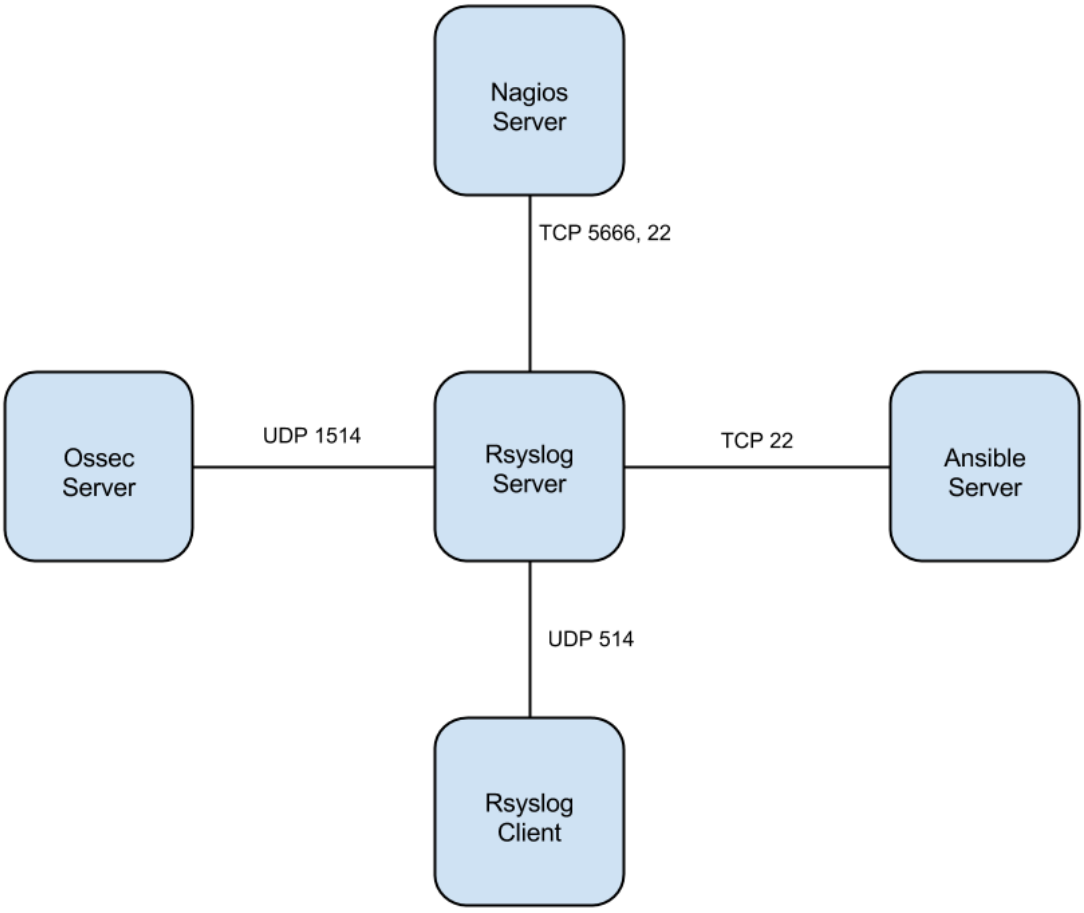
Rsyslog Server

1. Introduction

The rsyslog server provides the support for building a central logging system, where a copy of the logs from the other nodes is forwarded to the rsyslog server for security purposes. If a node is compromised then the attacker can potentially modify or delete the logs present on the compromised node. This limits the usability of the locally stored logs on a node, after the node has been compromised.However an attacker cannot modify a copy of the logs sent by the node to the rsyslog server. Attacker can at most send more spurious log messages to the log server, but he/she cannot affect the existing logs created during the machine compromise. Attacker can also not affect the order of existing stored logs on the central log server.Thus initial logs which are created during break-in are available in chronological order on central log server for enabling Root Cause Analysis (RCA) of the break-in using log messages. Without performing RCA it is not possible to prevent the attacker from again compromising the machine with reasonable confidence.The setup of rsyslog server as a central storage system requires configuring all other nodes to send a copy of their log messages to the rsyslog server. Thus the rsyslog server requires other nodes of the cluster to be configured as the rsyslog clients

2. Diagram



3. Implementation

- Creates a password for rsyslog-server and configures so that this container will be active with internet.

```
---
- name: Set root password
  command: vzctl set 1004 --userpasswd root:{{container_root_password}}

- name: copy interface ifcfg-eth1 file
  template: src=ifcfg-eth1 dest=/vz/private/1004/etc/sysconfig/network-scripts/

- name:  Network restart
  command: vzctl exec 1004 service network restart
# tasks file for rsyslogserver
```

- dependencies

```
dependencies:
   - common-vars
```

- rsyslog Private NetworkConfigures the network-interface in /etc/sysconfig/network-scripts/ifcfg-eth1 of rsyslog-server with the following fields

```
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
NM_CONTROLLED=no
IPADDR=10.100.1.4
GATEWAY=10.100.1.1
NETMASK={{net_mask}}
```