_repos
    The prompt changes to vdc_repos=#.

11. Update registered Probe process info in the repos database.
    Note: If you have more than 1 probe you will have to make the updates for each probe entry.
    a. Retrieve the Probe ID
       vdc_repos=# **select name,id from server.process_info where type_id = 1;**



       Copy the Probe ID(s) to a text file for use in subsequent commands.

    b. Update the Probe Name (SP###.###.###) to new Probe Name and Probe IP address (###.###.###) to new Probe IP address. Run this command for each probe on your system.
       Note: The three lines below are one long command. When you copy, drag to select all three lines and it will paste as one line.
       vdc_repos=# **update server.process_info set name = '$NewProbeName',option**

= format('<opt serviceType="1"
url="rmi://$NewProbe_IP:12004/RmiService"/>')::xml where id = '$ProbeID';

Example:
vdc_repos=# update server.process_info set name = '**SP192.168.111.73**',option = format('<opt serviceType="1"
url="rmi://**192.168.111.73**:12004/RmiService"/>')::xml where id = '**53969044-6a5b-11e8-9c51-000c29c6350b**';

12. Update registered SDB in the repos database. Run this command for each probe on your system.
    a. Retrieve the SDB ID
    vdc_repos=# **select name,id from mac.sdb;**

```
vdc_repos=# select id,name from mac.sdb;
                  id                  |        name
--------------------------------------+--------------------
 5395ee50-6a5b-11e8-a657-000c29c6350b | sdb192.168.111.74
(1 row)
```

    Copy the SDB ID to a text file for use in subsequent command.
    Note: The SDB ID is a similar but different number than Probe ID above. Please copy and save as requested. You will need both IDs in subsequent commands

    b. Update the SDBName (sdb###.###.###) to the new SDBName and Probe IP address (###.###.###) to new Probe IP. Run this for each probe on your system.
    vdc_repos=# **update mac.sdb set name = '$NewSDBName', jdbcurl = 'jdbc:postgresql://$NewProbe_IP:5432/vdc_sdb?sslmode=verify-ca&user=root&ApplicationName=sdb', host = '$NewProbe_IP' where id = '$SDBID';**

    Example:
    update mac.sdb set name = '**sdb192.168.111.73**', jdbcurl = 'jdbc:postgresql://**192.168.111.73**:5432/vdc_sdb?sslmode=verify-ca&user=root&ApplicationName=sdb', host = '**192.168.111.73**' where id = '**5395ee50-6a5b-11e8-a657-000c29c6350b**';

13. Exit repos database
    vdc_repos=# **\q**

14. Reset permissions.
    # /opt/VDC/bin/setperm

15. Stop the postgres processes
    # su - postgres -c "/usr/local/pgsql/bin/pg_ctl -D /usr/local/pgsql/data stop -m immediate"

Stage 5 - On the Master Server

1. Clear the current application directory.
   # rm -rf /opt/VDC
   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # rm -rf /opt/VDC/*
   # rm -rf /opt/VDC/*.*

2. Restore the application from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # cd /opt/
   # tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS

3. Restore python libraries.
   Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
   a. Stop any current running Python processes
      # ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'
   b. Remove the current Python libraries
      # rm -rf /usr/local/lib/python3.5/site-packages/
   c. Restore the Python libraries from the backup
      # tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar
   d. Set permission
      # chmod -R 755 /usr/local/lib/python3.5/site-packages/

4. This step is only required if you're new server is CentOS/RedHat 7.* and the old server was CentOS/RedHat 6*. There are 2 commands that need to be run.

   a. **# cp /opt/VDC/tomcat/conf/server.xml /opt/VDC/tomcat/conf/server.xml.back**

   b. The lines that follow are one line, copy and paste into the command line.
      # sed -i -e 's/Connector address="vdchost-server" port="80" protocol="org.apache.coyote.http11.Http11NioProtocol/Connector address="localhost" port="12008" protocol="org.apache.coyote.http11.Http11NioProtocol/g' /opt/VDC/tomcat/conf/server.xml

5. Run the newip command twice to update Master DB and Master entries.
   # /opt/VDC/bin/newip OLD_MasterDB_IP NEW_MasterDB_IP
   # /opt/VDC/bin/newip OLD_Master_IP NEW_MasterDB_IP

   Example: *# /opt/VDC/bin/newip 192.168.111.64 192.168.111.60*
   Note: Ensure that you are only entering actual IP addresses. If your OLD IP address is

127.0.0.1 contact support for additional instructions.

6. In the .conf file you need to replace any instances of the old IP addresses with new IP addresses.
   a. Change to the /opt/VDC directory
      # cd /opt/VDC
   b. Backup the existing .conf file.
      # cp .conf conf-backup
   c. Run the following command twice to update Master DB IP and Master IP address entries in the .conf file.
      # sed -i -e 's/OLD_MasterDB_IP/NEW_MasterDB_IP/g' /opt/VDC/.conf
      # sed -i -e 's/OLD_Master_IP/NEW_Master_IP/g' /opt/VDC/.conf

7. Verify the changes were made.
   # grep NEW_MasterDB_IP .conf
   You should see these 3 lines from the file with the new MasterDB_IP address.
   ```
   VDCDBIP@ibuilder/conf/.ib.rc=192.168.111.73
   VDCDBIP@/opt/VDC/db/conf/30min.dbjobs.properties=192.168.111.73
   VDCDBIP@/opt/VDC/VDCMPCollect/conf/rpt_collect.properties=192.168.111.73
   ```
   # grep NEW_Master_IP.conf
   You should see this 1 line from the file with the new Master_IP address.
   ```
   VDCIP@/opt/VDC/vdcmon/conf/content=192.168.111.74
   ```

8. Run /opt/VDC/bin/vdcconf to push values from the .conf file to all the appropriate locations.
   # /opt/VDC/bin/vdcconf

9. Update the URL.
   Note: If the URL has not been changed, you can skip this step.
   # /opt/VDC/bin/newurl OLD_URL NEW_URL

   Example: *# /opt/VDC/bin/newurl luisvdc50-7064 vdc54-3060.opi.zone*

10. Remove the old license file.
    # rm -rf /opt/VDC/.vdc/*.vdc

11. Place the new license file from the prerequisite stage in /opt/VDC/.vdc.

12. Reset permissions.
    # /opt/VDC/bin/setperm

Stage 6 - On the Probe Server(s)

1. From root change to the postgres user.
   # su - postgres

2. Start the database.
   $ **/usr/local/pgsql/bin/pg_ctl -D data start**
   Hit enter until you see the prompt.
   Confirm the database is started.
   $ **ps -ef |grep postgres**

```
-bash-4.1$ ps -ef |grep postgres
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

3. Drop vdc_sdb.
   The command below is multiple lines, copy all of the bold text and paste after the command line prompt. The <<__EOF__ tags allow for multiple commands and multiple lines.

   /usr/local/pgsql/bin/psql -h 127.0.0.1 -U root postgres <<__EOF__
   UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'vdc_sdb';
   ALTER DATABASE vdc_sdb CONNECTION LIMIT 1;
   SELECT pg_terminate_backend (pg_stat_activity.pid) FROM pg_stat_activity WHERE pg_stat_activity.datname = 'vdc_sdb';
   DROP DATABASE vdc_sdb;
   __EOF__

4. Create the new Postgres database instance.
   $ **/usr/local/pgsql/bin/createdb -h vdchost-probe -U root vdc_sdb**

5. Run the import command for vdc_sdb to import the desired backup file "sdb.MMDDYY.HHMMSS"

   $ **/usr/local/pgsql/bin/psql -h vdchost-probe -U root vdc_sdb < /opt/Install/sdb.MMDDYY.HHMMSS**

   Note: The import time varies depending on the size of your database. The system will return to the prompt when the import is finished.

6. Exit postgres user.
   $ **exit**

7. Clear the current application directory.
   # **rm -rf /opt/VDC**
   Note: If you have /opt/VDC as a partition run the following commands to clear the directory.
   # **rm -rf /opt/VDC/***
   # **rm -rf /opt/VDC/*.***
8. Restore the application from the backup file vdc.MMDDYY.HHMMSS using tar extract.
   # **cd /opt/**
   # **tar -xvf /opt/Install/vdc.MMDDYY.HHMMSS**

9. Restore trend data from the backup file spool/MMDDYY.HHMMSS using tar extract.
   # **tar -xvf /opt/Install/spool.MMDDYY.HHMMSS**

10. Restore python libraries.
    Note: If there is not a site-packages.tar file in the /opt/Install directory, DO NOT execute any part of this step.
    a. Stop any current running Python processes
       # **ps -ef|grep python3|grep -v grep|awk '{system("kill -9 "$2)}'**
    b. Remove the current Python libraries
       # **rm -rf /usr/local/lib/python3.5/site-packages/**
    c. Restore the Python libraries from the backup
       # **tar -C /usr/local/lib/python3.5/ -xvf site-packages.tar**
    d. Set permission
       # **chmod -R 755 /usr/local/lib/python3.5/site-packages/**

11. Login to the sdb database.
    # **/usr/local/pgsql/bin/psql -h vdchost-probe -U root vdc_sdb**
    prompt changes to vdc_sdb=#

12. Update the IP address in rc.sdb_info. You will use the $SDBID you retrieved earlier.
    Note: Ensure that you are using the $New_SDBName and $SDBID that corresponds to the current probe server.

    vdc_sdb=# **update rc.sdb_info set name = '$New_SDBName' where id = '$SDBID';**

    Example:
    vdc_sdb=# update rc.sdb_info set name = '**sdb192.168.111.73**' where id = '**5395ee50-**

6a5b-11e8-a657-000c29c6350b';

13. Quit from the vdc_repos database to return to root.
    vdc_sdb=# **\q**

14. Run the newip command to update some of the entries.
    Note: On the probe you will need to update the ip addresses for the Master DB, Master and current Probe servers. You will run newip three times.
    Note: If newip is not present on the probe, copy it from the Master.

    a. # **/opt/VDC/bin/newip OLD_MasterDB_IP NEW_MasterDB_IP**
       Example: *# /opt/VDC/bin/newip 192.168.111.49 192.168.111.81*
       Note: Ensure that you are only entering actual IP addresses. If your OLD IP address is 127.0.0.1 contact support for additional instructions.

    b. # **/opt/VDC/bin/newip OLD_Master_IP NEW_Master_IP**
       Example: *# /opt/VDC/bin/newip 192.168.111.50 192.168.111.82*
       Note: Ensure that you are only entering actual IP addresses. If your OLD IP address is 127.0.0.1 contact support for additional instructions.

    c. # **/opt/VDC/bin/newip OLD_Probe_IP NEW_Probe_IP**
       Example: *# /opt/VDC/bin/newip 192.168.111.64 192.168.111.60*
       Note: Ensure that you are only entering actual IP addresses. If your OLD IP address is 127.0.0.1 contact support for additional instructions.

15. In the .conf file replace any instances of the old IP address with new IP address.
    Note: On the probe you will need to update the ip addresses for both the master and the current probe. You will run the sed command twice.

    a. Change to the /opt/VDC directory
       # **cd /opt/VDC**
    b. Backup the existing .conf file.
       # **cp .conf conf-backup**
    c. Run the following command to make the changes to the .conf file.
       # **sed -i -e 's/OLD_Probe_IP/NEW_Probe_IP/g' /opt/VDC/.conf**
    d. Run the following command to make the changes to the .conf file.
       # **sed -i -e 's/OLD_Master_IP/NEW_Master_IP/g' /opt/VDC/.conf**
    e. Verify the changes were made for NEW_Probe_IP.
       # **grep NEW_Probe_IP .conf**

You should see these 4 lines from the file with the new IP address.

```
[root@vdc54-3073 ~]# grep .73 /opt/VDC/.conf
SDBNAME@/opt/VDC/bin/sdbinit.sh=sdb192.168.111.73
AGENTTRAPIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties=192.168.111.73
AGENTNAME@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties=SP192.168.111.73
AGENTRMISERVICEIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Agent.properties=192.168.111.73
```

f. Verify changes were made for NEW_Master_IP.
 # grep NEW_Master_IP .conf

You should see these 4 lines from the file with the new IP address.

```
[root@vdc54-3073 ~]# grep .74 /opt/VDC/.conf
DISCOVERYMASTERHOST@/opt/VDC/monitor/vms/webapps/discovery/WEB-INF/classes/master.properties=192.168.111.74
MDBIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/MDB.properties=192.168.111.74
EMPSERVERIP@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/Probe.properties=192.168.111.74
VDCDBIP@/opt/VDC/tools/SNMPAgent/config/SAS.rc=192.168.111.74
[root@vdc54-3073 ~]#
```

16. Run /opt/VDC/bin/vdcconf to push values from the .conf file to all the appropriate locations.
/opt/VDC/bin/vdcconf

17. Remove the old license file.
rm -rf /opt/VDC/.vdc/*.vdc

18. Place the new license file from the prerequisite stage in /opt/VDC/.vdc.

19. Reset permissions.
/opt/VDC/bin/setperm

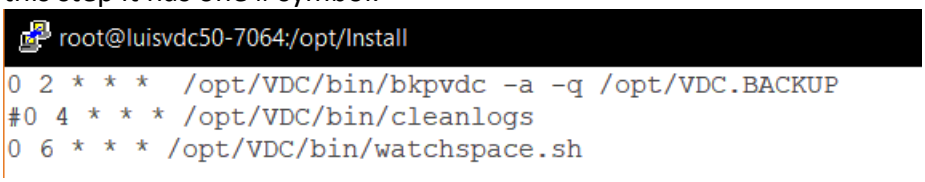
Stage 7 - On the Master DB Server

1. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
   a. For OS 6.*
   # ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc
   b. For OS 7.*
   # systemctl enable vdc
   You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

2. Enable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.



For user root:
crontab -e
After deleting one # from each line, save and exit.
esc
:wq

Switch to vdc user.
su - vdc
$ **crontab -e**
After deleting one # from each line, save and exit.
esc
:wq

3. Exit vdc user
   $ **exit**

4. End the script capture log file.
   # **exit**
   Output when successfully exiting the script:
   ```
   Script done, file is /tmp/backup.log
   ```

5. Reboot the server.
   # **reboot**

6. After the Master reboots wait at least 10 minutes for the server to completely boot up. Confirm the server is fully functional by checking for the postgres process. Find the postgres line as highlighted below.

   # **ps -ef | grep postgres**

```
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

7. The Master DB is now completely restored.

Stage 8 - On the Master Server:

1. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
   a. For OS 6.*
      # ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc
   b. For OS 7.*
      # systemctl enable vdc
      You should see the following message if the command ran properly.
      ```
      [root@vdc54mdb-3072 opt]# systemctl enable vdc
      Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
      ```

2. Enable cronjobs for root user and then for the vdc user.
   To edit the crontab use the “crontab -e” command.
   The crontab editor functions like the vi editor.
   You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

   This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.

   ```
   root@luisvdc50-7064:/opt/Install
   0 2 * * *  /opt/VDC/bin/bkpvdc -a -q /opt/VDC.BACKUP
   #0 4 * * * /opt/VDC/bin/cleanlogs
   0 6 * * * /opt/VDC/bin/watchspace.sh
   ```

   For user root:
   # crontab -e
   After deleting one # from each line, save and exit.
   esc
   :wq

Switch to vdc user.
 # su - vdc
$ **crontab -e**
After deleting one # from each line, save and exit.
esc
:wq

3. Exit vdc user
   $ **exit**

4. End the script capture log file.
   # **exit**
   Output when successfully exiting the script:
   ```
   Script done, file is /tmp/backup.log
   ```

5. Reboot the server.
   # **reboot**

6. After the Master reboots wait at least 10 minutes for the server to completely boot up. Confirm the server is fully functional by checking for the jsvc processes. There are two jsvc process, one run by root and one run by vdc.
   # **ps -eaf | grep jsvc**

7. The Master is now completely restored.

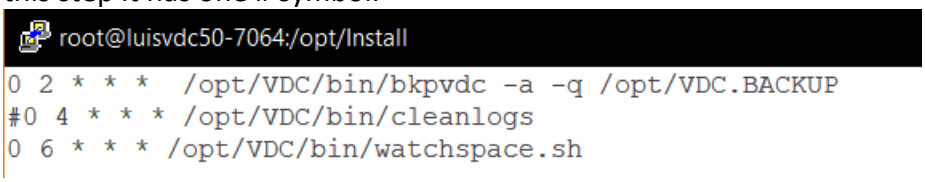
Stage 9 - On the Probe Server(s):

9. Enable the Auto-Start – this creates a symbolic link to start the system every time linux starts.
   a. For OS 6.*
   # ln -s /etc/init.d/vdc /etc/rc5.d/S99vdc
   b. For OS 7.*
   # systemctl enable vdc
   You should see the following message if the command ran properly.

```
[root@vdc54mdb-3072 opt]# systemctl enable vdc
Created symlink from /etc/systemd/system/multi-user.target.wants/vdc.service to /etc/systemd/system/vdc.service.
```

10. Enable cronjobs for root user and then for the vdc user.
    To edit the crontab use the "crontab -e" command.
    The crontab editor functions like the vi editor.
    You will be removing one # symbol at the beginning of each and every line, the lines that have ## will be left with one #.

    This example shows a crontab where the cleanlogs process was already disabled so after this step it has one # symbol.



    For user root:
    # crontab -e
    After deleting one # from each line, save and exit.
    esc
    :wq

    Switch to vdc user.
    # su - vdc
    $ crontab -e
    After deleting one # from each line, save and exit.
    esc
    :wq

11. Exit vdc user
    $ **exit**

12. End the script capture log file.
    # **exit**
    Output when successfully exiting the script:
    ```
    Script done, file is /tmp/backup.log
    ```

13. Reboot the server.
    # **reboot**

14. After the Master reboots wait at least 10 minutes for the server to completely boot up. Confirm the server is fully functional by checking for the postgres and vms processes.
    a. Confirm the database is started. Find the postgres line as highlighted below.
    # **ps -ef | grep postgres**

```
root     11092  8107  0 13:41 pts/2    00:00:00 su - postgres
postgres 11093 11092  0 13:41 pts/2    00:00:00 -bash
postgres 11139     1  1 13:44 pts/2    00:00:00 /usr/local/pgsql/bin/postgres -D data
postgres 11140 11139  0 13:44 ?        00:00:00 postgres: logger process
postgres 11143 11139  0 13:44 ?        00:00:00 postgres: checkpointer process
postgres 11144 11139  0 13:44 ?        00:00:00 postgres: writer process
postgres 11145 11139  0 13:44 ?        00:00:00 postgres: wal writer process
postgres 11146 11139  0 13:44 ?        00:00:00 postgres: autovacuum launcher process
postgres 11147 11139  0 13:44 ?        00:00:00 postgres: stats collector process
postgres 11156 11093  0 13:44 pts/2    00:00:00 ps -ef
postgres 11157 11093  0 13:44 pts/2    00:00:00 grep postgres
```

    b. Confirm that vms has started.
    # **ps -ef | grep vms**

15. The Probe is complete.

16. The system is ready for use, test web and 3D Client connections and monitoring activity to confirm.

17 HTTPS Configuration

Some customers require secure connections to the application via the use of https configuration. The following examples show how a system can be configured using https for secure access or reverting from https back to standard http.

Enable HTTPS

Customer is responsible for acquiring the two files needed to enable HTTPS on the application server. These files will have a .crt and .key file extension.

- Ensure the filenames of these two files are server.crt and server.key.
- Place these files on the Master server in the /tmp directory.

Run this command on the Master server:

/opt/VDC/bin/confhttps.sh -e -c server.crt -k server.key

If an intermediate certificate is available, then run this command on the Master server:

/opt/VDC/bin/confhttps.sh -e -c server.crt -k server.key [-i intermediate_certificate_file]

After running this command take these steps to finalize the configuration:

- Confirm the server.crt and server.key files are in the /opt/Server/Admin/conf/ssl/ directory on the Master server.
- Generate a new license request and apply an updated license. The new license activation key will permit access to the application with the https access.

The following is an example of the command to run for configuring https on the server:

#/opt/VDC/bin/confhttps.sh -e -c /tmp/server.crt -k /tmp/server.key

>>>>>>>>Web HTTPS has been enabled on this master server. Please send the license request file, /tmp/my.req, to support for a new HTTPS license. When the new HTTPS license file is received, remove the current license file under /opt/VDC/.vdc/, copy the new HTTPS license file to /opt/VDC/.vdc/, run /opt/VDC/bin/setperm and reboot. Wait about 10 minutes after the reboot to access the Web server using HTTPS.<<<<<<<<

Disable HTTPS

Run the following command to convert from an HTTPS configuration back to a HTTP configuration for the application instance. After disabling https, a new application license key will be required to access the application on the standard http URL.

/opt/VDC/bin/confhttps.sh -d

For example:

#/opt/VDC/bin/confhttps.sh -d

>>>>>>>>Web HTTPS has been disabled on this master server. Please send the license request file, /tmp/my.req, to support for a new HTTP license. When the new HTTP license file is received, remove the current license file under /opt/VDC/.vdc/, copy the new HTTP license file to /opt/VDC/.vdc/, run /opt/VDC/bin/setperm and reboot. Wait about 10 minutes after the reboot to access the Web server using HTTP.<<<<<<<<

Confirming HTTPS

To confirm the new https secure configuration is working users should follow these instructions:

- Open a supported web browser
- Ensure browser cache history has been cleared
- Access the https://myhostname where myhostname matches the URL used for your application installation.
- Confirm the application login screen is received for the application

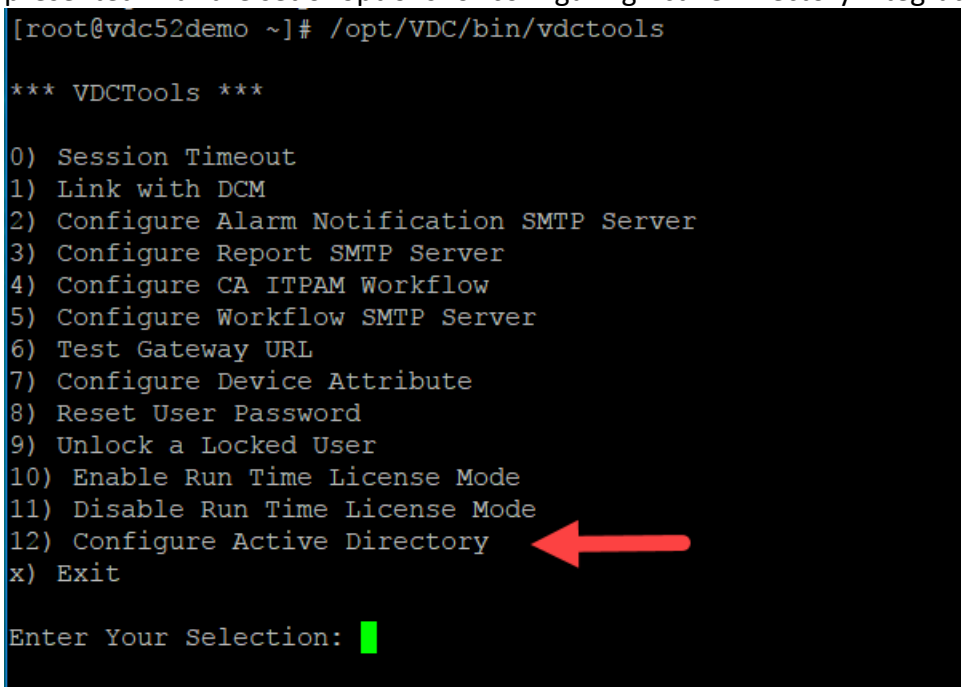
18 Active Directory Configurations

The application fully supports integration with third party directory systems such as Active Directory. When a user accesses the login page for the application, a configuration setting will determine whether authentication is performed against the local directory in the application or against the Active Directory system. To properly establish the Active Directory integration, changes to configuration must be made against both the application server and the Active Directory server.

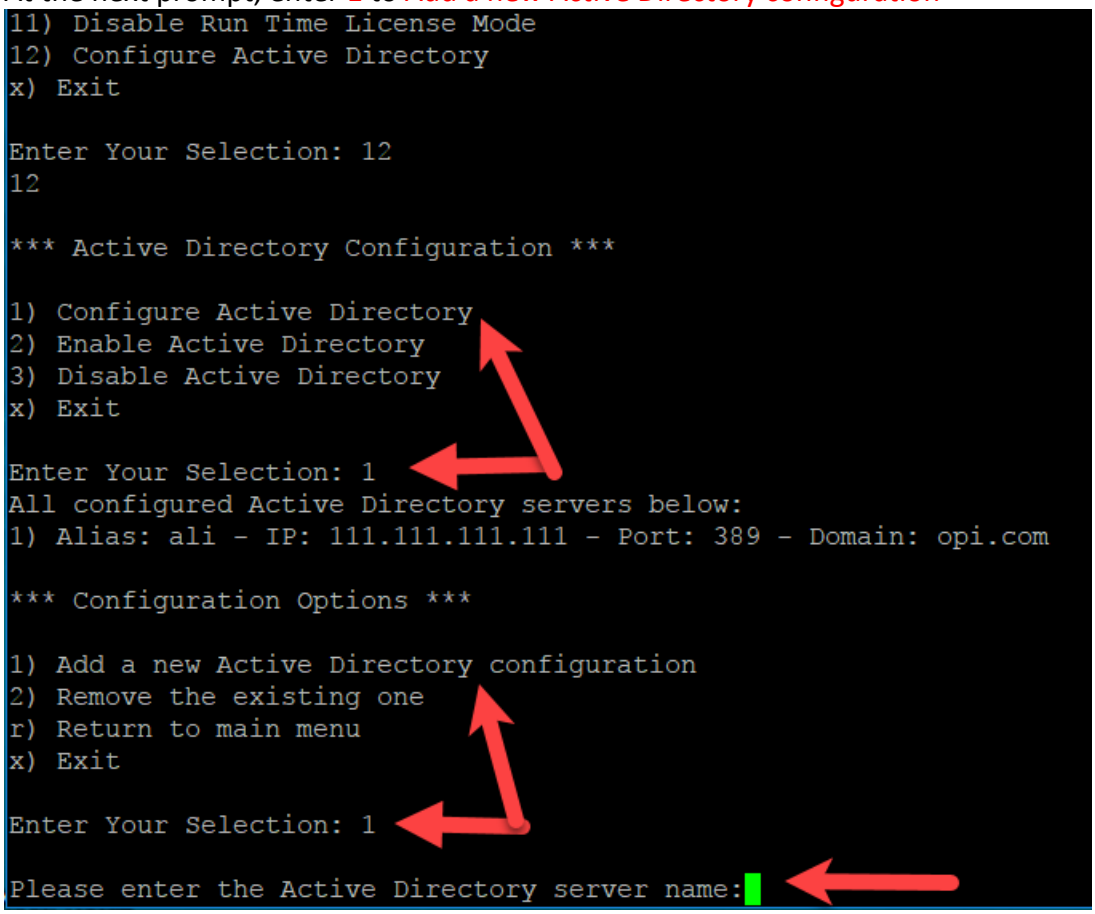
Application Server Configurations

The following changes must be made on the application server to enable Active Directory integration:

- Define the user group access privileges in the application by creating User Groups on the System Tab in the application. These user groups will define the access rights related to devices, locations and functions within the application for members of the group.
- As the root user, run /opt/VDC/bin/vdctools to configure and enable the Active Directory integration with the application.
- From the main menu, enter 12 to Configure Active Directory where you are presented with the set of options for configuring Active Directory integration.

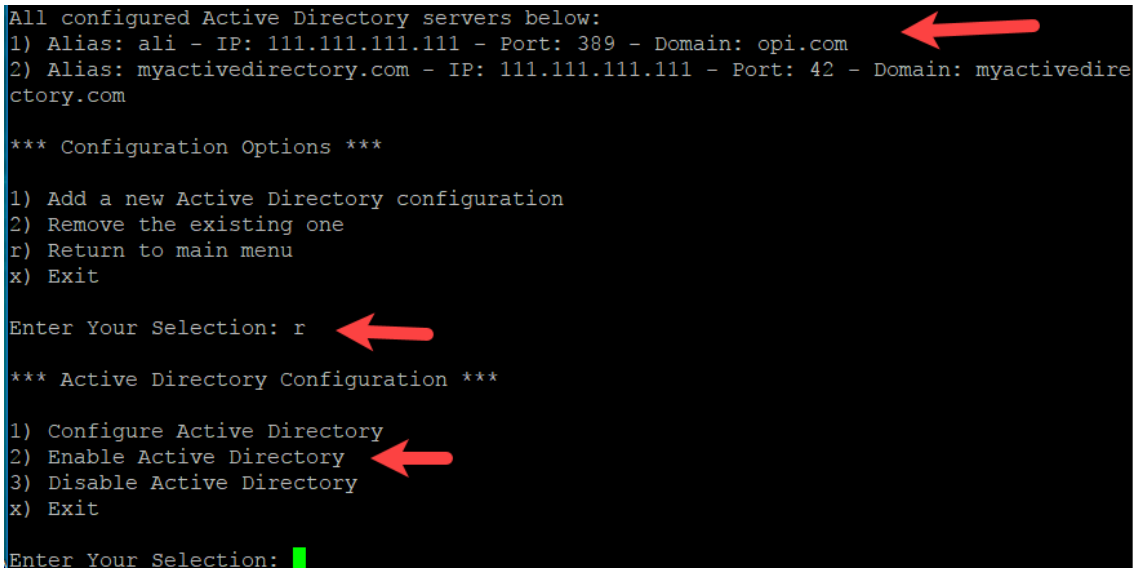


- From the secondary menu, enter 1 to Configure Active Directory
  Note, option has same name as previous selection
- At the next prompt, enter 1 to Add a new Active Directory configuration



- Next you will be prompted to enter the following:
  - Enter the Active Directory Server Name
    Note, this is a user defined name for reference with this application
  - Enter the Active Directory server IP
  - Enter the Active Directory server port
  - Enter the Active Directory server domain
    Note, if you need to configure more Active Directory domains repeat steps to Add a new Active Directory configuration.

- The console window will show All configured Active Directory Servers.



- Enter *r* to return to the main menu
- Enter 2 to Enable Active Directory
- Enter a Company name – it will be created as a company in the application if it doesn't already exist
- Enter a Department name – it will be created as a department in the application if it doesn't exist

  Note, at this point the application server will restart itself and please wait for it to completely restart before attempting to login.

Active Directory Operational Notes

- Except for the "super administrator", the server authenticates users against the Active Directory database instead of the server database.
- A user is permitted to login when these conditions are met:
    - The user ID and password are authenticated by Active Directory.
    - The user belongs to at least one Active Directory-mapped application group.
- For a user already logged into Visual Data Center, deleting the user or changing the user's group membership will have no impact on the user until the user logs out and logs back in.
- Once a user is permitted to login to the application, the application will create/update mirrored user info in the application when necessary. The following Active Directory attributes are significant to the application:

Active Directory Attribute	VDC Usage
sAMAccountName	Mapped as User ID
memberOf	Mapped as Group Names
company	Mapped as the Company container for the user. If the company field is empty, the user is assigned to "Unknown" company. If the company does not exist in the application, it will be created automatically.
department	Mapped as the Department container for the user. If the department field is empty, the user is assigned to "Unknown" department. If the department does not exist in the application, it will be created automatically.
givenName	Mapped to First Name
sn	Mapped to Last Name
mail	Email
mobile	Phone

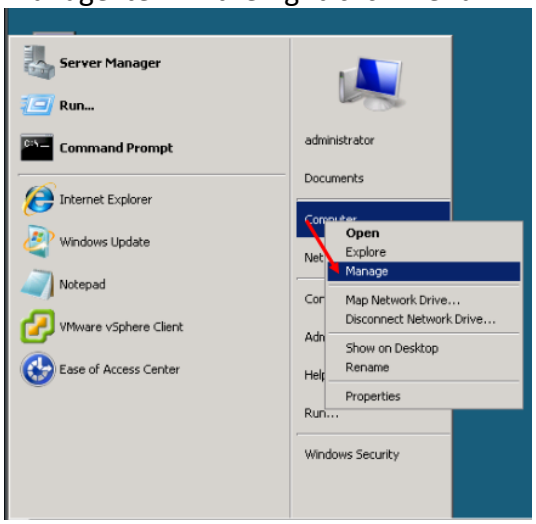
Active Directory Server Configurations

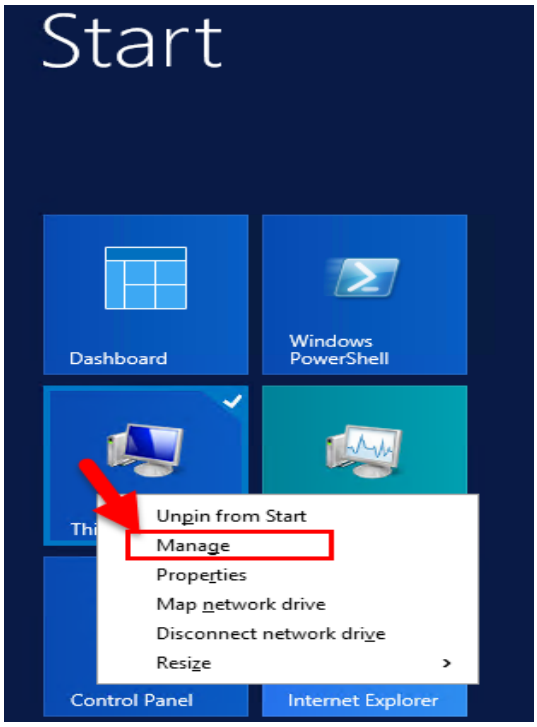
The Active Directory server needs to be configured to work properly with the application server. The following changes can be made to enable the authentication from the application interface against the Active Directory user database.

- Create identical named groups in Active Directory. These groups created in the Active Directory are standard Active Directory groups and, with the exception for their names must match the user group names provisioned in the application, there are no special settings which need to be defined in the Active Directory interface.

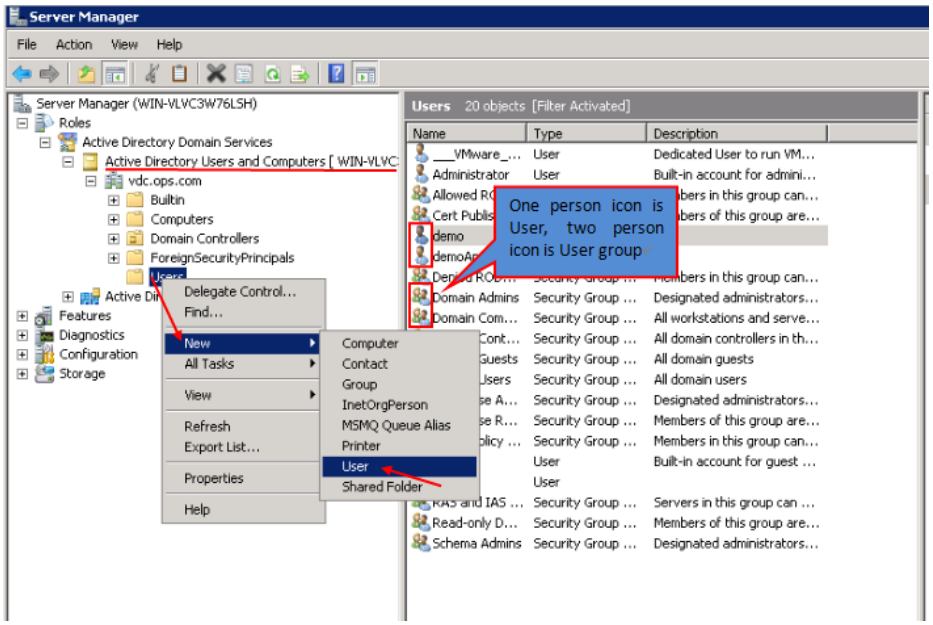
The following steps show a sample configuration of an Active Directory server to work with an instance of the application.

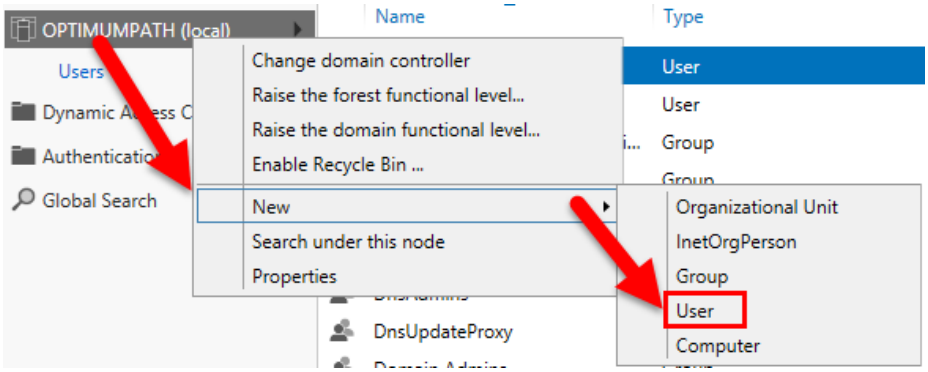
- RDP into the Active Directory server, right-click on the Computer to select the Manage item in the right-click menu.



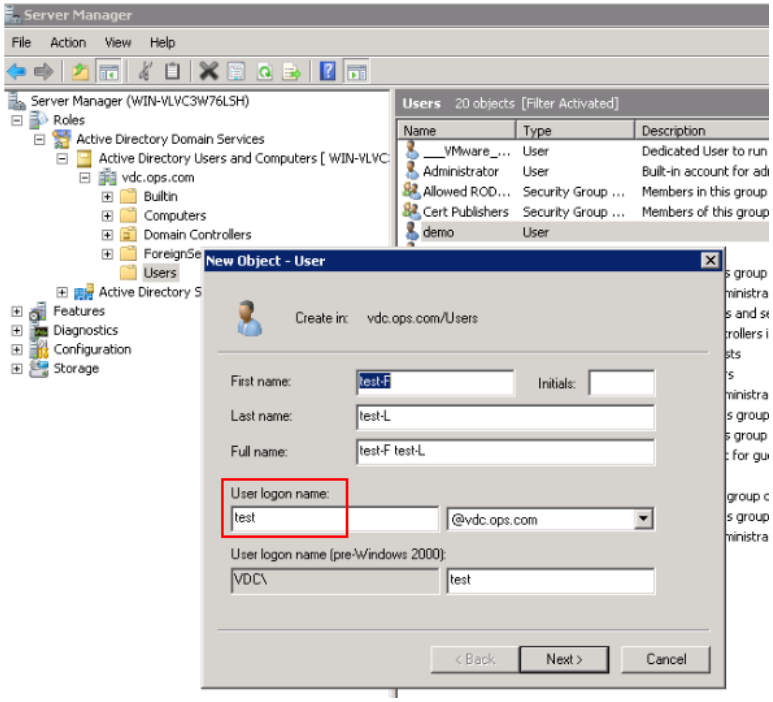


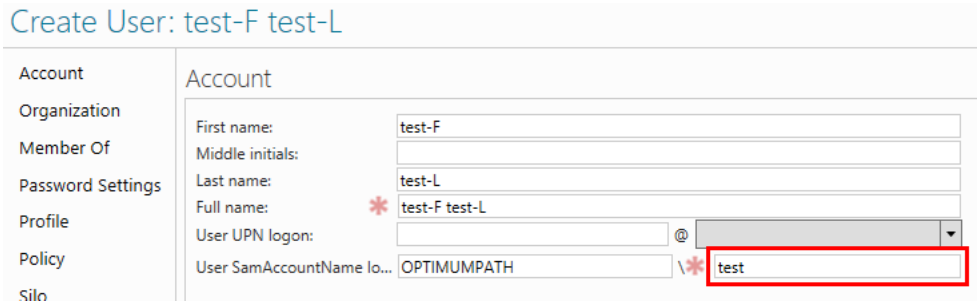
- In the Server Manager window, right click on Users to add a New User as indicated in the following screenshot. Note, the Users list will present a list of Users and Groups defined on the server.



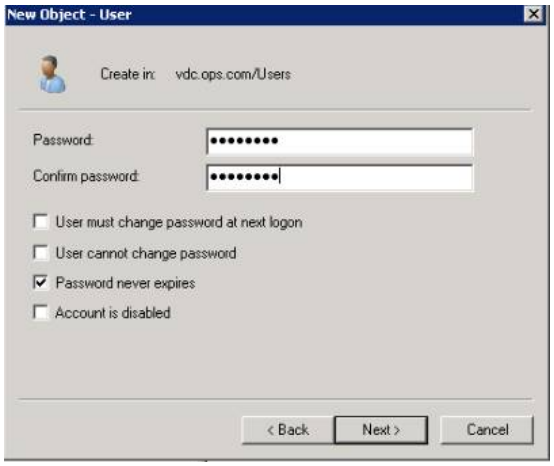


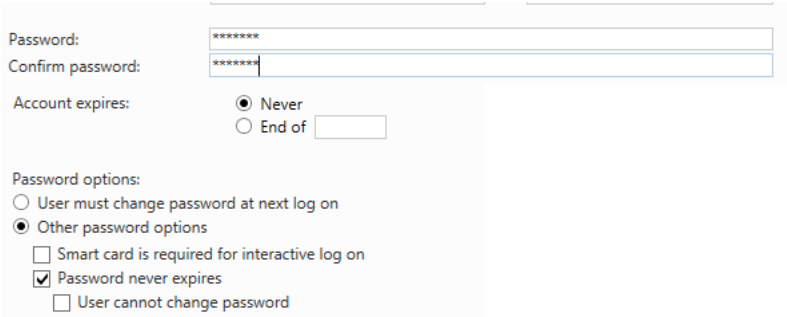
- Enter the user information in the Add User window. Make sure the user logon name, first name and last name fields are defined with settings to be used in the application.



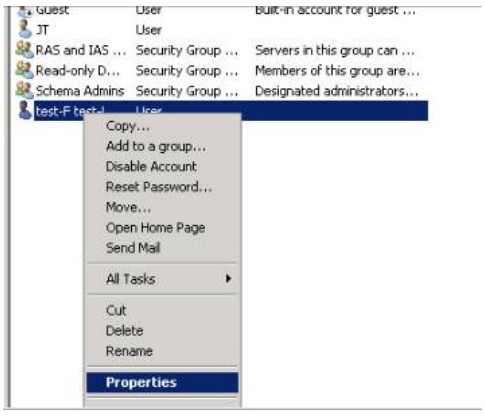


- Enter a secure/strong password in Active Directory.

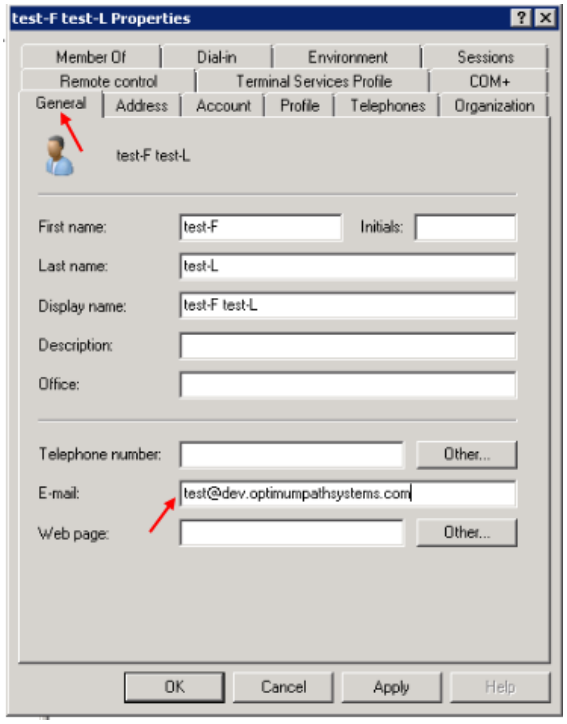


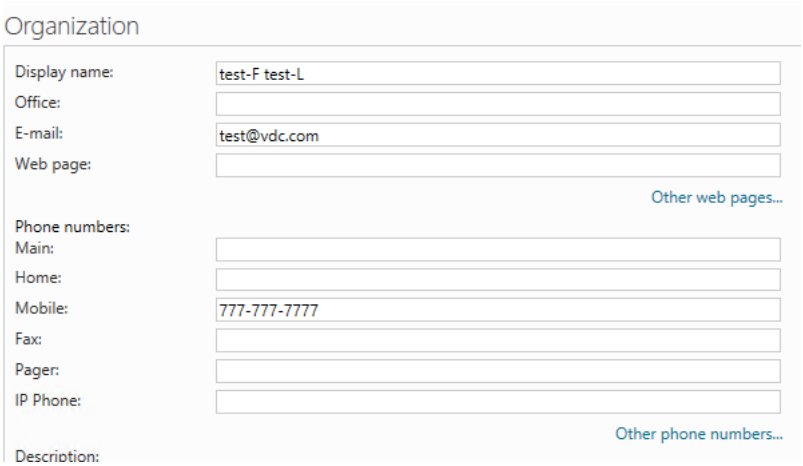


- Finish creating the new user in Active Directory by setting up additional properties for the user as the following:
    - Right-click on the new user, and select Properties:

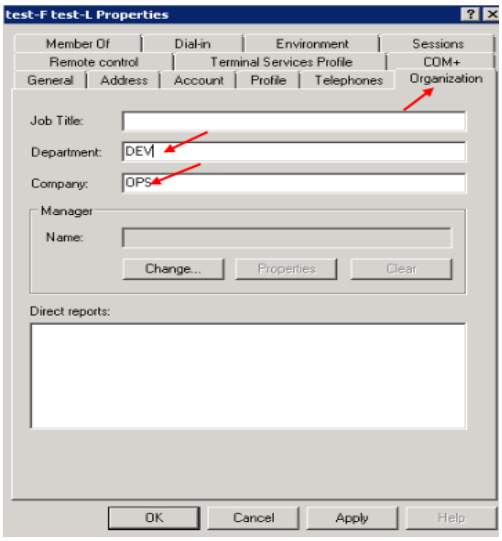


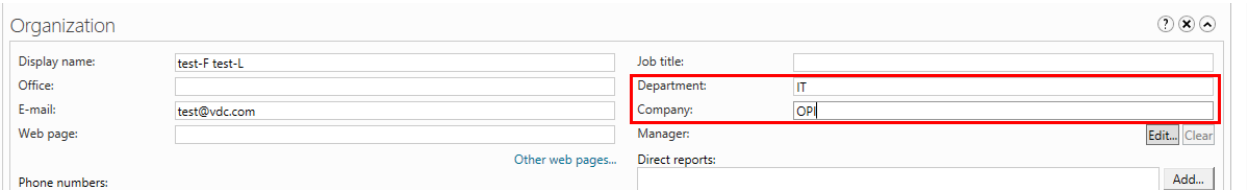
- Add the email-address for this user on the General tab.



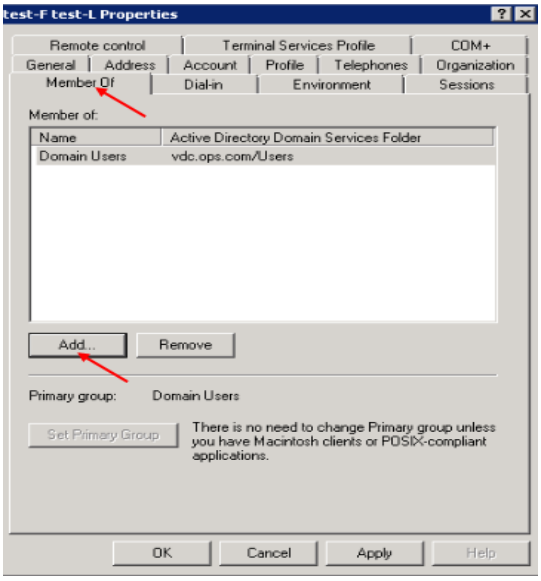


- Add the Department and Company for this user on the Organization tab. The Company and Department will be created in the application on the System Tab in the Companies and Departments lists when a user logs into the application if they are not already in the lists.

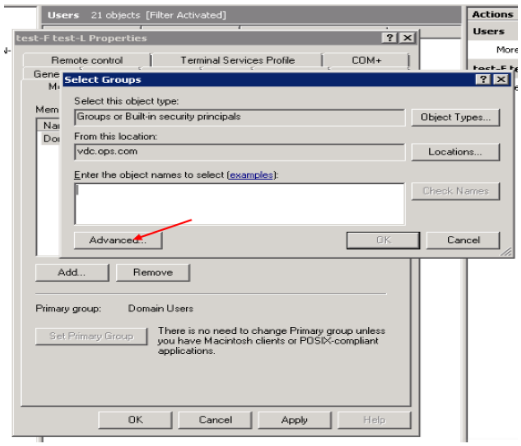


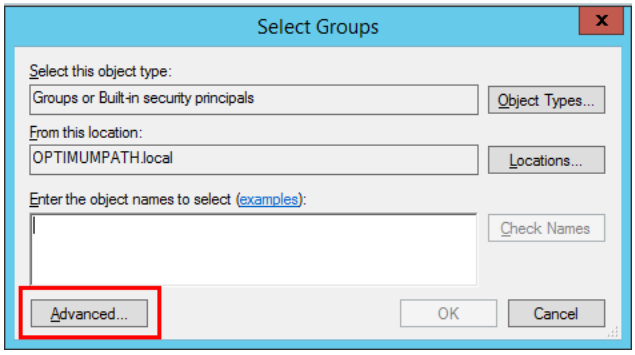


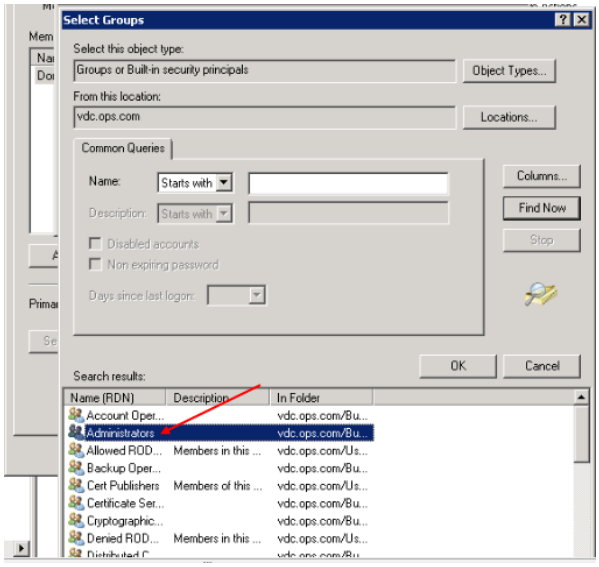
- To add the user to the application's admin group, click the Add button on the Member Of tab on the Active Directory server. In the Select Groups popup window, click the Advance button to select the Administrators group. Click OK to finish.

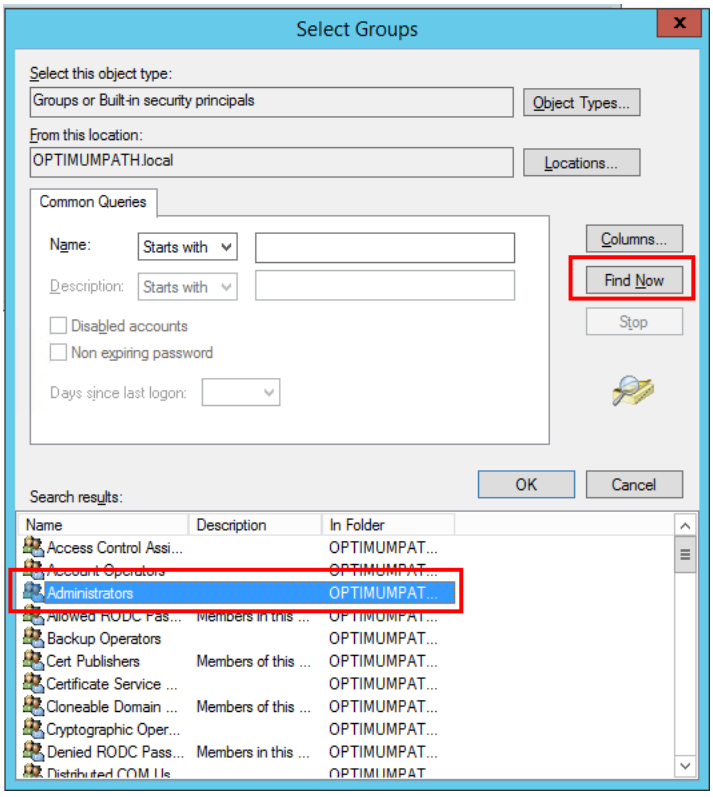


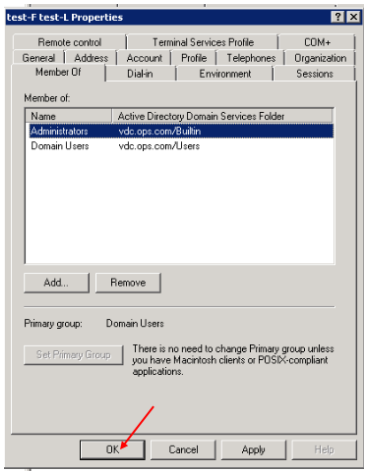

Create User: test-F test-L
TASKS
SECTIONS
Account
Organization
Member Of
Password Settings
Profile
Policy
Silo
Member Of
Filter
Name
Active Director...
Primary
Add...
Remove
This object will be added to the default Active Directory group.

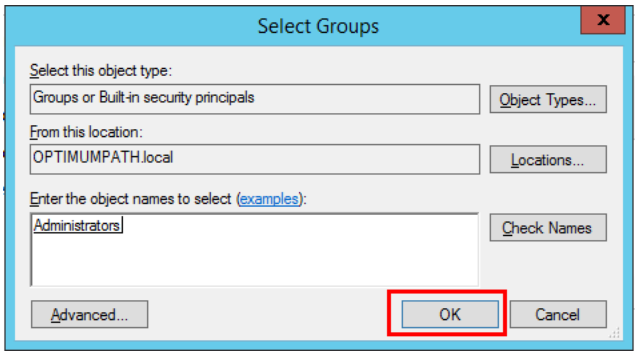

Users 21 objects [Filter Activated]
Actions
Users
test-F test-L Properties
Remote control
Terminal Services Profile
COM+
Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
vdc.ops.com
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help


Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
OPTIMUMPATH.local
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel


Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
vdc.ops.com
Locations...
Common Queries
Name:
Starts with
Description:
Starts with
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name (RDN)
Description
In Folder
Account Oper...
vdc.ops.com/Bu...
Administrators
vdc.ops.com/Bu...
Allowed ROD...
Members in this ...
vdc.ops.com/Us...
Backup Oper...
vdc.ops.com/Bu...
Cert Publishers
Members of this ...
vdc.ops.com/Us...
Certificate Ser...
vdc.ops.com/Bu...
Cryptographic...
vdc.ops.com/Bu...
Denied ROD...
Members in this ...
vdc.ops.com/Us...


Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
OPTIMUMPATH.local
Locations...
Common Queries
Name:
Starts with
Description:
Starts with
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name
Description
In Folder
Access Control Assi...
OPTIMUMPAT...
Administrators
OPTIMUMPAT...
Backup Operators
OPTIMUMPAT...
Cert Publishers
Members of this ...
OPTIMUMPAT...
Certificate Service ...
OPTIMUMPAT...
Cloneable Domain ...
Members of this ...
OPTIMUMPAT...
Cryptographic Oper...
OPTIMUMPAT...
Denied RODC Pass...
Members in this ...
OPTIMUMPAT...





Following the completion of the Active Directory changes, the application server will be able to successfully authenticate users against the Active Directory instance.

Disabling Active Directory Integration

If the application has been configured with Active Directory integration but this is no longer needed, then users can remove the configuration settings. This change is made by accessing the VDCTools menu with the /opt/VDC/bin/vdctools script and selecting option 6 for Disabling Active Directory.

After this change has been made, all user authentication will be directed to the local user database within the application. Note, any users that were accessing using Active Directory need to be provisioned to the application. There is no automatic synch of user information from Active Directory to the local database.

Active Directory Integration Notes

The following notes detail the functionality of the integration with Active Directory.

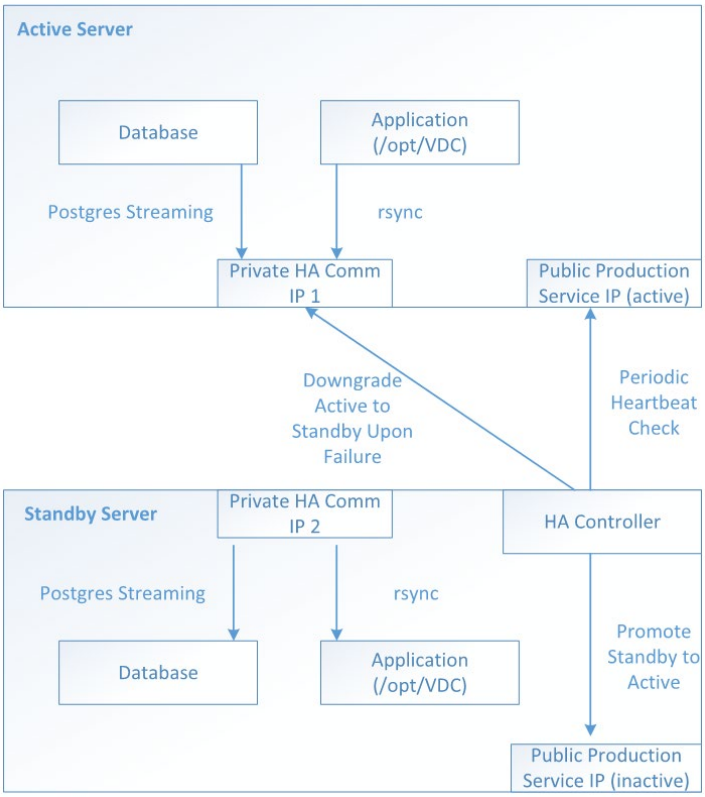
- After the Active Directory integration is enabled, the application will authenticate the user ID and password directly against the Active Directory Server.
- The user name will not need to have any reference to the domain included. The domain which is defined with the Active Directory integration will be automatically combined with the user name for authentication to the Active Directory server.
- Note that the super administrator account admin will always be authenticated against the local database in the application rather than Active Directory.
- With Active Directory enabled, the application will not store any user ID or password information in its own database other than the admin user ID and password.
- If the Active Directory Server successfully authenticates the user, the application will obtain the user's group membership from the Active Directory Server. Since these user group names are identical to the ones provisioned in the application User group settings page, the user will be assigned the proper access rights to components and features.
- If none of the Active Directory group names exists in the application User Groups list, the user login will be denied.

19 High Availability & Disaster Recovery

When the IT infrastructure supports high availability and disaster recovery configurations, such as VMWare vCenter, it is always recommended to utilize the capabilities at this infrastructure level. In absence of this option for providing platform redundancy and reliability, the application provides options for enhancing system availability.

High Availability

High availability allows for protections against standard system level failures within the platform or server. The application includes a native active/passive high availability solution as described below.



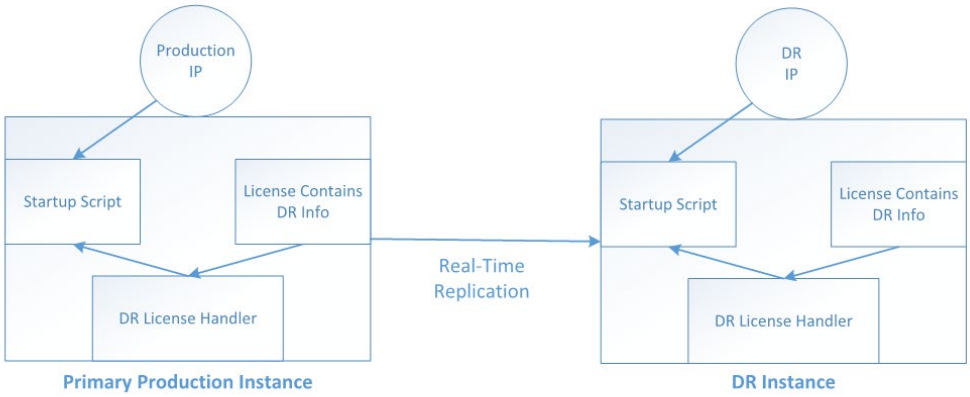
- Each application server can have a HA pair: an active server + a passive/standby server. The active server is a fully functional server running an instance of the application, while the passive/standby server only syncs its database and application files from the active application server in realtime. Both application servers have trusted SSH relationships established so that one server is able to run remote commands on the other server.

- Each application server has at least two network interfaces: the public-facing application-service network interface and a private HA-communication-only network interface, which is used for HA related communications between these two servers. The public-facing application-service network interface has the SAME IP on both servers. At any given time, only one of these network interfaces is active. Whichever application server has the active IP is the current active production server.
- The HA Controller runs on the Passive/Standby Server. Its heartbeat tool monitors the active application server periodically. If after 3 retries, the heartbeat check is still unsuccessful, the HA Controller will:
    - Issue remote commands through the Private Comm IP on the current active application server to shutdown its public production service IP, application processes, database and downgrade it to the passive/standby server.
    - Activate the Public Production Service IP on the current passive/standby server to promote it to the active server.
    - Start the HA Controller on the new passive/standby server
    - Send out alert messages to system administrators.

Note, after a failover event has occurred and the standby server is the active server, users must revert server status manually back to the primary server when it is back online.

Disaster Recovery

A Disaster Recovery option will provide protection for disastrous events to the overall platform. In general, the DR solution will allow users to sustain events which happen to the building, city, etc so they generally include some form of geographic redundancy as part of the protection mechanism. An example of the fully implemented disaster recovery configuration is detailed below.



DR Architecture

- Both Production and DR application servers are using identical hardware setup.
- The Production Server's file system (include both the application files and the database) are replicated in real-time onto the DR Server.
- A new license file, along with DR-compatible license module, will be installed for the customer to support the DR capability.
- The application production server and DR server will be using the same URL to access UI.
- The application production server and DR server will be using different IP addresses for accessing the application.
- Both the IP address and MAC address of the DR server will be locked and stored in the new DR-compatible license file.
- When the startup script is called, it will identify whether the current application instance is Production or DR (by comparing the current IP address) and change the server configuration automatically. Note, this script will be run manually by systems administrators when an event has occurred which requires the DR instance to be used as the Production instance.
- When a user logs into the DR instance, the user will be notified that the current instance is a DR instance.

Note, it is very important that after the DR instance failover occurs, the Production-to-DR replication should stop until the Production instance comes back online again. This will prevent the replication of damaged, corrupt or incorrect data from the previous production system to the newly activated DR system.

20 VDCMon Tool

VDCMon is an external program which resides on the application server that monitors the system and self-repairs operational issues automatically when possible. The following is a list of tasks performed by the VDCMon tool:

- Checks license status
- Checks the following for all the application servers and their processes:
  - Server disk usage, CPU load, and memory consumption
  - All VDC Process statuses
- If any application process fails to report status within 15 minutes, VDCMon will attempt to restart the process automatically.
- Sends the notification to the administrator if there is any exception or abnormal situation.

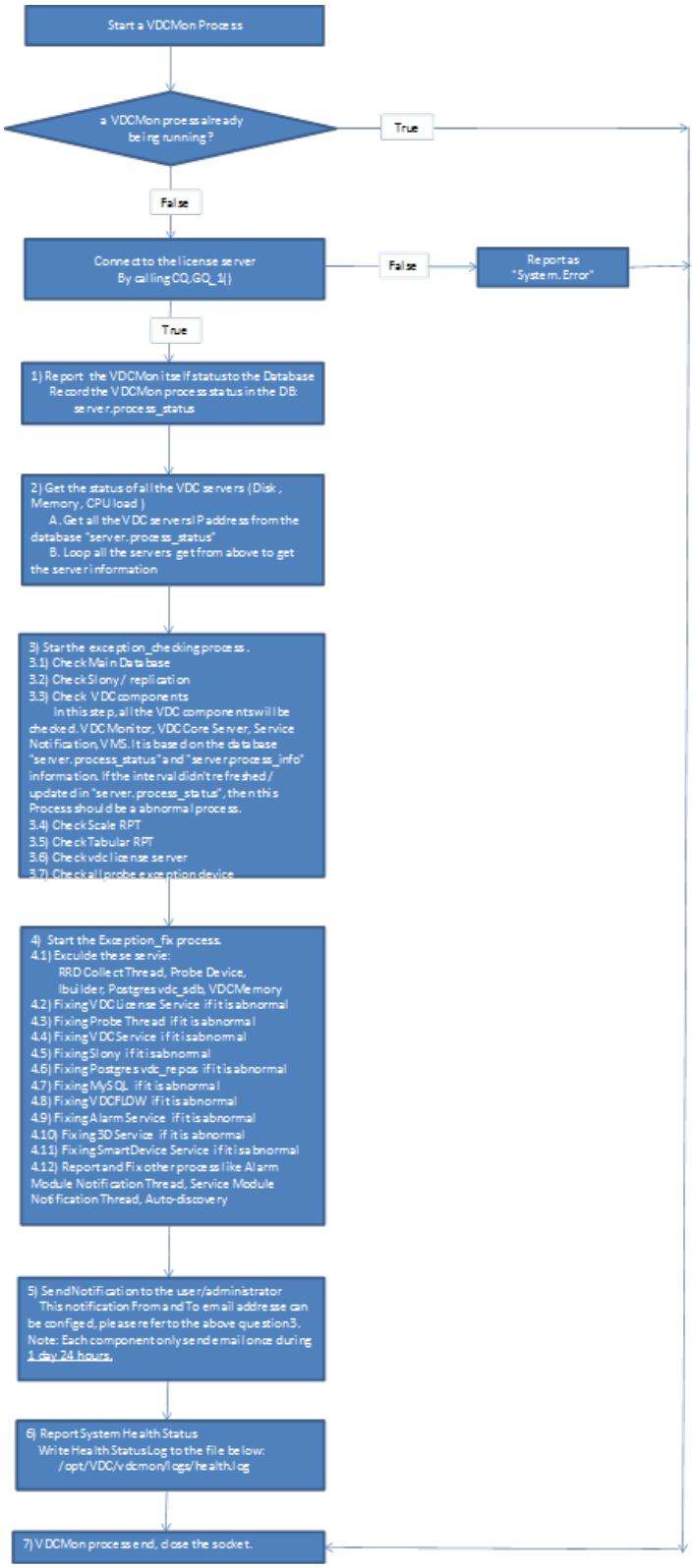
The VDCMon SMTP configuration is done using the Server Admin Tool, Email Server Settings. The Server Admin Tool writes to the /opt/VDC/.conf file and the settings are pushed to the /opt/VDC/vdcmon/conf/vdcmon.properties file.

Note, do not edit the vdcmon.properties file. Your edits will be overwritten by the push from the .conf file. The contents of the vdcmon.properties file:

- email.monitor.host – SMTP host to use for notification delivery
- email.monitor.from – From address to be used on the emails delivered as a notification
- email.monitor.to – Administrator user to be notified when issues are discovered by the VDCMon tool
- email.monitor.username – If SMTP authentication is required this is the username to be used for the authentication
- email.monitor.password – If SMTP authentication is required this is the password to be used for the authentication
- email.monitor.auth – Defines if SMTP authentication is required. Options for this configuration parameter are false or true

Administrators have the ability to customize the message content delivered in the notification message. The VDCMon notification message content template is defined at the following location: /opt/VDC/vdcmon/conf/.content. In addition, the VDCMon notification message subject can be defined in: /opt/VDC/vdcmon/conf/subject.

The VDCMon overall process flow is shown in the following diagram:


Start a VDCMon Process
a VDCMon process already being running?
True
False
Connect to the license server By calling CQ.GQ_1()
False
Report as "System. Error"
True
1) Report the VDCMon itself status to the Database Record the VDCMon process status in the DB: server.process_status
2) Get the status of all the VDC servers (Disk, Memory, CPU load)
A. Get all the VDC servers IP address from the database "server.process_status"
B. Loop all the servers get from above to get the server information
3) Start the exception_checking process.
3.1) Check Main Database
3.2) Check Slony / replication
3.3) Check VDC components
In this step, all the VDC components will be checked. VDC Monitor, VDC Core Server, Service Notification, VMS. It is based on the database "server.process_status" and "server process_info" information. If the interval didn't refreshed / updated in "server.process_status", then this Process should be a abnormal process.
3.4) Check Scale RPT
3.5) Check Tabular RPT
3.6) Check vdc license server
3.7) Check all probe exception device
4) Start the Exception_fix process.
4.1) Exculde these servie:
RRD Collect Thread, Probe Device, Ibuilder, Postgres vdc_sdb, VDCMemory
4.2) Fixing VDC License Service if it is abnormal
4.3) Fixing Probe Thread if it is abnormal
4.4) Fixing VDC Service if it is abnormal
4.5) Fixing Slony if it is abnormal
4.6) Fixing Postgres vdc_repos if it is abnormal
4.7) Fixing MySQL if it is abnormal
4.8) Fixing VDCFLDW if it is abnormal
4.9) Fixing Alarm Service if it is abnormal
4.10) Fixing 3D Service if it is abnormal
4.11) Fixing SmartDevice Service if it is abnormal
4.12) Report and Fix other process like Alarm Module Notification Thread, Service Module Notification Thread, Auto-discovery
5) Send Notification to the user/administrator
This notification From and To email addresse can be configed, please refer to the above question 3.
Note: Each component only send mail once during 1 day 24 hours.
6) Report System Health Status
Write Health Status Log to the file below:
/opt/VDC/vdcmon/logs/health.log
7) VDCMon process end, close the socket.

21 Cron Jobs

Cron jobs submit tasks at set times according to the host's clock. This list of tasks can be any script or application that you desire to have executed and commonly you will find maintenance-types of tasks in the crontabs. This application uses several scheduled cron jobs to help with the operations of the application and data.

Many of the key functions of the application take place in the cron job portion of the Linux operating system. These cron jobs are explained at a high level in this section. For more detailed information on how to configure or manage cron jobs, please refer to a Linux Administrator Guide as reference.

There are cron jobs defined under both the root and vdc users on the Visual Data Center systems. To access these cron job lists, the user must be logged into the Linux system as that particular user and then run one of the commands below.

Crontab Options

The following command options are typically used to manage the crontab entries.

- crontab - l List – display the current crontab entries
- crontab - e Edit the current crontab
- crontab - r Remove the current crontab

Each line in the cron table is defined with the schedule for which it should be executed. The first five fields in the crontab entry line will provide the schedule for the listed task to be executed. Note, if one of these fields contains an asterisk then all possible options for that field will be used in the scheduled task execution.

Field	Description
1	Minute (0-59)
2	Hour (2-24)
3	Day of month (1-31)
4	Month (1-12)
5	Day of week (0-6) 0 = Sunday

Root User Crontab

While logged in as the root user type crontab –l at the system prompt and a list of root cron jobs will be listed. The following is a description of the typical cron jobs that are configured to run under the root user for the application.

```
[root@tampa128 VDC.BACKUP]# crontab -l
0 2 * * *  /opt/VDC/bin/bkpvdc -a -q /opt/VDC.BACKUP
0 4 * * * /opt/VDC/bin/cleanlogs
0 6 * * * /opt/VDC/bin/watchspace.sh
```

bkpvdc

This cron job provides backup services for the application and database files related to the application. Please consult the Backup & Recovery section of this document for more information on this process and the configuration parameters related to this cron entry. Please ensure the backup destination directory, /opt/VDC.BACKUP by default, is NOT located on the same physical disk as either /opt/VDC or /usr/local/pgsql. Otherwise, if the single-point-of-failure hard disk fails, the entire system will be lost without any possibilities of recovery. By default this process will run at 2AM server time nightly.

cleanlog

This cron job manages and rotates old log files beyond a specified amount of time. The default time to keep the log files is two days, but it is recommended to set this to seven days if space permits. The number of days to retain logs is defined with this parameter below:

- DAYS_MIN = 2

watchspace

This cron job will monitor the space of the monitor database table. One of the key functions in the application is to collect and store monitored data and these transactions can easily reach into the high millions in number. It is very important to ensure the database tables responsible for tracking utilization of these tables is operating properly.

VDC User Crontab

While logged in as the vdc user type crontab –l at the system prompt and a list of vdc cron jobs will be listed. The following is a description of the typical cron jobs that are configured to run under the vdc user for the application.

```
* * * * * /opt/VDC/ibuilder/bin/ib -d
0 0 * * * /opt/VDC/ibuilder/bin/ib -D
0 9 * * * /opt/VDC/monitor/bin/servicectl start
5,15,20,25,30,35,40,45,50,55 * * * * /opt/VDC/jdk/bin/java -jar -DINDEX_HOME=/opt/VDC/db/bin /opt/VDC/db/bin/DBJobs.jar 5min.dbjobs.properties
* * * * * /opt/VDC/jdk/bin/java -jar -DINDEX_HOME=/opt/VDC/db/bin /opt/VDC/db/bin/DBJobs.jar 1min.dbjobs.properties
0,30 * * * * /opt/VDC/jdk/bin/java -jar -DINDEX_HOME=/opt/VDC/db/bin /opt/VDC/db/bin/DBJobs.jar 30min.dbjobs.properties
0 * * * * /opt/VDC/jdk/bin/java -jar -DINDEX_HOME=/opt/VDC/db/bin /opt/VDC/db/bin/DBJobs.jar 1hour.dbjobs.properties
0 1 * * * /opt/VDC/jdk/bin/java -jar -DINDEX_HOME=/opt/VDC/db/bin /opt/VDC/db/bin/DBJobs.jar 1.24.day.dbjobs.properties
0 1 * * * /opt/VDC/monitor/bin/rrdctl scalar
0 3 * * * /opt/VDC/monitor/bin/rrdctl tabular
0,15,30,45 * * * * /opt/VDC/vdcmon/bin/vdcmon
0 0 * * * /opt/VDC/VDCMPCollect/bin/RPT
0 0 * * * /opt/VDC/bin/clearmon9.sh
#* */1 * * * /opt/VDC/bin/clearbms
*/5 * * * * nohup /opt/VDC/jdk/bin/java -jar /opt/VDC/monitor/lib/UIMAlarmCollector.jar 2517 &
0 0 * * * /opt/VDC/AutoRpt/bin/autorpt
0 1 * * 0 /opt/VDC/bin/pg_task
0 9 * * * nohup /opt/VDC/jdk/bin/java -jar /opt/VDC/monitor/lib/sw-noti.jar &
```

ib

The ib process is an index builder for the database and is added to the cron jobs to ensure continuous updates are made to the database records. This process will provide accurate data for device searches and other database search functions performed within the application. There are a few different switch options available for the ib process as defined below:

- ib –d – Incremental device index update.
- ib –D – Full device index update.

servicectl

This cron job is the notification service which is responsible for delivering SMTP and SMS notifications for alarm rules defined in the application.

5min.dbjobs.properties

These are scheduled internal database jobs which must be run at fixed intervals.

1min.dbjobs.properties

These are scheduled internal database jobs which must be run at fixed intervals.

30min.dbjobs.properties

These are scheduled internal database jobs which must be run at fixed intervals.

1hour.dbjobs.properties

These are scheduled internal database jobs which must be run at fixed intervals.

1.24.day.dbjobs.properties

These are scheduled internal database jobs which must be run at fixed intervals.

rrdctl tabular|scalar

These cron jobs are designed to process data for the trend charts which are maintained in the application.

vdcmon

Please refer to the section in this document for detail on the vdcmon process. This process is tracking and notifying administrators when issues occur with core processes needed for the application.

RPT

This cron job is a daily report processing service designed to process power related data for devices in the application.

clearmon9.sh

This cron job is a database housekeeping process to help conserve space by removing historical raw data which is no longer needed.

autorpt

This cron job will deliver reports which have been scheduled for delivery. The report jobs are defined in the Scheduled Reports feature of the application.

pg_task

This cron job performs database maintenance handling for the application.

sw-noti.jar

This cron job provides notification delivery for the service and warranty events. While the services and warranty calendars are defined in the Services function of the application, the notification rules will define the notifications which need to be delivered to users when service and warranty related events are triggered.

22 Configuration Files & Permissions

Maintaining a set of well-defined configuration options and permission settings is vital to the overall system health and operation of the application. There are core aspects of the application dedicated to helping maintain these settings which are described below.

.conf File

The central application configuration settings are stored in the file located in /opt/VDC/.conf and many of these are assigned values from the installation script. Each configuration setting in this file is represented in the form of *Attribute@Module=Value*, for example:

VDCTIMEZONE@.tz=US/Eastern

Attributes maintained in the .conf file are typically managed by using tools included with the application. These tools include the Server Admin tool, VDCTools script and other front end or scripts located on the server. Please use the provided tools to manage the settings of these attributes and consult a support member prior to making any manual changes to the .conf file.

vdcconf Process

After making any changes in the /opt/VDC/.conf file it is very important to invoke the command */opt/VDC/bin/vdcconf* which will propagate the changes to required components (.tmpl files) of the application. Most components require a restart to pick up the new configuration settings so it is recommended that a restart of all processes or a reboot of the server is required after running */opt/VDC/bin/vdcconf*.

setperm Process

File and directory ownership and permission settings are very significant to the successful operation of the application. Users should never manually adjust any file or directory ownership or permission under the /opt/VDC directory using either the *chown* or *chmod* command directly. Doing so may cause a complete system failure for the application.

The */opt/VDC/bin/setperm* command is designed to repair permission issues automatically. After creating or moving any files under /opt/VDC, it is always recommended to run */opt/VDC/bin/setperm* afterwards to ensure the correct settings for key files/directories ownership and permissions.

Root Permissions

Many customers have issues allowing any access to the root user to execute processes on the application server. In the application there are very few processes, such as the backup process (*/opt/VDC/bin/bkpvdc*), which require root privilege to execute. Most of the processes require the vdc user to start (refer to the /etc/init.d/vdc script for startup commands for processes). If a process designed to be started by the vdc user is incorrectly started by the root user, it will not only cause interoperability issues (because the data/log from the root run process may not be readable by other vdc run processes) but also may cause operation issues by damaging the designed access control hierarchy.

If any vdc process is accidentally started by the root user, then immediately stop the process by running "*kill -9* PID" and then run */opt/VDC/bin/setperm*. Once completed the user can then run the process again using the correct vdc user.

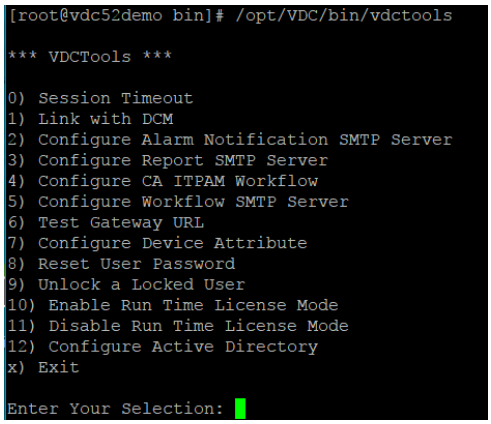
23 VDC Tools Menu

Although administrators have access to manage many of the configuration settings directly in the configuration files there is a menu of commonly managed settings which can be used to help expedite these configuration updates. Please note, there are password reset tools included in this set of options so it is important to only permit access to this toolset for authorized administrators of the application. The tool is accessed with the following command and the available options are explained below. At the main menu users can type x and then Enter to exit the configuration tool.

/opt/VDC/bin/vdctools

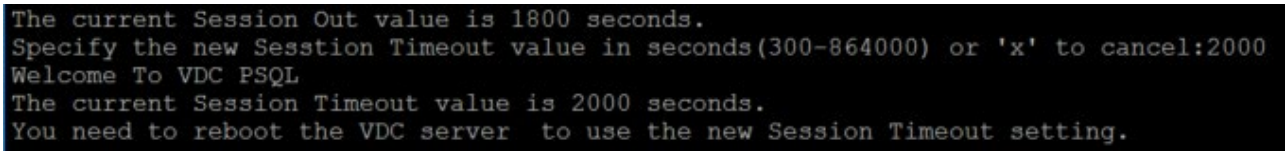
To ensure the updated settings are used with the application it is recommended that users restart services after any changes are made to the configuration settings. This can be done with a reboot of the server by issuing the following command:

reboot



0) Session Timeout

This option allows users to set the timeout length for a logged in session of the product. This setting is applied universally to all users of the application. The change is made by the script updating the appropriate table in the master database. A reboot of the server will be required for the effects to take place.



1) Link with DCM

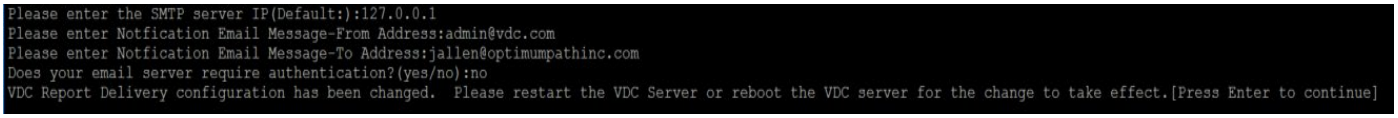
The application has the ability to integrate with the Intel Data Center Manager (DCM) application. To enable this integration this option can be used to define the configurations needed to enable the integration with that third-party application.

2) Configure Alarm Notification SMTP Server

This option will configure the product with the customer's mail server information to allow the product to send out notification emails based on alarms present in the system. When alarms are triggered and there are associated alarm notification rules, then the application will deliver SMTP notifications to users based on these email server settings. Alternatively, these changes can be managed using the Server Admin tool which is documented in its own section of this document.

3) Configure Report SMTP Server

This option will configure the product with the customer's mail server information to allow the product to send out scheduled reports. Scheduled reports are defined on the Reports feature of the application and allow administrators to define the specific reports, recipients and frequency for delivery tasks. Alternatively, these changes can be managed using the Server Admin tool which is documented in its own section of this document.



4) Configure CA ITPAM Workflow

The application has the ability to integrate with CA Process Automation Manager to provide integrated management of workflow tasks. This option will prompt for the key parameters and configuration options to complete and activate the integration with this third-party solution.

5) Configure Workflow SMTP Server

This option will configure the application with the customer's mail server information to allow for the delivery of SMTP email notifications to users related to the Projects, Tasks and Work Order management features. These features typically require review and approval of submitted items which are then emailed to approvers for review. Alternatively, these changes can be managed using the Server Admin tool which is documented in its own section of this document.

```
Please enter VDC email hostname/ip:127.0.0.1
Does the VDC email server require authentication?(yes/no):no
Please enter VDC email FROM address:admin@vdc.com
```

6) Test Gateway URL

The application supports integration with the CA ecoMeter and CA UIM software solutions which utilize an XML gateway configuration file. This option will test integration with those software solutions.

7) Configure Device Attribute

Allows administrators to define mandatory attributes for devices. For example, some companies may require the Serial Number attribute to be a mandatory attribute for device creation.

8) Reset User Password

This option allows an administrator to reset any users password by entering the username and the new password. Please note, password resets can be performed by users themselves in the Personal Settings feature or can be managed by administrators from within the application using the Users menu on the System Tab.

9) Unlock a Locked User

When a user submits three consecutive failed attempt to login then the user account will be locked by the application. Using this option an administrator can reset the failed attempts counter to 0 so the user can once again try to login. If the user no longer knows their password then the administrator can reset their password with either the vdctools tool or from within the application in the Users Menu on the System Tab. To use this option, the administrator provides the user name for the user to unlock.

Note, there is a system timeout for the duration of the locked status of an account. After this time has passed, the user will once again be able to complete a successful login for the account.

10) Enable Run Time License Mode

There are multiple license configuration options which are supported for the application including the hardware signature mode and the run time license mode. The majority of customers will use the standard license activation key which is tied to the hardware signature of the server, but in some cases, users will need to implement the run time license server. To enable the run time license option administrators must run this vdctools option and provide the required license server information. Note, by default, all instances of the application are configured to support the standard hardware key license option during an installation. For more information on how to install and configure the run time license server option please consult with a support consultant.

11) Disable Run Time License Mode

If an instance of the application is configured to support the run time license mode, then running this option will deactivate support the run time license mode and revert license support to the standard hardware key license mode.

12) Configure Active Directory

This option takes you to a sub-menu for the configuration of Active Directory. Please go to the Chapter 17 Active Directory for details.

24 Change Application Server IP Address

In some cases, a customer will need to move an existing instance of the application to a new server IP address. In these situations, it is important to properly configure the application to respond on the new IP address setting. The newip tool is available to help update IP configuration references within the application so it can properly operate on the new IP address.

Please note that it is very important not to swap the old_ip and new_ip argument positions as it will make unintended updates to the application server settings. Do not use the new_ip script to change IP if the local loopback IP, 127.0.0.1, is involved. There are valid references to 127.0.0.1 which will be overwritten if this setting is used.

The newip tool is located in the opt/VDC/bin directory.

1. cd /opt/VDC/bin
2. Run ./newip old_IP new_IP
    - ./newip 192.168.111.12 192.168.222.46 will change the IP settings from 192.168.111.12 to 192.168.222.46.
3. Reboot the server to restart all processes and commit the changes into the application.

Note, a new application license key is NOT required for changes to the server IP Address settings.

25 Change Application Server URL

During the installation of the application the installer is prompted to define the URL which will be used to access the application. This URL is an important setting within the application and is referenced in many places including the license activation key. If a customer needs to change the URL on which the application is accessed for an existing instance of the application, then the newurl tool must be run.

Please note that it is very important not to swap the old_url and new_url argument positions. Do not use the new_url script to change URL if the local loopback IP, 127.0.0.1, is used as the URL. There are valid references to 127.0.0.1 which will be overwritten if this setting is used. Due to the find/replace nature of this tool, please do not use this tool to configure the application with common strings which may already be in the configuration files (ie vdc, , host, etc). The URL should be a unique reference to URL.

1. cd /opt/VDC/bin
2. Run ./newrul old_url new_url
    - ./newurl old.app.url newurl will changes the URL used to access the application from http://old.app.url to http://newurl.
3. Changing the URL on the server requires a new license activation key. Follow these instructions to generate and apply a new license key to the server:
    - Run /opt/VDC/bin/keyreq > /tmp newkey.txt
    - Send the /tmp/newkey.txt file to the support team for a new license activation key
    - Move the existing license activation key located in the /opt/VDC/.vdc folder to a different location for archiving purposes.
        - mv /opt/VDC/.vdc/* /var/tmp
    - Copy the new license activation key provided by support into the /opt/VDC/.vdc folder.
    - Run /opt/VDC/bin/setperm
    - Reboot the server to restart the processes using the new license activation key
4. Reboot the server to commit the changes to the application settings and restart the processes.

26 Change Application Server Hostname

A application license is bound to both the server's hostname and hardware (CPU and motherboard) signature. If the application server's hostname is changed, a new activation license will be required for use with the new hostname. One of the activation license key requirements is that a valid host name must be assigned to the application server instead of using the default localhost.localdomain hostname. During the application installation process, the installer script will prompt and set the hostname if the hostname is found to be undefined.

On a RedHat/CentOS 6.x server follow these steps to change the hostname. Note these commands must be performed as the root user.

#	Step Description	Commands / Examples
1	Login to the application server as root user	
2	Update the hostname at the command prompt	hostname my_new_hostname
3	Change the value of HOSTNAME= to the new hostname, save the file change and exit the text editor.	vi /etc/sysconfig/network HOSTNAME=my_new_hostname
4	Reboot the server	reboot

Following the change of the hostname, a new application license activation key must be retrieved and applied to the server. This is due to the fact that the hostname definition is embedded in the application license. Follow these instructions to generate and apply a new license key to the server:

- Run /opt/VDC/bin/keyreq > /tmp newkey.txt
- Send the /tmp/newkey.txt file to the support team for a new license activation key
- Move the existing license activation key located in the /opt/VDC/.vdc folder to a different location for archiving purposes.
    - mv /opt/VDC/.vdc/* /var/tmp
- Copy the new license activation key provided by support into the /opt/VDC/.vdc folder.
- Run /opt/VDC/bin/setperm
- Reboot the server to restart the processes using the new license activation key

27 Change Application Server Email Settings

There are some functions in the application designed to deliver SMTP email notifications or files to users. The application must be configured to use the customer SMTP mail server to properly deliver these emails to end users. In general, the mail configuration settings require the administrator to define the server IP/host of the mail server, port and, if authentication is required for the SMTP connection, the authentication details for the connection. These settings are provided by the installer during the installation of the application, but the settings are maintained in separate configuration parameters to allow for changes as needed. Alternatively, these changes can be managed using the Server Admin tool which is documented in its own section of this document.

Note, the Server Admin tool sets all of the mail settings in the /opt/VDC/.conf file to the same values for the SMTPHOST, SMPTFROM, SMTPUSER, SMTPPWD and SMPTAUTH. If you require different settings for the functions described below you can use VDC Tools (/opt/VDC/bin/vdctools) as noted in the VDC Tools Menu section or edit the /opt/VDC/.conf file.

In the application, there are five separate functions which allow for email delivery which need to be configured. The configuration parameters are located in the /opt/VDC/.conf file which is the central configuration file for the application. The specific parameters associated with each mail configuration option are located in the description of each functional part of the application which has the ability to send emails.

- Alarms – Alarm notifications are generated when alarm triggers occur on devices for Warning, Critical, Unreachable and Return to Normal status options. The Notification Rules define the alarm events to pass to recipients with email notifications. Restart the vms process for these changes to take effect.
- Services – Service and warranty notifications are generated when devices have an upcoming service event or warranty expiration date. The Notification Rules define the alarm events to pass to recipients with email notifications.
- Reports – Scheduled reports can be configured and delivered to recipients in PDF files on a regular schedule. Restart the Tomcat jsvc processes for these changes to take effect.
- Projects – The project feature has approval cycles for defined projects, tasks and work orders which are delivered via email notifications to defined approvers. Restart the Tomcat jsvc processes for these changes to take effect.

- VDCMon – The vdcmon process monitors the health of the application server and is configured to notify an administrative user when there are issues with processes or overall health of the server. Restart the Tomcat jsvc processes for these changes to take effect.

THIS NEEDS TO BE UPDATED FOR 6.3.0

INFO FROM 6.3.0 RELEASE NOTES

Function	Conf file	Server	VDCtools	Comments
Report	/opt/VDC/tomcat/webapps/vdc/WEB-INF/config/conf.properties	**Master**	3) Configure Report SMTP Server	Need to restart the jsvc process
Notification	/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/SN.properties	**Probe**	2) Configure Alarm Notification SMTP Server	Need to restart the vms process
Project	/opt/VDC/tomcat/webapps/vdc/WEB-INF/classes/vdc.properties	**Master**	5) Configure Workflow SMTP Server	Need to restart the jsvc process
Reset Password	/opt/VDC/tomcat/webapps/vdc/WEB-INF/classes/vdc.properties	**Master**	5) Configure Workflow SMTP Server	Need to restart the jsvc process
Server Admin	/opt/VDC/conf/general.email.properties	**Master**	Cannot configure it in vdctools	Need to restart the jsvc process
VDCMON	/opt/VDC/vdcmon/conf/vdcmon.properties	**Master**	3) Configure Report SMTP Server	Need to restart the jsvc process
Service	Not support now, will handle it once the feature is converted to H5			

ORIGINAL INFORMATION IN 6.2.1 ADMIN GUIDE:

Name	Configuration Keys	VDC Tool Option	Server	Comments
Alarm Notification	EMAILHOST@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/SN.properties= EMAILSENDERADDRESS@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/SN.properties= EMAILSENDERUSER@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/SN.properties= EMAILSENDERPASSWORD@/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/SN.properties= EMAILAUTHPOLICY@/opt/VDC/monitor/vms/w	2) Configure Alarm Notification SMTP Server	In Probe Server	Restart VMS

	ebapps/vms/WEB-INF/config/SN.properties=			
Service Notification	EMAILHOST@/opt/VDC/monitor/conf/sw/SW.properties= EMAILSENDERADDRESS@/opt/VDC/monitor/conf/sw/SW.properties= EMAILAUTHPOLICY@/opt/VDC/monitor/conf/sw/SW.properties= EMAILSENDERUSER@/opt/VDC/monitor/conf/sw/SW.properties= EMAILSENDERPASSWORD@/opt/VDC/monitor/conf/sw/SW.properties=	2) Configure Alarm Notification SMTP Server	In Master Server	
Report Notification	VDCSMTPHOST@/opt/VDC/tomcat/webapps2/reportsystem/WEB-INF/classes/conf.properties= VDCSMTPFROM@/opt/VDC/tomcat/webapps2/reportsystem/WEB-INF/classes/conf.properties= VDCSMTPUSER@/opt/VDC/tomcat/webapps2/reportsystem/WEB-INF/classes/conf.properties= VDCSMTPPWD@/opt/VDC/tomcat/webapps2/reportsystem/WEB-INF/classes/conf.properties= VDCSMTPAUTH@/opt/VDC/tomcat/webapps2/reportsystem/WEB-INF/classes/conf.properties=	3) Configure Report SMTP Server	In Master Server	Restart Tomcat
Projects	VDCWFSMTPHOSTIP@/opt/VDC/tomcat/webapps/axis2/WEB-INF/classes/mail.properties= VDCWFSMTPHOSTAUTH@/opt/VDC/tomcat/webapps/axis2/WEB-INF/classes/mail.properties= VDCWFSMTPHOSTAUTHUSER@/opt/VDC/tomcat/webapps/axis2/WEB-INF/classes/mail.properties= VDCWFSMTPHOSTAUTHPWD@/opt/VDC/tomcat/webapps/axis2/WEB-INF/classes/mail.properties= VDCWFEMAILFROM@/opt/VDC/tomcat/webapps/axis2/WEB-INF/classes/mail.properties=	5) Configure Workflow SMTP Server	In Master Server	Restart Tomcat
VDCMon	VDCSMTPHOST@/opt/VDC/vdcmon/conf/vdcmon.properties=	3) Configure	In Master Server,	

	VDCSMTPFROM@/opt/VDC/vdcmon/conf/vdcmon.properties= VDCSMTPTO@/opt/VDC/vdcmon/conf/vdcmon.properties= VDCSMTPUSER@/opt/VDC/vdcmon/conf/vdcmon.properties= VDCSMTPPWD@/opt/VDC/vdcmon/conf/vdcmon.properties= VDCSMTPAUTH@/opt/VDC/vdcmon/conf/vdcmon.properties=	Report SMTP Server	More fields highlight red	
Reset Password	VDCSMTPHOST@tomcat/webapps/vdc/WEB-INF/classes/vdc.properties= VDCSMTPPORT@tomcat/webapps/vdc/WEB-INF/classes/vdc.properties= VDCADMINEMAIL@tomcat/webapps/vdc/WEB-INF/classes/vdc.properties= VDCSMTPHOST@tomcat/webapps/vdc/WEB-INF/classes/vdc.properties= VDCSMTPAUTH@tomcat/webapps/vdc/WEB-INF/classes/vdc.properties= VDCSMTPUSER@tomcat/webapps/vdc/WEB-INF/classes/vdc.properties= VDCSMTPPWD@tomcat/webapps/vdc/WEB-INF/classes/vdc.properties=	3) Configure Report SMTP Server		

If changes are made to the .conf file settings, users must run the /opt/VDC/bin/vdcconf tool which will push configuration updates to the respective modules. Please note the configuration changes which require the restart of processes for the changes to take effect.

Note that each of these configuration changes can be done using the vdctools script which is documented separately in this document. This script can be accessed at /opt/VDC/bin/vdctools. Alternatively, these changes can be managed using the Server Admin tool which is documented in its own section of this document.

28 Time and Time Zone

It is very important to ensure the system clocks are synchronized among all application servers. Incorrect or out-of-sync system clocks can cause data replication issues, false alarm timestamps, incorrect history point-in-time values, etc. Also, the Master Server will refuse client connection login attempt if the time difference is found to be greater than 36 hours between the server and client. By default, the application installation script sets up a Network Time Protocol (NTP) daemon on all application servers. Please refer to the following link for details on NTP: http://doc.ntp.org/4.1.0/ntpd.htm.

Note that there are two time zone settings considered in the operation of the application:

Master Server Time Zone

The significance of the Master Server time zone is that all daily/weekly/monthly rollup data analysis and report processing jobs are executed according to this time zone. In other words, the Master Server time zone defines the exact starting and ending timeline for days, weeks and months. This is very important to understand, for example, for billing reports and other report output.

Probe Server Time Zone

The time zone of a Probe Server is typically set to the same local time zone where the Probe Server is physically located. This is because the exact local timestamp of a monitor data point and associated alarm may impact the urgency of such an alarm. For example, a 4AM Critical Alarm is usually more urgent than a 4PM Critical Alarm. For this reason, the Probe Server always associates its monitored data and alarms with the local Probe Server time zone.

To see all available time zones which can be defined on the application server, view the third column (the "TZ" column) in the file /usr/share/zoneinfo/zone.tab. Each time zone is represented in the *Region/City* format.

To change the time zone of the application server on a Redhat/CentOS 6.x server follow the commands below. Substitute Europe/Amsterdam in the example with your desired time zone specification. For a list of available Internet Time Servers, refer to http://tf.nist.gov/tf-cgi/servers.cgi.

1) Create the backup of the current time file.
   mv /etc/localtime /etc/localtime-old

2) Create a link between the intended time zone file to the settings file.
   ln -sf /usr/share/zoneinfo/Europe/Amsterdam /etc/localtime
3) Set the system time based on the selected Internet Time Server IP Address.
   /usr/bin/rdate -u -s 129.6.15.28
4) Set hardware clock to the current system time.
   /sbin/hwclock --systohc
5) Reboot the server for all settings to take effect.
   reboot

29 SMS Notification Delivery

Alarm notification rules allow for the recipients to receive an SMS message or an SMTP email message. For the SMS delivery to work properly, the application must be configured with a valid SMS gateway which can accept and deliver the notifications from the application to the end recipients. The customer must provide the SMS gateway information to use for the delivery of these messages.

The SMS configuration settings are defined in the following file:

/opt/VDC/monitor/vms/webapps/vms/WEB-INF/config/SN.properties

The configuration options needed are as follows:

- Sms.script.path – This script is based upon the specific SMPP gateway service which is used by the customer and is obtained from the SMPP service provider.
- Sms.port – Port to use for communicating with the SMS Gateway.
- Sms.success.flag – Indication of what string is returned for a successful delivery of the message. If this string is not matched on deliver then the application will determine the send attempt has failed.
- Sms.address – Address of the SMS Gateway to use for delivery of SMS messages.

When notification rules are configured to deliver SMS to a recipient, the phone number used in the User record will be used for the message delivery. Note, if SMS gateways are not available, most cell carriers provide an SMTP address which can be used for the mobile device which can be used in place of the SMS delivery method.

30 SNMPAgent

The application includes an SNMP simulation tool to help with staging and testing application features. Administrators can define the specific SNMP settings where this process will run and the list of OID and associated values it will return when queried by the application. This simulation tool is located in the following directory:

/opt/VDC/tools/SNMPAgent

To stop and start the process the following commands can be issued:

/opt/VDC/tools/SNMPAgent/snmpagenctl stop

/opt/VDC/tools/SNMPAgent/snmpagenctl start

There are two primary files which manage the configuration of the simulation tool. These files are located in the log /opt/VDC/tools/SNMPAgent/config folder:

- SAS.rc – Defines the key parameters for the SNMP protocol. Users can vi this file to make edits to the configuration. Note, any changes to this file will not be active until the SNMPAgent process is stopped and restarted. Key parameters are defined in the table below.

```
[root@vpm10-3150 config]# cat SAS.rc
SAS.TotalThreadNum:2
SAS.Protocol:UDP
SAS.Community:public
SAS.SNMPVersion:v2c
SAS.StartThreadPort:2162
SAS.RuleFile:/opt/VDC/tools/SNMPAgent/config/SAS.rules
SAS.LogPath:/opt/VDC/tools/SNMPAgent/config/log4j.xml
SAS.IP:127.0.0.1
SAS.LogLevel:Debug
SAS.Trace:Off
SAS.Separator=1.3.6
SAS.SpoolPath:/opt/VDC/tools/SNMPAgent/spool
SAS.AgentBC:/opt/VDC/tools/SNMPAgent/config/SNMP4JTestAgentBC.cfg
```

SAS.Community	SNMP Get community string
SAS.SNMPVersion	SNMP version to be used for the communication with the simulation tool. Options are v1, v2c and v3.
SAS.StartThreadPort	Port where the simulation engine will be running.

SAS.RuleFile	Location of the file which contains the list of OIDs to report using the simulation tool.
SAS.IP	IP Address where the simulation tool will respond to the SNMP queries. Note, best practice is to use 127.0.0.1 so this is running locally on the application server.

- SAS.rules – Lists the OIDs and associated values to return when the SNMP simulation tool is queried for data. The file is simply a list of OIDs with simulated values to be used in driving data into the application. Each OID listed in the SAS.rules file must begin with the standard .1.3.6.1.2.1 OID values. After this prefix, users can use any pattern of OID settings for the simulated data. Note the following options when defining the values for the OID:
    - Fixed Value - Enter only the value to be returned each time the OID is queried.
      .1.3.6.1.2.1.1000.1.55 = 1090
    - Random Range – Enter the range of values to be returned. A random value will be returned from the defined range each time the OID is queried.
      .1.3.6.1.2.1.1000.1.92 = rand(10-125)
    - Random Array – Enter a list of values to be returned. A random value will be returned each time the OID is queried.
      .1.3.6.1.2.1.1000.1.16 = rand_num(0,1,4,9,22)
    - Combination Random – Provide a random number from a range OR a defined array of values. For example a random number from 0-10 OR 22.
      .1.3.6.1.2.1.1000.1.16 = rand(0-10);22
      String – Provide an array of string options to return random strings from the list of values in the array.
      .1.3.6.1.2.1.1000.1.16 = on;off;starting;stopping
    - Note there is a line at the end of the file with default = ##. If the application polls the simulation engine with an OID that is not in the SAS.rules then this value will be retuned for the query. The default setting is 40.

To drive simulated data to device in the application users can manage standard monitoring implementation steps as follows:

- Define Target and Target Members using the OIDs specified in the SAS.rules file
- Link the Target Member data points to the Monitor Attributes for the devices which need to be monitored.
- Assign the IP Address and SNMP settings to the device to activate monitoring.

31 Rack PDU Simulator

There are a few SNMP simulators which are able to take snmpwalk output from real devices as input and respond to SNMP queries according to the snmpwalk data. These simulators allow for simulated discovery and monitoring of Rack PDU devices. Such SNMP simulators are extremely helpful for testing when physical hardware is not accessible.

One such SNMP simulator is the SNMP Agent Simulator from http://snmpsim.sourceforge.net/. The SNMP Agent Simulator is also great to emulate large scale devices for capacity and performance testing. On a 12-core 64GB server, it is capable of handling at least 2000 rackmount PDU devices. Please refer to the website for code and instructions on how to utilize this advanced simulation tool for lab environments.

We do not recommend installing these simulation tools onto the same server which is installed and running the application.

32 Export Floor Tool

The Export Floor tool allows an administrator to export the location data from one system to another. Note that this tool only handles location data. Specific device data export/import is handled by the device Export/Import function built inside the Web UI on the Device Tab. The process below can be followed to move floor and related device data from one instance of the application to another instance of the application.

Important notes related to the operation of this tool:

- If the implementation is a multi-host architecture, then these commands must be run on the Master Database server
- Tool fully supports import/export of floors created in either the web or 3D interface when export and import are performed on identical versions of the application.
- Export from older versions with an import to a newer version is fully supported
- Export from a newer version with an import into the older version may encounter issues

Export Floor from Server

Follow these instructions to export an existing floor from an instance of the application which can then be imported to a different instance of the application.

- Logon the application server console as the vdc user and run the following.
  - su – vdc (this is only required if the current logged in user is the root user)
  - /opt/VDC/bin/exportfloor
- Enter 1 to select the Export Floor option
- Enter the City Name, Building Name, Floor Name to be exported

```
-bash-4.2$ /opt/VDC/bin/exportfloor
################
1) Export Floor
2) Import Floor
3) Update Building Location
x) Exit
################
Enter Your Selection: 1
Start export floor.
Specify the City Name:Mobile
Specify the Building Name:B1
Specify the Floor Name:F1
Export floor:46
Export floor end
46
################
```

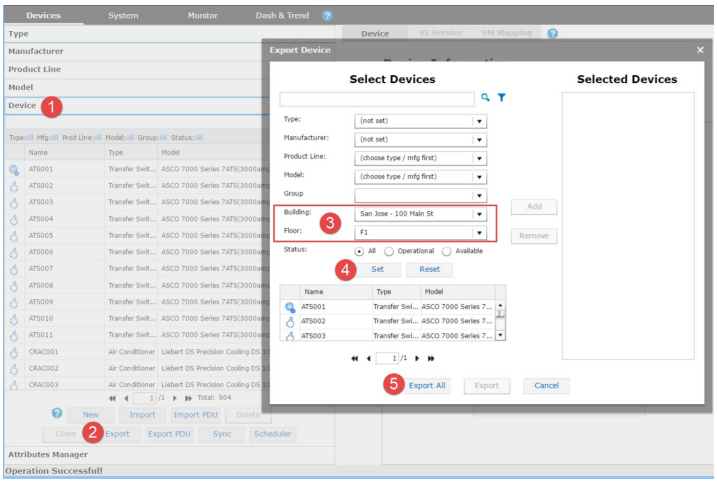
The exported floor data will be saved to the /opt/VDC/data/floor directory. The default directory for this exported data will be named floor. If multiple exports will be performed on the same application instance, it is recommended to rename this floor directory prior to executing subsequent export operations. Each time the export process is run, the contents of the floor directory will be replaced with the new exported data.

Export Devices from Server

If there are devices which are mounted to the floor being exported, users may want to move these devices to the new server as well. This process is completed using the standard Export/Import device process which is located on the Device Menu on the Device Tab.

- Logon the application web interface
- Go to the Devices tab, then click on Export button on the Devices Menu.
- Filter the full device list to match the Building and Floor being exported and click on Set to apply the filter conditions.
- Click on Export All to export the devices to an Excel spreadsheet.
- Rename the device export spreadsheet to match the floor being exported.

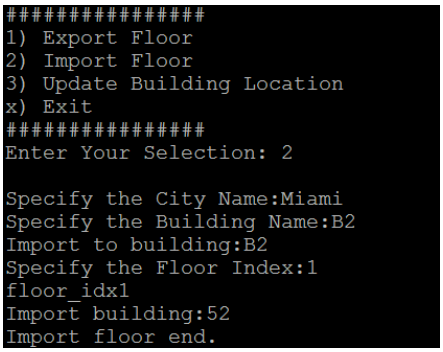
This file will contain all of the device data, attributes and location information which can be used to import to the new floor which is created on the separate application instance.



Import Floor to New Server

Users can import an exported floor from a different system onto the new instance of the application. Please note the restrictions on version compatibility at the beginning of this section when attempting a Floor Import process. The following instructions will allow users to import the floor.

- Ensure the navigation tree nodes needed to support the imported floor are created in the new server application instance. The Country, State, City and Building nodes must be created prior to the Import process being executed.
- Copy the exported floor data package from the original server to the new application server in this folder: /opt/VDC/data/floor. If the exported floor directory was renamed on the original server it will need to be reverted to this default folder name for the import process to complete successfully.
- Logon the application server console as the vdc user and run the following.
  - su – vdc (this is only required if the current logged in user is the root user)
  - /opt/VDC/bin/exportfloor
- Enter 2 to select the Import Floor option.
- Enter the City Name, Building Name and the Floor Index where the floor should be imported. Note, the floor index is a reference to the order in the building floor list where this floor should be referenced. For example, the floor with index 1 will be listed at the top of the navigation tree under the building name.



- Login to the application and confirm the floor is included in the navigation tree.

Import Devices to New Server

When a floor has been imported to a new instance of the application, users can easily move devices onto the floorplan. Assuming the devices have been exported from the previous application server instance, the following instructions will import devices to the newly imported floorplan.

- Logon the application web interface
- Go to the Devices tab and click on the Import button on the Devices Menu.
- Select the spreadsheet to import.

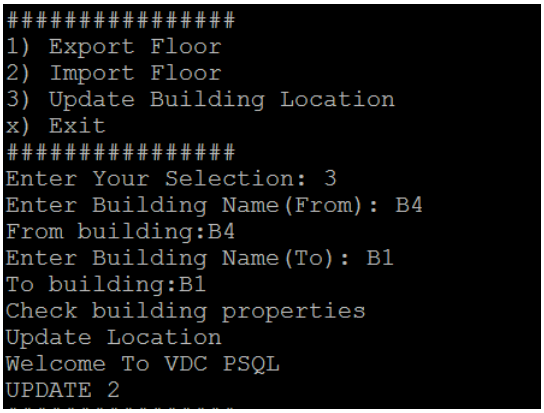
When you return to the application you will need to refresh the device list and floorplan views to see the newly imported devices.

Update Building Location

In some cases a user may incorrectly create floors or buildings in the wrong city or location. The Update Building Location option will allow users to change the location of floors to a different level of the navigation tree.

- Logon to the application server console as the vdc user and run the following.
  - su – vdc (this is only required if the current logged in user is the root user)
  - /opt/VDC/bin/exportfloor
- Enter 3 to select the Update Building Location option.
- Enter the building name for where the floors are currently located.
- Enter the building name for where the floors need to be moved.

The tool will relocate the floors from the original to the destination building along with all devices which were located on the source floors. Location information for the devices will be updated to the new building location information.



33 Support Portal

Logging into the Optimum Path Support Portal

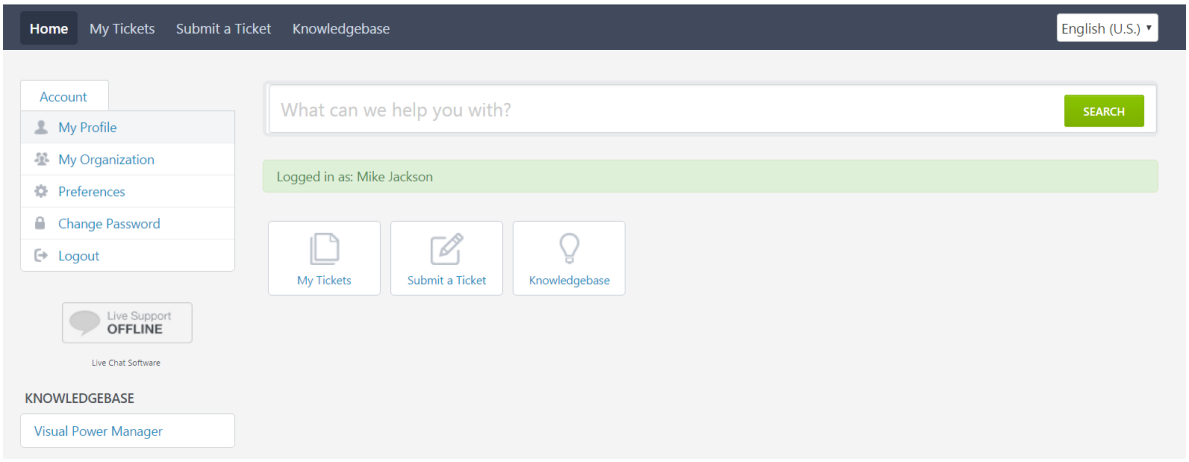
The Optimum Path Support Portal can be accessed at the following URL:

https://support.optimumpathinc.com

1. Point your web browser to the support portal URL
2. Enter the provided username and password, If you do not have a user account please have the authorized representative from your company send the support team a request to provision an account.
    a. If you forget your password, click the “Lost password” link below the password field and an email will be sent to the email address that is associated to the username that you entered.
3. Once information is entered correctly, you will be directed to the customer support ticket home page.

Basic Portal Navigation

The support portal provides users access to product information, knowledgebase information and the ability to manage support tickets related to the product. The following is a basic overview of the portal layout to help define the tools available to provide support for the product.



- Home – Home screen which provides access to all support functions.
- My Tickets – List of tickets submitted by the currently logged in user. If the user is configured as a manager for the company then a list of all company tickets will be listed.
- Submit a Ticket – Allows user to open a new ticket to submit for support.
- Knowledgebase – Searchable list of articles written to address common issues encountered with the products.
- Search – Allows user to quickly search Knowledgebase, News or other support tools for a list of relevant articles for troubleshooting.
- Account Links
    - My Profile – Personal information for the logged in user.
    - My Organization – Details of the Organization.
    - Preferences – Timezone and Language settings.
    - Change Password – Ability to change password for the current account.
    - Logout – Logout of the application.

Using the Knowledgebase Feature

The Knowledgebase feature is a powerful way for support portal users to easily access key information on common issues prior to opening a support ticket. This area contains short

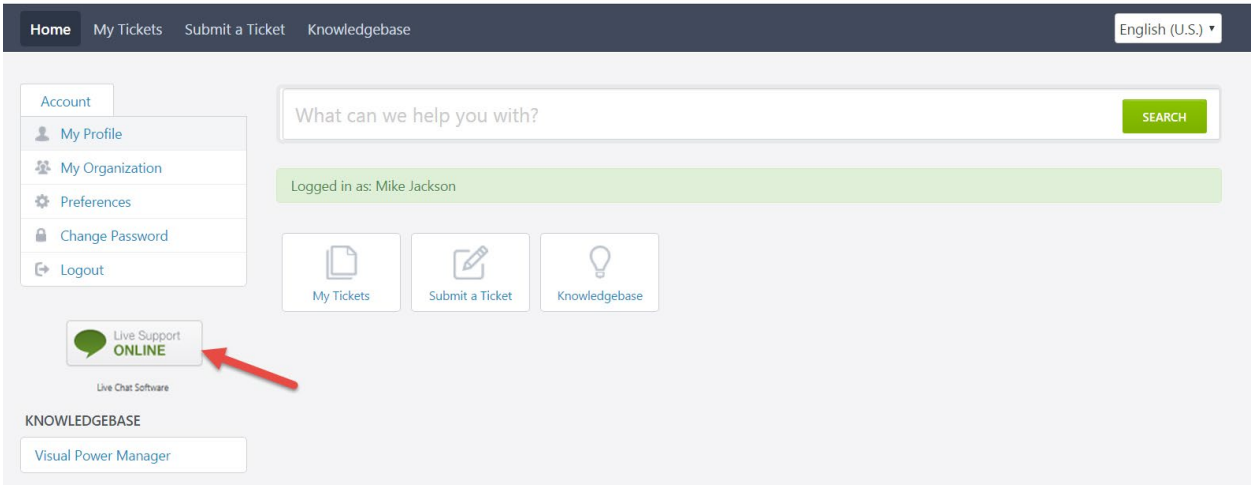
articles to instruct users on how to perform certain functions in the application and how to resolve common trouble issues.

The Knowledgebase is divided into key functional areas related to the application so articles are grouped together to ease the troubleshooting process. In addition, the Search function at the top will allow for instant, key word searching of the list of articles in the Knowledgebase tool.

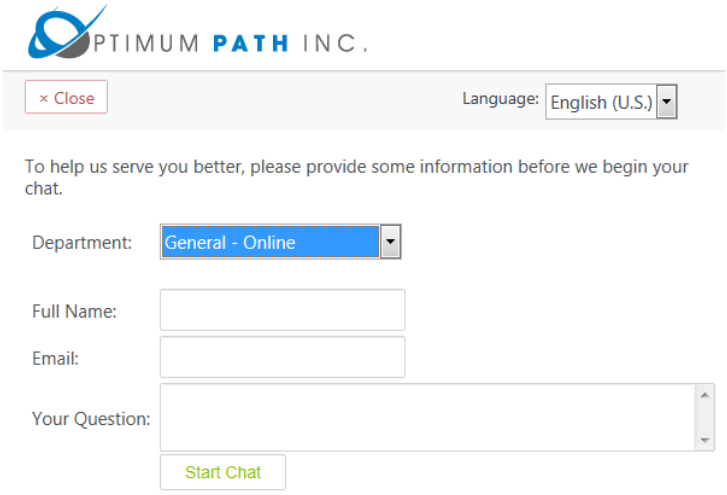
Note the Knowledgebase will be built over time as support tickets are submitted and resolved. Staff members will create articles related to common fixes, tips and tricks for use of the application.

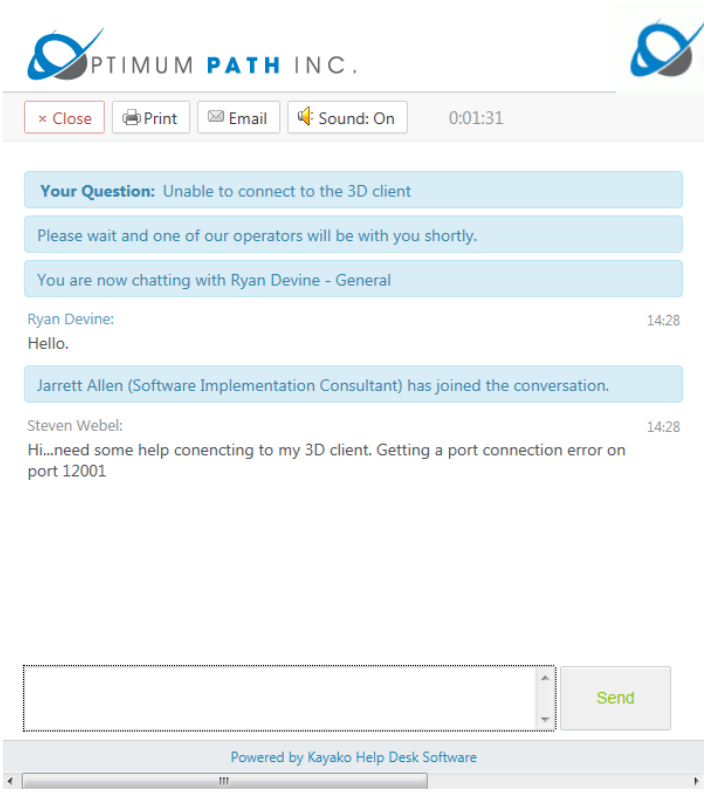
Using the Live Support Chat Feature

The Live Support Chat feature allows support portal users to connect directly with an Optimum Path support engineer in an online chat session to receive support for their issues. At any time while navigating the support portal a user can click on Live Support button to chat with one of our support professionals.



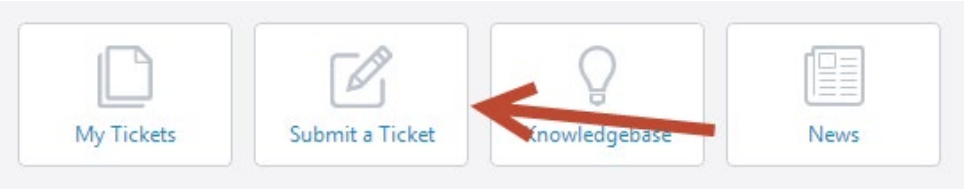
Users will be prompted for basic information related to the issue and an online Chat session will begin with one of our Support Engineers. The chat window will allow users to Print or Email the contents of the chat session.


PTIMUM PATH INC.
× Close
Language: English (U.S.)
To help us serve you better, please provide some information before we begin your chat.
Department: General - Online
Full Name:
Email:
Your Question:
Start Chat

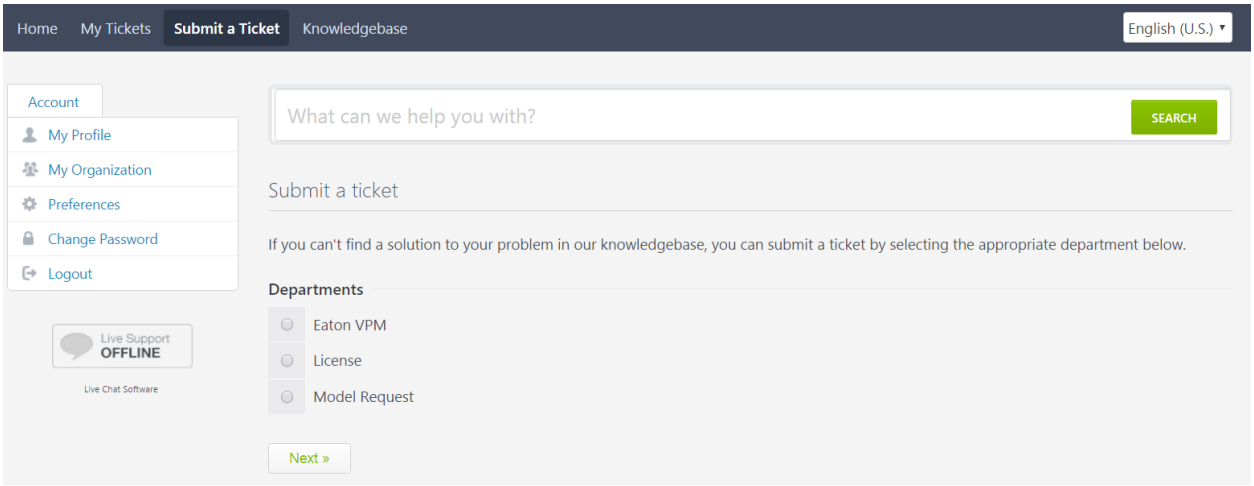

PTIMUM PATH INC.
× Close
Print
Email
Sound: On
0:01:31
Your Question: Unable to connect to the 3D client
Please wait and one of our operators will be with you shortly.
You are now chatting with Ryan Devine - General
Ryan Devine:
14:28
Hello.
Jarrett Allen (Software Implementation Consultant) has joined the conversation.
Steven Webel:
14:28
Hi...need some help conencting to my 3D client. Getting a port connection error on port 12001
Send
Powered by Kayako Help Desk Software

Creating a New Support Ticket

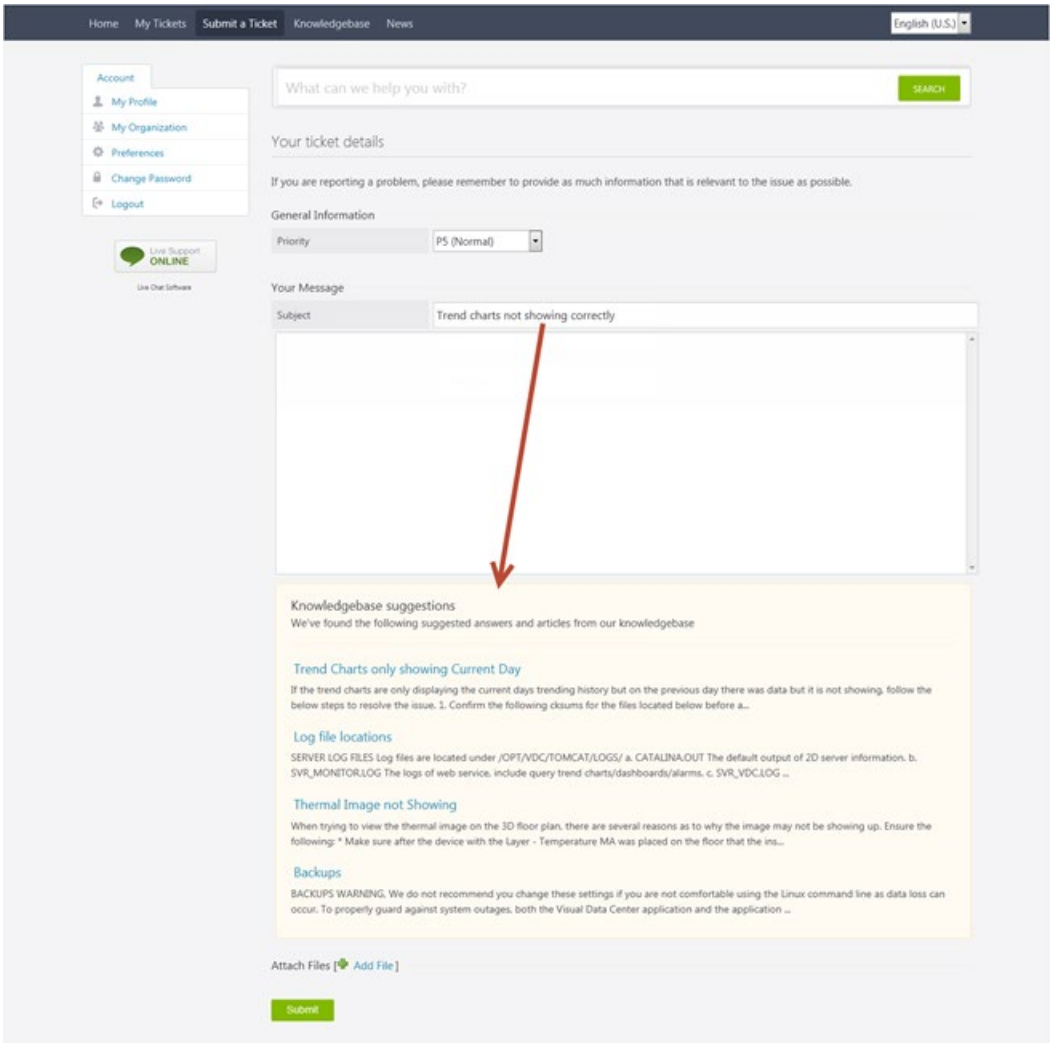
Follow these steps to create a new support ticket in the support Portal:



1. Select “Submit a Ticket” from the ribbon bar located at the top of the window.
2. Select the appropriate ticket option:
    a. Technical Issues – Technical issue related to the software functions
    b. License – Request for a new or updated license activation key
    c. Model Request – Request to add support for a model in the model library



As the user is entering the Subject of the ticket, a list of related Knowledgebase articles will be listed under the ticket submission form. If users are unable to find an answer to their support issue in the articles, they can Submit the ticket and it will be logged into the account.



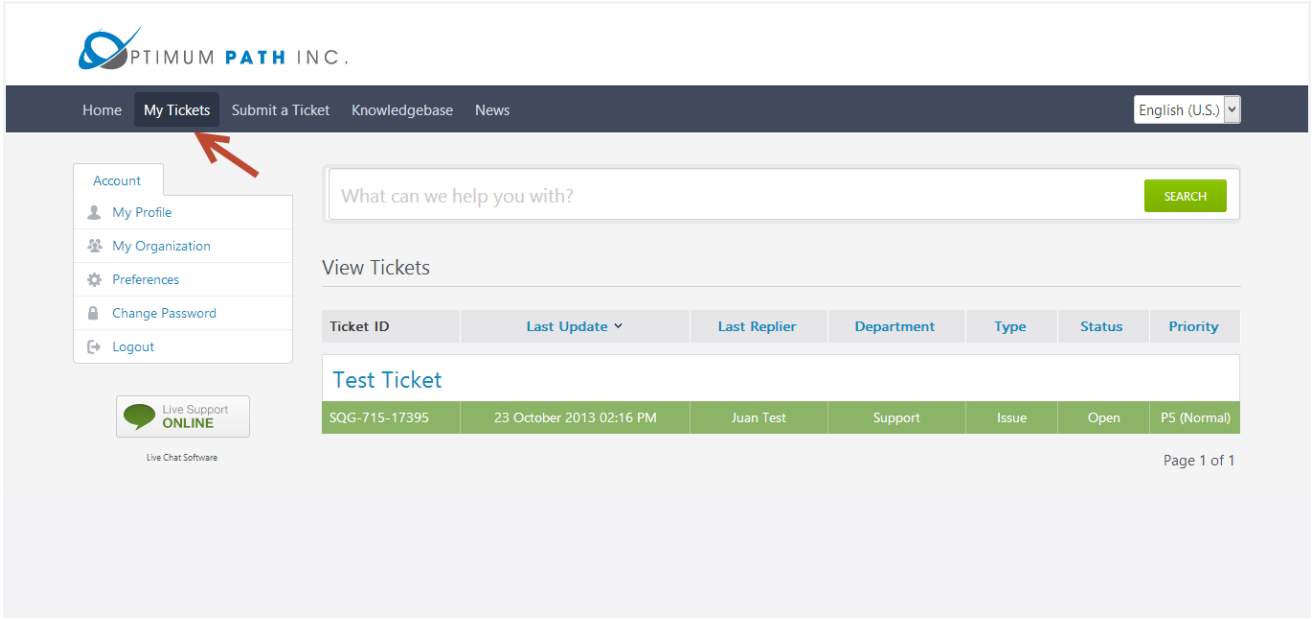
Note, the following ticket priority definitions should be used when submitting a new ticket. While there may be specific circumstances which may require special handling of tickets, the rules here should be used for the cast majority of ticket submissions:

Priority	Title	Description
P1	Critical	Unable to access the application.
P2	Major	Major loss of functionality to core features of the application.
P3	Normal	Technical issue related to an isolated part of the application.
P4	Minor	Technical issue with a feature but a workaround is available to continue use of the application.
P5	Enhancement	Documentation update, usability or workflow enhancement request to the application.

Viewing Tickets

Follow these steps to view tickets which have already been submitted to the ticket portal:

1. Select the “My Tickets” tab at the top of the Optimum Path Inc. Support Portal
2. Select the ticket from the list to view more detail, edit or update status of that ticket.



34 getsupportinfo Tool

The getsupportinfo tool provides an automatic way to collect 100+ important system information elements on the server to submit to technical support teams for troubleshooting analysis. The output data from getsupportinfo is the best way to provide support a holistic view of the entire system without support teams accessing the application server.

The tool is included in the base version of the installation package and can be run from the /opt/VDC/bin directory. The tool is executed with the following command.

Note, this tool may take up to 20 minutes or longer to run. For best results, this tool should be run as the root user. While it can be run as the vdc user for customers who have concerns with root access, the output will be limited with the vdc user.

/opt/VDC/bin/getsupportinfo.sh or /opt/VDC/bin/getsupportinfo.sh -S

There are three options for running this key troubleshooting tool.

- No arguments runs the tool in "quick mode" where individual file consistency check is disabled. The quickmode allows getsupportinfo.sh to finish significantly faster.
- **-S option** collects some additional information and restarts the application processes as part of its execution.
  Note, Given the process restarts, this method is more intrusive to live production systems with active users so it should be used with caution. If the current application is accessible via the web interface with a login then it is recommended to NOT use the -S option which restarts the processes. **If the web interface is not accessible it is recommended to use the -S option.**
- **-q option** enables the file consistency check and takes significantly longer to run.

The script will generate an output file which contains the details gathered from the series of commands executed on the server. This file should be sent to the technical support team for a review of the server to help isolate issues and determine causes for reports support tickets.

/var/tmp/getsupportinfo.log.bz2

Latest Version of getsupportinfo Tool

The getsupportinfo script is updated regularly to provide more information in the log. Retrieve the latest version of the tool from this link:

https://support.optimumpathinc.com/getsupportinfo.sh

Follow these these steps to place on the VDC server and run:

1. SCP the downloaded getsupportinfo.sh script onto VDC server under /tmp
2. Login VDC server as root or vdc user
3. Run "bash /tmp/getsupportinfo.sh"
4. Wait until the script finishes and email OPI Support the file: /var/tmp/getsupportinfo.log.bz2

35 checkprotocols Tool

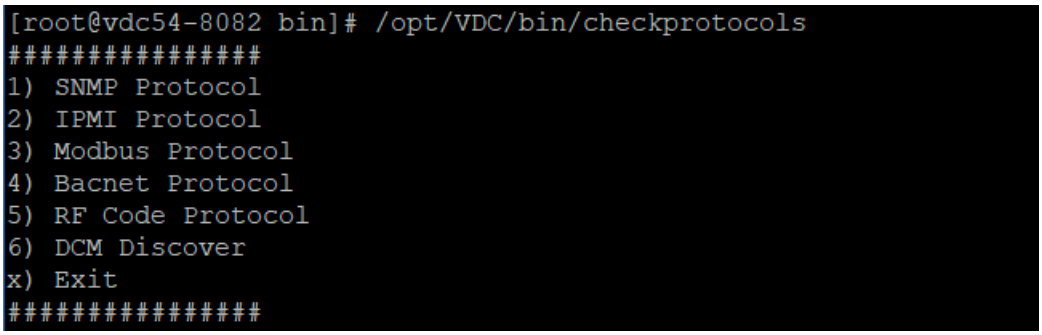
The checkprotocols tool allows users to verify connectivity between the application server and specific devices over designated protocols. If monitoring configuration is failing to reach a device, this tool can be used to verify connectivity at a basic level.

The tool is included in the base version of the installation package and can be run from the /opt/VDC/bin directory. This tool should be run as the root user.

The tool is executed with the following command.

/opt/VDC/bin/checkprotocols

The tool presents a menu list of protocols. Each menu pick has a set of parameters to input for testing.



When you enter your selection, you will see a Parameters string showing what values you will be prompted to enter. Most tools also include some details or notes regarding those entries.

Output is displayed on the screen and written to the file:
/opt/VDC/tools/protocoltools/log/protocol.log

- Option 1 – SNMP Protocol
  Parameters: snmpget/snmpsubtree/snmpwalk version getcommunity ip port [setcommunity] [username] [password] [auth] [privacyProtocol] [privacyPassword] [context] oid
  - Please enter your command: snmpget/snmpsubtree/snmpwalk
  - Please enter your SNMP Version: v1/v2/v2c/v3
  - Please enter SNMP Protocol (TCP or UDP):
  - Please enter IP Address:
  - Please enter Port:
  - Please enter OID:

    - Please enter Get Community:
- Option 2 – IPMI Protocol
  Parameters: ip port username password command sensor
    - Please enter IP Address:
    - Please enter Port:
    - Please enter User Name:
    - Please enter Password:
    - Please enter Command:
    - Please enter sensor:
- Option 3 – Modbus Protocol
  Parameters: ip port register deviceid
    - Please enter IP Address:
    - Pelase enter Port:
    - Please enter Register:
    - Please enter Daviceid:
- Option 4 – Bacnet Protocol
  Parameters: ip port Device_Instance_Num Object_Ident Property_Ident Object_Instance_Num
    - Please enter IP Address:
    - Please enter Port:
    - Please enter Device_Instance_Num:
    - Please enter Network Number (default 0):
    - Please enter Ojbect_Ident (Leave it blank of you don't know):
    - Please enter Property_Ident (Leave it blank if you don't know):
- Option 5 – RF Code Protocol
  Parameters: cmd ip port username password [tag]
    - Please enter Command:
    - Please enter IP Address:
    - Please enter Port:
    - Please enter User Name:
    - Please enter Password:
- Option 6 DCM Discover
  Parameters: startip endip netMask protocol[SNMPv1v2c/SNMPv3] community
    - Please enter ip:
    - Please enter ip:
    - Please enter netmask:
    - Please enter protocol:
- Option x - Exit

36 Troubleshooting Tips

The following sections can be used to troubleshoot some common issues with application installations.

Unable to Access Web Login Page with HTTP Connection

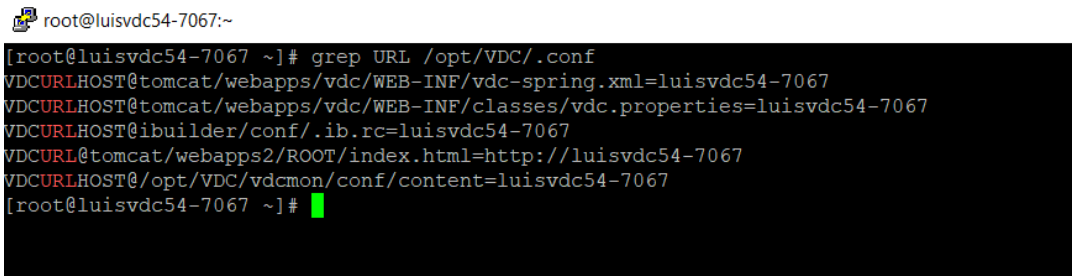
Tips:

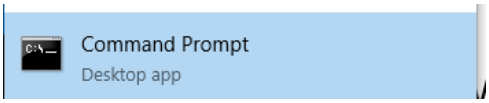
- Ensure that you have a proper license installed for your VDC architecture and method of access HTTP or HTTPS.
- Ensure that if your server is a VM (Virtual Machine) Vmotion is disabled for this server.
    - The license is tied to the machine and its hardware signature. A VM switching hosts will change the hardware signature thus invalidating the license and resulting in the product not running.
    - This is commonly in the properties section of the VM host configuration. You can consult with your VM admin regarding this configuration setting. The "base" VDC license does not support Vmotion. If Vmotion is a requirement in your architecture, please reference the License Configuration options and Real Time License Server in this manual.
- Note, the License is stored in /opt/VDC/.vdc
    - The .vdc directory is hidden
    - When accessing the .vdc directory with Win-SCP and similar programs it will not be visible unless the program is enabled to see hidden directories.
    - The .vdc directory can only contain one license file.
- The license file owner permissions, name and file extension must not be changed
- Follow the procedure in the Server & OS Installation Guide, Licensing the Application section for proper license installation
- All-in-one server requires one license installed
- Multi-server architecture requires a license on each server. In this architecture, always ensure the Master server (includes the Master database) license is installed and rebooted before installing any of the Probe server licenses.

Login:

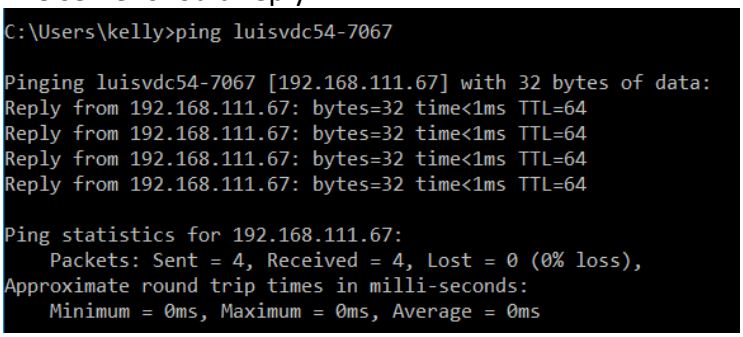
- Web interface (2d) and VDC 3D Client require the use of the URL defined during installation to login.
    - No other method is acceptable
    - Do not use the IP address or hostname of the server as a URL. This may cause configuration errors and confusion in the VDC environment.
    - As of v5.5 an error will pop up if you try to use the IP address or a different URL from the one defined during installation.

- Confirm the URL by running the following in a command line window on the application server:
  grep URL /opt/VDC/.conf
  Below is an example output, note the URL = http://luisvdc54-7067



- Web interface (2d) and VDC 3D Client require the use of the ports stipulated in Server Ports section of the Server & OS Installation Guide. These ports must be available to the PC workstation you are using and the network environment to which the PC workstation is connected. Confirm this with your network admin.
- Ensure that your PC workstation can reach the VDC Master server URL
- Open the windows cmd tool 

- Ping the VDC server's URL for example: **ping luisvdc54-7067**
- The server should reply:



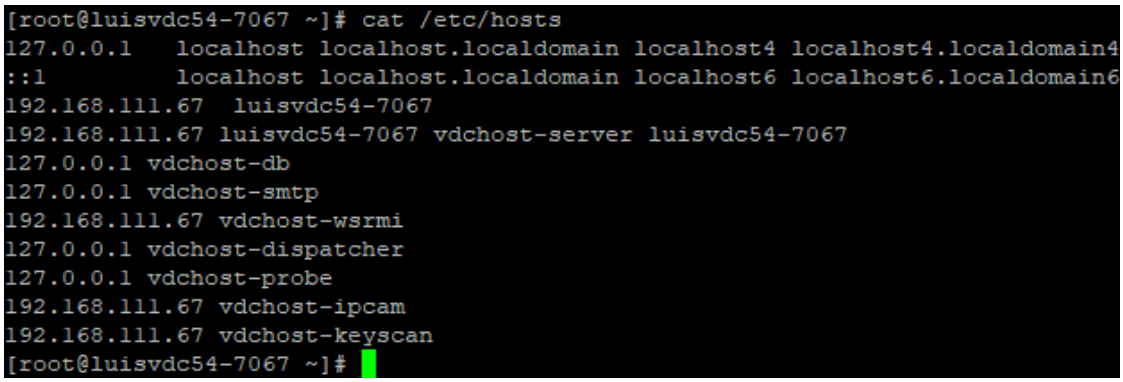
- If there is no reply check with your PC workstation admin to ensure that the PC workstation local hosts file is configured or that the network DNS is configured to resolve the VDC Master server URL.
- The PC workstation local hosts file is commonly located in this path: Windows\System32\etc\hosts
- If you cannot locate this file consult with the PC workstation admin. You must typically have admin rights to edit this file.
- Confirm that there is a proper entry for the VDC Master server for example: **111.111.111.111 luisvdc54-7067**

- Advanced Trouble shooting may require the PC workstation admin to check connection to the VDC Master using "telnet". The telnet client for windows may not be enabled. To enable telnet client use the windows Control Panel > Programs > Turn Windows features on or off > check Telnet Client. You may need admin rights to enable telnet.
- Start a command window
- At the prompt enter **telnet URL port#**
  For example: **telnet luisvdc54-7067 80**
  This will connect to port 80
- A failed connection will report as: "connection falied"
- A good connection produces a blank window, no prompts

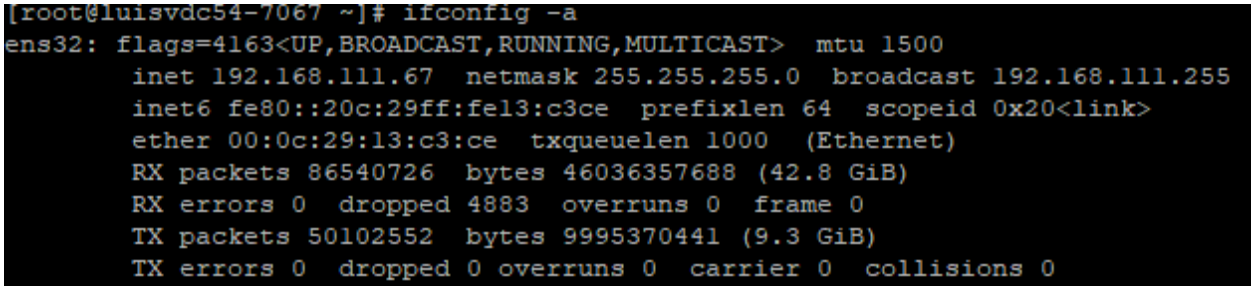
Confirming the VDC Master server hosts file and base network configuration.

- Confirm proper hostname configuration on the VDC Master.
- At the command line prompt run this command: **hostname -i**
- The output should return the hostname "pointed" to its own IP address .
  As an example:

- If the above output is not correct edit the /etc/hosts file .
- The VDC Master hosts file is located at this path: /etc/hosts.
  You can view this file with the cat command: **cat /etc/hosts**



- The VDC Master's current running network configuration can be displayed by running this command: **ifconfig -a**



- Note that in the above examples the hosts file contains this entry: 192.168.111.67 luisvdc54-7067 vdchost-server luisvdc54-7067 . This entry ensures that vdc host server is connected to the IP 192.168.111.67. (the public IP address).
- The ifconfig -a command output confirms that the network is using "ens32" the defined network connection (commonly an Ethernet port on a "nic" card) on the server. Note the IP address 192.168.111.67 is properly configured and running on this Ethernet connection.

Server Hard Drive Full

Server hard disk space full issues are the most commonly seen issue. To avoid the server hard disk space full issue, follow these best practices:

1) Ensure architectures are created or reviewed by support team prior to recommending to customers. Starting with incorrect sizing with the initial hardware will plague the relationship until new resources are provisioned.
2) Always keep at least 30GB+ free disk space for /usr/local/pgsql, 40GB+ free disk space for /opt/VDC and 50GB+ free disk space for /opt/VDC.BACKUP. Activities such as database self-maintenance, patch installation, upgrade/migration, backup/recovery, etc, requires a lot of disk space.
3) If possible, create separate disk partitions for /usr/local/pgsql and /opt/VDC. This will help reduce the risk of data corruption.
4) Always mount /opt/VDC.BACKUP onto a different hard disk or network mount-point to avoid a single point of failure for the production data and the backup images. Never under any circumstances mount or link /opt/VDC.BACKUP under /opt/VDC.

If server disk space does become full, follow these steps to correct the issue:

1) Ensure there is at least one known-good full application system backup under /opt/VDC.BACKUP
2) If the server is a virtual server, create a VM snapshot
3) Remove the /opt/VDC/patch directory by carefully running command: *rm -rf /opt/VDC/patch*. Re-check the command twice to make sure the directory name is spelled exactly as indicated before hitting the Enter key.
4) Remove tomcat log files by carefully running command: *rm -f /opt/VDC/tomcat/logs/**. Re-check the command twice to make sure the directory name is spelled exactly as indicated before hitting the Enter key.
5) Remove monitor log files by carefully running command: *rm -f /opt/VDC/monitor/vms/logs/**. Re-check the command twice to make sure the directory name is spelled exactly as indicated before hitting the Enter key.
6) Run command: *df -k* to see if both /usr/local/pgsql and /opt/VDC have at least 5GB+ free space. If not, run command: *find . -type f -print0 | xargs -0 du -s | sort -n | tail -10 | cut -f2 | xargs -I{} du -sh {}* to view the top 10 file disk space used to see if there is any anomaly. If there is enough free disk space, reboot the server.
7) The above steps are temporary steps to help to get the system running again. Please work with the Linux system administrator to add/expand the file systems immediately.

Database Memory Tuning

In order to take full advantage of available physical memory on a server, the key Postgres database configuration parameters must be tuned to the following suggested values in /usr/local/pgsql/data/postgresql.conf. After these parameters are modified, Postgres database must be restarted or reboot the server for the changes to take effect.

Physical Memory Size	Recommended Key Postgres Database Configuration Parameters
16GB	maintenance_work_mem = 819MB max_stack_depth = 8MB effective_cache_size = 12288MB shared_buffers = 3277MB checkpoint_segments = 64 wal_buffers = 16MB work_mem = 5MB
20GB	maintenance_work_mem = 1000MB max_stack_depth = 8MB effective_cache_size = 15000MB shared_buffers = 5000MB checkpoint_segments = 64 wal_buffers = 16MB work_mem = 7MB
24GB	maintenance_work_mem = 1229MB max_stack_depth = 8MB effective_cache_size = 18432MB shared_buffers = 4915MB checkpoint_segments = 64 wal_buffers = 16MB work_mem = 31MB
32GB	maintenance_work_mem = 1638MB max_stack_depth = 8MB effective_cache_size = 24576MB shared_buffers = 6554MB checkpoint_segments = 64 wal_buffers = 16MB work_mem = 41MB
48GB	maintenance_work_mem = 2400MB max_stack_depth = 8MB effective_cache_size = 36000MB

	shared_buffers = 12000MB checkpoint_segments = 64 wal_buffers = 16MB work_mem = 50MB

Device is Not Returning Monitored Data

A common issue in the application is a device showing an Unreachable alarm when the user expects data to be successfully retrieved. There are a few obvious troubleshooting steps to take to try and isolate the source of the issue. In general, the issue will be one of the following:

- Is the target device powered on and behaving properly? Note, many devices have a native web interface which can be accessed to view data. This is a good initial place to look for issues with the device itself.
- Is the device configured to respond to the query for data? Some devices require a whitelist of data collectors to which it will respond or requires an activation of the protocol in the device settings. For example, a device needs to be activated with SNMP may require the device administrator to define the port, community string and SNMP version on which it will respond.
- Are there issues with the network which are preventing the application probe server from reaching the device to collect data?
    - Ping the device IP address from the application console. If the device is configured to respond to ping and there is no response then consult the network team to resolve the network access issue.
    - If ping is successful then you can try to telnet to the device on the port used for monitoring. The following protocol and standard ports:
        - SNMP – Port 161
        - Modbus – Port 502
        - Bacnet – Port 47808
    - Note the Bacnet protocol has some very specific switch configuration requirements to pass the Bacnet traffic thru to a different network. If using Bacnet and there are issues accessing the device or gateway then investigate these details of the Bacnet protocol as this is a common issue while polling Bacnet device.

- Is the device configured properly in the application? There are different levels of configuration required to properly enable data collection for a device. Using the Verify button on the Device Monitor page will simulate a data collection cycle and produce results. This is a good way to confirm the configuration settings are good in the application.

Note, if the Verify results in an Unreachable status, users can submit command line SNMP commands to check protocol settings. The command line bypasses the application altogether and is a great way to isolate issues in the network vs the application configuration. The following are sample SNMP commands which can be used to test settings.

For SNMP V1 Protocols:

- **snmpwalk -On -O e -v1 -c** *REPLACE_WITH_COMMUNITY REPLACE_WITH_IP* **.1.3.6 >** *REPLACE_WITH_FILENAME*
- **snmpwalk -On -O e -v1 -c public 192.168.111.188 .1.3.6.1.2.1**

For SNMP V2C Protocols:

- **snmpwalk -On -O e -v2c -c** *REPLACE_WITH_COMMUNITY REPLACE_WITH_IP* **.1.3.6 >** *REPLACE_WITH_FILENAME*

- **snmpwalk -On -O e -v2c -c public 192.168.111.188 .1.3.6.1.2.1**

- See the checkprotocols tool section and use the tool to verify connectivity between the application server and specific devices over designated protocols. If monitoring configuration is failing to reach a device, this tool can be used to verify connectivity at a basic level.

37 Helpful Linux Commands

Administrators of the application will need to be familiar with the command line Linux commands to quickly troubleshoot issues and manage the implementations. Some of the common Linux commands needed for installation and management of the application are listed below:

Command	Description	Example
cat	Outputs entire content of a file onto the screen	cat /opt/VDC/.conf
cd	Change directory	cd /opt/VDC
chmod	Used to change the permissions of files or directories	chmod +x test.sh
chown	Changes the user or group of a file or directory	chown vdc demo.txt
cp	Copy files or directories	cp /tmp/a.txt /opt/a.txt
date	Display the time on the server	date
df	Displays size statistics about a file system	df -h
du	Displays size statistics about a directory	du -sh
find	Used to locate files or directories	find /opt/VDC .conf
grep	Used to search text or files containing a certain pattern	cat a.txt |grep “abc”
kill	Forces processes to end	kill -9 Process_Id
ls	List contents of a directory	ls /opt/VDC
mv	Move	mv /tmp/a.txt /opt/a.txt
ps	Process list	ps -ef | grep jsvc
pwd	Shows current location in the directory tree	pwd
rm	Remove	rm -rf /opt/a.txt
scp	Secure copy	scp a.txt root@123.123.123.123:/opt
ssh	Connect with secure shell	ssh root@123.123.123.123
su	Change to a different user	su - vdc
sudo	Allows user to run command as another user	sudo cat /opt/VDC/.conf
free	Gives information about RAM, cache and swap space	free -m
dmesg	Used to write the kernel messages to the screen	dmesg
lsb_release	Prints certainLSB and Distribution information	
netstat	Used to check network configuration and activity	netstat -nr
lsof	List files opened by various processes.	lsof
tar	Compress or extract a set of files or directories	tar -C a.tar /opt/
tail	Show the last number of lines of a log file	tail -n 100 /opt/VDC/a.log

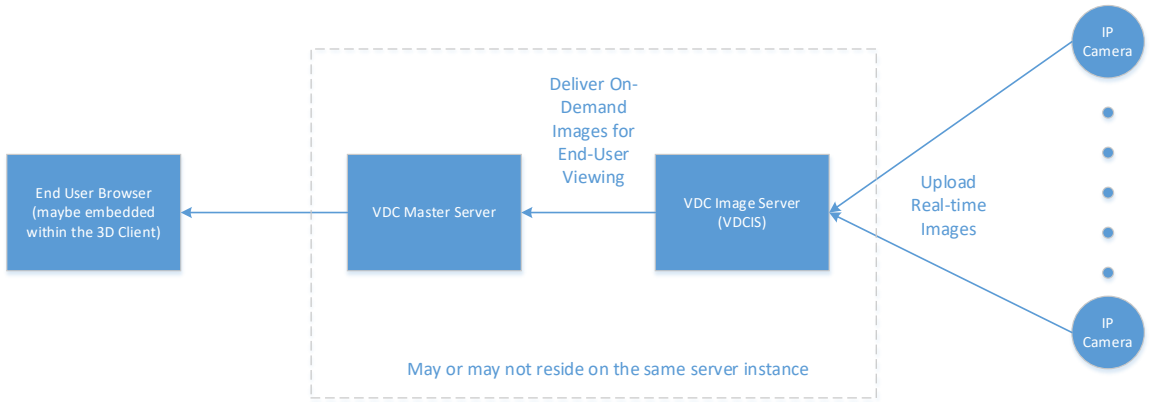
38 Image Server

The purpose of this section is to provide technical information for the installation and configuration of the Visual Data Center Image Server. This application feature is designed to capture images from IP Cameras and display them within the Visual Data Center application.

Almost all IP Cameras support uploading images via the FTP protocol. Visual Data Center Image Server creates a central repository for the images uploaded by multiple IP cameras. The Visual Data Center Web Server fetches up-to-date images from its Image Server to deliver real time images to the end user.

Architecture

The VDC Image Server (VDCIS) is a standalone server instance which is installed using a standalone VDCIS Installer. VDCIS can co-reside with the VDC server on the same server or it can be installed on a separate server. The following figure illustrates the high level architecture.



High Level VDC-VDCIS Architecture

The main concern of such an architecture is that the network and server performance impact caused by the perpetual camera image uploading data traffic. Assuming each camera image is 100K in size and each camera is uploading 1 image per second, 100 of such cameras will consume 80Mbits/second network throughput. Such an impact on the network throughput is permanent since the data uploading is perpetual. It is highly recommended to install multiple network interfaces on the VDCIS server so that the IP Camera data traffic stays on its own subnet without degrading the network throughout for everything. Also, each camera will consume 8GB+ hard drive space per day. Thus, the retention policy must be designed properly

according to the available physical hard drive space. The VDCIS installer provides a tool for space estimation to assist with these decisions on the retention policy.

VDCIS Installation

Visual Data Center version 4.13 and above supports the use of the VDC Image Server. Only use the compatible VDC Image Server release for the specific VDC release being used by the customer. The VDC Image Server can be installed prior to or after the VDC Server has been installed.

Prequisites:

- VDC Master server hostname and IP address must be in the VDCIS /etc/hosts file prior to VDCIS installation

The VDC Image Sever installer usage is as the following:

Usage: VDCIS-INSTALLER

./install [-p ftp_port][-r retention_days][-s average_image_size]

When the –s option is used, the installer will only suggest the maximum number of IP cameras it can support without installing anything. If the -p option is not used the default port is “21”.

For example:

 # ./install -r 3 -s 100000

VDCIS-INSTALLERstarts...

Specified retention days is 3.

Given the average size for each image is 100000 bytes, 3 retention days and available 183821444 KB available disk space under /opt/VDCIS/ftpserver/res/home/, this system can support at most 7 (assuming each camera uploads 1 image per second)

Follow these steps to install the VDC Image Server:

#	Description	Commands

1	SCP the installer onto the server under /opt/install	
2	Login the server as root user and change directory to /opt/install	# cd /opt/install
3	Extract the package	*# tar –xvf VDCIS-INSTALLER-6.2-20021401.tar*
4	Change directory to the VDCIS-INSTALLER-6.2. Use the installer to understand how many IP cameras it can support where –r is the retention days and –s is the average size of the images to store.	*# cd VDCIS-INSTALLER-6.2* *# ./install -r 3 -s 100000* Example output: Specified retention days is 3. Given the average size for each image is 100000 bytes, 3 retention days and available 89587384 KB available disk spa ce under /opt/VDCIS/ftpserver/res/home/, this system can support at most 3(assuming each camera uploads 1 image per second)
5	Invoke the installer with the desired retention days	*# ./install –r 3*
6	The server processes will be automatically started after the installation. No need to reboot. However, to stop and start VDCIS use this command.	/etc/init.d/vdcis stop /etc/init.d/vdcis start
7	To check for running VDCIS run this command there should be three processes related to the ftp server.	ps -ef |grep ftp root 4271 10632 0 15:35 pts/1 00:00:00 grep ftp root 21430 21422 0 13:56 ? 00:00:00 /usr/libexec/openssh/sftp-server root 25481 1 0 14:21 pts/1 00:00:00 /bin/sh ./ftpd.sh ./res/conf/applicationContext.xml root 25514 25481 0 14:21 pts/1 00:00:05 /opt/VDC/jdk/bin/java -classpath :/opt/VDCIS/ftpserver/bin/.
8	The VDCIS Home directory is	/opt/VDCIS
9	VDCIS tools are in bin :	/opt/VDCIS/bin

	Add, delete, update, mon, view Usage example: ./addftpuser	addftpuser deleteftpuser updateftpuser vdcisconf vdcismon viewftpuser
10	Create ftp account on the VDCIS server for *each* IP camera which will be managed. See detail in the section below on managing ftp accounts on the VDCIS server.	*/opt/VDCIS/bin/addftpuser ipcamera_name password* Usage: ./addftpuser ftpuser_id ftpuser_pwd
11	Login to the Admin Interface for each IP Camera to save the FTP settings and instruct the camera to upload images continuously	Note, these instructions are camera specific but a reference is provided below for common practices used by cameras for managing this feature.

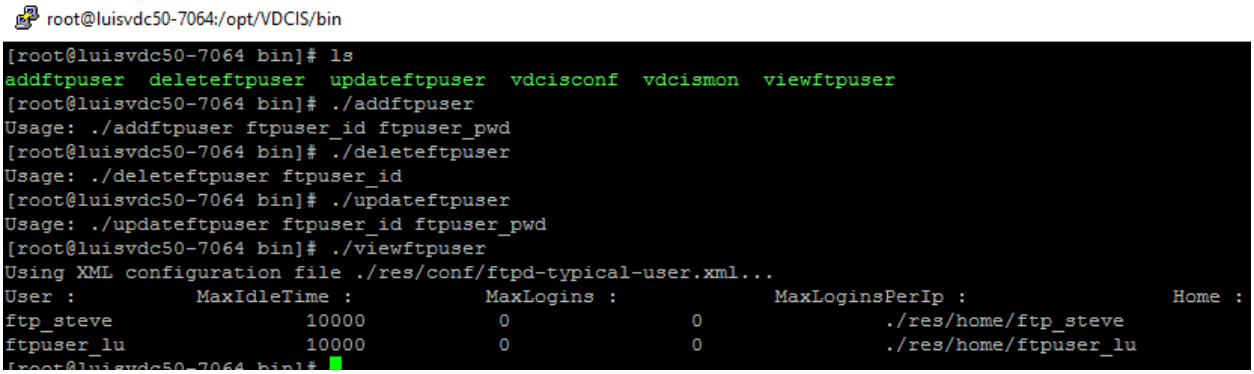
Managing VDCIS FTP Accounts

Each camera to be managed by the VDCIS server needs to have an FTP account created to establish communication and a dedicated file repository for that camera. The following instructions are provided to manage the FTP accounts on the VDCIS server.

1) Log in Image Server as root user
2) Run: cd /opt/VDCIS/bin
3) Run to view files in bin (VDCIS tools): ls
4) There are six available VDCIS tool commands:

   addftpuser deleteftpuser updateftpuser vdcisconf vdcismon viewftpuser

5) Usage:



Below is a sample path to check the incoming image files updates for an FTP user RackCam:

/opt/VDCIS/ftpserver/res/home/RackCam/2017/5/18/9

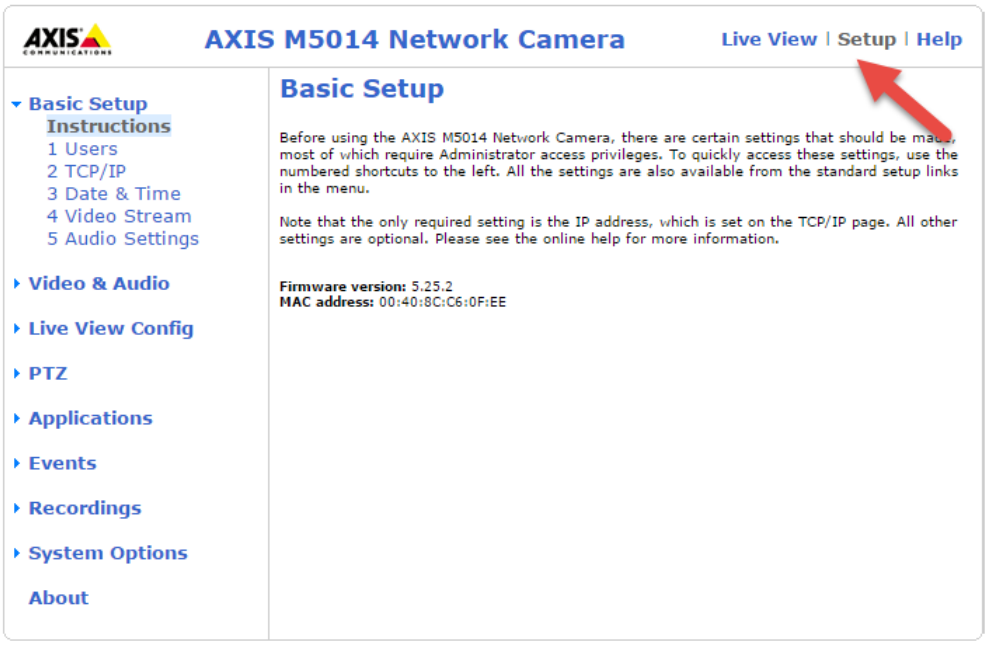
IP Camera FTP Settings

Each camera manufacturer will have a different menu item to configure and manage the FTP settings and the event triggers to deliver the images to the VDCIS server. The goal for our integration is to configure the cameras to use the FTP account created above to deliver camera images to the VDCIS system so they can be displayed in the Visual Data Center application.

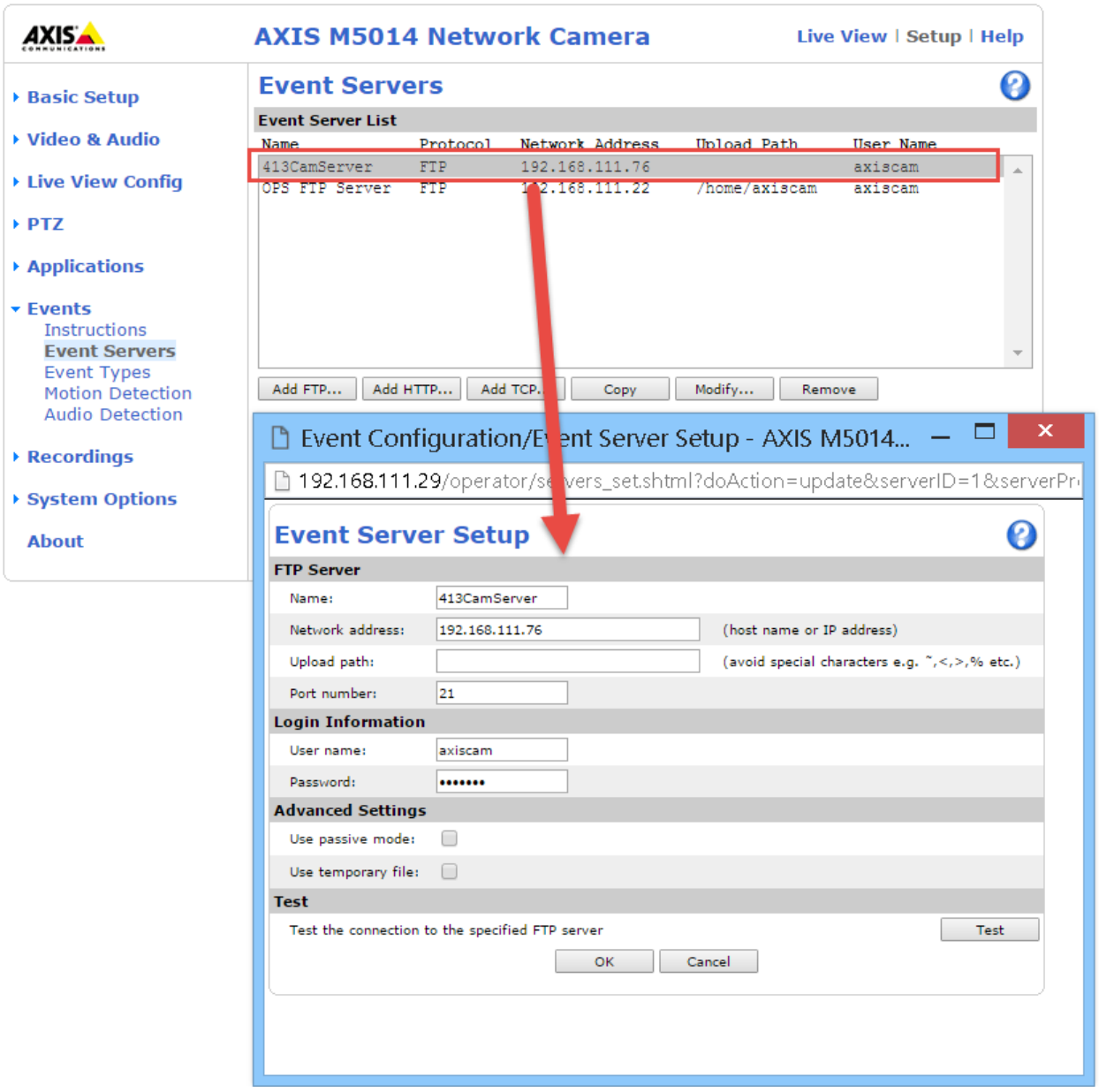
The instructions below are for an Axis IP Camera device. The general process to configure IP Cameras is similar to what is documented below, but please consult the manufacturer documentation to configure specific IP Addresses.

Configure the FTP Connection to VDCIS

- Access the web interface for the camera
- Enter the Setup configuration page for the camera



- Configure the FTP connection using the VDCIS IP Address, the VDCIS FTP Port number (default is 21) and the FTP user created on the VDCIS system for this camera.

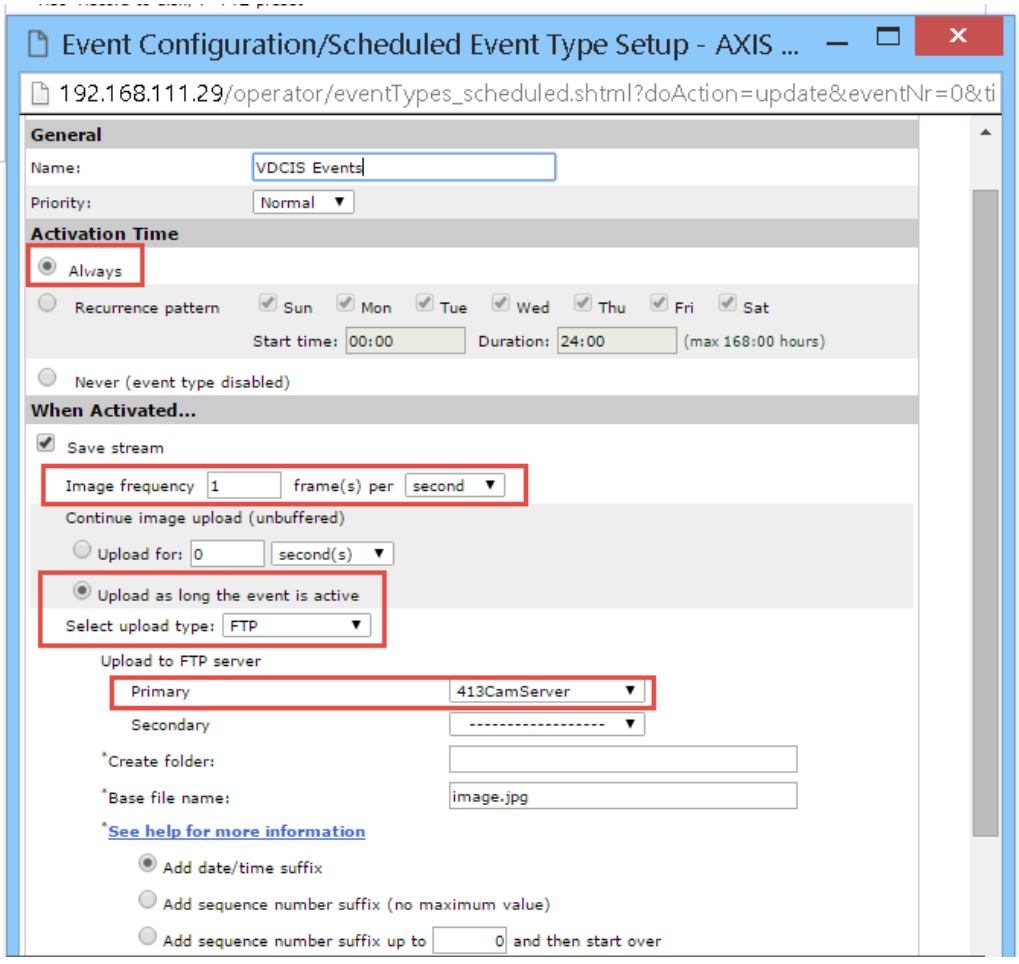


- Click the Test button to confirm the camera image can be delivered to the FTP server configured. The Test feature is a common tool used with most major IP Camera manufacturers.

Configure Event Triggers

After the FTP Connection is successfully defined an Event Trigger needs to be defined to deliver the camera images to the VDCIS FTP server. In general, we recommend events no more frequent than 1 frame per second to be sent to the VDCIS system. This frequency will help manage the bandwidth, disk space, etc of the overall architecture so there are no negative impacts of camera management to the overall system. The event shown below has these key parameters to trigger the frame capture and delivery to the VDCIS system:

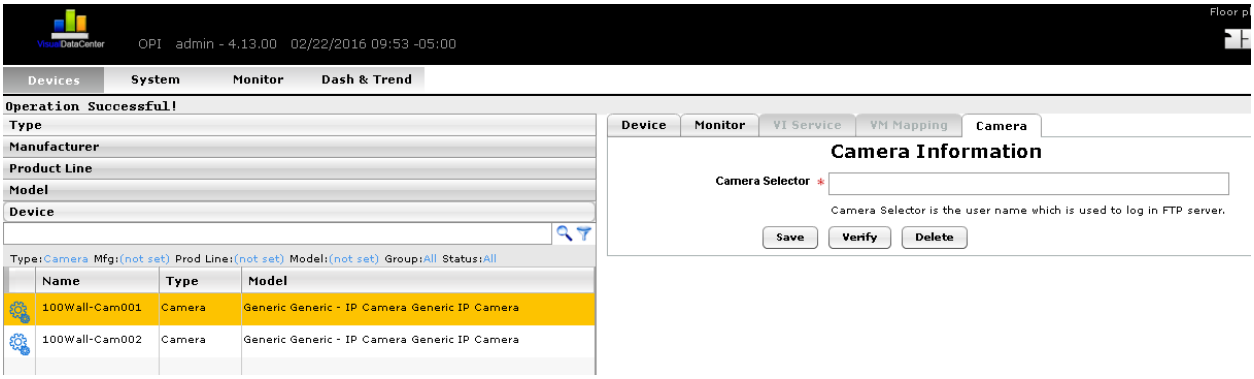
- Schedule is set to Always to allow for perpetual delivery of images to the VDCIS system
- Image Frequency is set to 1 Frame per second
- The Upload protocol is set to FTP so we can select the FTP server defined in the section above
- The Primary server is the FTP server connection defined in the section above.



Visual Data Center Camera Settings

The server and camera configurations above will result in the successful delivery of images from the FTP camera to the VDCIS server. Confirm that images are received by checking the path to the previously created ftp user as described in the " Managing VDCIS FTP Accounts" section. Next the Visual Data Center devices need to be configured to display the images stored in the VDCIS system.

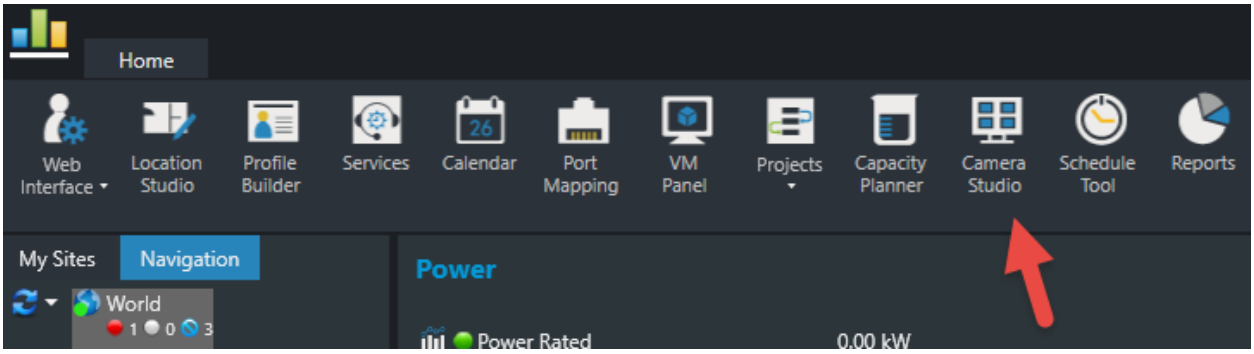
- Create a device in Visual Data Center with the Device Type = Camera. Only this device type will be enabled with the Camera settings needed to display camera images.
- In the Visual Data Center web interface, select the camera device on the Device menu.
- Select the Camera tab to define the camera information. Provide the FTP user name on the VDCIS server in the Camera Selector field.
- Click the Verify button to confirm the configuration successfully retrieves camera images from the VDCIS server.



Camera Studio 3D Client

Visual Data Center provides an interface which allows users to view camera images and configure multi-camera views for cameras created in the Visual Data Center device list. This interface is accessed by logging into the 3D Visual Data Center interface. The 3D client is available from the help tab of the 2d web interface. Insure that you have downloaded the VDC 3d client and have installed the client as per the 3D Client installation guide.

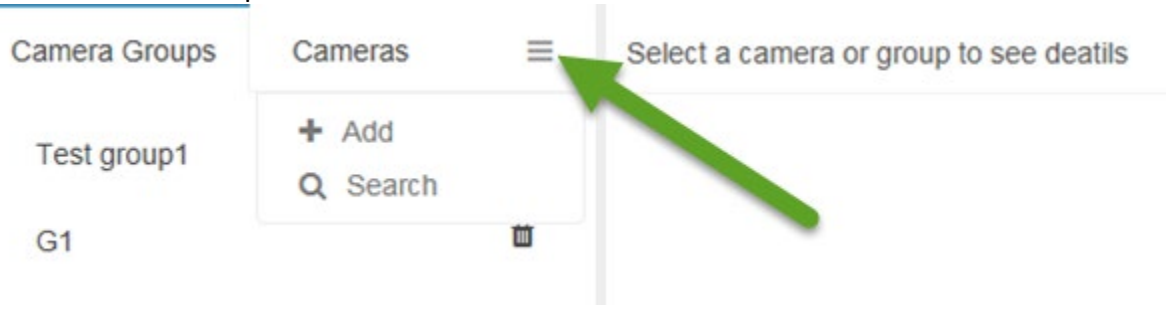
Open Camera Studio by clicking the Camera Studio icon in the main ribbon bar. Launching this interface will open a new window with dedicated functions for managing and configuring camera views.



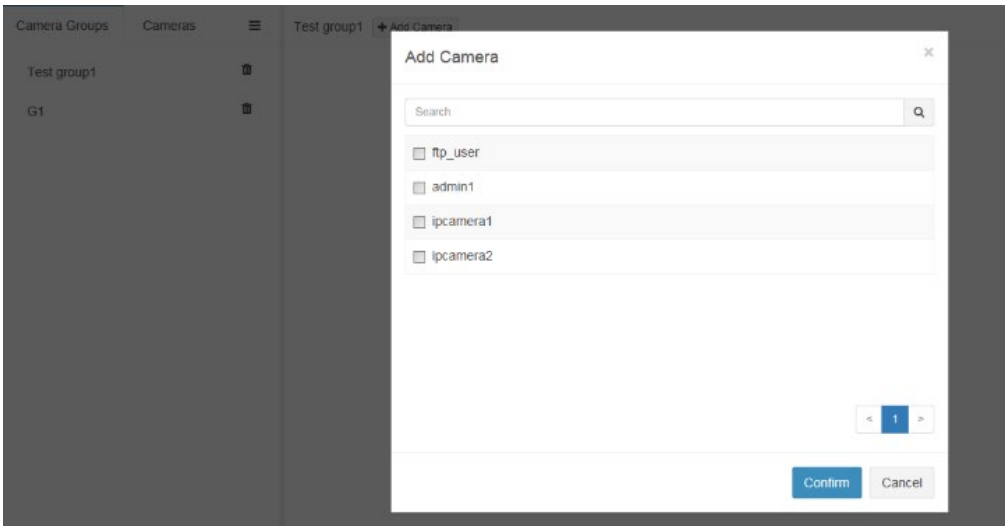
The Camera Console window allows for these functions to be performed:

The Green arrow indicates the "drop down menu" which allows the addition of a camera group.

- Create Camera Group

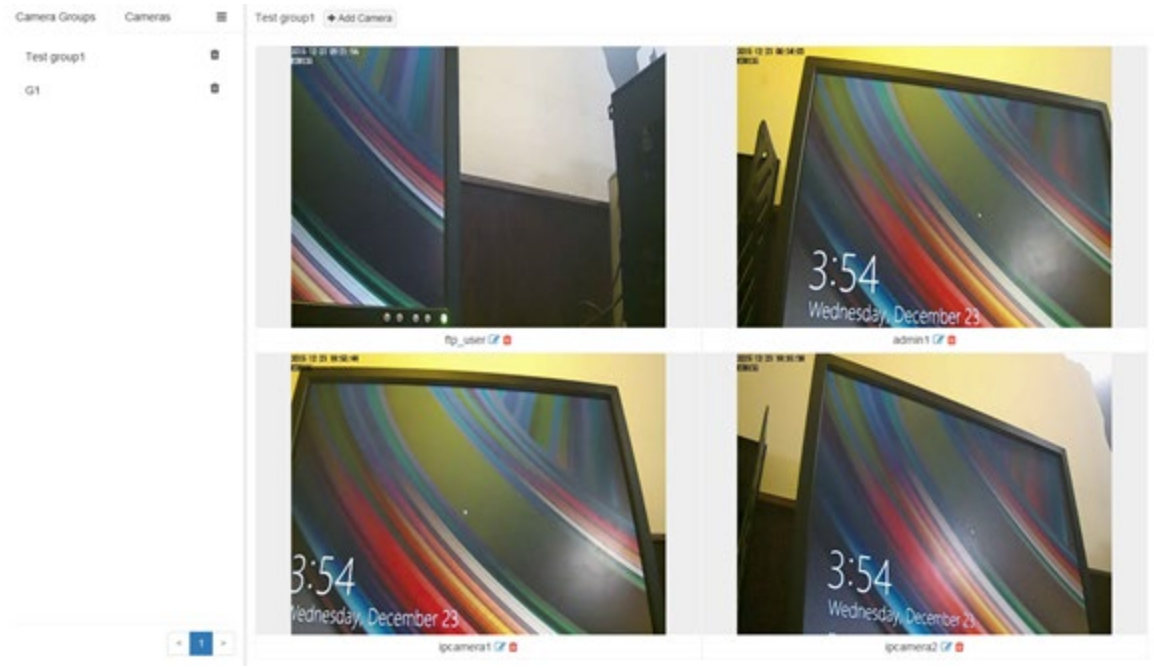


- Delete Camera Group
- Add Camera to Camera Group



- Remove Camera from Camera Group

Once the Camera Groups have been defined, selecting the Camera Group or the Camera from the list will display the real time camera images from the VDCIS server. Note, the multi-camera views are automatically configured based on the number of cameras included in the view.



Troubleshooting Camera Issues

The following notes will assist with troubleshooting efforts to resolve camera configuration problems.

- Verify the server firewall is not blocking communication from the VDCIS server to the cameras or to the VDC server.
- Images from cameras are saved into the following location on the VDCIS server. Check this location for current images to ensure the camera is successfully connecting to the FTP server and depositing images.

  /opt/VDCIS/ftpserver/res/home/{USER}/{YEAR}/{MONTH}/{DAY}/{HOUR}

- VDCIS server communicates with the IP camera via port 21. The IP Camera must be able to connect to VDCIS port 21.

  Use the following command on the VDCIS server to check if port 21 is open. LISTEN means the server is listening for a connection at this port. ESTABLISHED means a connection is established at this port. Results of this command must have LISTEN and at least 1 ESTABLISHED in the result.

  netstat -anp | grep ":21"

```
[root@vdcis-2225 bin]# netstat -anp | grep ":21"
tcp        0      0 :::21                       :::*                        LISTEN      2333/java
[root@vdcis-2225 bin]#
```

- The VDCIS server is configured to work with a single instance of Visual Data Center, but a single Visual Data Center server can support multiple VDCIS servers. The VDCIS server hosts file includes the following entry where the IP Address would be for the Visual Data Center Master Server.

  vdchost-server 192.168.111.70

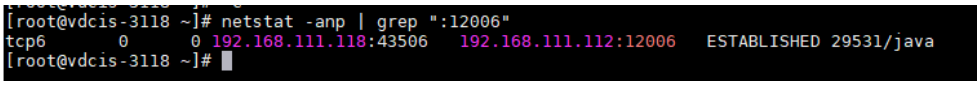
  To change the VDC server used by the VDCIS images perform the following steps:

  1. Update the vdchost-server setting in the VDCIS server hosts file to use the IP Address of the Master server for VDC.
  2. Restart the VDCIS process on the VDCIS server:
     a. /etc/init.d/vdcis stop

b. /etc.init.d.vdcis start

3. Check the connection between the VDC and VDCIS server by running the following command on the VDCIS server. The ESTABLISHED connection shows the connection is successfully made between the two servers.

   netstat -anp | grep ":12006"



- The VDCIS server communicates with the Visual Data Center server via port 12006.

Use the following command on the VDCIS server to check if it can reach the Visual Data Center server.

telnet vdchost-server 12006

Use the following command on Visual Data Center server to check if port 12006 is open. LISTEN means the server is listening for a connection at this port. ESTABLISHED with source VDCIS server means the connection with VDCIS server is established at this port.

netstat -anp | grep ":12006"

- If the FTP user commands to add, delete, update or view return error messages then make sure the FTP server is running on the VDCIS server. The vdcis process must run for the commands to run correctly:

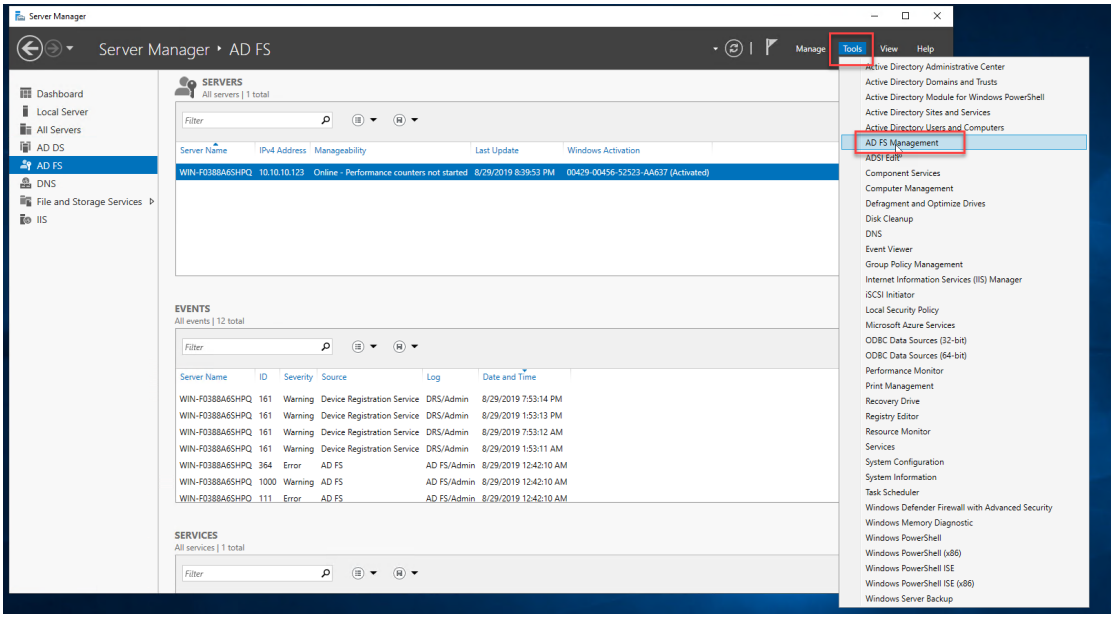
/etc/init.d/vdcis start

39 SAML

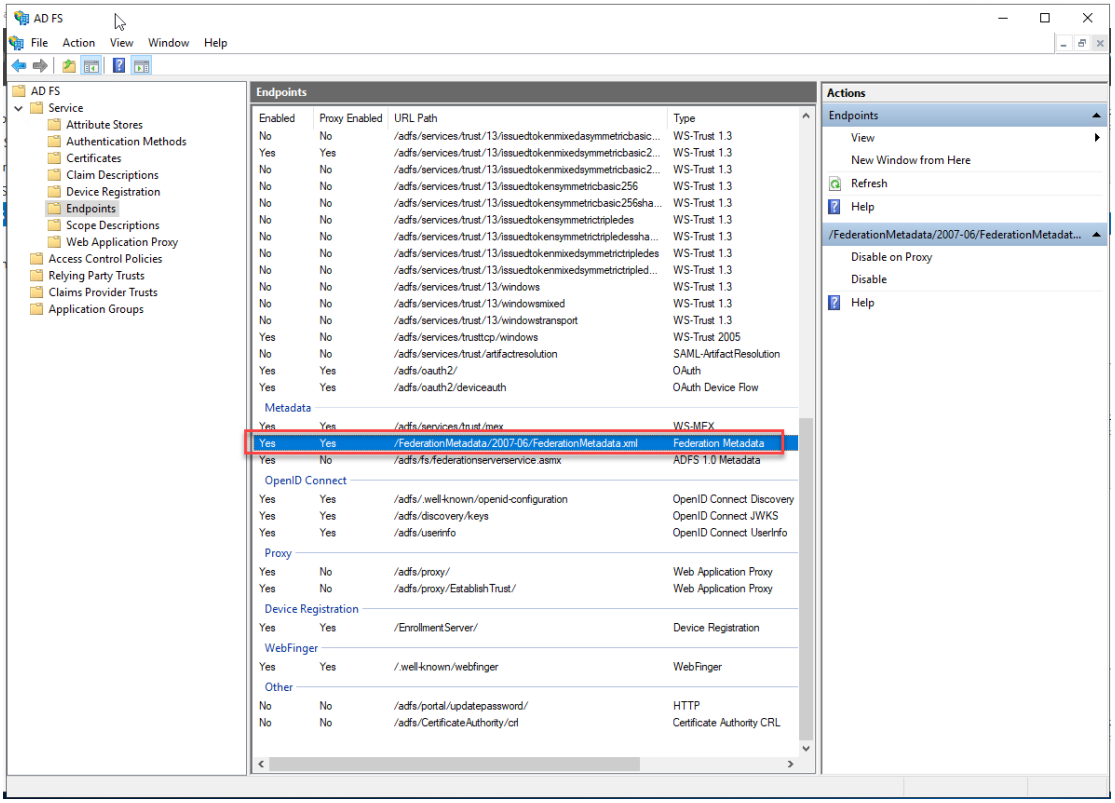
VDC 6.3.0 and above supports SAML 2.0. This document provides configuration instructions for VDC to integrate with Microsoft Active Directory Federation Services in order to provide the SAML 2.0 support. Please note that either the Microsoft Edge Browser or Microsoft IE Browser is required for SAML 2.0.

Export AD SAML2.0 Server Metadata

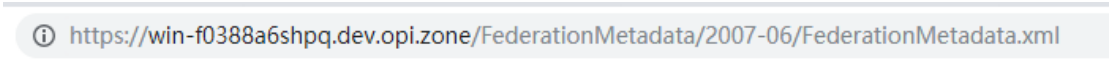
1. On AD Server, open **Server Manager -> AD FS -> Tools -> AD FS Management**



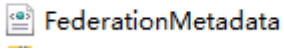
2. On AD FS window, open **AD FS -> Service -> Endpoints**, find Type "**Federation Metadata**" and copy the URL Path, make sure it is enabled

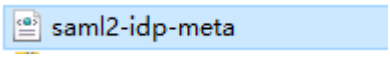


3. In a browser open the link to download the file: https://<AD_HOST>/<federation_metadata_url_path>



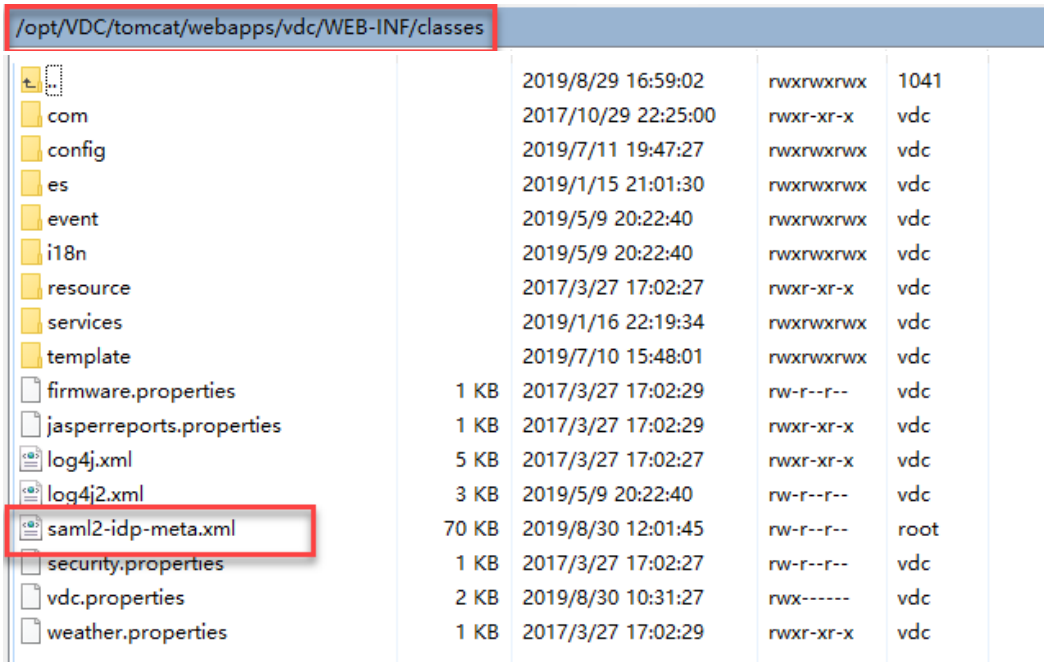
Then rename the file name to **saml2-idp-meta.xml**

a. Downloaded file: 

b. Rename file: 

Enable SAML2 Authentication for VDC Server

1. Upload the downloaded file **saml2-idp-meta.xml** on to the VDC server in **/opt/VDC/tomcat/webapps/vdc/WEB-INF/classes/**



2. When syncing IDP users to VDC, it MUST contain the following attributes
    a. NameID
    b. email
    c. phone
    d. company
    e. department
    f. memberOf

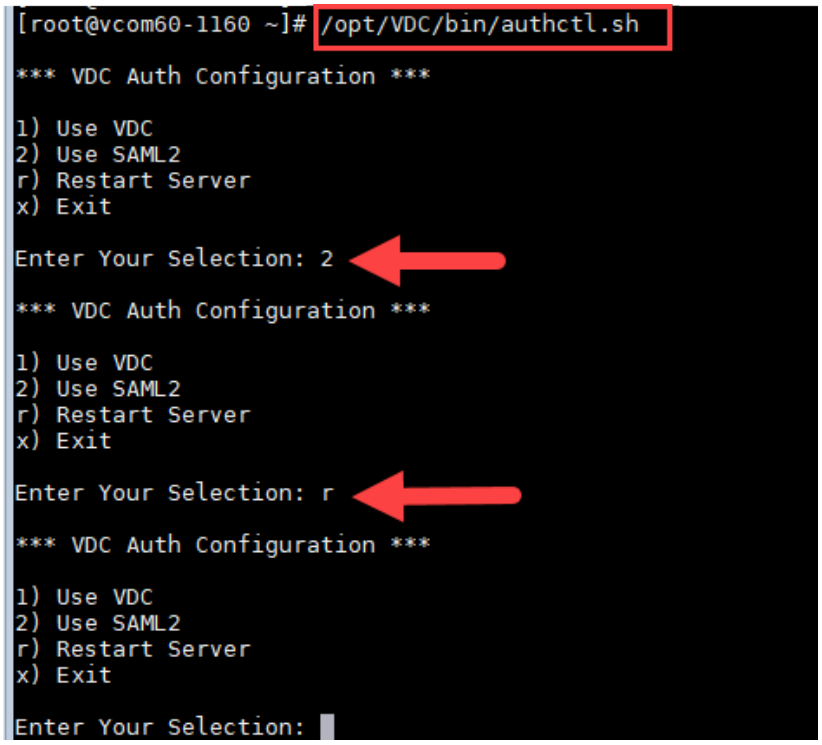
    The attribute mappings between IDP users and VDC users is as follows:

AD Server Attribute	VDC Server Attribute
NameID	User Name
email	Email
phone	Mobile
company	Company
department	Department

memberOf	User Groups

3. The relevant **companies, departments and user groups** MUST be manually created in VDC before enabling sync IDP users.
4. To enable SAML2, on the Master Server run the tool: **/opt/VDC/bin/authctl.sh**
5. Input option 2 to enable SAML2: **2**
6. Input option r to restart VDC: **r**

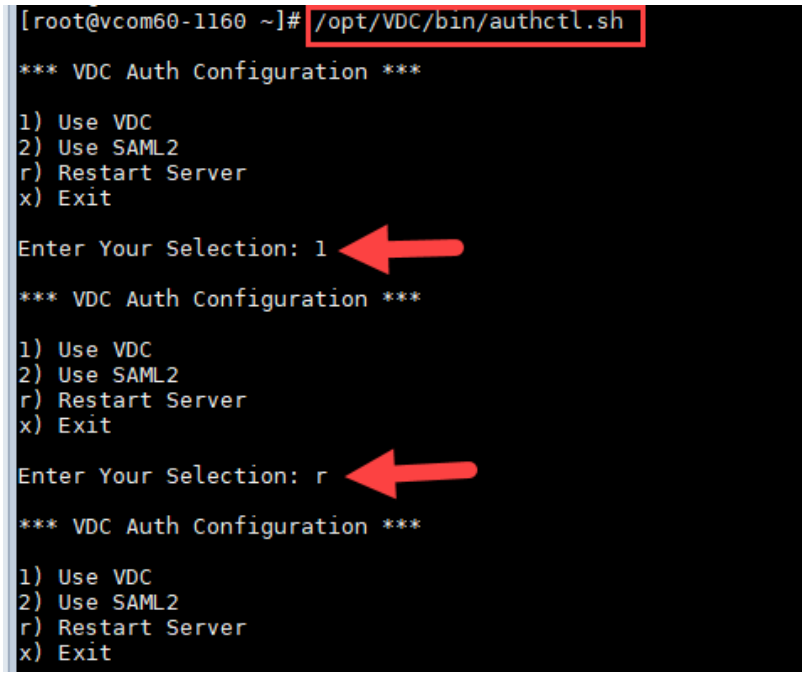
Note: It may take about 5 minutes to restart VDC



Disable SAML2 Authentication for VDC Server

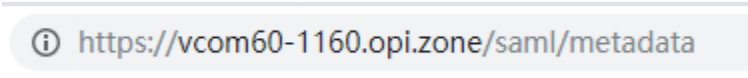
1. On the Master Server run the tool: **/opt/VDC/bin/authctl.sh**
2. Input option 1 to disable SAML2: **1**
3. Input option r to restart VDC: **r**

   Note: It may take about 5 minutes to restart VDC

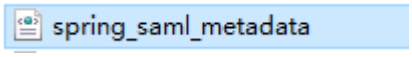


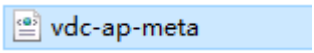
Export VDC SAML2.0 SP Metadata

1. In a browser open the link to download the file: **https://<VDC_HOST>/saml/metadata**

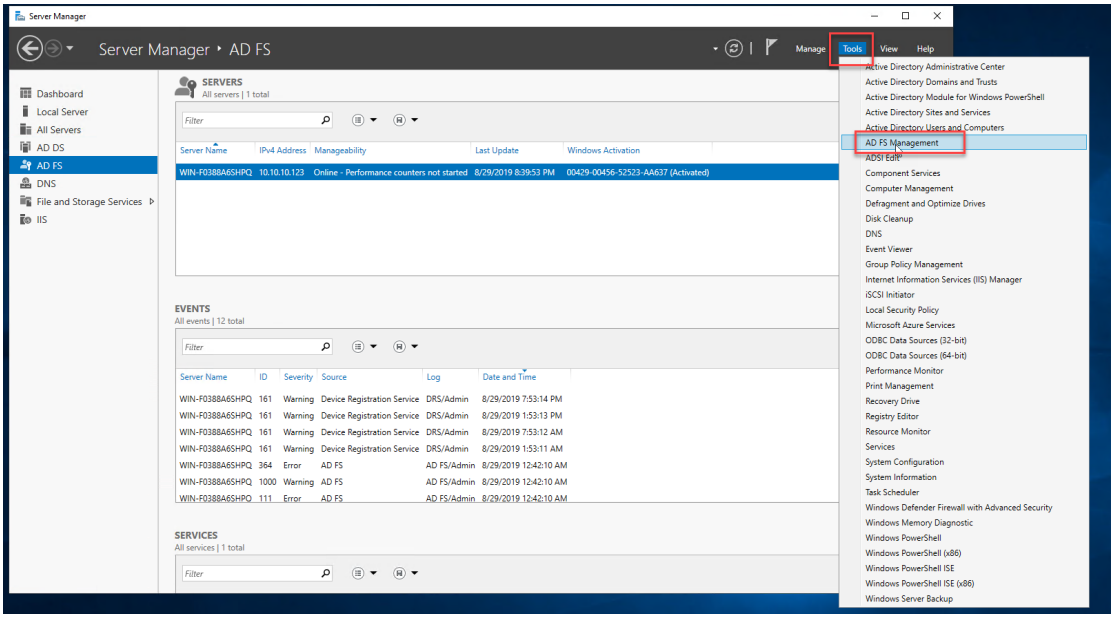
   Download the file and rename it to **vdc-ap-meta.xml**

   a. Downloaded file: 

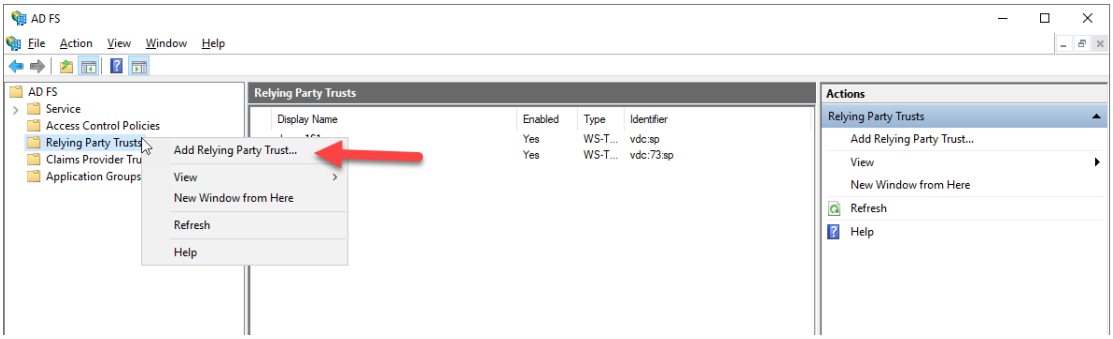
   b. Rename file: 

Configure SAML2 Server

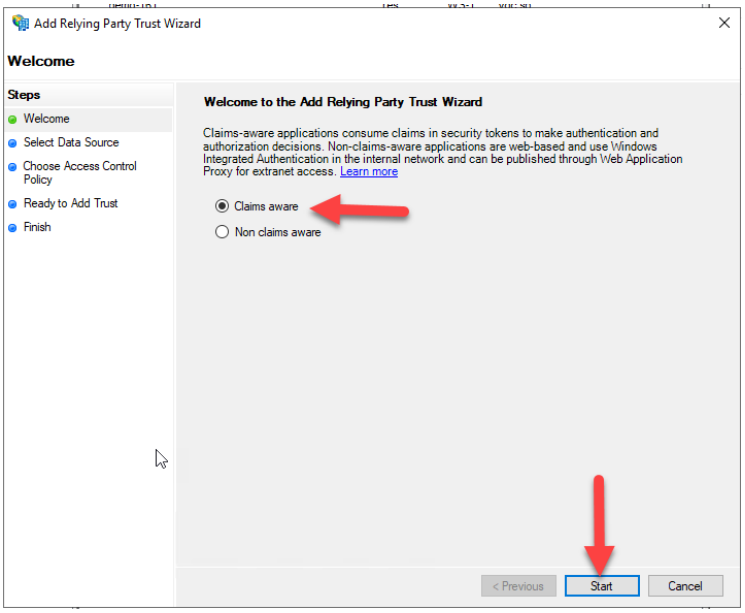
1. On AD Server, open **Server Manager -> AD FS -> Tools -> AD FS Management**



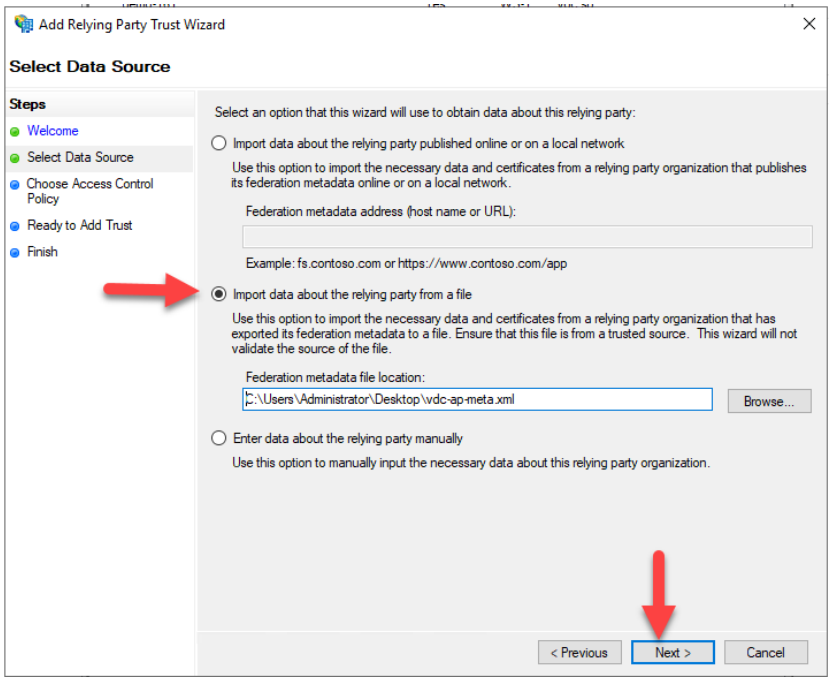
2. On AD FS window, open **AD FS -> Relying Party Trusts -> Add Relying Party Trust**



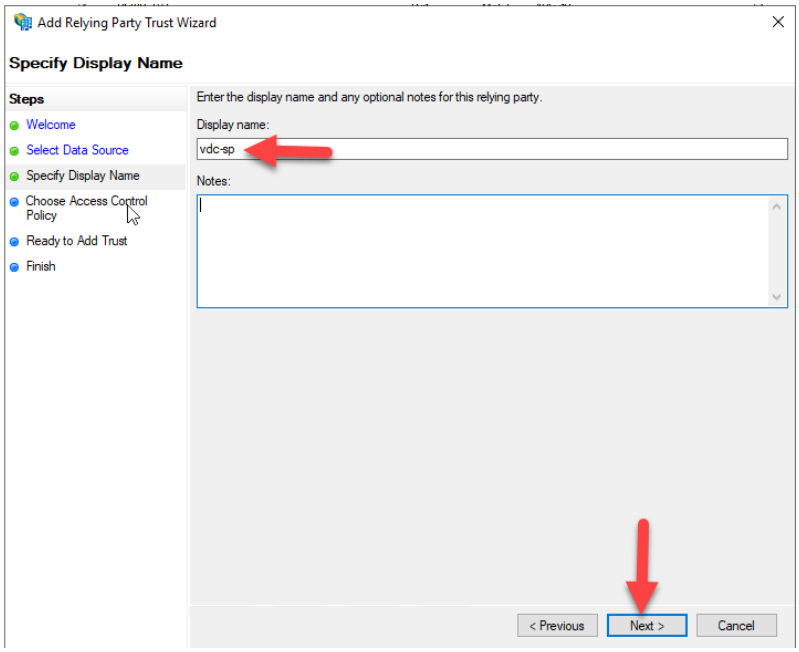
3. In the Add Relying Party Trust Wizard Welcome window, check **Claim aware** and click **Start.**



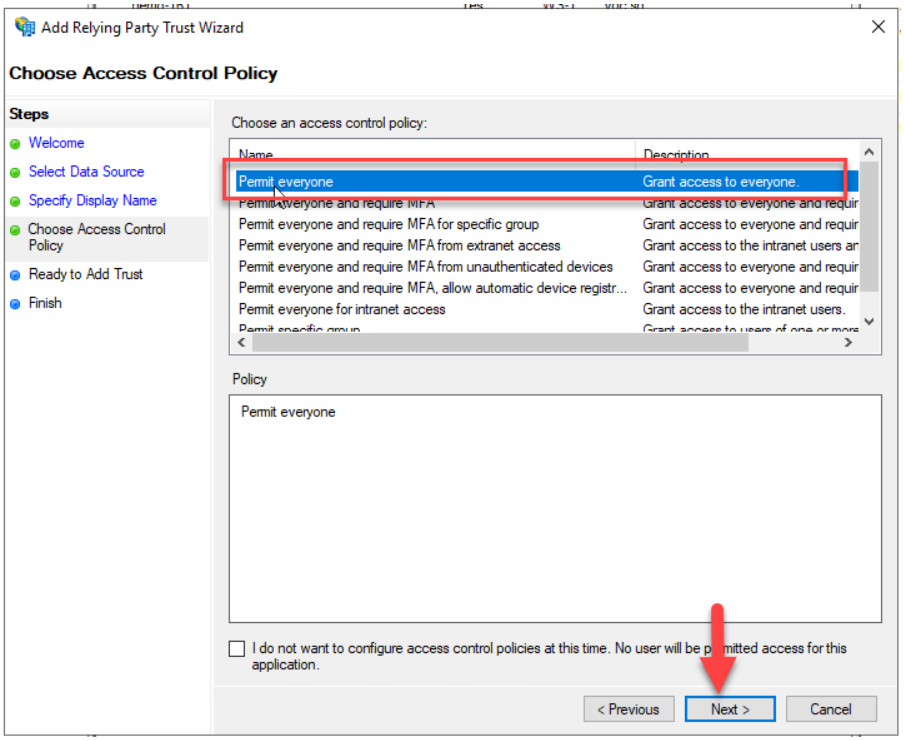
4. In the Select Data Source window, check **Import data about the relying party from a file** and **Browse** to select the file **vdc-ap-meta.xml** which was generated in the Export VDC SAML2.0 SP Metadata section and click **Next.**



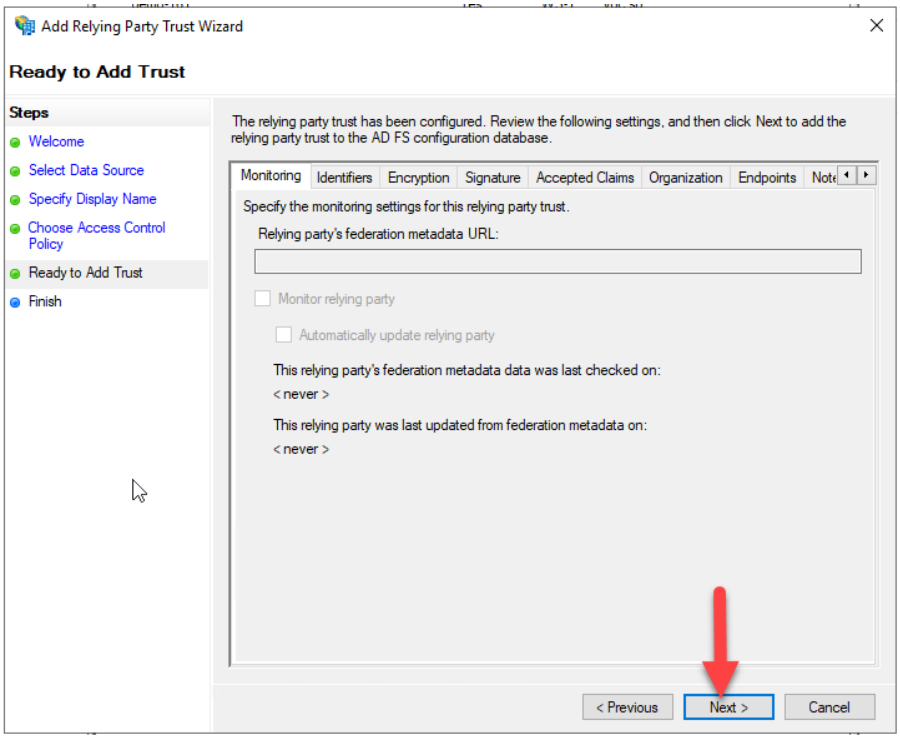
5. In the Specify Display Name window, input **vdc-sp** and click **Next**.



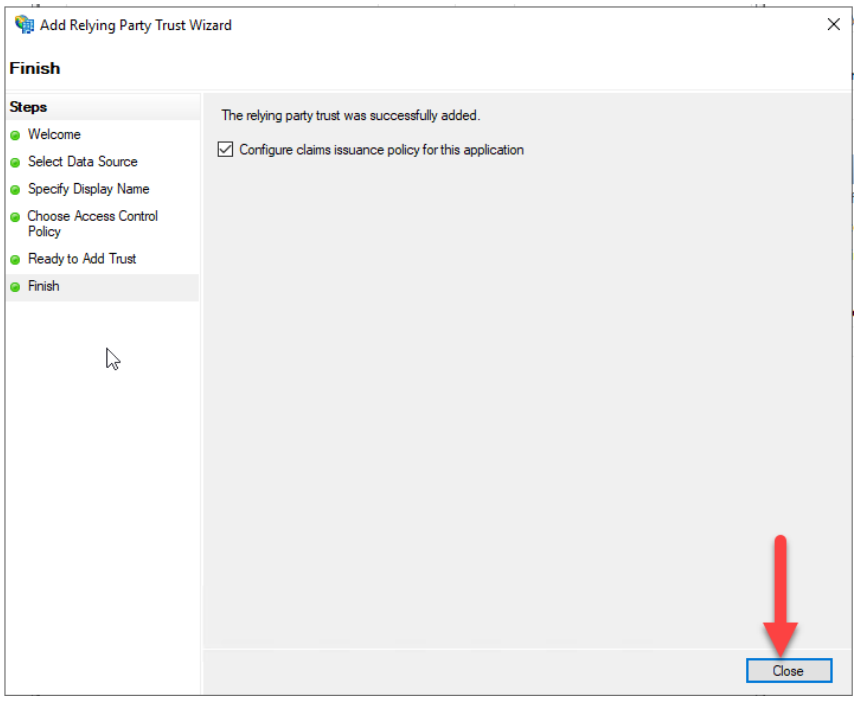
6. In the Choose Access Control Policy window, select **Permit everyone** and click **Next**.



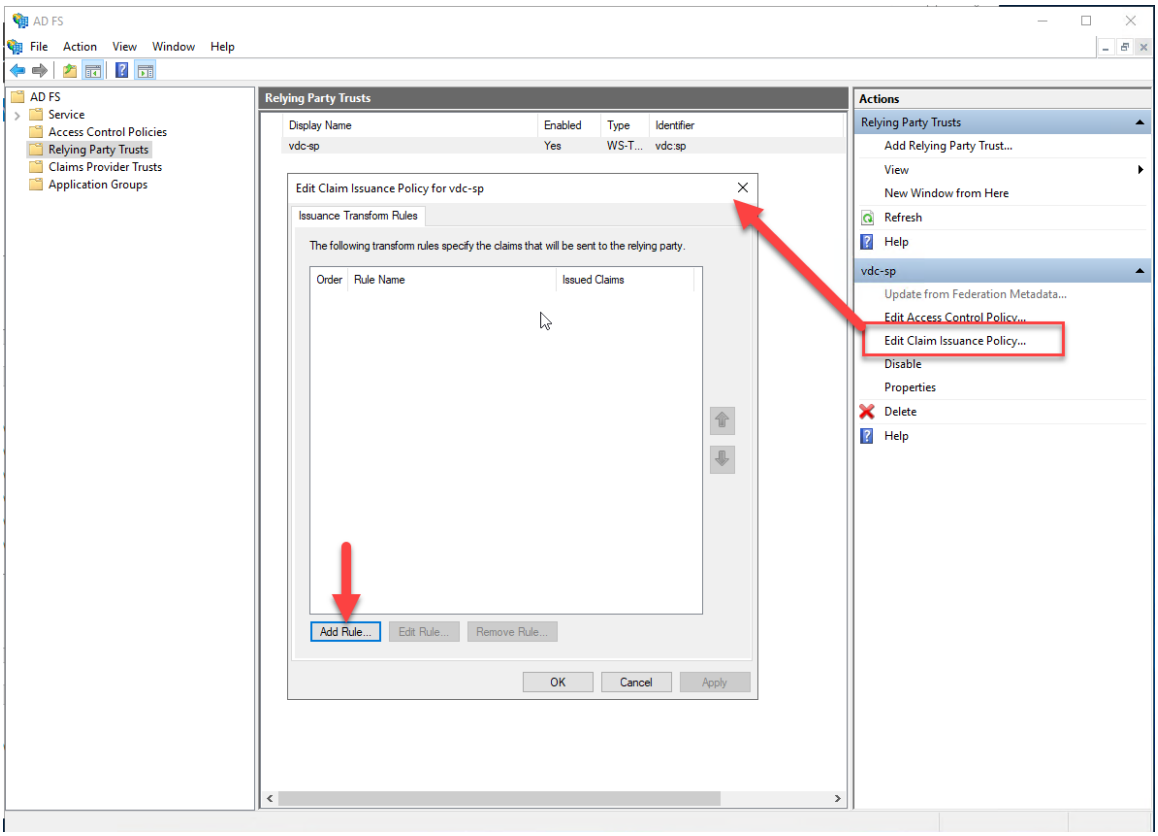
7. In the Ready to Add Trust window, click **Next**.



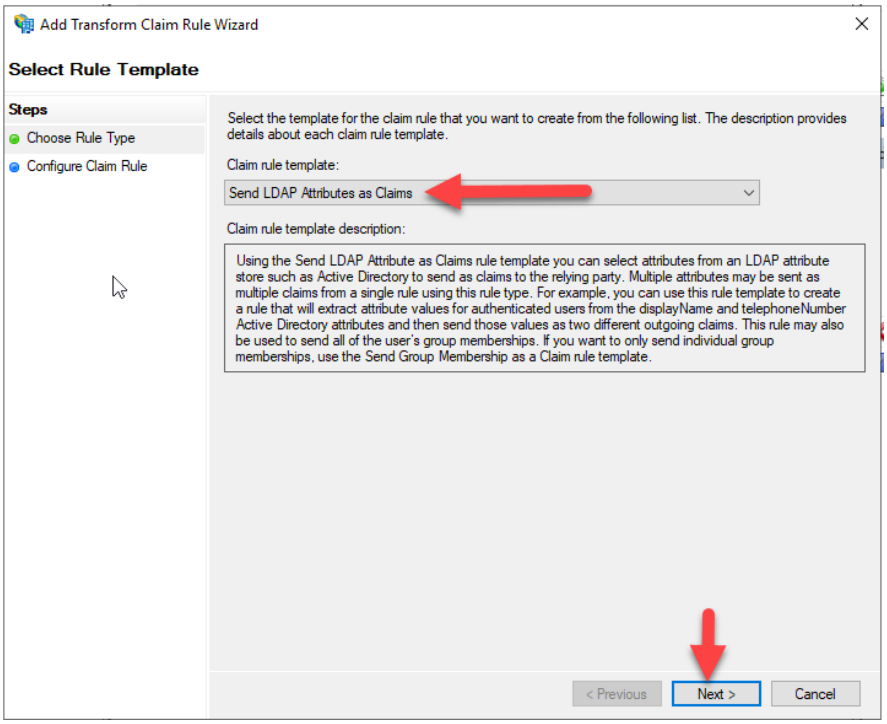
8. In the Finish window, click **Close** to complete the configuration.



9. Click on **Edit Claim Issuance Policy -> Add Rule**



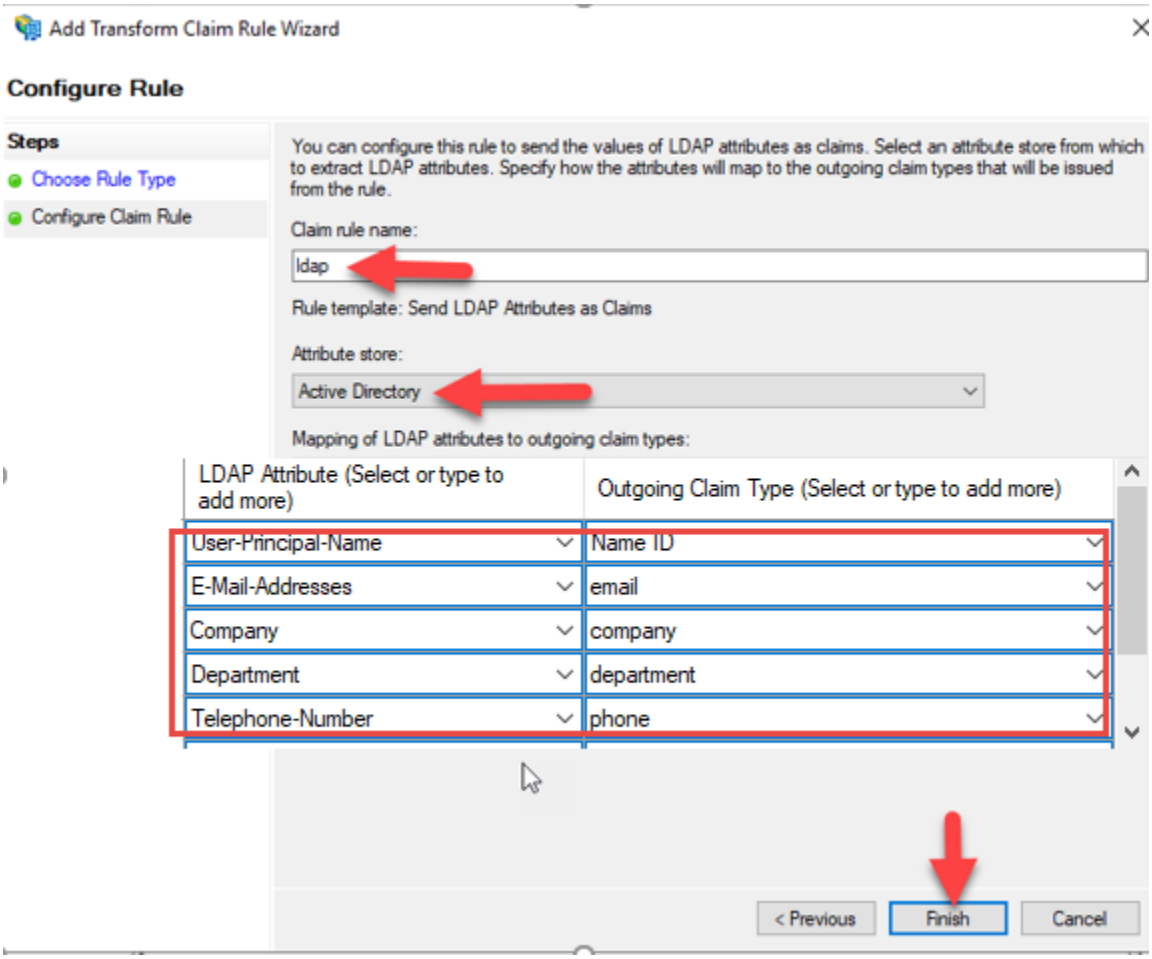
10. On the Choose Rule Type tab, select **Send LDAP Attributes as Claims** and click **Next.**



11. On Configure Claim Rule tab, input **ldap** for Claim rule name, select Attribute store -> **Active Directory**.

    Configure Mapping of LDAP attributes to outgoing claim types as follows:

LDAP Attribute	Outgoing Claim Type
User – Principal-Name	Name ID
E-Mail-Addresses	email
Company	company
Department	department
Telephone-Number	phone
Is-Member-Of-DL	memberOf



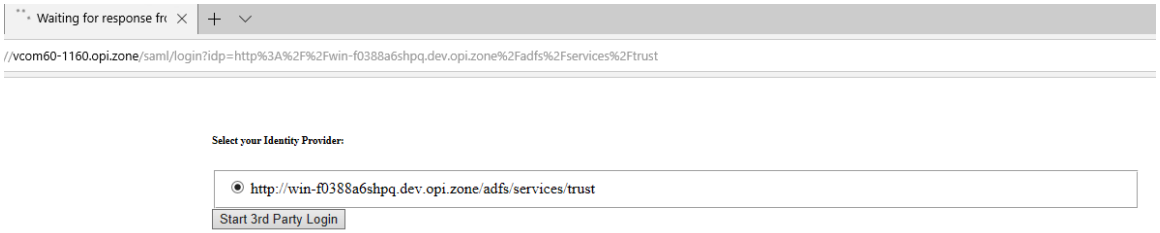
Logging In to VDC

When Visual Data Center is configured properly for SAML 2.0, it allows VDC to seamlessly integrate with the Windows authentication system. If a user successfully logs into a Windows PC using the user's Active Directory credentials with the Windows Domain name, the user will not be prompted for a user ID and password again when logging into VDC.

Note: Only Microsoft Edge and IE browsers support this feature.

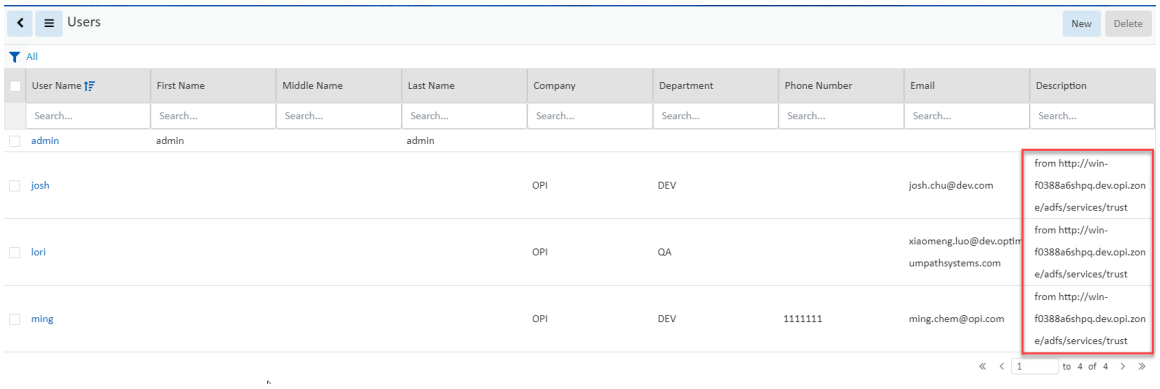
First Time VDC Login

The first time you login to the VDC web interface, it may display the following page to show you the Identity Provider. If there is only one Identity provider, it will auto skip this step and login directly.



Users Created in VDC

After the AD users login VDC, the users are auto created in VDC with descriptions of the AD server information.



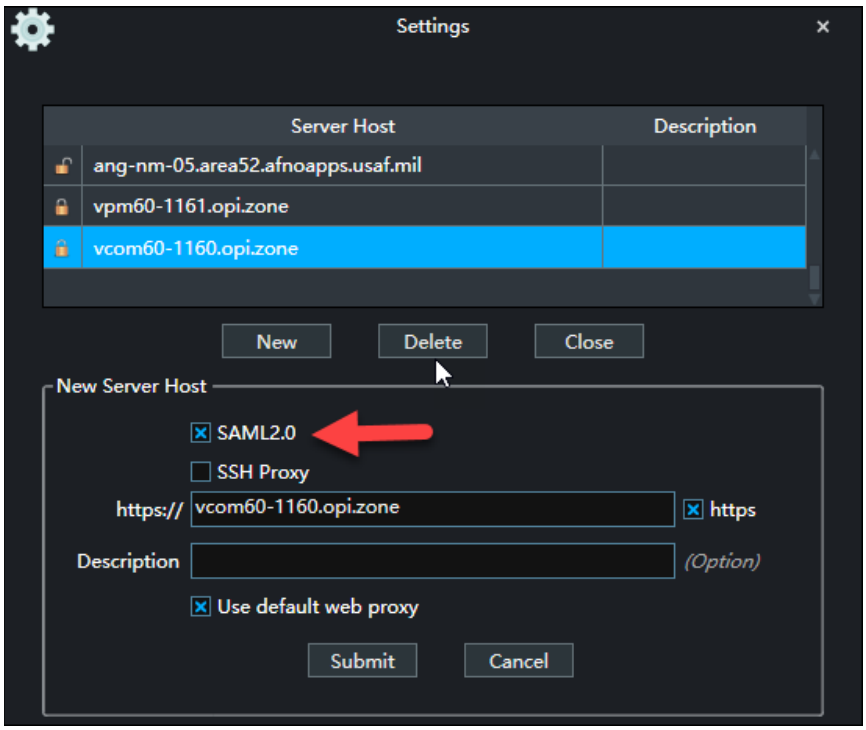
Note: The VDC user groups for the AD users are the same as the user groups on the AD server.

VDC 3D Client Login

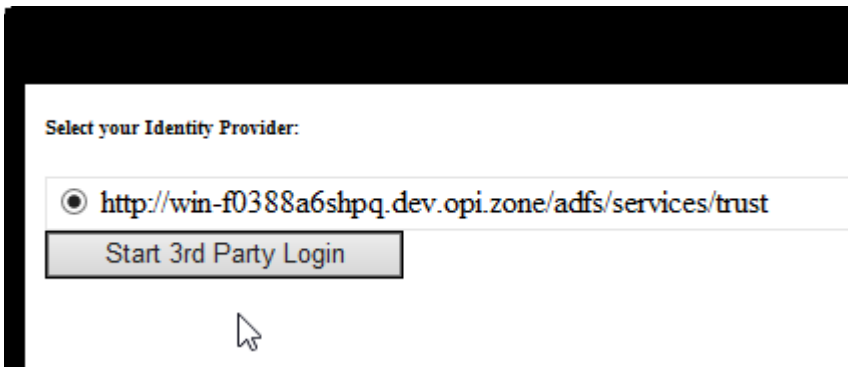
If VDC is not running on WIN10, the IE version will need to be IE11 or higher to run the 3D client.

After the 3D client is installed, users can open the 3D client file and open the Settings tool.

A new checkbox “SAML2.0” is added for SAML2.0 in 3D client Settings. Users should check it to login with the IDP user.



Login 3D client will need users to manually click the **Start 3rd Party Login** button.



If the current user is already logged into the Microsoft domain for which the SAML 2.0 integration is performed in VDC, the user will not be challenged with ID and password prompt. Otherwise, enter login credential when prompted: