山西联通3G 1 oss网管证书更新方案

Method of Procedures - OSS14B CA &CERT Renewal

[1. 系统运行情况检查 2](#_Toc42183753)

[2. OMSAS 更新无影响CA&Cred 2](#_Toc42183754)

[3. OMSAS 更新可能有影响CA&Cred (PS:山西联通实际操作下来也对现网无影响) 3](#_Toc42183755)

[4. Renew 续订MSCertCA，这需要在Admin上重新启动MC 4](#_Toc42183756)

[5. Fallback 6](#_Toc42183757)

[6. 风险管理和应急计划 6](#_Toc42183758)

[7. Reason Codes 6](#_Toc42183759)

[8. 遇到的问题重新enrollment 站点不同步 7](#_Toc42183760)

[9. 操作完成后系统检查 8](#_Toc42183761)

摘要该文介绍了O14B版本的山西联通OSS 证书续订的步骤，以解决将于2020年10月下旬发生的证书过期问题。

# 系统运行情况检查

|  |  |
| --- | --- |
| **Step** | **Action** |
| Check System Status | 1.通过ILO检查Admin，COMINF和OMSAS的硬件状态，确保没有报告有关硬件的错误 2.对磁盘容量和服务状态进行必要的健康检查： a.＃df -h 3.检查管理员是否存在任何服务错误： #df -h  ＃tail -200 /var/adm/messages | grep -i error ＃ipadm show-addr  ＃dladm show-phys  ＃svcs -a &svcs -xv ＃smtool -list  ＃hastatus -sum ＃ifconfig -a  OEX，CEX和ALV可以在UAS Citrix上打开。 |
| Backup | 1.以root用户身份登录到OMSAS，INFRA主服务务器和从服务器。 2.在OMSAS，INFRA主服务器和从服务器上执行以下命令  # /opt/ericsson/secinst/bin/backup.sh  创建备份文件 /var/tmp/ERICsinst/backup/secinst\_<hostname>\_backup.zip,  其中主机名是OMSAS或O&M Infra服务器的主机名  将备份文件放到安全的地方 |

# OMSAS 更新无影响CA&Cred

|  |  |  |
| --- | --- | --- |
| **Step** | **Action** | **Comments** |
| Update the ynctlteemas1TORSbiCA  on omsas | #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts  #/opt/ericsson/cadm/bin/pkiAdmin ca renew -name ynctlteemas1TORSbiCA -reason [4](#_Reason_Codes)  #/opt/ericsson/cadm/bin/pkiAdmin ca revoke\_old -name ynctlteemas1TORSbiCA  #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts |  |
| Update the TORWebCA (ExternalSystemsCA) on omsas | #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts  #/opt/ericsson/cadm/bin/pkiAdmin ca renew -name ExternalSystemsCA -reason 4  #/opt/ericsson/cadm/bin/pkiAdmin ca revoke\_old -name ExternalSystemsCA  #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts |  |
| Update the TORMgmtRootCA (ExternalSystemsCA) on omsas | #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts  #/opt/ericsson/cadm/bin/pkiAdmin ca renew -name TORMgmtRootCA -reason 4  #/opt/ericsson/cadm/bin/pkiAdmin ca revoke\_old -name TORMgmtRootCA  #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts |  |
| Update the TORMediationRootCA on omsas | #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts  #/opt/ericsson/cadm/bin/pkiAdmin ca renew -name TORMediationRootCA -reason 4  #/opt/ericsson/cadm/bin/pkiAdmin ca revoke\_old -name TORMediationRootCA  #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts |  |
| Update the aiws\_bsim on omsas | #/opt/ericsson/cadm/bin/pkiAdmin cred bsim aiws list  #/opt/ericsson/cadm/bin/pkiAdmin cred bsim aiws renew -reason 4  #/opt/ericsson/cadm/bin/pkiAdmin cred bsim aiws revoke\_old  #/opt/ericsson/cadm/bin/pkiAdmin cred bsim aiws list |  |

# OMSAS 更新可能有影响CA&Cred

|  |  |  |
| --- | --- | --- |
| **Step** | **Action** | **Comments** |
| 1. Update LTEIPSecSEGRootCA on OMSAS | #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts  #/opt/ericsson/cadm/bin/pkiAdmin ca renew -name LTEIPSecSEGRootCA -reason 4  # /opt/ericsson/cadm/bin/pkiAdmin ca revoke\_old -name LTEIPSecSEGRootCA  #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts |  |
| 2. Update LTEIPSecNEcusRootCA on OMSAS | #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts  #/opt/ericsson/cadm/bin/pkiAdmin ca renew -name LTEIPSecNEcusRootCA -reason 4  #Delete the ra credential on INFRA: # cp /opt/ericsson/racrs/domains/racrs/config/LTEIPSecNEcus\_Sceprakeystore.p12 /opt/ericsson/racrs/domains/racrs/config/bakLTEIPSecNEcus\_Sceprakeystore.p12  # rm /opt/ericsson/racrs/domains/racrs/config/LTEIPSecNEcus\_Sceprakeystore.p12  Renew the ra credential:# /opt/ericsson/secinst/bin/config.sh -p ERICracrs:racertProcess request/ response files.Perform on INFRA:# scp /var/tmp/ERICsinst/config/secinst\_<INFRA\_hostname>\_config.zip root@<OMSAS\_hostname>:/var/tmp/Perform on OMSAS:# /opt/ericsson/secinst/bin/config.sh -R /var/tmp/secinst\_<INFRA\_hostname>\_config.zip# scp /var/tmp/ERICsinst/config/secinst\_<INFRA\_hostname>\_response.zip root@<INFRA\_hostname>:/var/tmp/Perform on INFRA:# /opt/ericsson/secinst/bin/config.sh -p ERICracrs:racert -r /var/tmp/secinst\_<INFRA\_hostname>\_response.zip  #/opt/ericsson/secinst/bin/config.sh -p ERICracrs  3. Update the ra credential on INFRA Slave. See Step 2.  4. Refresh settings in CADM on OMSAS:  # /opt/ericsson/secinst/bin/config.sh -p ERICcadm:scepcfg  5. Perform on OMSAS:  /opt/ericsson/secinst/bin/config.sh -p ERICcadm:cpptrusted -f  6. Restart cadm on OMSAS:#svcadm restart cadm  #/opt/ericsson/cadm/bin/pkiAdmin ca revoke\_old -name LTEIPSecNEcusRootCA  #/opt/ericsson/cadm/bin/pkiAdmin ca list -cacerts | 如果：/opt/ericsson/secinst/bin/config.sh -p ERICracrs:racert 的输出提示 # racert .. Certificate will expire in 7 days. 或者racert .. incomplete,那么按这些步骤走完之后，再次做/opt/ericsson/secinst/bin/config.sh就会显示ok |
| 2. Update ra\_ipsec on OMSAS | #/opt/ericsson/cadm/bin/pkiAdmin cred ra\_ipsec list  #/opt/ericsson/cadm/bin/pkiAdmin cred ra\_ipsec renew -server om\_serv\_master -reason 4  #/opt/ericsson/cadm/bin/pkiAdmin cred ra\_ipsec renew -server om\_serv\_slave -reason 4  #/opt/ericsson/cadm/bin/pkiAdmin cred ra\_ipsec list |  |

# Renew 续订MSCertCA，这需要在Admin上重新启动MC

|  |  |  |
| --- | --- | --- |
| **Step** | **Action** | **Comments** |
| 1. Update MSCertCA on OMSAS | #/opt/ericsson/cadm/bin/pkiAdmin cred ms list  #/opt/ericsson/cadm/bin/pkiAdmin cred ms renew -reason 4  #/opt/ericsson/secinst/bin/credentialsmgr.sh -installMsCerts ynctlteemas1  #/opt/ericsson/secinst/bin/credentialsmgr.sh -msCredentials ynctlteemas1 |  |
| 2. Update MSCertCA on Admin | --------------------------------------------------------------------------------------------------------------------------  山西联通ynctlteemas1RootCA 不需要更新,所以跳过此步  Note: This step can be skipped if <MS\_hostname>RootCA is not renewed.  Install old <MS\_hostname>NECertCA on Master Server:  #/opt/ericsson/secpf/scripts/bin/security.ksh -installTrustCert /var/tmp/<MS\_hostname>NECertCA.pem  --------------------------------------------------------------------------------------------------------------------------  Copying of p12 file to Mate/EBAS/Peer Servers:  Log on to Master Server（oss side) as root.  a. Go the path cd /ericsson/config/  eg:scp /ericsson/config/ossrc.p12 root@oss1b:/ericsson/config/  b. Copy ossrc.p12file in above path to Mate and EBAS Servers.  c. Copy ossrc.p12 file to Peer Servers if exists.  d. After copying, the rights must be set by issuing the following  commands:  #chown nmsadm:nms /ericsson/config/ossrc.p12  #chmod 440 /ericsson/config/ossrc.p12  e. Check ls -l /ericsson/config/ossrc.p12 will returns  following output:  -r--r----- 1 nmsadm nms ... /ericsson/config/ossrc.p12  Note: After installation of p12 server restart is required. Execute following command in the server  # init 6  6. Restart all Managed Components on the MS and wait until everything is  restarted successfully:  su nmsadm -c "/opt/ericsson/nms\_cif\_sm/bin/smtool -coldrestart -all -reason=other -reasontext=\"MSCredentialRenewal\""; smtool p;  可以考虑直接重启ossfs side  7. Get new scs.ior on OMSAS:  # rm /opt/ericsson/cadm/conf/masterserver.iors/ynctlteemas1  # /opt/ericsson/secinst/bin/config.sh -p ERICcadm:msior -p ERICcadm:smfservice  8. Update the cadm trust by using the following command on OMSAS as  root user:  #/opt/ericsson/secinst/bin/config.sh -p ERICcadm:iiopissuer -p ERICcadm:iiopcert -f  Restart cadm on OMSAS:  #svcadm restart cadm  Revoke old ms credential on OMSAS:  # /opt/ericsson/cadm/bin/pkiAdmin cred ms revoke\_old   检查证书：# /opt/ericsson/cadm/bin/pkiAdmin cred ms list  以上操作结束后，OSS group和sybase group都在一边，记得把sybase group切到另一边,以及相关系统检查。  #hagrp -switch Sybase1 -to ynctlteemas1a |  |
| 3. Restart UAS server | Restart all UAS (UAS1 and UAS2) of the system:  # init 6 |  |

# Fallback

倒回步骤

|  |  |  |
| --- | --- | --- |
| **Step** | **Action** | **Comments** |
| Rollback on **OMSAS, COMINF and Admin** | 1. 以root用户身份登录OMSAS和COMINF Server  2. # /opt/ericsson/secinst/bin/backup.sh -r <backup file>  3. 通过运行以下命令验证配置：  # /opt/ericsson/secinst/bin/config.sh  所有步骤都应该OK.  4. 再次运行OSS-RC CA证书更新中提到的步骤（还原备份后），以使网络元素具有旧证书。  但是，如果网元已经使用更新了的证书，则此还原过程将不会更新网元上的证书。 |  |

# 风险管理和应急计划

1、停机时间  
在MSCertCA更新期间，需要在Admin上重新启动MC，这将导致OSS所有服务的停机时间在30分钟左右，以及数据库切边会导致Heartbeat告警时间批量刷新。

2、解决方案

为了防止在停机期间造成任何潜在的不便，需要通知此情况以防止在续订期间使用OSS

# Reason Codes

Reasons and reason codes are defined in RFC5280 standard. Use of either reasonname or reason code is allowed. The following reasons are supported:

|  |  |
| --- | --- |
| Reason name | Reason code |
| keyCompromise | 1 |
| cACompromise | 2 |
| affiliationChanged | 3 |
| superseded | 4 |
| cessationOfOperation | 5 |
| certificateHold | 6 |
| privilegeWithdrawn | 9 |
| aACompromise | 10 |

# 操作完成后系统检查

北向/ENIQ/OSS等业务系统。