Puppet Enterprise

Milestone 2

Ryan Flett (S3633011)

November 16, 2016

CPT264
Unix Systems Administration

S3633011@student.rmit.edu.au
Ryan Flett

Table of Contents

/manifests/site.pp

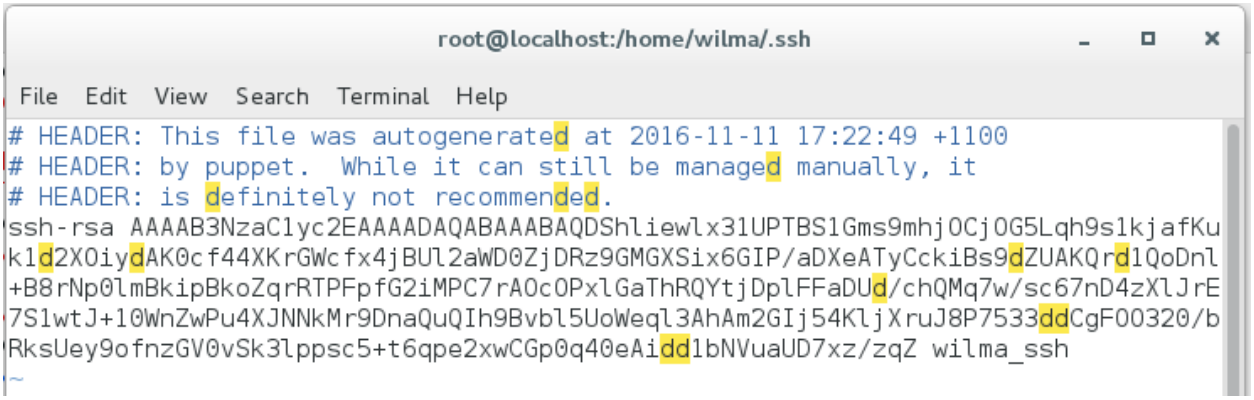
Line 40: The generate function is used to run the date command and store the date in the time variable in the format '14:40:30'.
Line 43: Send a notify message to the puppet agent that displays the time the agent was run.
Line 46: Ensure package 'ruby-augeas' is present.
Line 51-52: Include userman and sub class sshfs_setup when running the agent on the 'default' node.
Line 55: Include the puppetconf class when running the agent on the 'default' node.
Line 58-70: Include the packages and sub classes when running the agent on the 'default' node.
Line 73: Include the sysman class when running the agent on the 'default' node.

/modules/userman/manifests/

Init.pp

Line 21-38: Ensure the groups 'sysadmin', 'cars', 'trucks' and 'ambulances' are present on the system.
Line 44-56: Ensure the home directories exists for each user 'becca', 'fred', and 'wilma', and that they are directories. Each home directory requires that the user exists before it will be ensured present.
Line 62: Use augeas to add /bin/csh to the shells file in /etc/shells.
Line 69: Ensure the user 'becca' is present on the system. Her uid is 10013011, her shell is /bin/bash and her home directory must be managed at /home/becca. She is a part of the sysadmin and cars group and has a password 'test'.
Line 80: Ensure the user 'fred' is present on the system. His uid is 10023011, his shell is /bin/csh and is home directory must be managed at /home/fred. He is a part of the trucks, cars and wheel (sudo) groups and has a password 'test'. The user resource for 'fred' requires that the augeas 'etc/shells' resource has been run.
Line 92: Ensure the user 'wilma' is present on the system. Her uid is 10033011, her home directory is managed at /home/Wilma and she is a part of the trucks, cars, and ambulances group. She has a password 'test'.
Line 102: Use the ssh_authorized_key resource type to add an ssh key for the user Wilma. This key is of type rsa and the key is supplied.
Line 109: Using the file resource type ensure that the /etc/profile.d/bin.sh file exists, this file's owner and group is root and has permissions 0640. The contents of this file exports the environment PATH variable with the new directory appended to it.

```
[rflett@localhost ~]$ cat /etc/group | grep 'sysadmin\|cars\|trucks\|ambulances'
sysadmin:x:1003:becca
cars:x:1004:becca,fred,wilma
trucks:x:1006:fred,wilma
ambulances:x:1007:wilma
[rflett@localhost ~]$ cat /etc/passwd | grep 'becca\|fred\|wilma'
becca:x:10013011:1005::/home/becca:/bin/bash
fred:x:10023011:1008::/home/fred:/bin/csh
wilma:x:10033011:1009::/home/wilma:/bin/bash
[rflett@localhost ~]$ ls /home
becca  fred  rflett  wilma
[rflett@localhost ~]$ sudo cat /etc/profile.d/bin.sh
export PATH=$PATH:/usr/local/bin[rflett@localhost ~]$
[rflett@localhost ~]$ echo "$PATH"
/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/bin:/sbin:/home/rflett/.local/bin:/home/rflett/bin
[rflett@localhost ~]$
```



Sshfs_setup.pp

Line 29: Store the contents of the public rsa key file generated on titan to in a variable called titan_rsa_id_content.

Line 32: Store the contents of what will be a script in the titan_script variable. This file's contents uses sshfs to mount the remote titan directory to becca's home directory. The ssh key will be used to validate the user.

Line 35: File resource type ensures that '/home/becca/.ssh' exists because this is where the ssh key will be placed. This directory has owner and group root and permissions 0640.

Line 43: Ensure that the file titan_id.pub exists in the above directory. This file has owner and group root and permissions 0640. This resource will not be executed unless the file resource '/home/becca/.ssh' has been executed.

Line 52: Ensure that the directory where the remote mount will occur exists. This directory is /home/becca/titan and has owner and group root and permissions 0640. This directory requires that the home directory exists already.

Line 61: Ensure that the directory /etc/init.d exists and its permissions are 0755 (executable). This is where the script will be placed.

Line 67: Ensure the file /etc/init.d/titan.sh exists and that it's owner and group are root and permissions 0640. This file requires that the /etc/init.d, /home/becca/.ssh/titan_id.pub and '/home/becca/titan directories and files exists. The contents of titan.sh is the titan_script variable.

Line 77: Run the exec resource type to ensure that titan.sh script is added to the list of scripts that will run during startup. This is done by running the 'update-rc.d titan.sh defaults 3' command in the working directory /tmp. The paths required for this are /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin. This exec will only run when it receives an event as its refresh only is set to true. This exec resource requires that the titan.sh script exists.

/modules/sysman/manifests/init.pp

Line 19: Using the host resource type, ensure the entry for the ip 131.170.5.131 is mapped to titan.csit.rmit.edu.au. This entry is called 'titan', and as such this ip can be used anywhere by using the 'titan' reference.
Line 26: Using the host resource type, ensure the entry for the ip 131.170.5.132 is mapped to jupiter.csit.rmit.edu.au. This entry is called 'jupiter, and as such this ip can be used anywhere by using the 'jupiter reference.

Line 33: Using the host resource type, ensure the entry for the ip 131.170.5.135 is mapped to saturn.csit.rmit.edu.au. This entry is called 'saturn, and as such this ip can be used anywhere by using the 'saturn reference.

```
[rflett@localhost ~]$ sudo cat /etc/hosts
# HEADER: This file was autogenerated at 2016-11-15 13:29:15 +1100
# HEADER: by puppet.  While it can still be managed manually, it
# HEADER: is definitely not recommended.
127.0.0.1       localhost       localhost.localdomain localhost4 localhost4.localdomain4
::1     localhost       localhost.localdomain localhost6 localhost6.localdomain6
131.170.5.131   titan   titan.csit.rmit.edu.au
131.170.5.132   jupiter jupiter.csit.rmit.edu.au
131.170.5.135   saturn  saturn.csit.rmit.edu.au
[rflett@localhost ~]$
```

/modules/puppetconf/manifests/init.pp

Line 19: Using the augeas resource type make changes to the puppet.conf file located in /etc/puppetlabs/puppet/ such that the configuration entry 'runinterval' is set to 1200 under the 'agent' heading.

```
root@localhost
File  Edit  View  Search  Terminal  Help
[main]
    certname = localhost
    server = localhost
    user  = pe-puppet
    group = pe-puppet
    archive_files = true
    archive_file_server = localhost
    module_groups = base+pe_only


[agent]
    graph = true


runinterval=1200
[master]
node_terminus = classifier
storeconfigs = true
storeconfigs_backend = puppetdb
reports = puppetdb
certname = localhost
always_cache_features = true
```

/modules/packages/manifests/

Init.pp

Line 15: Define empty class packages. Sub classes are derived from this.

Dia2code.pp

Line 28: Store the URL to the dia2code RPM file in the rpm_url variable

Line 29: Store the package dependencies for dia2code in an array called dependencies.

Line 32: Use the package resource type to install the packages stored in the dependencies array.

Line 27: Ensure the dia2code package is installed from the RPM provider. The RPM URL is provided with the rpm_url variable and this package requires the dependencies package has been installed.

```
[rflett@localhost ~]$ dia2code
dia2code version 0.8.1, Copyright (C) 2000-2001 Javier O'Hara
Dia2Code comes with ABSOLUTELY NO WARRANTY
This is free software, and you are welcome to redistribute it
under certain conditions; read the COPYING file for details.

Usage: dia2code [-h|--help] [-d <dir>] [-nc] [-cl <classlist>]
       [-t (ada|c|cpp|idl|java|php|python|shp|sql)] [-v]
       [-l <license file>] <diagramfile>
[rflett@localhost ~]$
```

Emacs.pp

Line 18: Using the package resource type ensure that the emacs package is present on the system.

```
[root@localhost rflett]# yum list installed emacs
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.swin.edu.au
 * epel: mirror.intergrid.com.au
 * extras: ftp.swin.edu.au
 * updates: mirror.as24220.net
Installed Packages
emacs.x86_64                                        1:24.3-18.el7
```

Gcc.pp

Line 18: Using the package resource type ensure that the gcc package is present on the system.

```
[root@localhost rflett]# yum list installed gcc
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.swin.edu.au
 * epel: mirror.intergrid.com.au
 * extras: ftp.swin.edu.au
 * updates: mirror.as24220.net
Installed Packages
gcc.x86_64                                          4.8.5-4.el7
```

Httpd.pp

Line 18: Ensure the httpd package is present
Line 23: Ensure the file /etc/httpd/conf exists and is a directory with owner and group root and permission 0640. This directory requires that the httpd package has been installed.
Line 32: Ensure the httpd.conf file exists in the above directory and has owner and group root and permissions 0640. This File requires that the httpd package exists.
Line 41: Ensure that the document root directory exists with owner and group root and permissions 0640. This file requires that the httpd package is installed.
Line 50: Ensure the httpd service is running and will start on boot. This service is subscribed to the http.conf file so will restart when changes are made to this file.
Line 57: Use augeas to edit the httpd.conf file. The changes are made to the document root directive and directory in the httpd.conf file. This resource depends on the config file and the document root directory to exist.

```
#
# DocumentRoot: The directory out of which you will se
# documents. By default, all requests are taken from t
# symbolic links and aliases may be used to point to o
#
DocumentRoot "/var/www/s3633011"

#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/s3633011">
    #
```

Gdb.pp

Line 18: Using the package resource type ensure that the gdb package is present on the system.

```
[root@localhost rflett]# yum list installed gdb
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.swin.edu.au
 * epel: fedora.uberglobalmirror.com
 * extras: ftp.swin.edu.au
 * updates: mirror.as24220.net
Installed Packages
gdb.x86_64                                      7.6.1-80.el7
```

Lynx.pp

Line 18: Using the package resource type ensure that the lynx package is present on the system.

```
[root@localhost rflett]# yum list installed lynx
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.swin.edu.au
 * epel: mirror.intergrid.com.au
 * extras: ftp.swin.edu.au
 * updates: mirror.as24220.net
Installed Packages
lynx.x86_64                                  2.8.8-0.3.dev15.el7
[root@localhost rflett]#
```

Mysql.pp

Line 18: Ensure the mysql package is present on the system.
Line 23: Ensure the file /etc/mysql exists and is a directory with owner and group root and permissions 0640. This file requires that the mysql package is present.
Line 32: Ensure that the my.cnf file exists which is the configuration file for my mysql. This file must have owner and group root and permissions 0640. This file requires that the mysql package is present.

```
[root@localhost etc]# tree mysql/
mysql/
└── my.cnf

0 directories, 1 file
[root@localhost etc]# ls -l mysql/my.cnf
-rw-r-----. 1 root root 0 Nov 14 18:18 mysql/my.cnf
[root@localhost etc]#
```

Openssh.pp

Line 18: Ensure the openssl-libs package is installed. The openssh package is dependent on this being installed.
Line 23: Ensure the openssh package is present. This package requires that the openssl-libs package is present to run.
Line 29: Ensure the openssh-server package is present on the system. This package is dependent on the openssh package being present.
Line 35: Ensure the /etc/ssh/ directory exists with owner and group root and 0640 permissions. This directory requires that the ssh-server package is present.
Line 44: Ensure that the sshd_config file exists in the /etc/ssh directory with owner and group root and permissions 0640. This file requires that the openssh-server package is installed.
Line 53: Ensure the sshd service is running and that it will run on boot. The sshd service is subscribed to the sshd_config file so that if changes are made the service will restart.
Line 60: Use augeas to edit the sshd config file to disable root logins. This resource requires that the sshd_config file exists.

```
[root@localhost etc]# yum list installed openssh
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.as24220.net
 * epel: mirror.intergrid.com.au
 * extras: mirror.as24220.net
 * updates: mirror.as24220.net
Installed Packages
openssh.x86_64                                  6.6.1p1-25.el7_2
[root@localhost etc]# yum list installed openssh-server
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.swin.edu.au
 * epel: mirror.intergrid.com.au
 * extras: ftp.swin.edu.au
 * updates: mirror.as24220.net
Installed Packages
openssh-server.x86_64                           6.6.1p1-25.el7_2
[root@localhost etc]#
```

```
PermitRootLogin no
```

Tmux.pp

Line 18: Ensure the ncurses-devel package is installed.

Line 23: Ensure the glibc-static package is installed.

Line 28: Install the tmux package. This package requires that the ncurses-devel and glibc-static packages are already present to run.

```
[root@localhost etc]# yum list installed tmux
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.swin.edu.au
 * epel: mirror.intergrid.com.au
 * extras: ftp.swin.edu.au
 * updates: mirror.as24220.net
Installed Packages
tmux.x86_64                                          1.8-4.el7
[root@localhost etc]#
```

Sshfs.pp

Line 18: Store the dependencies for fuse-sshfs in an array called dependencies.

Line 21: Install the dependencies in the dependencies array.

Line 26: Ensure the fuse-sshfs package is present. This package is installed with the RPM provider from the URL supplied in the source parameter. This package requires that the fuse-libs package is installed to continue.

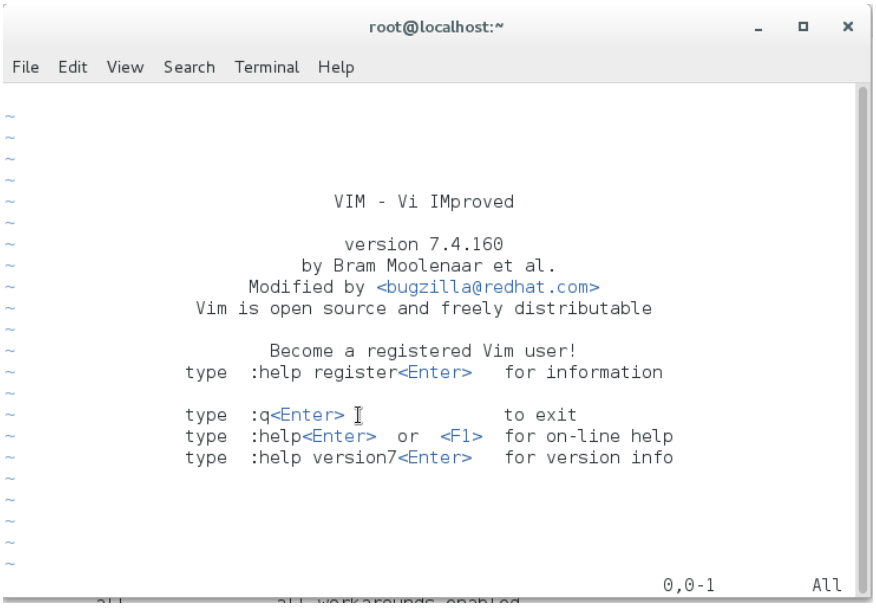
```
[root@localhost etc]# sshfs --help
usage: sshfs [user@]host:[dir] mountpoint [options]

general options:
    -o opt,[opt...]        mount options
    -h   --help            print help
    -V   --version         print version

SSHFS options:
    -p PORT                equivalent to '-o port=PORT'
    -C                     equivalent to '-o compression=yes'
    -F ssh_configfile      specifies alternative ssh configuration file
    -1                     equivalent to '-o ssh_protocol=1'
    -o reconnect           reconnect to server
    -o delay_connect       delay connection to server
    -o sshfs_sync          synchronous writes
    -o no_readahead        synchronous reads (no speculative readahead)
    -o sync_readdir        synchronous readdir
    -o sshfs_debug         print some debugging information
    -o cache=BOOL          enable caching {yes,no} (default: yes)
    -o cache_timeout=N     sets timeout for caches in seconds (default: 20)
    -o cache_X_timeout=N   sets timeout for {stat,dir,link} cache
    -o workaround=LIST     colon separated list of workarounds
```

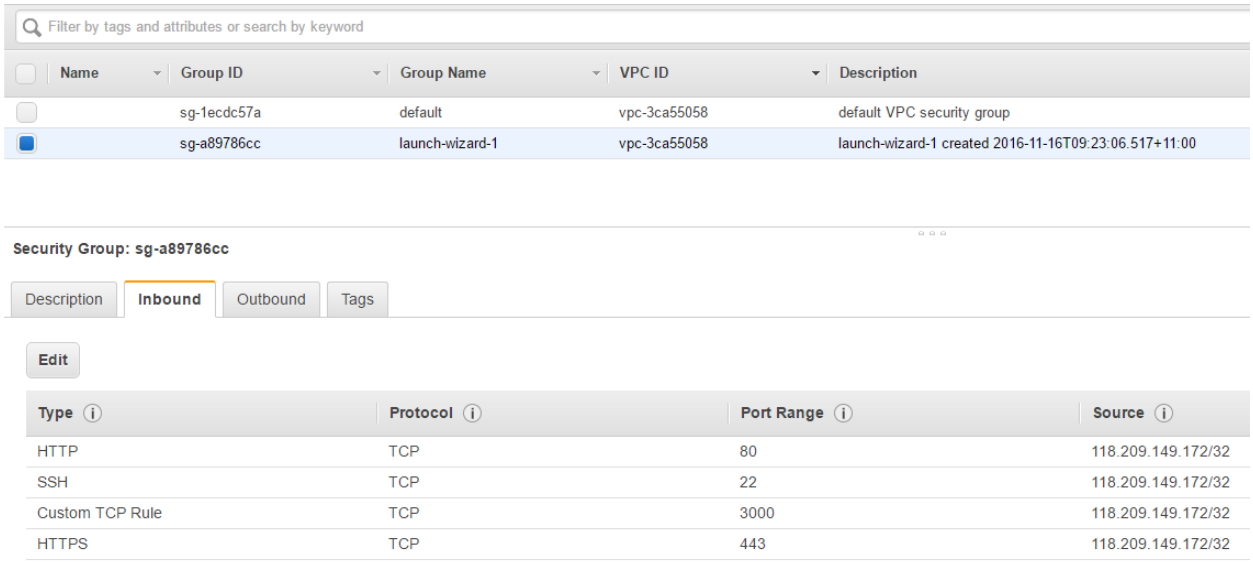
Vim.pp

Line 18: Ensure the vim package is present on the system.



Amazon Web Services

Secure installation



Filter by tags and attributes or search by keyword

Name	Group ID	Group Name	VPC ID	Description
	sg-1ecdc57a	default	vpc-3ca55058	default VPC security group
	sg-a89786cc	launch-wizard-1	vpc-3ca55058	launch-wizard-1 created 2016-11-16T09:23:06.517+11:00

Security Group: sg-a89786cc

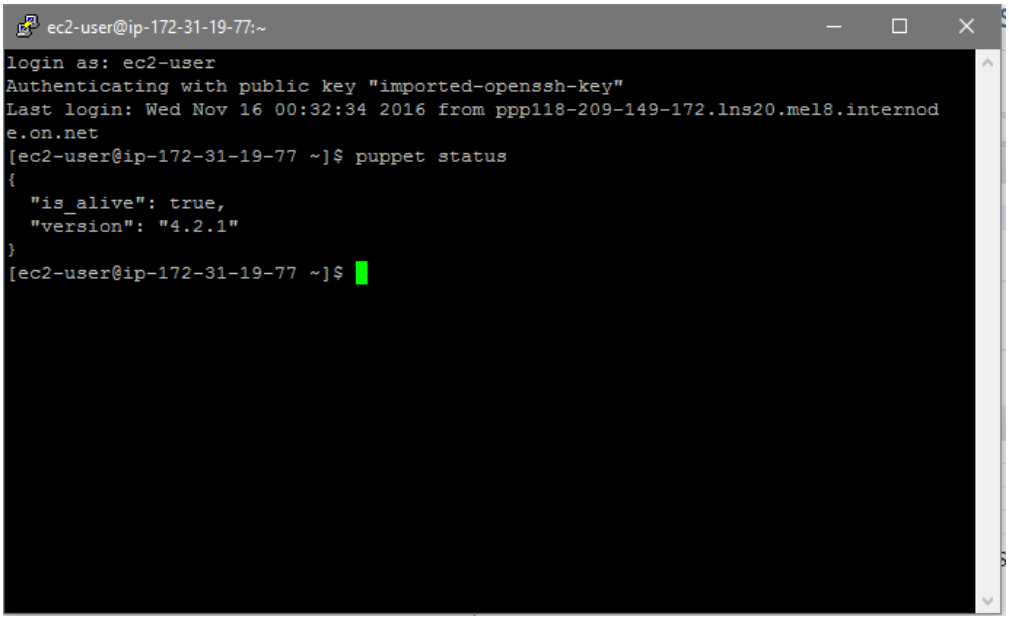
Description | Inbound | Outbound | Tags

Edit

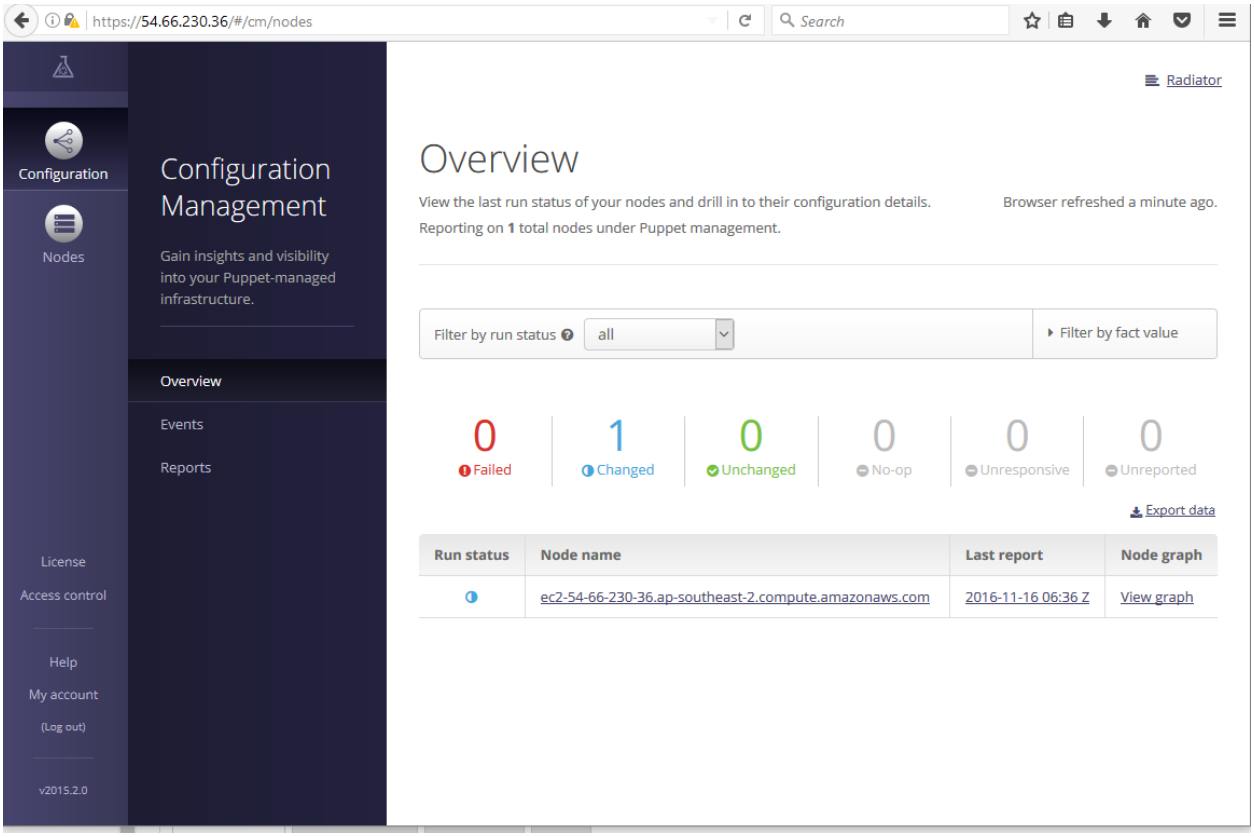
Type	Protocol	Port Range	Source
HTTP	TCP	80	118.209.149.172/32
SSH	TCP	22	118.209.149.172/32
Custom TCP Rule	TCP	3000	118.209.149.172/32
HTTPS	TCP	443	118.209.149.172/32

Only ports 80 (HTTP), 443 (HTTPS), 22 (SSH) and 3000 (Puppet) through the TCP protocol are allowed through the firewall to my external IP.

Puppet running



Successful puppet agent run




```
[root@ip-172-31-19-77 manifests]# /usr/local/bin/puppet agent --test
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts
Info: Caching catalog for ec2-54-66-230-36.ap-southeast-2.compute.amazonaws.com
Info: Applying configuration version '1479278156'
Notice: Agent run starting at 01:35:56
```

```
Notice: Applied catalog in 12.82 seconds
[root@ip-172-31-19-77 manifests]#
```