Employee Handbook Webscale Cloud Host Service:

**River Web Services**

**Table of Contents**

[**Overview**](#_f8374z4mensz) **5**

[**RWS Hierarchy**](#_s8sv5m296a8p) **6**

[**Meet The RWS Team!**](#_e5r741m4fq8w) **7**

[**RWS Tributaries**](#_j439rsoeq9o6) **9**

[**Environment Orientation**](#_p4azqtld0adn) **10**

[**Open Nebula Infrastructure Notes**](#_x9kevp9btu3p) **32**

[LDAP Fix For Onboarding Customers](#_8wnhn0emlbxm) 35

[**Company Policies**](#_bmrq56x3w1hr) **36**

[**Intrusions**](#_m8e8hv7vhj4c) **39**

[Directory](#_mwbxscz2ic7m) 40

# Overview

Welcome to River Web Services, where our corporate vision is:

“River Web Services offers cloud website hosting solutions that provide businesses, nonprofits, and governmental organizations with a flexible, highly scalable, and low-cost way to deliver their websites and web applications.”

We are an innovative web service that specializes in the deployment of cloud hosted virtual machines. We are constantly seeking to attract new customers through our customized security services and flexible virtualization solutions. We are always looking to expand our base services and our competitive edge! We also provide our customers with front facing web hosting and offer web design and support services.

We are delighted that you are joining our team as our new system administration and information security team. Your role in RWS is mission critical in ensuring the uninterrupted, excellent service that we provide to our customers. River Web Services sinks or swims with you!

We look forward to your first day of work on March 24, 2017. Please review the following information in the packet to familiarize yourself with our organization, as well as your position description and duties.

During your first days here, you will be given some simple orientation tasks to help you learn about how we run our business and how you can help us keep our unparalleled, world-class uptime.

# RWS Hierarchy



# Meet The RWS Team!

**Board of Directors**

The Board is comprised of five members and the Chair, Charlotte Williams. Board members include: Joseph Bowers, Frances Yuen, Arthur Criss, Bobby Bradley, and Lilla East. This group is responsible for giving a vision to the organization’s top managers. Along with the senior personnel of RWS, the board will develop corporate strategies. Through a clearly defined vision, the board of directors, along with top professionals, develop a viable, coherent and shared understanding of the goals, objectives and policies of the organization.

**Founder and Chairman of the Board - Charlotte Williams**

The senior most position in River Corporation is that of the Founder of the company who is also the Chairman of Board, Charlotte Williams. She is not only the most respected individual in the company but also the most powerful one. All main decisions and powers lie with her.

**President and CEO - Maria Rogers**

The President is also the CEO. The main role of the president is to work on the rules and principles of the company, and make sure all decisions are being taken for the betterment of RWS.

The top level managers work closely with the CEO. They are responsible for shaping the implementation process for policies and goals formulated for corporate development at upper levels of the hierarchy. These are the personnel who draw guidance from the vision statement of the organization and define critical long-term objectives for the employees of the organization. Their responsibilities also include the critical analysis of available resources and define their role in the accomplishment of the organization objectives. The senior managers also work on the objectives that focus on profitability, market share and quality assurance, and formulate the policies to achieve these objectives. These top level managers include:

**CTO and Senior Vice President, Global** - Dorothy Irving

This position in the company is associated with handling all the technology related affairs at RWS.

**Chief Financial Officer** - David Bryan

**Senior Vice President, Legal Affairs, General Counsel** - Kenneth Spink

**Senior Vice President, Finance Department** - Odessa Hayward

**Senior Vice President, Human Resources** - Jacob King

**Senior Vice President, Corporate Communications** - Gregory Johnson

All new domain purchases go through this office

**Legal Office** - Bradley Amon

**Human Resources** - Ramona Vu

**Public Relations** - Yolanda Mundo

The next level of flow are managers and groups just like you! Their major task is to diagnose the policies, objectives and goals and translate them into specific measurable outcomes with clearly stated timeframes. The major task of middle-level managers is to recognize the development objectives pertaining to their department & area of specialization, and work in the right direction to achieve them.

**IT Supervisor** - Jose Young (was boss for previous group, but there’s been turnover)

**IT Team Lead** - ~~James Lindsay~~ **You!**

# RWS Tributaries

**What is a “Tributary”?**

A tributary is a smaller river that flows into a larger river. More information can be found here: <https://en.wikipedia.org/wiki/Tributary>

**Tributaries and RWS:**

RWS has many smaller branches that are a part of the RWS corporate hierarchy. You should think of corporate as the parent river and you belong to a branch or a tributary of the parent corporation. As such, we want you to embrace your tributary nature and refer to yourselves as “t##” where ## is the numerical designation for your specific tributary, or branch. Corporate will supply you with your numerical designation and once they do you are required to only use “t##” as an identifier.   
  
Any reference to other identifying names (such as your Alma Mater) will provoke a stern reprimand.

**Why “t##”:**

We use the “t##” designation to refer to our branches, or as we like to call them tributaries. Using this designation is not only required, but enforced on all communications channels.

**On-Premise Personnel:**

Aside from the 8 members of the IT staff at each tributary, there are Corporate Representatives. Strangely enough, every Corporate Rep at every tributary answers to the nickname “Judge”.

Only IT Staff and Corporate Representatives are allowed to be on-premise.

# Environment Orientation

**Network Overview**

Below is the network map that was left with us from our previous team after their initial handling of the environment. The map was created some time ago, so it is most likely not up to date.

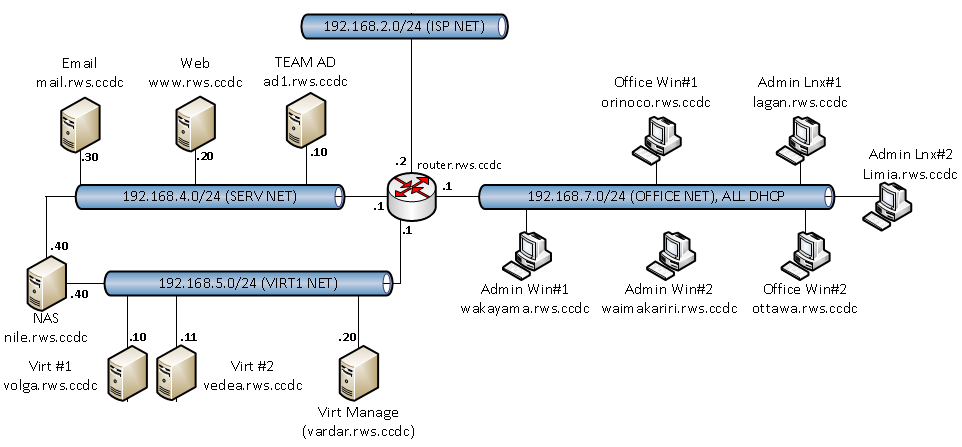


Figure 1. Network Diagram

ad1.corp.ccdc

**Credentials:** NONE - Corporate Server

Special requests to this server should be accompanied by a detailed email explaining the need and intent to: support@corp.ccdc

**Certificate Authority (CA)**

This server acts as the root CA for the environment. Any certificate requests that cannot be addressed locally can be handed off to this server for signing:

* <https://ad1.corp.ccdc/certsrv>

Teams manage their own subordinate CA, and are expected to act as a good-faith CA during the event. This means they may sign any type of request for any domain (or subdomain) that they control. Signing a certificate for a domain they do not control for public use will result in the revocation of their subordinate CA (i.e., teams will no longer be able to sign new certificates, and all existing certificates will be invalidated).

**Domain Name System (DNS)**

This server acts as the root DNS for the environment. Teams may use any of the following DNS servers:

* ad1.rws.ccdc (192.168.4.10)
* ad1.isp.ccdc (192.168.3.10)
* ad1.corp.ccdc (192.168.64.10)

It is recommended that teams use the RWS DNS first, but this is not required. **DO NOT** use a real public DNS such as 8.8.8.8 as the CCDC TLD is not a real TLD. The environment has been set up with acceptable DNS configurations, and it is **NOT** expected that teams will need to update their settings for existing hosts to achieve functionality.

Teams manage their own DNS that has been delegated RWS.CCDC, and are expected to act as a good-faith DNS during the event. This means they may create DNS records for any domain (or subdomain) that they have been delegated. Creating a new domain for public use without first purchasing it from the root DNS will result in the revocation of all domains delegated to teams (i.e., teams will no longer be able to create new DNS records and all existing DNS records for their domains will be removed).

ad1.isp.ccdc

**Credentials:** NONE - Corporate Server

This server hosts a second global DNS that teams can use. This host is primarily used for internal infrastructure resolution (e.g., beacons that track network latency and connectivity).

ad1.rws.ccdc

**OS:** Windows Server 2008 R2

**IP Address(es):** 192.168.4.10

**Credentials:** administrator / R00tp@ss

**Services:**

* DNS
* AD
* AD CS (with web enrollment)

This windows server is the primary DNS, user management, and certificate authority for tributary management.

**Domain Management**

All internal domains used for this event are from the CCDC TLD (not a real TLD). Tributaries have been delegated the **rws.ccdc** domain for use, but may purchase more domains from the CCDC TLD as is necessary. Requests for new domains can be made through a special request sent to **support@corp.ccdc**. Teams will need to establish a SOA (start of authority) for the new domain before making a purchase request.

Uptime will be awarded for keeping this service online directly through uptime checks as well as indirectly through resolution to other hosts (i.e., you can’t get uptime checks for [www.rws.ccdc](http://www.rws.ccdc) if this hostname fails to resolve). Uptime performance will be negatively affected for publicly using domains that have not been purchased (i.e., creating a domain rws2.ccdc and using it for public services without first buying the domain will result in end-users not being able to resolve the domain and teams being penalized as a result). Use of arbitrary subdomains for any domain delegated to tributaries is acceptable.

**User Management**

This AD server is primarily used for tributary user management and authentication. However, tributaries are welcome to use the AD for non-it staff authentication (i.e.., this can be used as the authentication backend for end-user accounts). Setting up and managing such authentication means is left up to the tributaries.

Uptime performance will not be directly awarded for keeping this service online. Uptime performance may be indirectly lost if this service is being used for end-user authentication, but configuration or outages affect its use.

**Certificate Authority**

Tributaries have been issued a subordinate certificate authority, which allows them to sign various certificates (e.g., certificates for web servers, emails, user authentication, etc) that will be accepted by all computers within the environment. End-users may make requests from tributaries to sign certificates, and it is up to the tributaries to determine if the request is reasonable.

Uptime will be awarded for keeping certificates valid across your entire environment, and for keeping the web enrollment (<https://ad1.rws.ccdc/certsrv>) service online and accepting requests in a reasonable timeframe. Uptime performance may be lost for not using certificates on public resources and not using valid certificates on these resources. Tributaries are expected to act as good-faith CAs, so uptime performance will also be lost for signing certificates for domains that tributaries have not been delegated (unless given permission through a special request). Repeated violation of this policy will result in revocation of the subordinate certificate authority effectively invalidating all certificates within the environment and preventing the signing of any new certificates.

beacon-X.isp.ccdc

**Credentials:** NONE - Corporate Server

Beacons are deployed on each LAN for diagnostic and troubleshooting purposes. These beacons are NOT targetable by the RED TEAM, and **may not be disabled by the by the tributaries**. They are on the network at the highest IP address on each LAN (so the .254 for each LAN in the tributary environment). The beacons perform the following checks:

* Ping to the LAN gateway
* Ping to the ISP router (192.168.2.1)
* Accessing the Team website by IP address (192.168.4.20)
* Resolving the Team website (www.rws.ccdc) using the default DNS server
* Accessing the Team website by DNS name (www.rws.ccdc)
* Accessing the Corp website by IP address (192.168.64.40)
* Resolving the Corp website (www.corp.ccdc) using the default DNS server
* Accessing the Corp website by DNS name (www.corp.ccdc)
* Accessing the Google website by IP address
* Resolving the Google website (www.google.com)
* Accessing the Google website by DNS name (www.google.com)

These checks are not used by the scoring engine, but may provide you with some insight into how your environment is operating from a variety of locations around the network.

You will not be provided with direct access to the beacon VMs, but the current and historical status of the checks performed by the beacons can be found at http://monitor.isp.ccdc/icingaweb2 using the following credentials:

Username: rwsuser

Password: radehune11

gitlab.rws.ccdc

**OS:** Ubuntu 12.04 Server

**IP Address(es):** 192.168.4.60

**Credentials:**

* root/roopass (Is this a mistake and not rootpass)?
* mgr / mgr
* root / 5iveL!fe (for gitlab service login)

**Services:**

* GitLab
* SSH

**Source Code Repository (GitLab)**

GitLab is a web-based Git repository manager with wiki and issue tracking features. Source code repositories provide companies with method of managing developer permissions, tracking issues and progress, and serves as an audit log amongst other features. It is expected that all new public facing, custom software projects or additions to existing projects will be committed to the GitLab repository as this will be one of the methods used by your bosses to ensure work is being done in a timely manner. Good commit comments are also expected.

GitLab also comes with various features for Continuous Integration (CI), which can be used for deployment into a live or production environment. It is up to you to decide what features (if any) will be useful to configure for deployments or management. For instance, you may choose to use the internal GitLab wiki or issue tracker instead of the public issue tracker for certain types of tasks. As long as the source code is accessible to your boss via the GitLab web and SSH interfaces, no other management tasks will be required.

mail.rws.ccdc

OS: Ubuntu 12.04 Server x64

IP Address(es): 192.168.4.30

**Credentials:** mgr / mgr

**Services:**

* Postfix (SMTP)
* Dovecot (IMAP)
* Roundcube (Webmail)

This is the tributary mail server. It has local authentication, and your teammates have not yet been given accounts. The server uses postfix and dovecot to send and receive messages. It signs its own certificates. There are a handful of administrative virtual accounts:

|  |  |
| --- | --- |
| administrator | mailpass |
| postbot | mail |
| webmaster | mail |
| support | supportpass |

Adding and deleting users from the mail server: /usr/local/sbin/adddovecotuser; /usr/local/sbin/deldovecotuser

Commands can be executed as follows:

adddovecotuser abcname@rws.ccdc

<enter password>

<repeat password>

and

deldovecotuser abcname@rws.ccdc

y (to delete all dovecot credentials)

y (to delete all related mail directories)

monitor.isp.ccdc

This host provides the current and historical status of the checks performed by the beacons, and can be accessed at http://monitor.isp.ccdc/icingaweb2 using the following credentials:

Username: rwsuser

Password: radehune11

Successful passing does not mean that the checked service is healthy. Success indicates that a monitoring system component was able to conduct a basic host health check. Success does not indicate that the service is 100% and you are still required to verify correct operation. For more information look at the beacon information above.  
  
Failure means that traffic was not able to pass through the checked network. The service is absolutely down for external machines and is a serious issue that should be rectified.

router.rws.ccdc

**OS:** pfSense v2.1.5

**IP Address(es):** 192.168.2.2 (rhine.rws.ccdc) ISP NET

192.168.4.1 SERVER NET

192.168.5.1 VIRT1 NET

192.168.6.1 VIRT2 NET

192.168.7.1 OFFICE NET

**Credentials:** admin/pfsense

**Services:**

* Web-based configuration UI

This is your edge router. It connects to the upstream ISP via the gateway 192.168.2.1. The ISP is currently routing the entire 192.168.4.0/22 netblock to this router (i.e., through 192.168.2.2, which is the WAN interface of this router).

**Note:**   
Corporate is talking about getting into PAN networking equipment. Hopefully, they will give us an option and let us use either at least for a trial basis.

rt1.isp.ccdc

**Credentials:** NONE - Corporate Server

This ISP router (which is your default gateway for the branch router, router.rws.ccdc) can be found at 192.168.2.1

thames.rws.ccdc

**OS:** Ubuntu 12.04 x64

**IP Address(es):** 192.168.4.70

**Description:** Issue tracking/ticketing system for blue team to receive and handle customer issues. Running ticketing system [osTicket](http://osticket.com/).

**Credentials:**

* System users:

|  |  |
| --- | --- |
| **Username** | **Password** |
| issuetracker | rootpass (should probably change) |
| root | rootpass |

* mysql:

|  |  |
| --- | --- |
| **Username** | **Password** |
| root | rootpass |
| osticket | osticket |

**Services:**

PHP 5.3.10

MySQL 5.5

Apache2 2.2

osTicket 1.9.12-32

mysql.rws.ccdc

**OS:** Ubuntu 12.04 Server

**IP Address(es):** 192.168.4.50

**Description:** This serves as the primary database server used by most RWS services. It is expected that users (and services) will need to access this database server remotely in order to work properly.

**Credentials:**

* mgr / mgr
* root / rootpass (MySQL)

**Services:**

* SSH
* MySQL

nile.rws.ccdc

**OS:** FreeNAS 9.3

**IP Address(es):** **192.168.5.40** VIRT NET

**192.168.4.40**

**Description:** Storage host for the customer VMs and data for the virtualization infrastructure.

**Credentials:** root: rootpass

**Services:**

**Todo:**

* Config MOTD
* Email notification setting
* setup the iSCIS
* Samba
* NFS

**Troubleshooting FAQ:**

**Hanging Boot**

FreeNAS 9.X hangs on first boot, need to reboot to complete booting sequence: <https://bugs.pcbsd.org/issues/6562>

Vardar

**OS:** Ubuntu 14.04 Server 64 Bit

**IP Address(es):** 192.168.5.20/24 <VIRT1>

**Description:** Front end manager/monitor of the virtualization infrastructure

**Local Credentials:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Username** | **Password** |
| limited admin | System Administrator | administrator | rootpass |
| OpenNebula User |  | oneadmin | IgoagEitMet5 |

**OpenNebula Credentials:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Username** | **Password** |
| OpenNebula User |  | oneadmin | IgoagEitMet5 |
|  |  | administrator | rootpass |

**Services:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service Name** | **Role** | **Port** | **Version** | **Additional Doc** |
| OpenSSH server | Remote Shell Access | 22 |  |  |
| ON Sunstone GUI | Web Admin of ON | 9869 | 4.14.2-2 | [ON User Administration](https://docs.google.com/document/d/1c4x5LxGjTGyYerH_SzhYCvDXIdCZiWRYwOk6q144PsA/edit#heading=h.jsp18j8glp0p) |
| NFS | FS share of ON service | default |  |  |

**Todo:**

See about giving domain names to the new customer vmsa

<http://serverfault.com/questions/614455/linux-bridging-for-kvm>

<http://superuser.com/questions/743733/bridge-does-not-forwarding-packets-centos>

http://www.linux-kvm.org/page/Networking

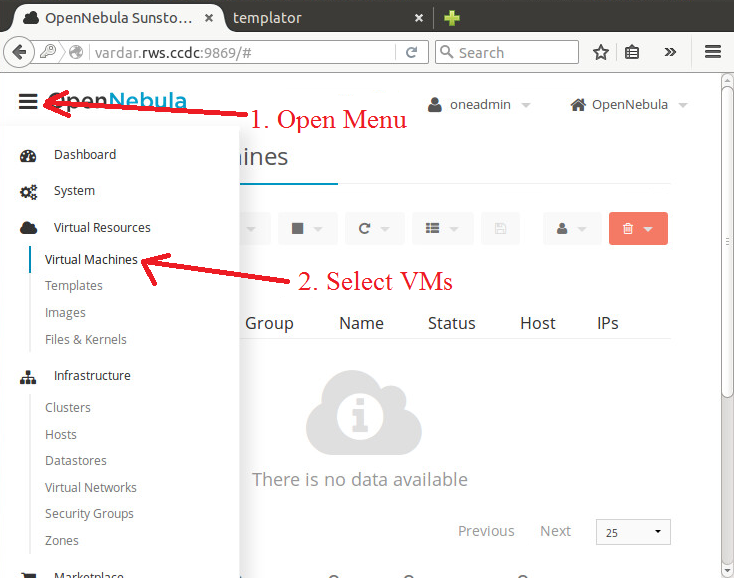
**Notes:**

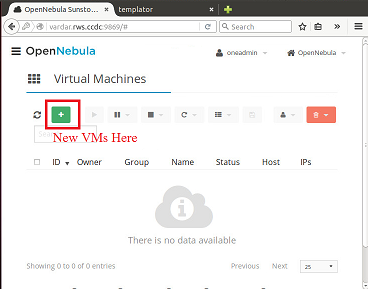
Access to Ubuntu 14.04 is through logging in as root with key id\_vm under oneadmin’s profile

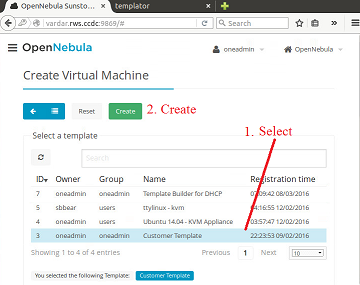
**VM Templates**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Servers** | **Disk Size (G)** | **User** | **Passwd** |
| Customer Template | LAMP, SSH | 3 | administrator | rootpass |
| Ubuntu 14.04 | SSH | 10 | root | need ssh key |

**VM Creation Process**







**Troubleshooting FAQ:**

If the NAS starts to timeout, ensure that it resolves to the 192.168.5.40 address.

**Glossary:**

**Sunstone:** Web based frontend for managing the OpenNebula Infrastructure.

**Datastores:**

* System: Images for running VMs
* Images: Disk image repository: cloned/shared out to System datastores
* Files: Special file types, used for RAM disks and kernels.

Vedea

**OS:** Ubuntu 14.04 Server 64 Bit

**IP Address(es):** 192.168.5.11 <VIRT1>

192.168.6.11 <VIRT2>

**Description:** Compute host for the OpenNebula virtualization service.

**Credentials:**

**-Local**

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | Username | Password |
| root |  | root | rootpass |
| limited admin | System Administrator | administrator | rootpass |
| OpenNebula User |  | oneadmin | IgoagEitMet5 |

**Services:**

Libvirt (/etc/libvirt/qemu.conf onadmin user&gp permissions, non-dynamic)

KVM

OpenSSH (Accepts passwordless ssh key access for oneadmin)

**Notes:**

rc.local: mounts nfs shares from vardar and nas

**Troubleshooting FAQ:**

If the NAS starts to timeout, ensure that it resolves to the 192.168.5.40 address.

Volga

**OS:** Ubuntu 14.04 Server 64 Bit

**IP Address(es):**  192.168.5.10 <VIRT1>

192.168.6.10 <VIRT2>

**Description:** Compute host for the OpenNebula virtualization service.

**Credentials:**

**-Local**

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | Username | Password |
| root |  | root | rootpass |
| limited admin | System Administrator | administrator | rootpass |
| OpenNebula User |  | oneadmin | IgoagEitMet5 |

**Services:**

Libvirt (/etc/libvirt/qemu.conf onadmin user&gp permissions, non-dynamic)

KVM

OpenSSH (Accepts passwordless ssh key access for oneadmin)

**Notes:**

rc.local: mounts nfs shares from vardar and nas

**Troubleshooting FAQ:**

If the NAS starts to timeout, ensure that it resolves to the 192.168.5.40 address.

[www.rws.ccdc](http://www.rws.ccdc) and www-dev.rws.ccdc

**OS:** Ubuntu 12.04 server

**IP Address(es):** 192.168.4.20

**Description:** Webserver for each tributary

**Credentials:**

* root/r00tpass!
* itstaff/letmein
* Django admin: jdyoung/Enzo2002

**Services:**

* Web server with static site and django creds site.

Admin Machines

**Credentials:**

**WINDOWS VMs**

* admin / admin

**UBUNTU VMs**

* mgr / mgr
* root / rootpass

Special requests to this server should be accompanied by a detailed email explaining the need and intent to: support@corp.ccdc

**Your Workstation**

As the new it team this office box will serve as your workstation throughout the competition.

Office Win 7

**Credentials:** admin / admin

Special requests to this server should be accompanied by a detailed email explaining the need and intent to: support@corp.ccdc

**Your Workstation**

This is a workstation that is used by RWS employees. IT Staff may use it while there is no other need by any other RWS employee.

# Open Nebula Infrastructure Notes

As you may know, we are in the business of providing an unparalleled service of Infrastructure as a Service (IAAS). Given that we have seen a recent competitor suffer a serious outage, we have boosted our ad campaigns to make the most of the situation. Let’s not fall into the same mistakes they have! To be sure there is room for improvement, the previous team’s contract came up before we could flush all the rough edges out of the service. But that is why you are here! Just be sure to pass up any changes to the systems for approval, we don’t want to be suffering the same issue that our competitors underwent!

Virtual stack to host customer VMs. Two hosts and a management server.

Email Server - RWS employees and Customer Email

WWW - website, production and development

Issue Tracking - Support ticket website tracking, handling, and support

Customer Credential Server

Service Start Order

There were a number of quirks in the systems that the old team put together that they did not have time to fix before the end of their contracts. The listings below is the only documentations that we have in addressing the issues.

**Virtualization Stack Service Dependence**

One the issues is that the virtualization stack need to be brought up online in a specific order. Is is illustrated in Figure 2 below. The virtualization stack requires two services to be running: DNS and NFS.

DNS is required for the stack to find the resources on the network, if DNS is down we are all going to have a bad day.

Our FreeNAS host provides NFS. All the OpenNebula hosts attempt to mount that drive during their boot as all ISOs, virtual hard disks, and metadata of the customer virtual machines resides there. There are a number of different solutions supported by the software stack, but this is what the previous team could get spun up. There is also a NFS share that comes from the manager that gives the running customer VMs information to the nodes. See figure 3 for illustration.



Figure 2. Virtual Stack Dependency Boot Order

Hosts nile.rws.ccdc and ad1.rws.ccdc must be in fully serviceable state before the remaining OpenNebula stack can be booted without manual intervention. Best to bring up the NFS datastore and then reboot the OpenNebula hosts. Figure 3 below shows the NFS dependency between the different hosts.

## 

Figure 3: OpenNebula Stack NFS Dependency

**Virt Stack Trust Relations**

Looking at the services between the management interface and the virtualization nodes, it appears that there is an absolute trust for the managing host to deploy and modify VMs. Utmost care should be taken when it comes time for upgrading or making changes to this infrastructure. The OpenNebula framework requires SSH access from the manager host to the nodes for the to login and manage the hosts. There is a trusted SSH key that facilitates this connection.

#### 

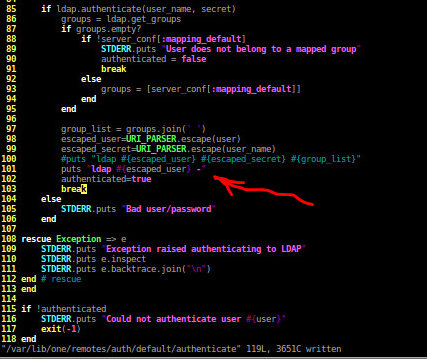
#### 

#### 

#### 

#### **LDAP Fix For Onboarding Customers**

During setup, there was a [fix for script](https://www.mail-archive.com/users@lists.opennebula.org/msg11831.html)  required to get the management server to hook into the active directory. Figure 4 illustrates the required update. Hooking into the AD is for the registration process for customers. Can’t very well have a IAAS without giving people access to manage their hosts!



# Company Policies

**Password Policy**

IT personnel talk ad nauseum about “having good passwords”. At RWS our customers want passwords that work. Our IT staff will set a password policy, but user passwords will not be changed without informing the user. A user should not have to contact us to access their services. Users include customers, corporate, and local staff personnel.

IT Staff will reset user’s passwords at the user’s request which may come through our Help phone number, email, or the ticket system. IT Staff can contact a user through these means:

Phone- If the user is locked out of their email

Work Emails- If the issue is not email related

Personal Email- Request to reset work emails are not uncommon from users emails.

If you are unsure about whether or not to reset that password you can always contact the person's supervisor or the client company’s owner. IT Staff is in charge of all non-user passwords and these may be changed as the IT Staff sees fit. IT Staff can use the passwords in the infrastructure notes, but if they change a password they should call themselves to reset it.

At the end of this handbook is a RWS directory with contact information for every user.

**User Support Policy**

In addition to user password management, IT Staff is also in charge with user tech support. RWS employees should be assisted extensively as their success is our success. Customers need to be able to access their paid services and should be assisted in common tasks. More complicated customer questions can be answered by providing the customer with online tutorials or guides. Most importantly, every user should be handled patiently and with the high quality customer support RWS is world renown for.

The I.T. employees are not the only people RWS employs. Do not be surprised if you see some office machines moving when you sign on to do maintenance. It could be anyone from corporate to RWS sales staff. It is worth noting since sales staff make the company money and you cost the company money that they will be given priority on the machines should a conflict arise. Other RWS employees are given priority on the office machines, that’s why you have admin boxes.

At the end of this handbook is a list of our customers and employees.

**Server Access Policy**

Corporate has decided to try out an experimental IoT lock this year to provide a physical barrier to our undisclosed remote server facility (codename Watershed).

The IoT lock is called “Really Secure Lock”. This system employs advanced encryption, and, as we understand it, is really secure. Authorized users have a 5 digit pin number to access Watershed.

IT staff is responsible for providing access to Watershed authorized personnel by entering access codes when asked to. Once entered, the system will remotely unlock the facility. IT staff will also be responsible for keeping unauthorized personnel from accessing Watershed.

IT staff will be expected to provide access codes to new employees as well as assisting employees having issues with their access codes (for example, an employee needing to reset a forgotten access code). Occasionally, there will be third party vendors that will need to be given temporary access to Watershed. IT staff is tasked with providing these codes.

If there are any unauthorized access Watershed, or attempts to access, IT staff is expected to dial 119 and contact RWS security immediately.

To login to reallysecurelock.com, tributaries will use their tributary name (tXX) as their username. Passwords to this account will be given to you by your supervisor.

**ISP Tech Support Policy**

Occasionally we have had issues with our ISP, however these are few and far between. They have also recently finished a compliance service check and have confirmed everything is working. IT Staff can contact the ISP tech support if they believe a network issue is not internal. However, ISP Tech Support is very expensive and calling about internal issues will be reflected in IT Staff performance reviews. The reflection will be based upon the cost of the support requested. ISP Tech Support can offer these services of increasing cost:

Confirmation of working ISP network

Advice concerning a tech issue

Remote Tech Support

Machine Redeployment (Snapshot Management)

Other services by request (Cost to be determined by ISP)

Additionally be prepared for your tech support phone call by having the below information ready:

**Information: Example**

Tributary Name t99

Machine(s) Affected t99-orinoco-rws-ccdc

Machine(s) IP 192.168.0.0

Expected Issue “The ISP DNS server is down”

Reasoning “Internal DNS resolves, external does not”

Confirmation by “Confirmed by doing nslookup on 5 different

Machines: admin, office, ad1, www, and volga”

The number for ISP Tech Support is 9001. If your phone system is down you contact ISP Tech Support via email support@virtualccdc.com. As a last resort, if all other methods have failed, you may have your Corporate Rep contact the ISP. They have asked that you call them “Judge”. “Judge” will then contact the ISP and will relay the issue or connect you with tech support at their discretion.

**Inject Submission Policy**

There is a prefered inject submission method: Use your rws email and reply to the corporate address that sent you the email. All injects should CC: corp@corp.ccdc on every email that is sent over the RWS email channel. This will be the primary channel for corporate to communicate business tasks with you.

We do however know that sometimes our internal email service may go down. All corporate employees will send a copy of all injects over the EXTERNAL GMAIL email accounts that were provided to every tributary. However, logging out of corporate email, into gmail, rewriting the email, and adding all tributaries emails takes a long time and you should expect a delay on injects sent on this EXTERNAL service. You may respond to all injects via

# Intrusions

**Intrusions Policy**

If you have determined through internal investigation that our systems have been breached please type up a report and send it to report@virtualccdc.com

Reports should include a detailed timeline of observed events of the attack (either from observing from real time or correlating from logs), hashes of any malware (i.e. backdoors) found, description of affected services, and a list of any of our IPs that can be attributed to the attack. Below is the format that you should use.

**Intrusion Report Format and Required Information**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Time |  | Tributary (Team) |
| Type of Incident |  |  |  |
| Affected Users |  |  | Affected Machines |
| Description |  |  |  |
| Details |  |  |  |
| Response |  |  |  |

## 

## 

## Directory

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **First** | **Last** | **Title** | **Phone Number** | **Key Code** |  |
| Charlotte | Williams | Founder and Chair of the Board | 3665 | 14213 |  |
| Joseph | Bowers | Secretary To The Founder | 3060 | 42214 |  |
| Frances | Yuen | Board Member | 3471 |  |  |
| Arthur | Criss | Board Member | 3448 |  |  |
| Bobby | Bradley | Board Member | 3258 |  |  |
| Lilla | East | Board Member | 3630 | 24322 |  |
| Maria | Rogers | President and CEO | 3331 | 43124 |  |
| Jimmy | Bissette | Secretary To The President | 3537 |  |  |
| Dorothy | Irving | Chief Technical Officer and Senior VP Global | 3874 | 33321 |  |
| David | Bryan | Chief Financial Officer | 3233 |  |  |
| Kenneth | Spink | Senior VP Legal Affairs, General Counsel | 3686 |  |  |
| Odessa | Hayward | Senior VP Finance Department | 3574 |  |  |
| Jacob | King | Senior VP Human Resources | 3011 |  |  |
| Gregory | Johnson | Senior VP Corporate Communications | 3342 |  |  |
| Bradley | Amon | Legal Counsel | 3494 |  |  |
| Ramona | Vu | Human Relations | 3332 |  |  |
| Yolanda | Mundo | Public Relations | 3646 |  |  |
|  |  |  |  |  |  |
| **RWS Non-IT** |  |  |  |  |  |
| Pamela | Bradford | Office machine operator | 3635 | 13312 |  |
| Jim | Potts | Computer technology trainer | 3330 | 41243 |  |
| Clara | Holeman | Judiciary interpreter | 3334 |  |  |
| Christopher | Barnes | Office machine operator | 3301 | 41311 |  |
| Matthew | Joyce | Employment consultant | 3617 |  |  |
| Tom | Jordan | Office machine operator | 3046 | 22412 |  |
| James | Vallery | Wire installer | 3292 | 32233 |  |
| Paul | Carter | Sorter | 3939 |  |  |
| Richard | Jacobs | Billing and posting clerk | 3297 |  |  |
| Henry | Stevenson | Marketing | 3299 |  |  |
| Etta | Johnson | Marketing | 3083 |  |  |
| Regina | Acosta | Commissioner | 3095 |  |  |
| Georgia | McGrath | Data Center Operator | 3002 | 21131 |  |
| Robert | Marsh | Electromechanical equipment assembler | 3565 | 31124 |  |
| Johnnie | Hernandez | Data Center Operator | 3854 | 12141 |  |
| Elizabeth | Martin | HVAC technician | 3841 | 14413 |  |
| Eric | Rice | Data Center Operator | 3611 | 11113 |  |
| Nancy | Bunn | Convention manager | 3299 |  |  |
| Emma | Murphy | Cable line installer | 3781 | 43144 |  |
| Stephen | Kindred | Market and survey researcher | 3937 |  |  |
| Irene | Shannon | Reporter | 3071 |  |  |
| Timothy | Erickson | Paper goods operator | 3638 | 31113 |  |
| Ilene | Larose | Technician | 3162 | 11214 |  |
| Joan | Crawford | Researcher | 3666 |  |  |
| Mark | Webb | Market Analyst | 3158 |  |  |
| Kala | Bernard | Custodial | 3402 | 41134 |  |
| Margaret | Kirkland | Custodial | 3359 | 42422 |  |
| Keith | Ellis | Custodial | 3619 | 44333 |  |
| Kevin | Alvarado | Security | 119 | 41332 |  |
| Blanca | Cooper | Security | 119 | 41224 |  |
|  |  |  |  |  |  |
| **RWS IT** |  |  |  |  |  |
| Jose | Young | IT Operations Manager | 3851 | 44131 |  |
| Grace | Roberts | Senior Database Administrator | 3193 | 22443 |  |
| James | Lindsay | Senior Programmer | 3876 | 31131 |  |
| Donna | Phillips | System Administrator | 3075 | 21441 |  |
| Stephanie | Shepherd | System Administrator | 3018 | 44413 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **RWS IT - Fired** |  |  |  |  |  |
| Dwight | Jung | Front End Developer | 3038 | 12244 |  |
| Cassandra | Reed | Java Developer | 3358 | 11244 |  |
| Jose | Thomas | Software Architect | 3262 | 24143 |  |
| Stacie | Bear | Programmer Analyst | 3231 | 21424 |  |
| Charles | Hankins | Network Architect | 3429 | 13221 |  |
| Patricia | Crane | Junior Software Engineer | 3066 | 13121 |  |
| Maggie | Baines | Security Specialist | 3783 | 42333 |  |
| Audrey | Smith | .NET Developer | 3022 | 33112 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **Customers** |  |  |  |  |  |
| Jeffrey | Yarbrough | Contract administrator | 4623 | 42312 | TMP 2/15 |
| Beulah | Fite | Motorboat operator | 4654 | 33141 | TMP 2/15 |
| Mary | Dale | Financial controller | 4136 | 42123 | TMP 3/25 |
| Nicholas | Johnson | Job binding worker | 4717 | 14424 | TMP 3/26 |
| Theresa | Smith | Clerk | 4930 | 21212 | TMP 1/6 |
| Natasha | Arnold | Financial consultant | 4384 |  |  |
| Deandre | Puckett | Monetary economist | 4060 |  |  |
| Lance | Stclair | Mail handler | 4803 |  |  |
| Shelby | Neill | Marshal | 4221 |  |  |
| Angela | Suiter | Securities | 4897 |  |  |
| Jennifer | Moore | Coache | 4341 |  |  |
| Helen | Santos | Maxillofacial radiologist | 4752 |  |  |
| Eve | Freeman | Surveillance agent | 4522 |  |  |
| Paul | Baum | Optical instrument assembler | 4865 |  |  |
| Louis | Corliss | Revenue agent | 4553 |  |  |
| Majorie | Navarro | Registrar | 4410 |  |  |
| Sandy | Mulligan | Real estate broker | 4627 |  |  |
| Jennifer | Evans | Multiple machine tool operator | 4552 |  |  |
| James | Griffin | Electronic newsgathering operator | 4065 |  |  |
| Joel | Counts | Bank teller | 4222 |  |  |
| Jennifer | Wood | Armed Forces | 4676 |  |  |
| Annie | Borgman | Amusement machine servicer | 4961 |  |  |
|  |  |  |  |  |  |
| **Other Numbers** |  |  |  |  |  |
| ISP | Tech Support |  | 9001 |  |  |