Cisco IronPort C-series / ESA CLI Cheat Sheet - 20140512

Jens Roesen – email – www - twitter

Prompt, cluster and command modes, default user & password, contacts
Being part of a cluster, the prompt will indicate the current mode: (Machine esa1.example.com)> vs. (Cluster Example.com-Cluster)> Some commands are restricted to cluster or machine mode, some may be run in any mode. If necessary, the ESA will prompt you for a change of mode. [25AC?][25AC?][25AC?][25AC?][25AC?][25AC?][25AC?][25AC?] If interactive commands require additional input from the user, the prompt will change to opening and closing square brackets enclosing a default value, if available. [25AC?][25AC?][25AC?][25AC?][25AC?][25AC?][25AC?][25AC?] Some commands like dig or aliasconfig support a batch mode allowing you to run a complete command with one single-line command input: esa1.example.com> dig -t mx example.com [25AC?][25AC?][25AC?][25AC?][25AC?][25AC?][25AC?][25AC?] The default username is admin and it's password is ironport. The default IP is 192.168.42.42 on Data1 on C1X0 appliances and Management Interface on all others. For access through serial console use 9600/8-N-1 with hardware flow control. [25AC?][25AC?][25AC?][25AC?][25AC?][25AC?][25AC?][25AC?] Send undetected spam to spam@access.ironport.com, false positives to ham@access.ironport.com, missed ads to ads@access.ironport.com and false positive ads to not_ads@access.ironport.com. Send each as RFC822 MIME encoded attachment. See Knowledge Base article 472.

Basic commands	
help command	View online help for command.
who	Show a list of currently logged in users.
whoami	Show name and groups for own user.
date	View current date and time.
passwd	Change password for the current user.
last	Show list of recently logged in users and session dates.
clear	Abandon all pending configuration changes.
commit	Commit pending configuration changes.
clustermode	Switch between machine, cluster and group mode.
shutdown	Shut down and power-off the appliance.
reboot	Reboot the appliance.
exit / quit	Exit CLI. Will warn you about uncommitted changes.

Infos and status	
version	Show brief hardware and software information.
ipcheck	Show extended hardware and software information.
status detail	View detailed system status.
commitdetail	View details about the last commit in the active session.
showchanges	View pending config changes as nested tree structure.
antispamstatus	Show status and latest update for enabled anti-spam engines.
antivirusstatus	Show status and latest update for active antivirus engines.
repengstatus	Show version and latest updates for SBRS engines.
outbreakstatus	Show status of Virus Outbreak Filters.
sbstatus	Show SenderBase status.
encryptionstatus	Show PXE engine status and last engine update.
dlpstatus	Show status of RSA DLP engine.
workqueue status	Display current work queue status.
workqueue rate n	Display number of pending, incoming and outgoing mails in the queue and refresh every n seconds.
topin	View top hosts by number of incoming connections.
rate n	Display in/out connections and recipient statistics. Updated every n seconds.
hostrate domain n	Similar to rate but limited to a single destination domain.
hoststatus domain	View statistics for domain including MX settings and latest 5xx delivery error.
tophosts	View the top 20 destination domains in the mail queue. Can be sorted in different ways to meet your requirements.
featurekey	View, activate and check for new feature keys.
dnsstatus	Show DNS statistics since counter reset / reboot / ever.
displayalerts n	Display the last n alerts sent by the appliance.
resetcounters	Reset all counters of a single machine.

Test network and configuration	
ping or ping6	Test network by sending a IPv4/IPv6 ping to a remote host.
traceroute or traceroute6	View IPv4/IPv6 network path/routing to a remote host.
telnet	Telnet to a remote host. Defaults to port 25, not 23!
dig	Run DNS queries. Supports batch mode.
nslookup	Run DNS queries.
packetcapture	Start a packet capture in AsyncOS versions up from 7.2.
tcpdump	Start a packet capture in AsyncOS versions up to 7.1.
tcpservices	Display information about running TCP/IP services.
netstat	Display current network connections, network statistics, interface status, listen queue size or routing table.
mailconfig	Send a mail with the XML configuration attached.
trace	Trace the mail flow through the system with a virtual test mail.
ldaptest	Run an LDAP query against a configured LDAP server.
ldapflush	Clear all cached LDAP query results.
dnslisttest	Manually test an IP against a DNS-based blacklist.
dnsflush	Flush DNS cache.
tlsverify	Test and verify a TLS connection to a remote MTA.

General configuration	
systemsetup	Run the system setup wizard. This will remove any existing listener and associated HAT configuration.
userconfig	View and manage users and external authentication.
adminaccessconfig	Configure banner message and restrict access to the ESA based on IP ranges. Check these when building SSH cluster.
interfaceconfig	Add, delete and edit IP interface settings (IPv4 and IPv6).
etherconfig	Configure ethernet settings like speed and duplex mode, VLANs or NIC pairing.
sethostname	Set system hostname.
setgateway	Set default gateway.
routeconfig	Configure static network routes.
dnsconfig	Configure DNS servers and domain DNS settings.
dnshostprefs	Configure global or per domain DNS resolver preferences.
dnslistconfig	Configure global settings for DNS blacklist queries.
featurekeyconfig	Enable/disable auto-download and activation of feature keys.
ldapconfig	Create, delete and manage LDAP server profiles.
snmpconfig	Enable SNMP, set community string and password, define trap targets.
ntpconfig	Configure NTP Servers and source interface for NTP queries.
sshconfig	Configure sshd settings and view, add, delete or modify SSH keys used for SSH access.
sslconfig	Configure SSL for HTTPS access (SSL Versions, Ciphers).
settz	Setup time zone.
tzupdate	Update time zone rules.
settime	Set system time and date as MM/DD/YYYY HH:MM:SS
alertconfig	Configure mail alert settings and mail alert recipients. 5
trackingconfig	Configure message tracking settings.
addressconfig	Set sender address to be used for mails generated by the system like bounces and notifications.
addresslistconfig	Configure and manage addresslists.
fipsconfig	Enable FIPS mode to meet FIPS 140-2 requirements.

Configuring SMTP	
smtproutes	Add, delete, edit and view SMTP routing.
listenerconfig	Configure and manage public, private or blackhole listeners.
deliveryconfig	Configure mail delivery settings.
destconfig	Configure destination control limits for a specified domain.
exceptionconfig	Configure and manage the domain exception table.
altsrchost	View, create and modify virtual gateway mappings for sender addresses or client IPs.
bounceconfig	Create and modify bounce profiles.
policyconfig	Configure and manage incoming and outgoing mail policies.
textconfig	Configure text blocks for use in disclaimers, anti-virus alerts, DLP, encryption notifications or bounces.
filters	Create, edit and view message filters.
sievechar	Configure the char used for sieve mail filtering. Only used in LDAP Accept and LDAP Routing.
dictionaryconfig	Create and manage content dictionaries.
sslconfig	Configure SSL for TLS connections (Versions, Ciphers).
certconfig	Manage certificates in PEM format and CA.
callaheadconfig	Configure, edit, view and test SMTP Call-Ahead feature.
smtpauthconfig	Configure and manage SMTP authentication profiles.
addresslistconfig	Configure and manage address lists.
aliasconfig	Configure and manage the alias table.
bvconfig	Configure bounce verification address tagging.
domainkeysconfig	Configure, manage and test tons of DKIM settings.
quarantineconfig	Configure and manage system quarantines.
incomingrelayconfig	Manage incoming mail relay settings.
localeconfig	Manage locale modification and enforcement settings.

Managing message queues and mails	
workqueue status	Display current work queue status.
workqueue rate n	Display number of pending, incoming and outgoing mails in the queue and refresh every n seconds.
showrecipients	Show messages from the queue by recipient host name, sender address or all mails in the queue.
deleterecipients	Delete messages from the queue by recipient host name, sender address or all mails in the queue.
bouncerecipients	Bounce messages from the queue by recipient host name, sender address or all mails in the queue.
redirectrecipients	Redirect all mails to a relay host.
showmessage	Show a complete message by MID in ASCII.
archivemessage	Archive a message by it's MID as mbox file to the /configuration directory.
removemessage	Remove a message from work, retry or destination queue.
oldmessage	Display Headers and MID of the oldest message in the queue.
delivernow	Attempt to deliver pending messages either by domain or simply reschedule all mails.
unsubscribe	Manage unsubscribe lists for recipient addresses that will always be bounced or dropped.
stripheaders	Strip all headers by name in this table from all mails.
resetqueue	Reinitialize queue. DELETES ALL QUEUED MAIL

AsyncOS management	
updateconfig	Configure update URLs and HTTP/HTTPS proxies to use. This will also affect Anti-Spam and Anti-Virus updates.
upgrade	List all available AsyncOS versions and perform an upgrade.
revert	Revert the appliance to a previously used AsyncOS version. Except network settings ALL configurations and logs will be lost.

Suspending and resuming receiving and/or delivering mails	
workqueue pause	Pause working queue.
workqueue resume	Resume working queue.
suspendlistener	Suspend receiving mails on one, several or all listeners. Shut down won't be graceful.
resumelistener	Resume receiving mails on one, several or all listeners.
suspenddel	Suspend delivering mails. Shut down won't be graceful.
resumedel	Resume delivering mails.
suspend	Suspend receiving and delivering all mails. Shut down won't be graceful.
resume	Resume receiving and delivering all mails.

ESA configuration files	
showconfig	View XML configuration file as paged output.
mailconfig	Send XML configuration file via mail.
saveconfig	Save XML configuration file in the /configuration directory.
loadconfig	Load XML configuration file from the /configuration directory or paste it directly into the CLI.
rollbackconfig	Roll back to one of the last 10 saved configurations.
resetconfig	Reset ALL configurations to factory default.

Working with logs	
grep	Search for a Regular Expression pattern inside a log file.
findevent	Find an event in the logs matching either a message id, a mail address (From/To) or a subject. Menu driven or batch mode.
tail	Continuously display new entries from the end of a log file.
rollovernow	Do a rollover on one certain or simply all log files.
logconfig	Configure and manage log files and delivery methods (FTP, SCP, Syslog). View public RSA/DSS key from users.

Managing engines	
updateconfig	Configure update URLs and HTTP/HTTPS proxies to use. This will also affect AsyncOS updates.
updatenow updatenow force	Manually update all components. Force updating with the option force. The force option also works with all other update commands below
antispamconfig	Configure IronPort anti-spam and Intelligent Multi-Scan.
antispamupdate	Manually request immediate anti-spam rules update.
antivirusconfig	Configure and view anti-virus settings and scanners.
antivirusupdate	Manually request immediate anti-virus definitions update.
scanconfig	Configure scanner options like skipped file types, scanning depth (nesting), maximum scan size, scanner timeout.
outbreakconfig	Enable, disable and configure Outbreak Filters.
outbreakupdate	Request immediate update of CASE rules and engine.
outbreakflush	Clear CASE rules cache.
encryptionconfig	Configure IronPort PXE mail encryption.
encryptionupdate	Manually request immediate PXE engine update.
dlpupdate	Manually request immediate RSA DLP engine update.
dlprollback	Rollback RSA DLP engine and config to the previous version.
repengupdate	Manually request immediate SBRS engine update.
senderbaseconfig	Configure SenderBase SBNP statistics sharing status.

Cisco IronPort Support and advanced diagnostics	
supportrequest	Open a support request with Cisco TAC.
techsupport	Enable or disable a (secured) tunnel for Cisco IronPort Support to access the appliance remotely.
diagnostic	Check RAID status, flush DNS/ARP/LDAP caches, test remote SMTP servers or check disk quota and usage.
enablediag	Login with this user if "admin" account fails. Same password as "admin". Provides several emergency options.

Centralized Management Cluster	
clusterconfig	Create SSH or CSS clusters, add or remove single ESAs to or from a cluster. Create and manage cluster groups. List machines in cluster and view cluster and connection status.
clustercheck	Check configuration databases for inconsistencies and resolve them if necessary.

Message Filter conditions (See “ESA Advanced Guide” for more info + examples)	
subject	Tests subject against a RegExp.
body-size	Tests size of entire message in bytes.
mail-from	Tests envelope sender against a RegExp.
mail-from-group	Tests envelope sender against LDAP group.
sendergroup	Tests against a HAT sender-group name.
rcpt-to	Tests envelope recipients against a RegExp.
rcpt-to-group	Tests envelope recipients with LDAP group.
remote-ip	Tests client IP for exact or IP range match.
recv-int recv-listener	Matches mails received on the named interface/listener.
date	Tests current date against value in US date format: MM/DD/YYYY HH:MM:SS
header(<string>)	Tests the given header against a RegExp.
random(<integer>)	Compares a random integer to given value.
rcpt-count	Checks recipient count against value.
addr-count()	Compares recipient count from header (To: and/or Cc:) against value.
spf-status	Checks the SPF status.
spf-passed	Checks if SPF verification was successful.
image-verdict	Scans attached images for category match.
workqueue-count	Checks number of mails in the workqueue.
body-contains(<regexp>)	Checks mail and attachments for a RegExp.
only-body-contains(<regexp>)	Checks message body for a RegExp.
encrypted	Tests if a message is S/MIME or PGP encrypted.
attachment-filename	Tests a file name against a RegExp.
attachment-type	Checks for MIME file type by signature.
attachment-filetype	Matches a file type fingerprint (not MIME).
attachment-mimetype	Checks for MIME file type in

Message Filter actions (See "ESA Advanced Guide" for more info + examples)	
alt-src-host()	Deliver mail from this named interface.
alt-rcpt-to()	Change all recipients of a message.
alt-mailhost()	Deliver mail via alternate mail host.
notify() notify-copy()	Notify specified recipient about a message (and include a copy of the original message).
bcc() bcc-scan()	Send a copy of this message to a new recipient. Treat the copy like a new mail and scan again.
log-entry()	Add a log message at INFO level to mail logs.
quarantine(<name>)	Send this mail to the named quarantine.
archive(<filename>)	Save copy of the message in mbox format file.
duplicate-quarantine(<name>)	Send copy of this mail to the named quarantine.
strip-header()	Look for a header and remove it.
insert-header()	Insert a header and its value into the mail.
add-footer(<footer>)	Add the footer named <footer> to the mail.
bounce-profile()	Apply a bounce profile to the mail.
encrypt-deferred()	Encrypt message before final delivery.
tag-message(<name>)	Add tag <name> for RSA DLS policy filtering.
skip-filters()	Skip all remaining message filters.
skip-spamcheck()	Skip all anti spam checks for this mail.
skip-viruscheck()	Skip all anti virus checks for this mail.
skip-vofcheck()	Skip all outbreak filters for this mail.
drop-attachments-by-name()	Drop all attachments with matching filename.
drop-attachments-by-type()	Drop all attachments with matching MIME type.
drop-attachments-by-filetype()	Drop all attachments with matching file type determined by type fingerprint.
drop-attachments-by-mimetype()	Drop all attachments with matching MIME type. Does not match on extension or scan archives.
drop-attachments-by-size()	Drop attachment by examining raw size.
drop-attachments-where-	Drop attachments that match a

Message Filter example
drop_huge_presentations: if (mail-from-group == "Sales") AND (attachment-filename == "(?i)\\.(ppt|pptx)$") AND (attachment-size >= 10M) { drop-attachments-where-contains ("(?i)\\.(ppt\|pptx)$", "Large presentation dropped."); }