Setup Rsyslog and Secure Syslog (Deprecated)

⚠ For secure syslog direct to dwcloud use the Splunk network input NOT rsyslog.

First let's make sure that the local firewall will allow syslog traffic which is normally on tcp/udp 514 or tcp 6514 for secure syslog. See here for more info on iptables or firewall-cmd

As root, run `iptables -L` or `firewall-cmd --list-all` to determine if we need to add syslog rules.

iptables

To add rules in iptables for syslog

```
iptables -I INPUT 3 -p tcp -m state --state NEW,ESTABLISHED -m tcp --dport 514 -j ACCEPT
iptables -I INPUT 3 -p udp -m state --state NEW,ESTABLISHED -m udp --dport 514 -j ACCEPT
iptables-save
iptables -L
```

To add rules in iptables for secure syslog

```
iptables -I INPUT 3 -p tcp -m state --state NEW,ESTABLISHED -m tcp --dport 6514 -j ACCEPT
iptables-save
iptables -L
```

firewall-cmd

To add rules in firewall-cmd for syslog

```
firewall-cmd --zone=public --permanent --add-port=514/tcp
firewall-cmd --zone=public --permanent --add-port=514/udp
firewall-cmd --reload
firewall-cmd --list-all
```

To add rules in firewall-cmd for secure syslog

```
firewall-cmd --zone=public --permanent --add-port=6514/tcp
firewall-cmd --reload
firewall-cmd --list-all
```

Syslog config file

Next we will need to create a conf file that tells rsyslog what to do. In `/etc/rsyslog.d/` create a file called `dw.conf`. If there is already a file there called vsoc.conf you can probably skip this step.

dw.conf should contain the following

```
#The command below enables debugging to see all the fields
##*.* /var/log/debugfmt;RSYSLOG_DebugFormat
$ModLoad imudp.so
$ModLoad imtcp.so
$umask 0000 # make sure nothing interferes with the following definitions
$FileCreateMode 0644
$DirCreateMode 0755

```

```
$template remote,"/opt/syslog/%$myhostname%/%$YEAR%-%$MONTH%-%$DAY%/%$HOUR%/%fromhost-ip%/%syslogfacility-text%.log"
$Ruleset remote
*.* -?remote
$InputUDPServerBindRuleSet remote
$UDPServerRun 514
$InputTCPServerBindRuleset remote
$InputTCPServerRun 514
#*.* /opt/syslog/syslog.log;RSYSLOG_DebugFormat
& ~
$RuleSet RSYSLOG_DefaultRuleset
```

This tells rsyslog to listen on both tcp and udp 514 and to store files in `/opt/syslog/yyyy-mm-dd/srcIPaddress/logfilename.log`

Secure syslog config file

rsyslog uses the gnu-tls library to run in TLS mode. You will most likely need to install this. To do this run

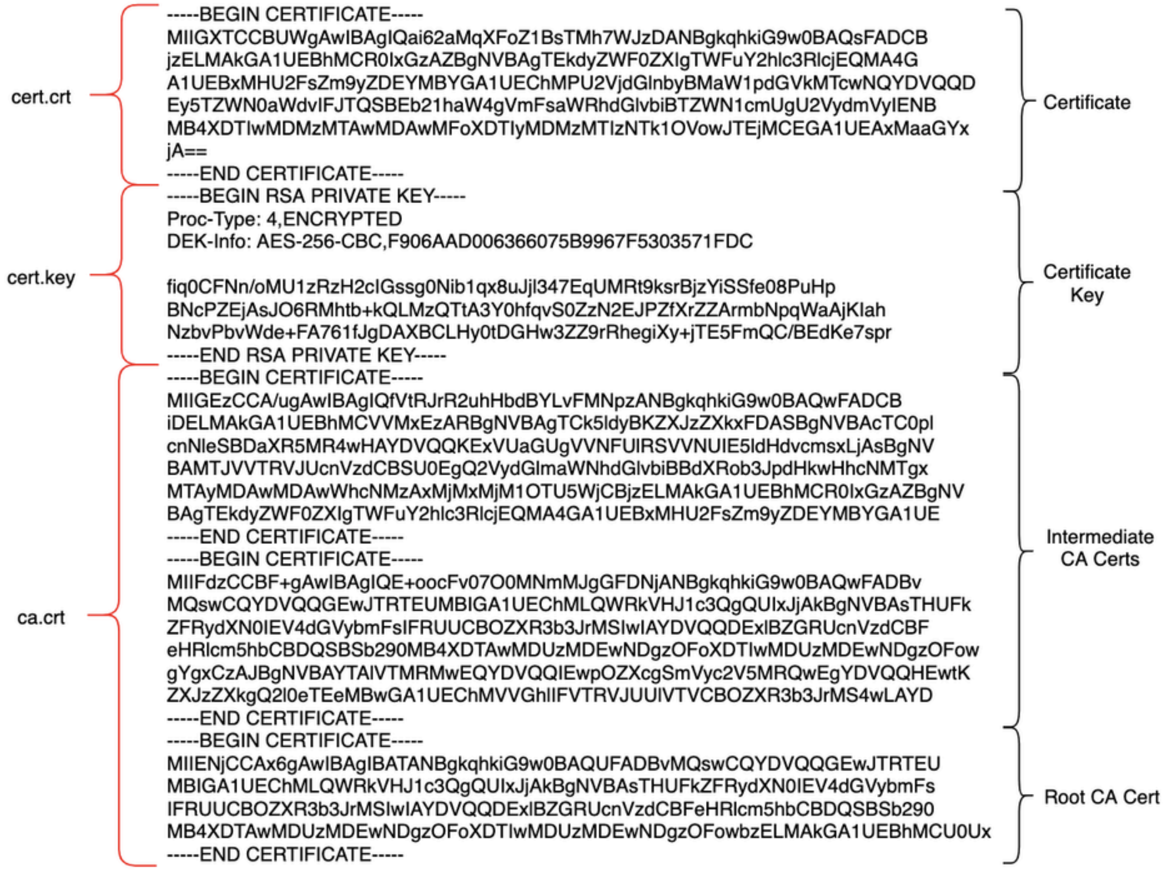
`yum install rsyslog-gnutls`

Next we will need to create a conf file that tells rsyslog how to receive logs securely. In `/etc/rsyslog.d/` create a file called `tls.conf`.

tls.conf should contain the following

```
$ModLoad imtcp # load TCP listener

# make gtls driver the default
$DefaultNetstreamDriver gtls

# certificate files
$DefaultNetstreamDriverCAFile  /etc/rsyslog.d/cert/ca.crt
$DefaultNetstreamDriverCertFile /etc/rsyslog.d/cert/cert.crt
$DefaultNetstreamDriverKeyFile  /etc/rsyslog.d/cert/cert.key

$umask 0000 # make sure nothing interferes with the following definitions
$FileCreateMode 0644
$DirCreateMode 0755

$template remote,"/opt/syslog/%$myhostname%/%$YEAR%-%$MONTH%-%$DAY%/%$HOUR%/%fromhost-ip%/%syslogfacility-text%.log"
$Ruleset remote
*.* -?remote
$InputTCPServerStreamDriverAuthMode anon
$InputTCPServerStreamDriverMode 1 # run driver in TLS-only mode
$InputTCPServerBindRuleset remote
$InputTCPServerRun 6514 # start up listener at port 6514

# *.* /opt/syslog/syslog.log;RSYSLOG_DebugFormat
& ~
$RuleSet RSYSLOG_DefaultRuleset
```

> ETG will most likely give you one certificate file if it is a publicly signed certificate. You will need to break this up into the separate files yourself (ca.crt, cert.crt, cert.key). Please refer to the diagram below. Remember to capture each section from the BEGIN line to the END line including those lines for each section.



```
-----BEGIN CERTIFICATE-----
MIIGXTCCBUWgAwIBAgIQai62aMqXFoZ1BsTMh7WJzDANBgkqhkiG9w0BAQsFADCB
jzELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4G
A1UEBxMHU2FsZm9yZDEYMBYGA1UEChMPU2VjdGlnbyBMaW1pdGVkMTcwNQYDVQQD
Ey5TZWN0aWdvIFJTQSBEb21haW4gVmFsaWRhdGlvbiBTZWN1cmUgU2VydmVyIENB
MB4XDTIwMDMzMTAwMDAwMFoXDTIyMDMzMTIzNTk1OVowJTEjMCEGA1UEAxMaaGYx
jA==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,F906AAD006366075B9967F5303571FDC

fiq0CFNn/oMU1zRzH2clGssg0Nib1qx8uJjl347EqUMRt9ksrBjzYiSSfe08PuHp
BNcPZEjAsJO6RMhtb+kQLMzQTtA3Y0hfqvS0ZzN2EJPZfXrZZArmbNpqWaAjKIah
NzbvPbvWde+FA761fJgDAXBCLHy0tDGHw3ZZ9rRhegiXy+jTE5FmQC/BEdKe7spr
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGEzCCA/ugAwIBAgIQfVtRJrR2uhHbdBYLvFMNpzANBgkqhkiG9w0BAQwFADCB
iDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCk5ldyBKZXJzZXkxFDASBgNVBAcTC0pl
cnNleSBDaXR5MR4wHAYDVQQKExVUaGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNV
BAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTgx
MTAyMDAwMDAwWhcNMzAxMjMxMjM1OTU5WjCBjzELMAkGA1UEBhMCR0IxGzAZBgNV
BAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UEBxMHU2FsZm9yZDEYMBYGA1UE
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFdzCCBF+gAwIBAgIQE+oocFv07O0MNmMJgGFDNjANBgkqhkiG9w0BAQwFADBv
MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTHUFk
ZFRydXN0IEV4dGVybmFsIFRUUCBOZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBF
eHRlcm5hbCBDQSBSb290MB4XDTAwMDUzMDEwNDgzOFoXDTIwMDUzMDEwNDgzOFow
gYgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpOZXcgSmVyc2V5MRQwEgYDVQQHEwtK
ZXJzZXkgQ2l0eTEeMBwGA1UEChMVVGhlIFVTRVJUUlVTVCBOZXR3b3JrMS4wLAYD
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU
MBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTHUFkZFRydXN0IEV4dGVybmFs
IFRUUCBOZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBFeHRlcm5hbCBDQSBSb290
MB4XDTAwMDUzMDEwNDgzOFoXDTIwMDUzMDEwNDgzOFowbzELMAkGA1UEBhMCU0Ux
-----END CERTIFICATE-----
```

This tells rsyslog to listen on tcp 6514, run in TLS mode and where the cert files can be found.

To create the cert files, please see [RETIRED] Generate an internally signed certificate

Save these certs as

`/etc/rsyslog.d/cert/ca.crt` - This is the CAs public key. You will probably need to share this with the syslog client (e.g. proofpoint)

`/etc/rsyslog.d/cert/cert.crt` - This is your server's public key. You will probably need to share this with the syslog client (e.g. proofpoint)

`/etc/rsyslog.d/cert/cert.key` - This is your server's private key. This should not be shared

Cron cleanup job

To clear out old logs you need to add an entry to root’s crontab

Run `crontab -e` then add the following line

```
0 */1 * * * /usr/bin/find /opt/syslog -mindepth 3  -type d -name '[0-2][0-9]' ! -mmin -1500 -exec rm -rf {} \; && /usr/bin/find /opt/syslog  -mindepth 2 -maxdepth 3 -type d -name '20[0-9][0-9]-[0-1][0-9]-[0-3][0-9]' -empty -delete
```

Restart Rsyslog service

You will need to restart the rsyslog service for these changes to take effect. Depending on OS version, this can be done in two ways.

`service rsyslog restart`

or

`systemctl restart rsyslog.service`

Troubleshooting

Make sure rsyslog is running and listening on 514 `netstat -lpn | grep rsyslog` you should see something like

```
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      4342/rsyslogd
tcp6       0      0 :::514                  :::*                    LISTEN      4342/rsyslogd
udp        0      0 0.0.0.0:514             0.0.0.0:*                           4342/rsyslogd
udp6       0      0 :::514                  :::*                                4342/rsyslogd
```

Make sure syslog packets are making it to the server. As root run `tcpdump -vnni <interface> port 514` you should see packets coming in from the IP that you are expecting.

Troubleshooting selinux and /opt/syslog

Selinux can cause issues when converting hosts where permissions are incorrectly set. You can view errors for selinux by `tail -f /var/log/messages`.

An example error:

```
May  7 15:48:53 azs-splunkhf-001 setroubleshoot: SELinux is preventing /usr/sbin/rsyslogd from write access on the directory /opt/syslog/azs-splunkhf-001. For complete SELinux messages run: sealert -l 4c40105c-7128-4bfb-a0e8-d942fc1dc63f
May  7 15:48:53 azs-splunkhf-001 python: SELinux is preventing /usr/sbin/rsyslogd from write access on the directory /opt/syslog/azs-splunkhf-001.#012#012*****  Plugin catchall_labels (83.8 confidence) suggests *******************#012#012If you want to allow rsyslogd to have write access on the azs-splunkhf-001 directory#012Then you need to change the label on /opt/syslog/azs-splunkhf-001#012Do#012# semanage fcontext -a -t FILE_TYPE '/opt/syslog/azs-splunkhf-001'#012where FILE_TYPE is one of the following: NetworkManager_log_t, abrt_var_log_t, acct_data_t, afs_logfile_t, aide_log_t, amanda_log_t, antivirus_log_t, apcupsd_log_t, apmd_log_t, asterisk_log_t, auth_cache_t, bacula_log_t, bitlbee_log_t, boinc_log_t, brltty_log_t, calamaris_log_t, callweaver_log_t, canna_log_t, ccs_var_lib_t, ccs_var_log_t, cert_t, certmaster_var_log_t, cfengine_log_t, cgred_log_t, checkpc_log_t, chronyd_var_log_t, cinder_log_t, cloud_log_t, cluster_var_log_t, cobbler_var_log_t, condor_log_t, conman_log_t, consolekit_log_t, container_log_t, couchdb_log_t, cron_log_t, ctdbd_log_t, cupsd_log_t, cyphesis_log_t, ddclient_log_t, deltacloudd_log_t, denyhosts_var_log_t, device_t, devicekit_var_log_t, dirsrv_snmp_var_log_t, dirsrv_var_log_t, dlm_controld_var_log_t, dnsmasq_var_log_t, dovecot_var_log_t, dspam_log_t, evtchnd_var_log_t, exim_log_t, fail2ban_log_t, faillog_t, fenced_var_log_t, fetchmail_log_t, fingerd_log_t, firewalld_var_log_t, foghorn_var_log_t, fsadm_log_t, ganesha_var_log_t, getty_log_t, gfs_controld_var_log_t, glance_log_t, glusterd_log_t, groupd_var_log_t, haproxy_var_log_t, httpd_log_t, icecast_log_t, inetd_log_t, initrc_var_log_t, innd_log_t, ipa_log_t, ipsec_log_t, iscsi_log_t, iwhd_log_t, jetty_log_t, jockey_var_log_t, kadmind_log_t, keystone_log_t, kismet_log_t, krb5_host_rcache_t, krb5kdc_log_t, ksmtuned_log_t, ktalkd_log_t, lastlog_t, mailman_log_t, mcelog_log_t, mdadm_log_t, minidlna_log_t, mirrormanager_log_t, mongod_log_t, motion_log_t, mpd_log_t, mrtg_log_t, munin_log_t, mysqld_log_t, mythtv_var_log_t, nagios_log_t, named_log_t, neutron_log_t, nova_log_t, nscd_log_t, nsd_log_t, ntpd_log_t, numad_var_log_t, openhpid_log_t, openshift_log_t, opensm_log_t, openvpn_status_t, openvpn_var_log_t, openvswitch_log_t, openwsman_log_t, osad_log_t, passenger_log_t, pcp_log_t, piranha_log_t, pkcs_slotd_log_t, pki_log_t, pki_ra_log_t, pki_tomcat_log_t, pki_tps_log_t, plymouthd_var_log_t, polipo_log_t, postgresql_log_t, pppd_log_t, pptp_log_t, prelink_log_t, prelude_log_t, privoxy_log_t, procmail_log_t, prosody_log_t, psad_var_log_t, puppet_log_t, pyicqt_log_t, qdiskd_var_log_t, rabbitmq_var_log_t, radiusd_log_t, redis_log_t, rhev_agentd_log_t, rhsmcertd_log_t, ricci_modcluster_var_log_t, ricci_var_log_t, rpm_log_t, rsync_log_t, rtas_errd_log_t, samba_log_t, sanlock_log_t, sectool_var_log_t, sendmail_log_t, sensord_log_t, setroubleshoot_var_log_t, shorewall_log_t, slapd_log_t, slpd_log_t, smsd_log_t, snapperd_log_t, snmpd_log_t, snort_log_t, spamd_log_t, speech-dispatcher_log_t, squid_log_t, sssd_var_log_t, stapserver_log_t,
stunnel_log_t, sudo_log_t, svnserve_log_t, syslogd_tmp_t, syslogd_tmpfs_t, syslogd_var_lib_t,
syslogd_var_run_t, sysstat_log_t, thin_aeolus_configserver_log_t, thin_log_t, tmp_t, tmpfs_t, tomcat_log_t,
tor_var_log_t, tuned_log_t, ulogd_var_log_t, uucpd_log_t, var_lib_t, var_log_t, var_run_t, varnishlog_log_t,
vdagent_log_t, virt_log_t, virt_qemu_ga_log_t, vmware_log_t, watchdog_log_t, winbind_log_t, wtmp_t, xdm_log_t,
xend_var_log_t, xenstored_var_log_t, xferlog_t, xserver_log_t, zabbix_log_t, zarafa_deliver_log_t,
zarafa_gateway_log_t, zarafa_ical_log_t, zarafa_indexer_log_t, zarafa_monitor_log_t, zarafa_server_log_t,
zarafa_spooler_log_t, zebra_log_t, zoneminder_log_t.#012Then execute:#012restorecon -v '/opt/syslog/azs-
splunkhf-001'#012#012#012*****  Plugin catchall (17.1 confidence) suggests
**************************#012#012If you believe that rsyslogd should be allowed write access on the azs-
splunkhf-001 directory by default.#012Then you should report this as a bug.#012You can generate a local policy
module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'rs:main Q:Reg'
--raw | audit2allow -M my-rsmainQReg#012# semodule -i my-rsmainQReg.pp#012
```

You can view the selinux permissions of a folder on the host with `ls -dZ`. This should provide you with enough context to be able to make an accurate diagnosis.

Working syslog folder:

```
drwxr-xr-x. root root system_u:object_r:var_log_t:s0   /var/log/
```

Non-functional syslog folder:

```
drwxrwxr-x. root root unconfined_u:object_r:usr_t:s0   /opt/syslog/
```

As you can see, the permissions are different. These permissions are laid out as `user:role:type:level`. In this particular case since we are changing where syslog writes files to disk, it is easiest to just copy there permissions from /var/log to /opt/syslog with the following:

```
chcon --reference /var/log /opt/syslog
```

Verify the change again with `ls -dZ /opt/syslog`

```
drwxrwxr-x. root root system_u:object_r:var_log_t:s0   /opt/syslog/
```

After the folder permissions have been changes, the filesystem permissions will need to be changed as well with the following:

```
semanage fcontext -a -t var_log_t "/opt/syslog(/.*)?"
```

Once this context has been changed, apply the changes with restorecon:

```
restorecon -R -v /opt/syslog/
```

Once the changes have been recursively applied to /opt/syslog, restart syslog. `tail -f /var/log/messages` should no longer show errors being generated.