Hidden Gems in CA NetMaster for TCP/IP: Come Explore where You May Have Missed Them

Craig Guess
CA Technologies

August 13, 2015
Session 17790
Agenda

- WebCenter
- Traffic Stats vs /Perf
- Event Detectors
- SmartTrace
- Growth Tracker
- Creating Emails
- Performance Charts and Graphs
- Integration to OPS/MVS, SYSVIEW
WebCenter

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
WebCenter

- No need for external web servers
- Easily configured and instantly available (/PARM..Interfaces/WebCenter)
- Can be secured with AT-TLS if required
- Can control access to WebCenter menu options programmatically by using the variables in the CC2DEXEC($W3MH01X)
Flexibility

Complete your session evaluations online at...
Traffic Stats vs /Perf
Traffic Summary - /IPSUM

Real-time information

• Real-time information on everything NetMaster is monitoring
  – Provides a way to view lots of data at a glance.
**Performance Overview**

Longer periods of time

### CSNM9 Performance Overviews Menu

<table>
<thead>
<tr>
<th>Command</th>
<th>Scroll</th>
<th>CSR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Business Views**
- Business Applications
- Telnet Applications
- Address Spaces
- CSM

**Sessions and Connections**
- Stack IP Connections
- Home Addresses
- Network IP Connections
- Stack Telnet Connections
- Network Telnet Connections
- Stack FTP Connections
- FTP Users
- Network FTP Connections

**Protocols and Ports**
- Stack IP, TCP, and UDP Ports

**IP Networking**
- Stack IP, TCP, and UDP
- IP Nodes

**Logical Devices**
- Enterprise Extender
- Enterprise Extender Connections
- APPN/HPR
- VIPA

**Devices and Links**
- Stack Network Interfaces
- OSA Cards
- Cisco Channel Cards (not monitored)
- NCPS

---

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Performance Overview

Review up to 10 weeks of data

- Allows one to review Hourly, Daily and Weekly information
  - Weekly Interval List, can drill down to see Days and hourly

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Stack</th>
<th>Summary</th>
<th>Hour</th>
<th>Baseline</th>
<th>% Diff</th>
<th>Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConActive</td>
<td>TCP/IP11</td>
<td>16.2</td>
<td>12:00</td>
<td>10.3</td>
<td>+65%</td>
<td>12.2</td>
</tr>
<tr>
<td>ConBytes</td>
<td>TCP/IP11</td>
<td>17.9M</td>
<td>12:00</td>
<td>8.1M</td>
<td>+120%</td>
<td>367.4M</td>
</tr>
<tr>
<td>ConConnects</td>
<td>TCP/IP11</td>
<td>737.0</td>
<td>12:00</td>
<td>1.0K</td>
<td>-20%</td>
<td>2.4K</td>
</tr>
</tbody>
</table>

**END**
Event Detectors
### Sample Event Detectors supplied

<table>
<thead>
<tr>
<th>Field</th>
<th>Event Detector Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Value</td>
<td><strong>CCTN3270</strong></td>
<td>Cisco Channel TN3270 Log Messages</td>
</tr>
<tr>
<td></td>
<td><strong>CONNECT</strong></td>
<td>Connection Monitor</td>
</tr>
<tr>
<td></td>
<td><strong>CONNSTAT</strong></td>
<td>TCP Connection Status</td>
</tr>
<tr>
<td></td>
<td><strong>CONSOLE</strong></td>
<td>z/OS Console Messages</td>
</tr>
<tr>
<td></td>
<td><strong>CUSTOM</strong></td>
<td>Custom Event Detector</td>
</tr>
<tr>
<td></td>
<td><strong>FRAGMENT</strong></td>
<td>IP Packet Fragmentation</td>
</tr>
<tr>
<td></td>
<td><strong>FTPFAIL</strong></td>
<td>FTP Failures</td>
</tr>
<tr>
<td></td>
<td><strong>ICMP</strong></td>
<td>ICMP Message Monitor</td>
</tr>
<tr>
<td></td>
<td><strong>LINUX</strong></td>
<td>Linux Messages</td>
</tr>
<tr>
<td></td>
<td><strong>LISTENER</strong></td>
<td>IP Port Listener Monitor</td>
</tr>
<tr>
<td></td>
<td><strong>MOLISTEN</strong></td>
<td>TCP Conn Attempt Fail No Listener Port</td>
</tr>
<tr>
<td></td>
<td><strong>RTPrEDE5M</strong></td>
<td>APPM RTP Pipe ARBmode=RED &gt;5min</td>
</tr>
<tr>
<td></td>
<td><strong>SSLHFAIL</strong></td>
<td>SSL Handshake Failure</td>
</tr>
<tr>
<td></td>
<td><strong>SURRESET</strong></td>
<td>TCP Server Connection RESET</td>
</tr>
<tr>
<td></td>
<td><strong>SYSLOGD</strong></td>
<td>USS Syslog Daemon Messages</td>
</tr>
<tr>
<td></td>
<td><strong>TCPEND</strong></td>
<td>TCP Connection Ended</td>
</tr>
<tr>
<td></td>
<td><strong>TCPSTART</strong></td>
<td>TCP Connection Started</td>
</tr>
<tr>
<td></td>
<td><strong>UMEVENT</strong></td>
<td>VM Events</td>
</tr>
<tr>
<td></td>
<td><strong>UMMSG</strong></td>
<td>VM Messages</td>
</tr>
</tbody>
</table>

**END**
Event Detectors – proactive management

- **CONNSTAT** – Monitors number of connections with a client.
  - Insure minimum number of connections present, i.e., EE requirements.
- **SVRRESET** – Monitors TCP connections that are reset by server.
  - Alerts if client trying to connect but can’t, helps insure PCI compliancy.
- **SSLHFAIL** – Monitors Secure Sockets Layer (SSL) handshake failures
  - Many levels of SSL Handshake errors possible, helps eliminate wasted time in determining cause of failure.
- **TCPSTART** – Monitors client/server connections.
  - Restrict the detection to specified client-server connections
- **TCPEND** – Monitor connection end and reason codes
Event Detector
TCP Connection Status – (CONNSTAT)

- Detects when a server has 0 connections
  - When you have mission-critical connections to a z/OS IP application that must remain up 24 x 7.
  - You must maintain a certain number of connections to a z/OS IP application to provide the necessary health indication, traffic throughput, or volume.

<table>
<thead>
<tr>
<th>TCP/IP : TCP Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command ====&gt;</td>
</tr>
<tr>
<td>Function=Browse</td>
</tr>
<tr>
<td>Short Description ..... SAMPLE: Server has 0 connections</td>
</tr>
<tr>
<td>Status INACTIVE</td>
</tr>
<tr>
<td>Monitor TCP Connection Status for:</td>
</tr>
<tr>
<td>Stack Name .................. TCPIP99</td>
</tr>
<tr>
<td>Server Host ................. 123.123.123.123</td>
</tr>
<tr>
<td>Server Ports ................. 12345</td>
</tr>
<tr>
<td>Client Host .................. 234.234.234.234</td>
</tr>
<tr>
<td>Connections Active ......... 1</td>
</tr>
<tr>
<td>Auto Alert Clear? .......... NO</td>
</tr>
</tbody>
</table>

Create Alert:
Description &$IPSTDDESC
Severity ... 4

Initiate Actions:
**NONE**
Event Detector

TCP Server Reset – (SVRRESET)

- Detects when an established connection is reset
  - All server reset connection failures involving a specific application.

  - Any server reset connection failures and who they are most often happening to.

---

CSNM9---------------- TCP/IP : TCP Server Reset Detector
Command ===> Function=Browse

Short Description ..... SAMPLE: RST sent by server 12345 Status INACTIVE

Monitor TCP Server Resets for:
Server Host ............ 123.123.123.123
Server Port ............ 12345
Active Alert Limit .... 5

Create Alert:
Description &$IPSTDDESC
Severity ... 4

Initiate Actions:
**NONE**
**Event Detector**

**SSL Handshake failure** – (SSLHFAIL)

- Detects when SSL security negotiation fails
  - You need to be notified of all connection failures of a specific critical secure connection.
  - You need to be notified of all connection failures to a secure application.
  - You want to know of any SSL handshake problems and where they are occurring most often.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function=Update</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Short Description</strong></td>
<td>SAMPLE: SSL failure for a server</td>
</tr>
<tr>
<td><strong>Monitor SSL Handshake Failures for:</strong></td>
<td>(F4 to set)</td>
</tr>
<tr>
<td>Server Host</td>
<td>123.123.123.123</td>
</tr>
<tr>
<td>Server Port</td>
<td>12345</td>
</tr>
<tr>
<td>Active Alert Limit</td>
<td>5</td>
</tr>
</tbody>
</table>

Create Alert: (F5 to set)

- Description: &$IPSTDDESC
- Severity: 4

Initiate Actions: (F6 to set)

- **NONE**
Event Detector
Connection started – (TCPSTART)

- Detects when a connection has started for local/remote host or port
  - You need to be notified of all connections from a specific remote host, such as an external gateway.
  - You want to know of all connections to a restricted application and where they come from.
  - You want to know all connections between specific remote host and application.
  - You want to know any connection is not a secured connection.

```plaintext
CSNM9--------- TCP/IP : TCP Connection Started Detector ----------
Command ==> Function=Browse
Short Description ..... SAMPLE: A connection has started Status INACTIVE
Monitor TCP Connections Started For:
Server Host ............ 123.123.123.123
Server Port ............ 12345
Client Host ............ 234.234.234.234
Active Alert Limit .... 5

Create Alert:
Description &$IPSTDDESC
Severity ... 4

Initiate Actions:
**NONE**
```

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Event Detector
Connection ended – (TCPEND)

- Detects when a connection has ended and its details match a specified criteria.
  - You want to know all connection failures due to a specific reason code.
  - You need to know the reason for all connection terminations between specific partners.
## TCPEND – Reason Codes to select from

### Field: Reason Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Error occurred during a send using FRCA(AFPA), possibly because the stack is terminating</td>
</tr>
<tr>
<td>12</td>
<td>A persistent socket used by FRCA (AFPA) was closed by a FIN</td>
</tr>
<tr>
<td>21</td>
<td>The connection was terminated because the stack was terminating</td>
</tr>
<tr>
<td>22</td>
<td>Last stack that can own the dynamic VIPA bound to the socket is terminating</td>
</tr>
<tr>
<td>31</td>
<td>Intrusion detection found the connection to be malicious and closed the connection</td>
</tr>
<tr>
<td>32</td>
<td>Connection was denied because of a NetAccess rule</td>
</tr>
<tr>
<td>33</td>
<td>ACK received in lastack state</td>
</tr>
<tr>
<td>41</td>
<td>The connection was terminated because of an administrator action (for example, using Netstat DRop/-D command or the MNI API)</td>
</tr>
<tr>
<td>42</td>
<td>The connection was terminated because the local IP address bound by the application has been deleted from the stack</td>
</tr>
<tr>
<td>51</td>
<td>The connection from a client was terminated because the application closed the socket before performing an accept()</td>
</tr>
<tr>
<td>52</td>
<td>The application using the socket, closed the connection using a close()</td>
</tr>
<tr>
<td>53</td>
<td>A pascal routine issued an orderly close request</td>
</tr>
<tr>
<td>54</td>
<td>A pascal routine issued a disconnect</td>
</tr>
<tr>
<td>55</td>
<td>An error occurred during a pascal accept</td>
</tr>
<tr>
<td>61</td>
<td>The connection was terminated because the client sent a reset</td>
</tr>
<tr>
<td>71</td>
<td>The connection was closed because the same packet was being re-transmitted multiple times</td>
</tr>
<tr>
<td>72</td>
<td>The connection was closed because the TCP window the client was reduced to zero and multiple window probes were not acknowledged</td>
</tr>
<tr>
<td>73</td>
<td>The connection was closed because multiple keepalive probes were not acknowledged</td>
</tr>
<tr>
<td>74</td>
<td>The connection was terminated because the stack timed out waiting for a fin in the finwait-2 state</td>
</tr>
<tr>
<td>ANY</td>
<td>Any non-zero reason code</td>
</tr>
</tbody>
</table>

**END**

8/12/2015
SmartTrace Gems

Both Simple and advanced options use the same set of tools and interface for viewing the trace – no additional learning curve.

- **SAVE** – stored all traces in one repository (no additional dataset required).

- **PRINT** – a choice of printers or external data sets/HFS or even email.

- **EXPORT** – to 3rd party formats CTRACE (IBM only) and libpcap (distributed platform), collect the packets in SmartTrace and use your favourite packet viewer.
**SmartTrace Utilities**

- Easy to use interface and utilities for managing traces
  - SAVE, EXPORT, PRINT

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Add SmartTrace Definition</td>
</tr>
<tr>
<td>L</td>
<td>List All SmartTraces</td>
</tr>
<tr>
<td>LA</td>
<td>List Active and Ended SmartTraces</td>
</tr>
<tr>
<td>LS</td>
<td>List All Saved SmartTraces</td>
</tr>
<tr>
<td>EE</td>
<td>EE SmartTrace Menu</td>
</tr>
<tr>
<td>IM</td>
<td>Import libpcap Trace File</td>
</tr>
<tr>
<td>CT</td>
<td>Packet Tracing using Component Trace (CTRACE)</td>
</tr>
<tr>
<td>X</td>
<td>Exit</td>
</tr>
</tbody>
</table>

---

**TCP/IP : Packet Tracing Menu**

**TCP/IP : Packet List**

<table>
<thead>
<tr>
<th>Link Name</th>
<th>CSNM9</th>
</tr>
</thead>
</table>
Exporting Traces and Reports

Export Trace

Exporting Traces and Reports

Exporting Traces and Reports

Export Trace

Exporting Traces and Reports

Exporting Traces and Reports

Export Trace

Exporting Traces and Reports

Exporting Traces and Reports

Export Trace

Exporting Traces and Reports

Exporting Traces and Reports

Export Trace

Exporting Traces and Reports

Exporting Traces and Reports

Export Trace
Growth Tracker

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Growth Tracker

Out-of-the-box historical reporting on network activity

– IP Volumes, connections counts and connection durations are summed each day

– Stored indefinitely

– Multiple timeframes for reports supported
  – 14,30,60,90 day reports
  – 6, 12 and ALL month reports

– Provides meaningful insights into network activity

– Assists in network planning
Growth Tracker

- Records growth in total mainframe IP usage over time.
  - IP Volumes, connections counts and connection durations are summed each day - stored indefinitely.
Total IP, TCP and UDP traffic

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
TCP traffic by server
TCP connections by duration
total UDP traffic
Predicting Growth

Problem quotes

• “Our SNA sessions to DB2 haven’t changed much for years… but surely DB2 remote access is growing? If I can show that, I can get more resources for my DB2 group.”

• “Maybe the growth is with users coming in with TCP/IP?”

Use Growth Tracker

• Illustrate the increase over time in mainframe IP network activity
• Out-of-the-box tracking, no setup, no databases
• Connection and Traffic totals are kept indefinitely
IP Growth Tracker, TCP Traffic Growth

**CA31 TCP Traffic by Server Last 30 Days**

<table>
<thead>
<tr>
<th>Date</th>
<th>TCP Bytes (Total)</th>
<th>CICS</th>
<th>DB2</th>
<th>IMS</th>
<th>MQ</th>
<th>IBM Telnet</th>
<th>IBM Web</th>
<th>TCP (Other)</th>
<th>TCP Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 APR</td>
<td>4,390,539,717</td>
<td>0</td>
<td>119,860,682</td>
<td>0</td>
<td>0</td>
<td>725,826</td>
<td>135,771,444</td>
<td>4,134,181,765</td>
<td>245,126</td>
</tr>
<tr>
<td>5 APR</td>
<td>23,828</td>
<td>231,128,422</td>
<td>0</td>
<td>0</td>
<td>640,416,837</td>
<td>719,469,879</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>6 APR</td>
<td>56,014,335,211</td>
<td>167,864</td>
<td>275,604,934</td>
<td>0</td>
<td>148,229,496</td>
<td>362,247,365</td>
<td>2,722,615,492</td>
<td>52,505,470,060</td>
<td>394,942</td>
</tr>
<tr>
<td>7 APR</td>
<td>42,764,851,062</td>
<td>7,230</td>
<td>394,128,108</td>
<td>0</td>
<td>181,341,750</td>
<td>1,376,375,200</td>
<td>1,733,115,914</td>
<td>39,079,882,860</td>
<td>340,622</td>
</tr>
<tr>
<td>8 APR</td>
<td>21,442,093,761</td>
<td>546,862</td>
<td>459,633,662</td>
<td>0</td>
<td>33,099,406</td>
<td>94,920,342</td>
<td>93,672,059</td>
<td>20,760,221,430</td>
<td>284,298</td>
</tr>
<tr>
<td>9 APR</td>
<td>19,606,701,833</td>
<td>40,095,093</td>
<td>549,289,569</td>
<td>0</td>
<td>0</td>
<td>844,782,057</td>
<td>2,533,143,911</td>
<td>15,639,391,203</td>
<td>494,922</td>
</tr>
<tr>
<td>10 APR</td>
<td>534,175,687</td>
<td>0</td>
<td>197,727,488</td>
<td>0</td>
<td>0</td>
<td>41,769,322</td>
<td>1,558,254</td>
<td>293,120,623</td>
<td>124,117</td>
</tr>
<tr>
<td>11 APR</td>
<td>10,818,018,168</td>
<td>0</td>
<td>231,231,626</td>
<td>0</td>
<td>0</td>
<td>444,675,045</td>
<td>267,484,367</td>
<td>9,874,627,130</td>
<td>698,175</td>
</tr>
<tr>
<td>12 APR</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13 APR</td>
<td>154,652</td>
<td>268,154,796</td>
<td>0</td>
<td>0</td>
<td>131,598,424</td>
<td>9,267,433,937</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>14 APR</td>
<td>22,238,183,725</td>
<td>13,191</td>
<td>255,481,129</td>
<td>0</td>
<td>0</td>
<td>74,130,762</td>
<td>636,777,449</td>
<td>21,271,781,194</td>
<td>353,671</td>
</tr>
<tr>
<td>15 APR</td>
<td>2,291,443,756</td>
<td>4,766</td>
<td>5,667,095</td>
<td>0</td>
<td>0</td>
<td>6,894,687</td>
<td>34,501,362</td>
<td>2,244,375,843</td>
<td>62,774</td>
</tr>
<tr>
<td>16 APR</td>
<td>989,183</td>
<td>2</td>
<td>2,446</td>
<td>0</td>
<td>0</td>
<td>2,976</td>
<td>14,893</td>
<td>968,865</td>
<td>27</td>
</tr>
<tr>
<td>17 APR</td>
<td>46,904,192</td>
<td>0</td>
<td>18,051,507</td>
<td>0</td>
<td>0</td>
<td>8,011</td>
<td>2,736,515</td>
<td>26,108,159</td>
<td>2,506</td>
</tr>
</tbody>
</table>
Creating Emails

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Where to find it

NMMSC---------------- Administration : Primary Menu ----------------
Select Option ===> /aladmin_

A - Alert Monitor Administration ALADMIN
R - Resource Administration RADMIN
S - Service Administration SADMIN
E - Event Administration EADMIN
G - Graphical Monitor Administration GADMIN
M - Multi-System Support Administration MADMIN
IP - TCP/IP Administration IPADMIN
SN - SNA Administration SNADMIN
AS - Automation Services Administration ASADMIN
CS - CSN Administration
X - Exit

NMMSC---------------- Alert Monitor : Administration Menu ----------------
Select Option ===> 

I - Define Trouble Ticket Interface
D - Define Trouble Ticket Data Entry
F - Define Filters
L - Define List Formats
ST - Alert Monitor Self Test
X

CSNM9------------------------ CAS : Valid Value List ------------------------
Scroll ===> CSR

S/=/Select (one only)

Field: TroubleTicket I/Face

<table>
<thead>
<tr>
<th>Abbrev</th>
<th>Full Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>CUSTOM</td>
<td>User Supplied NCL Procedure</td>
</tr>
<tr>
<td>E</td>
<td>EMAIL</td>
<td>Use eMail to Request Trouble Ticket</td>
</tr>
<tr>
<td>NONE</td>
<td>NONE</td>
<td>Clear Trouble Ticket Interface Type</td>
</tr>
<tr>
<td>S</td>
<td>SERVICEDESK</td>
<td>Create CA Service Desk Request</td>
</tr>
<tr>
<td><strong>END</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Alert Monitor
Email Interface set up
Alert Monitor
Total parameters available

- **Parameters**
  - `$AMAPPLID` Application that created the alert
  - `$AMDESC` Alert short description
  - `$AMDATE` Date when the alert was generated
  - `$AMDAY` Day of the week when the alert was generated
  - `$AMGMTOFFSET` Local time difference from Greenwich Mean Time (UTC)
  - `$AMLASTDATE` Date when the alert last occurred
  - `$AMLASTTIME` Time when the alert last occurred
  - `$AMOCCURRED` Number of times the alert has occurred
  - `$AMSERIALNM` Software generated alert identifier
  - `$AMSEVERITY` Severity of the alert
  - `$AMSYSTEMID` System that created the alert
  - `$AMTEXT*` Alert text line * (1 through 5)
  - `$AMTIME` Time when the alert was generated
  - `$AMUPDDATE` Date when the alert was last updated
  - `$AMUPDTIME` Time when the alert was last updated
  - `$AMRECM*` Alert recommended action line * (1 through 20) when not retrieved from a CAS message
  - `$AMCLASSID` Class of the alert
  - `$AMCLOSDATE` Date when the alert was closed
  - `$AMCLOSTIME` Time when the alert was closed
  - `$AMRESOURCE` Resource name causing the alert
  - `$AMRESID` Resource name if a second one is needed
  - `$AMRESCLASS` The resource class
  - `$AMRESTYPE` The resource class type
  - `$AMELAPTIME` The amount of time (hh:mm) between when
&DOWHILE .&ADDR&CNT NE .
    &WRITE LOG=YES COLOR=YELLOW DATA=&0 Mail sent to &ADDR&CNT
    -$AMEMAIL ACTION=SENDMAIL +
    -* ADDRESS=&ADDR&CNT +
    ADDRESS=guecr01@ca.com +
    SMTPJOB=SMTP + " SMTP Jobname
    -* CLASS=X + " output class
    -* SMTPNODE=USILCA31 + " SMTPNODE
    -* HOSTNAME=TCP1P31.V.CA.COM + " hostname
    SMTPNODE=USILCA11 + " SMTPNODE
    HOSTNAME=USILCA11.CAI.COM + " hostname
    FROM=testmail + " FROM
    TYPE=IBM
    &CNT = &CNT + 1
&DOEND
&END
Via Process definition

```
 automation services: process definition

command ===>

process definition

system name ++$process version ++ 0001
name ........ email
description .. send email message to a person or a pager

process steps

<table>
<thead>
<tr>
<th>stepname</th>
<th>condition</th>
<th>macro</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>step/RC</td>
<td>opr rc</td>
<td>startncl</td>
</tr>
<tr>
<td><strong>end</strong></td>
<td></td>
<td></td>
<td>start an ncl procedure</td>
</tr>
</tbody>
</table>

---------- automation services: startncl macro parameter definition

command ===> function=updat

ncl procedure details

ncl name .... email
region ...... bsys (aomp, blog, bmon, bsys, cnmp, logp or ppop)
parameters .. group=&group subject="&subject"
             text1="&text1"
             text2="&text2"
             text3="&text3"

segment multi-word parameter variables ... no (yes or no)
```
Charts and Graphs

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Being truly mobile doesn’t mean being tied to one device.

Our solution works anywhere the user needs to be.
Mobility in the workplace

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Performance Charts for Networks

What it does

Mainframe server retrieves mainframe network performance data from NetMaster, then generates graphical mobile web pages to display it.

• Real-time IP network flow analysis data helps problem diagnosis, and shows network usage patterns of critical mainframe applications and servers.

• Historical high level TCP/IP network traffic growth data helps operational reviews and capacity planning.

What it looks like

Complete your session evaluations online at www.SHARE.org/2015
Performance Charts for Systems

What it does

Mainframe server retrieves performance data from SYSVIEW then generates graphical mobile web pages to display it.

- SYSVIEW reaches deep into the operating system to measure every aspect of system, user and resource activity.

What it looks like

Complete your session evaluations online at www.SHAI
/PARMS

CSNM9--------------------- Customizer : Parameter Groups ------------------------86
Command ==> Scroll ===> CSR

S/B=Browse U=Update H=Help L=ILog SD=Set Default

Category

Parameter | Group ID | Short Description
---|---|---
$NM SMF | $NM SOCKETS | TCP/IP Sockets Interface
$NM SSI | SOLVE Sub-System Interface
$RM SYSLOGD | SYSLOGD Message Interface
$NM TELNETSRVR | Telnet Server Controls
$RM UNICENTER | MSM Agent Specification
$NM WEBCENTER | WebCenter Web Interface
$RM WSPEER | Workstation Peer Specification
$RF XCAPI | CA-XCOM Interface

CSNM9--------------------- Customizer : Parameter Group ------------------------Page 1 of 2
Command ==>  Function=Browse

WEBCENTER - WebCenter Web Interface

Web Interface Port ............... 8086 (NONE, 1 to 65535)
Access URL ........................ http://141.202.65.11:8086
Access URL Host Override .........
User Timeout ...................... 02.00 (hh.mm)
Enable SYSVIEW Interface ........ YES (YES or NO)
Enable Public IP Pages ............ YES (YES or NO)

Performance Charts
Enable Performance Charts ...... YES (YES or NO)
Color Thresholds ................. Smallest Small Medium Large
- Active TCP Connections ....... 0 5 10 20
- I/Os Per Second ............... 0 100 1000 10000
Integration to other CA Products

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
NetMaster – CA APM Integration

- Provides metric feeds from CA NetMaster®
- Viewed via CA APM
  - APM dashboards
  - APM reports

CA NetMaster® r12.1 and CA APM on Linux or Windows

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
NetMaster – OPS/MVS Integration

Alert forwarding from OPS/MVS EMA

NetMaster Links enables all alerts to be seen and processed on every NetMaster

OPS/MVS EMA network using LU 6.2 & CCI

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Integration with other products

SysView Command entry

- Issue Sysview commands from WebCenter
Hidden Gems in CA NetMaster for TCP/IP: Come Explore where You May Have Missed Them

August 13th, 2015
Session 17790
Hidden Gems in *CA NetMaster for TCP/IP*: Come Explore where You May Have Missed Them

Craig Guess
CA Technologies

August 13, 2015
Session 17790