APM Troubleshooting Guide

Sergio Morales
Principal Support Engineer
CA Technologies
Morse06@ca.com

Last Updated: November 2014

Table of Contents

Useful Links

- CA APM Community:
[Home](#)
[Tuesday Tips](#)
[Product Enhancement Request](#), click Create an Idea

- Product:
[Compatibility Guides](#)
[Release and Support Announcements](#)
[Release and Support Lifecycle Dates](#)

- Service Pack readmes:
[9.5.6](#), [9.5.3](#), [9.5.5](#), [9.5.2](#), [9.5.1](#), [9.1.7](#), [9.1.6](#), [9.1.5](#), [9.1.4](#), [9.1.2](#), [9.1.1](#), [9.1.0](#), [9.0.8](#)

- Recommended readings:
[Top 20 Knowledge Documents for CEM](#)
[Top 20 Knowledge Documents for EM](#)

- Bookshelves:
[CA Application Performance Management 9.6 -US English](#)
[CA Application Performance Management 9.5 -US English](#)
[CA Application Performance Management 9.1 -US English](#)

- Technical Advisories:
[Critical Issues](#)

- APM KB Articles Report:
[Oct 2014 Report](#)

- Supportability:
[Use CA Remote Engineer to Gather Diagnostic Files for APM Products](#)

- Sustaining:
[Fix Strategy](#) , [Defect Resolution Policy](#)

- Services:
[Global Delivery Solutions](#)

- Technical Support
[Policy, Terms and Limitations](#)

article 5 – Technical Support Limitations: *"CA shall not be obligated to provide technical support for non-CA software, CA software that is not used in accordance with the product Documentation, modifications to the CA*

software, custom code provided by you or any third party or otherwise not part of the base CA software product functionality or problems associated with software products running on unsupported hardware, operating systems, or third party software"

Common Issues

TIM

Important reminders
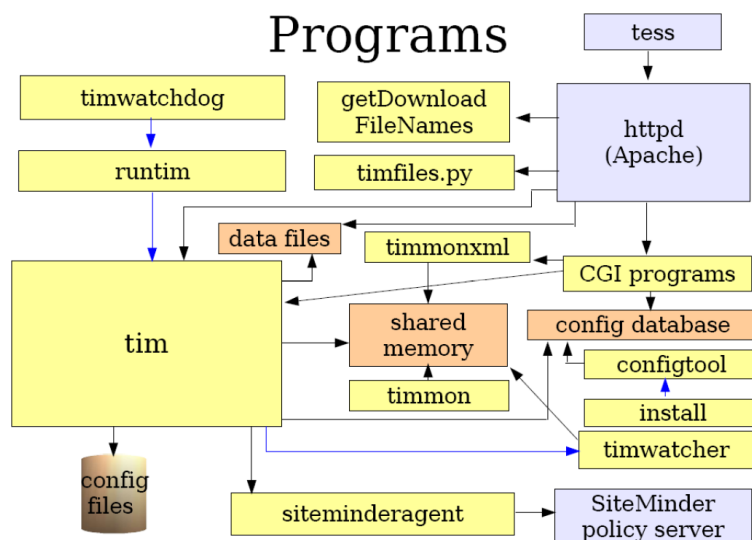
1. Architecture:
   a) TIM: monitors HTTP and HTTPS traffic. Information is kept into a shared memory segment and then saved in files:
      -Login, defects, events and recordings are saved every 5 seconds
      -Statistics are saved at the top of the hour
      Location: /etc/wily/cem/tim/data/out/: defects (include logins as well as defects), events, recordings and stats
   b) Timwatchdog: maintains the TIM process. If TIM crashes, Timwatchdog will restart it.
   c) Timwatcher: monitors TIM's memory size. NOTE: If TIM dies by unexpected OS signals before it writes the data files, data will be lost.
   d) Apache: handles request from TESS using one of the four methods, depending on the URL:
      -it calls getDownloadFileNames.py via CGI to get a list of available statistic files

         -it calls timfiles.py via mod_phyton to get the list of available defects, login, events and recording and then deletes these files

         -It gets events directly from the filesystem.

         -request to transfer TIM configurations

2. Limitation: DH Based Ciphers (DH/EDH – Diffie-Hellman) are not supported. DH is impossible to decipher when in passive mode.

3. TIM capacity factors:

   a. Environment factors:

   - Amount of data to monitor per unit time (throughput).

   - Quality of network packet delivery.

   - # of different monitored IPs

   - # of ports monitored

   - mix of HTTP and non-HTTP data

   - HTTPS vs HTTP traffic.

   - TIM device processing power

   b. Configuration factors:

   - # of defined transactions

   - Parsing complexity (transaction definitions): Excessive filtering and complexity of business Tx can have some impact. For example: complexity of business transaction definitions (reg expression matching). If possible avoid using "regular expression" for the pattern as it is very resource intensive.

   - Logging configuration

   - # of user/user groups definitions (dynamically discovered?)

   - # defects / rate

4. Best practices:

   - set web server filtering on TESS to reduce the traffic for each TIM

   - clean up outdated transaction definitions

   - avoid using the XML/SOAP, type component matching is still very CPU intensive for TIM. XML processing could tak up to 20% resources resulting in dropped packets

In 9.0:

TIM became a software appliance, customer buys hardware but we supply OS: Redhat 5.5 64bit only

TESS merged with Enterprise Manager

In 9.1.1:

The new option "Configure Tim Web Protect Options" was added to protect TIM webpages by requiring a web request ID. It is enabled by default. For example: http://timserver/cgi-bin/wily/packages/cem/tim/config/**protect?webRequestId=id_573033130394926393A35**

In 9.6:

- CA supply only TIM Software, customers need buys hardware and supported OS: Redhat 5.8 to 6.4 64bit Intel, same for CentOS.

- No more appliance web pages for web installer on TIM standalone only. In case of MTP, installation invoves 3 components that can be installed using the standard web installer (machine settings, MTP prerequisites, TIM image files)

- TESS not longer force synchronizes TIM machine time.

- TIM health page has been removed for both standalone TIM and MTP TIM.

- Support for SELinux, stand-alone and TIM doesn't support Napatech (restrictions due to Napatech software bundle)

TIM 9.6 installation issues

Checklist:

1.   Check that it is a supported OS.
NOTE: As of 9.6, if you have an OS issue, you need to contact Redhat. CA does not longer provide the license and support for the OS. We only support our TIM software running on the OS.

2.   Check that the required packages have been installed:
-If Redhat/CentOS 5.8, 5.9, run: yum install mod_ssl compat-libstdc++-33 pexpect unzip httpd nspr libpcap pstack mod_pyhton java-1.6.0-openjdk

```
[root@Taas Demo ~]yum install mod_ssl compat-libstdc++-33 pexpect unzip httpd nspr libpcap pstack mod_python java-1.6.0-openjdk
Loaded plugins: katello, product-id, security, subscription-manager
Updating certificate-based repositories.
Unable to read consumer identity
Excluding Packages in global exclude list
Finished
Setting up Install Process
Package 1:mod_ssl-2.2.3-63.el5.x86_64 already installed and latest version
Package compat-libstdc++-33-3.2.3-61.x86_64 already installed and latest version
Package pexpect-2.3-3.el5.noarch already installed and latest version
Package unzip-5.52-3.el5.x86_64 already installed and latest version
Package httpd-2.2.3-63.el5.x86_64 already installed and latest version
Package nspr-4.8.8-2.el5.x86_64 already installed and latest version
Package 14:libpcap-0.9.4-15.el5.x86_64 already installed and latest version
Package pstack-1.2-7.2.2.x86_64 already installed and latest version
Package mod_python-3.2.8-3.1.x86_64 already installed and latest version
Package 1:java-1.6.0-openjdk-1.6.0.0-1.24.1.10.4.el5.x86_64 already installed and latest version
Nothing to do
```

-If CentOS 6.0-6.4: mod_ssl, compat-libstdc++-33, pexpect, unzip, httpd, nspr, libpcap, gdb, mod_wsgi, java-1.7.0-openjk, policycoreutils-python

3. After installation, restart the apache server using: service httpd restart

What to collect:
1. result of rpm –qa
2. hostname –a
3. collect TIM log (/opt/CA/APM/tim/logs) and /tmp/configure-tim.log and /tmp/httpd.configtest

TIM is unable to see traffic or the right traffic

Checklist:

1. First, use a sniffer to verify that it can see the traffic. For example run: "tethereal -i eth1", "tshark –i eth1" or "tcpdump -i eth1 -s 5000 -w tcpdump.pcap". Make sure you see two-way traffic.

2. Go to the TESS UI:
- Select "Setup > Monitors", make sure the TIM(s) have been enabled and it is the correct IP/hostname
- Select "Setup > Web server filters", ensure the webserver filters are correct.

3. Go to the http://yourTIM
- Select "Configure Tim Network Interfaces", ensure that eth1 has been selected.

4. Go to http://yourTIM/cgi-bin/wily/packages/cem/tim/unsupported, select "View Tim Packet, CPU, and Memory Statistics (5 Seconds)." Check that TIM sees the traffic, "Packets Analyzed" should be > 0.
If you are using SSL:
-check for any possible SSL Decode failure or dropped packet. NOTE: Diffie-Hellman (DH or DHE) cypher is not supported.
-note that SSL decryption reduces TIM throughput by 50%
-make sure to use the correct private keys, ensure they have not expired and that they are in the right format.
-check that "Total SSL session" is higher than 0.

5. Go to the http://yourTIM
- Select "Configure Tim Trace Options.", enable "Trace HTTP components", try accessing a simple HTTP page as a test, go back to the TIM menu and select "View Tim log", search for words : "request", "response", "status=200", "443" and verify that the IP addresses are the ones you expect to see. For example:

Fri May 30 19:15:46 2014 21572 Trace: Component #48 request: 192.168.101.50/medrec/index.action client=[192.168.101.113]:58607 server=[192.168.101.50]:7011 at 19:15:46
Fri May 30 19:15:46 2014 21572 Trace: Full host: 192.168.101.50:7011
Fri May 30 19:15:46 2014 21572 Trace: Component #48 does not match a transet definition or an expected component
Fri May 30 19:15:46 2014 21572 Trace: Component #48 response header: status=200 at 19:15:46
Fri May 30 19:15:46 2014 21572 Trace: Component #48 response body at 19:15:46

What to collect:

1. Go to the TIM UI, select "Config Tim Settings", set MaxLogSizeInMB=100 (default log files are rotated very fast), put activity in the application
2. Go to the TIM UI, select "Collect Tim Log and Configuration files".
3. pcap file with network trace filtered on target host/IP address to verify the traffic:
        tcpdump -i eth1 -s 5000 -w tcpdump.pcap.
If you are using ssl, we need the output of ssldump. press Ctrl-C to terminate the ssldump command.
        ssldump -i eth1 -d -k yourkey.pem > output.txt 2>&1

TIM losing statistics data, TIM Restarts.

Checklist:

1. Has anything changed recently, such as adding a new application?

2. Go to the http://yourTIM
Select "View the Tim watchdog log" or open directly the /etc/wily/cem/tim/logs/watchdoglog file.
- If you see "tim exited with status 0", it means TIM stopped gracefully and the data in the memory has been saved before TIM stopped. Ensure TIM is currently up and running
- If you see "tim exited with signal N", it means TIM process stopped ungracefully by the OS signal N and data in the memory at the time is lost. Select "Configure Tim Watchdog Settings", increase "Number of TIM core dump files to keep" to 3.

3. Go to http://yourTIM/cgi-bin/wily/packages/cem/tim/unsupported, select "View Tim Packet, CPU, and Memory Statistics (5 Minutes)".

a) If you are using SSL:
-check for any possible SSL Decode failure or dropped packet. NOTE: Diffie-Hellman (DH or DHE) cypher is not supported.
-note that SSL decryption reduces TIM throughput by 50%
-make sure to use the correct private keys, ensure they have not expired and that they are in the right format.
-check that "Total SSL session" is higher than 0.

b) Make sure TIM is monitoring all the traffic, look at the "Packets Dropped" column, if necessary, add more web server filters to reduce the traffic. If the network has too much out-of-order packets, it will impact TIM's throughput.

c) If you see relatively Low throughput, lower than 100Mbps but a high TIM CPU usage, check if you have defined the port number for the web server filters. NOTE: Standard TIM cannot utilize multi CPU power. TIM will use its CPU to identify the HTTP protocol among the network stream if the web server filters do not have the port number defined.

d) If you see a high memory usage, open the /etc/wily/cem/tim/log/timwatcherlog, search for "killing tim process", check if timwatcher killed TIM because of a lack of memory, it is possible that TIM was handling too many defects/statistics. Go to TIM menu, select "Configure Tim Watchdog Settings", increase TIM memory.

4. There is known issue bug # 81254 - tim restarted when it processe invalid data. Fixed in 9.1.6 and 9.5.0

What to collect:

1. Go to the TIM UI, select "Collect Tim Log and Configuration files"
2. Collect core dump files

TIM – EM configuration error, 403 communication error

Checklist:

In the TIM:
- Select select "Config Tim Settings", make sure "TessCollectorIpAddr" (is the IP address of the TESS collector) and "TessIpAddr" (is the IP address of the MOM) have been set correctly.

In the CEM UI:
- Select "Setup > Services", ensure TESS services have been allocated to the correct servers, if not reconfigure it as appropriate.
- Select "Setup > Monitor" try removing and adding the TIM again.
- Ensure network configuration is correct in all MoM, Collector and TIM, review /etc/hosts in unix or C:\Windows\System32\drivers\etc\hosts that make sure IPs and hostnames are correct.
- In case of a cluster, check that the "entity.guid" in EM_HOME/config/internal/server/tess.internal.properties file is different on each of the Ems. If it is the same in one of the collectors, delete the tess.internal.properties file and restart the MoM and collectors.

- If pre 9.5, the problem could be related to bug 82776 - When "Tim collection service" is changed from one collector to another collector, the below error is displayed in the CEM ui: "Error: Switching services failed: old service did not stop"

What to collect:

1. Go to the TIM UI, select "Collect Tim Log and Configuration files"
2. Collect MOM_HOME\logs files
3. Screenshot of the error, if any.

MTP TIM

Important reminders

1. TIM can run on MTP appliance collector (CentOS 5.5) to take advantages of superior hardware. It is up to 6x time better than 9.0.5 and 4x better than 9.1 TIM on traditional hardware. MTP uses an optimized network card and hyper threading and provides a parallelization configuration mechanism for load balancing (balancer.cnf). Packet support is using capture cards from Napatech, supported configurations: 2x10 Gbps, 8x1 Gbps and 4x1 Gbps cards.
2. Architecture:
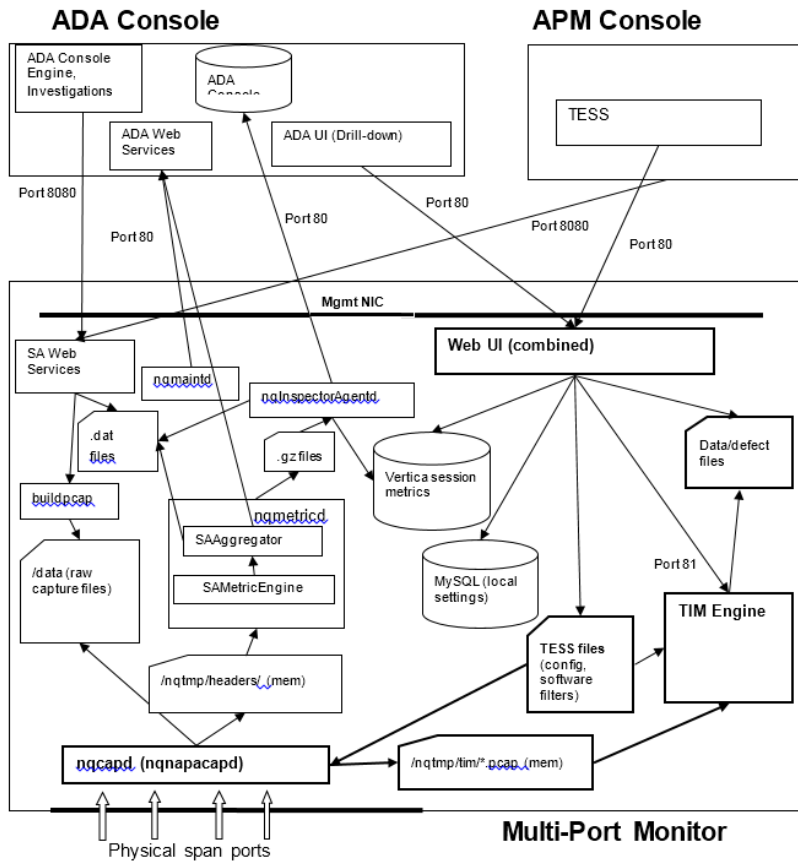
a) Span data from the Napatech card is processed by the nqncapd capture daemon.

b) Packet headers of all traffic are written to the /nqtmp/headers RAM disk for consumption by the nqmetricd process. In addition, full packets (but only those needed for TIM processing) are written to the /nqtmp/tim RAM disk for consumption by the TIM engine. File format of /nqtmp/tim is standard PCAP.

c) nqcapd will write out packets to /nqtmp/tim if packets meets following criteria:

- It is received on logical port for which TIM monitoring has been enabled. TIM is currently limited to only monitoring one logical port (feed).

- If any Web Server filters are configured in CEM console, it matches a Web Server filter definition.

Note: Matching the Web Server filters configured in CEM console is done by nqcapd and so requires more processing overhead.

d) The TIM engine periodically requests statistics from the nqcapd. The statistics are seen on the 'View Tim Packet Statistics pages within the TIM UI.

e) MTP provides also a web service for EM to request Network Health info for the "Defect Detail" page.

MTP-TIM installation, configuration issues, incorrect traffic.

Checklist:

1. Ensure installation is correct: upgrade MTP to v2.2, CentOS 5.5 and install on top ThirdParty and TIM software.

2. Go to the MTP
- Administration -> Data Collection > Logical Ports page and verify that TIM is monitoring only one logical port, If TIM data comes from multiple physical ports, map them to a single logical port. Click Filter, ensure "HTTP – Full Packets" is enabled.
- Administration > Maintenance > Processes page, restart nqcapd process
- System status page > capture card logical port statistics for traffic.

3. Go to TESS UI
- Setup > Web server filters - check the web server filters are correct
- Setup > Monitors - make sure the TIM has been added and MTP option has been enabled.

4. Follow same checklist as for TIM standalone

5. MTP does not support IPv6, note that you will not see any error/exception in the logs.

6. Go to MTP Analysis page: http://<MTP IP>/mtp/live/index.php, verify that the MTP machine can see the traffic between the client and app servers.

7. Check the below MTP/SA logs:
a) /opt/NetQoS/logs

b) Each daemon has log files (e.g. nqnapacapd_YYYYMMDD)
nqnapacapd_x.log – log file of nqcapd process, it logs several messages on start-up related to initializing the capture card and feeds including setting up filters. After that, every minute, it logs information on disk activity (number of files written, average size, some other disk performance stats), indicating the number of packets being written out for TIM:

08:42:52 TIM Feed=0 Packets: Captured=63103, Filtered-Color=59772, Filtered-WS=0,Forwarded=3331, Dropped-Card=0, Dropped-Disk=0, Dropped-Truncated=0, NoExtHdr=0

c) nqmaintd_x.log – log file of nqmaintd process; entries indicate when raw packets captures are being purged either routinely due to disk utilization usage or being over threshold. Also, it records any anomalies related to RAID or filesystem monitoring:
08:40:34 [Info]: /nqtmp/headers max hourly usage: 1% at 20111025-07:41:28
08:40:34 [Info]: /nqtmp/tim max hourly usage: 5% at 20111025-07:46:27

d) SAService_x.log – includes request from APM Console to retrieve network health statistics based on context from APM defect:
2011-10-27 13:40:15 GetTcpSessionData: id=600000000000000016, time=2011-10-27 14:39:01 for 916 seconds, feed=0, server=10.0.13.129:80, client=138.42.21.147, rc=0

What to collect:

1. Go to the TIM UI, select "Collect Tim Log and Configuration files"
2. Collect a PCAP from the MTP GUI > Analysis menu. The PCAP file might be too large to be opened in Wireshark, you can split the PCAP into separate files using SplitCap tool, then you can analyze it using Wireshark Expert Info for any of the following conditions as show in the screenshot : OOO packets, duplicate packets, retransmissions, etc.
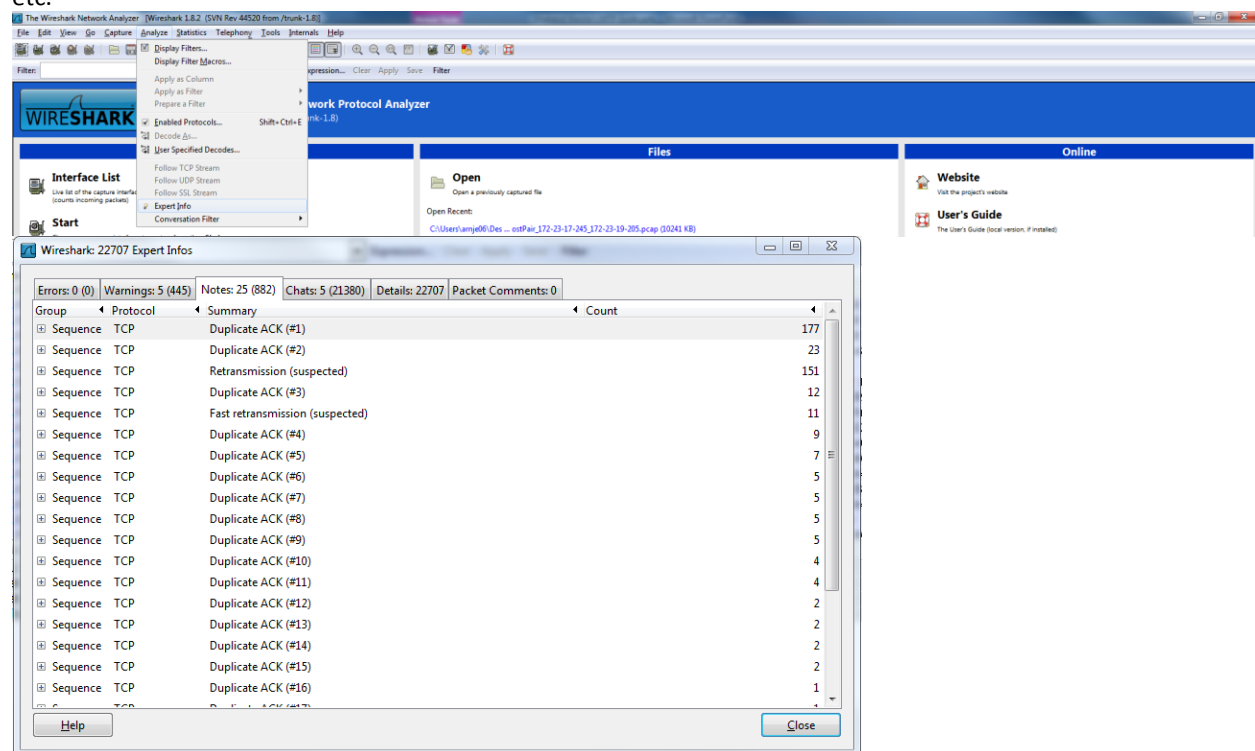
4. Go to the MTP server and collect:
- SAService_x.log
- nqnapacapd_x.log
- nqreport_x.log
- core files found in /nqxfs/corefiles
Output of "dmesg" - messages starting with 'ntki' are related to the Napatech driver
Output of "top"
Mcelog – will show if there is there is a memory problem

Output of "vmstat –s"
/var/log/messages
/var/log/httpd/access_log
/var/log/httpd/error_log

TESS

Important reminders
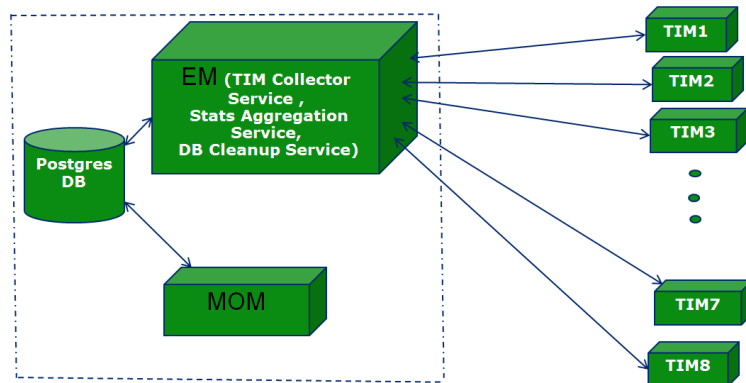
In 9.0:
1. TESS runs inside of the EM. The following services are available and each can run on a different EM collector:
a) Database cleanup service: responsible for removing the historical data based on retention settings defined in the Domain page.
b) TIM collection service (TCS): downloads and processes data collected by Tim
c) Stats aggregation service: aggregates Stats collected by Tim.

2. TIM Collection Service (TCS) poll tasks:
a) loginNameProcessor - see Login section
b) defect Processor - see Defects Section
d) statsCollector – see Statistics (Stats) section
e) event Processor (5 seconds interval): processes the event files and generates the respective events.
c) recordingProcessor: - see Recording using TIM section
f) timeSynchService: synchronizes its time with all enabled TIMs at EM startup and daily at 1:05 am. NOTE: Changing the system time or time zone in the middle of an aggregation process might corrupt aggregation statistics, duplicate aggregation statistics, or both.
g) BizEvent processor – see Incidents section.
h) btStats Processor - see Real Time Transaction Metrics (RTTM) section
i) autogenProcessor: see Automatic Transaction Discovery (ATD): useful when web-application changes frequently, it allows keeping Business Transaction definitions up to date. See Automatic Transaction Discovery (ATD) section

3. Added "Business Transaction recording by Agent": record transaction using Introscope Agents, see "Recording using Agents" section

Login

Important reminders

1. User Identification is the responsibility of TIM. TIM will identify the user and user groups according to the application configuration.
2. "TIM collection Service (Login processor)" retrieves the login files from TIM every 5 seconds; it manages the user and session correlation data.
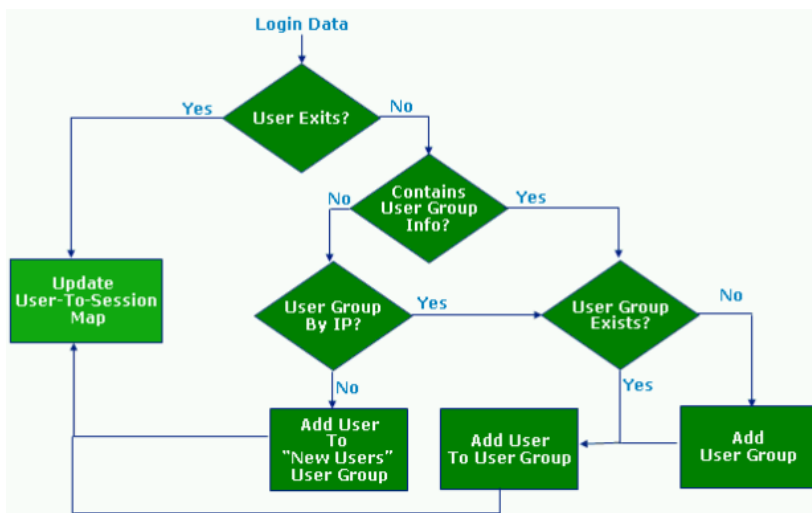
3. User groups:
   -A user can belong to only 1 group
   -Users can be grouped:
   a) manually
   b) by subnet: from the "Domain" page; it is only possible when the original IP and subnet are visible.
   c) by content within the request: from the "Business Application > User group identification" page (based on a URL string, HTTP header, WTG headers)

"Unspecified User, TIM is not identifying the user and session information"

Checklist:

In the CEM UI:
1. If the user session timeout is shorter than the Application's timeout, the defect and statistics will be associated with the "unspecified user". You should increase the session time-out from "Administration > Business Application > Your App > General".

2. Incorrect "User Identification" and/or "Session Identification". The combination of these 2 values will enable CEM to assign the correct user to each business transaction. You need to ensure these 2 values are correct.

In the TIM:
3. Go to the TIM, select "Configure Tim Trace options", enable "Trace sessions and logins" and review the Tim log.
- You should see entries like the one below when TIM is unable to identify user and sessions:
Trace: Component #46 request: no session id found for any appdef

- You should see messages like below when TIM successfully identifies the session, the trace will show the identified user and group:
Fri May 30 11:34:59 2014 21572   Trace: Component #33 request: session id for appdef 700000000000000000/"MedRec" is rRBpTLlcJcYv7N1Kt348YJt7qvJXzw12WQvTTJ3vN2Qb81Qhnns7!510215718
Fri May 30 11:34:59 2014 21572   Trace: TranSet #33: start TranSetDef=700000000000000000/"Login Prompt" at 11:34:59
Fri May 30 11:34:59 2014 21572   Trace: TranUnit #33: start TranUnitDef=700000000000000000/"Login Prompt" at 11:34:59
Fri May 30 11:34:59 2014 21572   Trace: TranComp #33: start TranCompDef=700000000000000000/"Login Prompt" at 11:34:59
Fri May 30 11:34:59 2014 21572   Trace: TranComp #33: TranSet=#33 TranUnit=#33
Fri May 30 11:34:59 2014 21572   Trace: Component #33: found login id "volley@ball.com"
Fri May 30 11:34:59 2014 21572   Trace: TranUnit #33: map login "volley@ball.com" to session "rRBpTLlcJcYv7N1Kt348YJt7qvJXzw12WQvTTJ3vN2Qb81Qhnns7!510215718" (new), user group ""
Fri May 30 11:34:59 2014 21572   Trace: TranComp #33: complete at 11:34:59

In the TIM Collector:
4. Open the TIM collector Server log, you should see entries like below that confirm that the login information has been collected successfully:
..
5/30/14 11:35:09.464 AM EDT [INFO] [TimPollThreadPool.Thread1]
[Manager.com.timestock.tess.services.tim.TimIo] File 'apmr5b3-login-14014641040000581896.xml-enc' read, length=624
5/30/14 11:35:09.692 AM EDT [INFO] [DefectLoginProcessingPool.Thread5]
[Manager.com.timestock.tess.util.DbUtils] Added user (id: 700000000000000004, app: 700000000000000000, login name: 'volley@ball.com', IP address: 192.168.101.113) to user group 'UserGroup-192.168.101.0'. …

What to collect:

1. Go to the TIM UI, select "Collect Tim Log and Configuration files"
2. Zipped content of the TIM_COLLECTOR_SERVER\logs

Defects

Important reminders

In 9.0:

1. "TIM collection Service" (Defect processor) retrieves the defects (xml files) from the TIM every 5 seconds and saves them in "ts_defects" table. NOTE: Defect polling interval is a configurable property, "tim.defectPollingInterval_Secs=" available in EM_HOME\config\tess-default.properties file

2. Defect processor manages the incident creation, Service Desk tickets and evidence collection.

3. Five minutes past each hour, defect process performs the hourly defects Aggregation of "ts_defect" rows and saves it into the "ts_defects_interval" tables.

4. When defect aggregation for an interval is already in progress or completed and a new defect(s) come for the same interval then "Defect Reaggregation" will happen to refresh the interval data.

5. Defects are purged based on the setting "Setup > Incident Settings > Delete defect after "

6. All reports running from "Analysis Graphs > Defects" page fetches data from the "ts_defect_interval" table.

7. Defects daily aggregations are stored in "ts_defects_YYYYMMDD" tables.

In 9.1:

8. No defects are purged from the "ts_defects" table until they are aggregated.

9. Performance improvement: by default defect aggregation runs on separate JVM, this behavior is controlled by the new property "defects.aggregateInSeparateJvm" in EM_HOME\config\tess-default.properties.

Bad rows error for defects, Aggregation failure, missing data in Analysis Graph defect CE reports and inability to view historical data

Checklist:

In the TIM:

1. TIM is responsible for the defect identification, Check that TIM is running and continuously monitoring the traffic – see "TIM losing statistics data, TIM Restarts."

2. Select "Configure Tim Trace Options.", enable "Trace HTTP components" and "Trace defects", ensure TIM is looking at the right traffic and that TIM is discovering the defects as expected. You should see an entry like below when TIM has detected a defect:

Fri May 30 11:35:09 2014 21572   Trace: TranSet #33: end size=3376, time=124, defects=1, total-defects=1 at 11:35:09

In the TIM Collector:

3. Review the TC logs, search for ERROR or WARN messages:

a) If defects have been collected and processed as expected you should see entries like below:

5/30/14 11:35:19.531 AM EDT [INFO] [TimPollThreadPool.Thread1] [Manager.com.timestock.tess.services.tim.TimIo] File 'apmr5b3-defect-14014641140000598108.xml' read, length=3810

5/30/14 11:35:19.542 AM EDT [DEBUG] [DefectLoginProcessingPool.Thread4] [Manager.com.timestock.tess.services.processors.DefectProcessor] Defect processing starting (1 defects, 1 details and 24 meta values) from monitor apmr5b3

5/30/14 11:35:19.923 AM EDT [DEBUG] [DefectLoginProcessingPool.Thread4] [Manager.com.timestock.tess.services.processors.DefectProcessor] Defect processing took 0.379 seconds (defects: 1, biz events: 1, users: -1)

b) If the hourly defect aggregation for the past hour completed correctly, you should see entries like below:
5/30/14 12:05:51.618 PM EDT [INFO] [Thread-142] [Manager.com.timestock.tess.services.scheduler.DefectAggregationTask] [main] [com.timestock.tess.services.scheduler.DefectAggregationTask] aggregating defects from 30-May-2014 11:00...
5/30/14 12:05:51.645 PM EDT [INFO] [Thread-142] [Manager.com.timestock.tess.services.scheduler.DefectAggregationTask] [main] [com.timestock.tess.services.scheduler.DefectAggregationTask] Aggregating 2 defects in interval from 30-May-2014 11:00 to 30-May-2014 11:59

..
5/30/14 12:05:51.952 PM EDT [INFO] [Thread-142] [Manager.com.timestock.tess.services.scheduler.DefectAggregationTask] [main] [com.timestock.tess.services.scheduler.DefectAggregationTask] 1 intervals processed; 2 rows added to ts_defects_interval

c) Ensure TIM Collector is running (there is a known issue bug#83999 with 9.5. Fixed in 9.5.1), in the logs you will see a message like:
[Manager.com.timestock.tess.services.service.CheckServices] Could not start service 'TIM.Collection.Svc' on entity 21: the service did not stop.
To solve the problem, run the below query and restart the collector:
UPDATE ts_entity_service SET ts_locked_by_entity=ts_entity_id WHERE ts_locked_by_entity='0';

4. Ensure APM db is accessible, search for JDBC errors in the EM log.

5. Default 128 MB for 'ThreadStackSize' could cause daily stats aggregation and defect aggregation not to start. In the TIM Collector log you might find messages like: "Bad rows processed" or "ERROR: relation ts_defects_yyyymmdd does not exist", this means that defects have not been aggregated, hence CEM reports will be empty. Open the TIM_COLLECTOR\config\tess-default.properties, increase XX:ThreadStackSize to 256 or higher value for both "defects.jvmArgs" and dailystats.jvmArgs properteis. You need to restart the TIM Collector service.

6. Check that hourly defect aggregation is up to date: after the hourly aggregation completes (10 minutes past the hour), the result of the sql "select max(ts_occur_date) from ts_defects_interval;" should be > than "select max(ts_occur_date) from ts_defects;". For example: 2014-05-30 20:59:59.999-04 > 2014-05-30 20:49:33-04

7. Starting from 9.1, for performance improvement, the defects aggregation process runs from a different JVM. Make sure to keep "defects.aggregateInSeparateJvm=true" in the tess-default.properties.

What to collect:

1. Go to the TIM UI, select "Collect Tim Log and Configuration files"
2. Zipped content of the TIM_COLLECTOR_SERVER\logs
3. apmdb backup: go to EM_HOME\install\database-scripts\windows (or Unix), run dbbackup-postgres.bat/sh [dbserverhostip] [dbinstalldir] [dbname] [dbuser] [dbpassword] [dbport] [dbbackupdir]". For example:
-If postgres,

(Win) dbbackup-postgres.bat 127.0.0.1 "C:\Program Files\CA APM\database" cemdb admin admin 5432

(Unix): dbbackup-postgres.sh 127.0.0.1 /opt/database cemdb admin admin 5432

-If Oracle, you need to use expd/impdp Oracle Tools, see "APM database" section.

Statistics (stats)

Important reminders
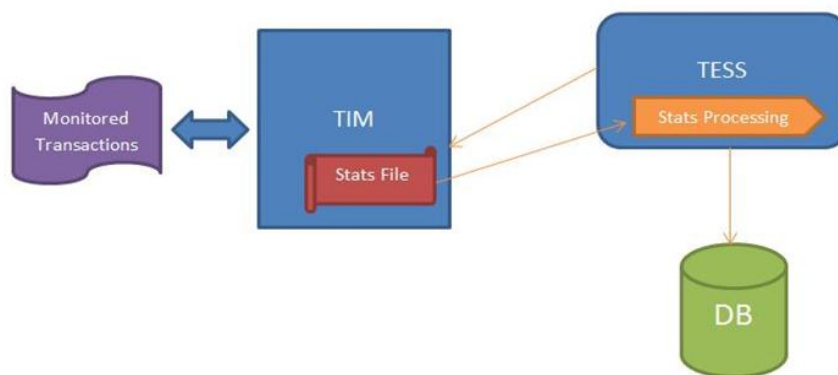
In 9.0:

1. "TIM collection Service" (Stats collector) downloads the statistics file generated by TIM (.stats) every hour and deletes them from the TIM.

2. The stats file is processed and data is inserted into base tables: TS_ST_'A'_'B'_INT_<year_month_day> where: A (TS=transet, TSGRP=transet group, TU=tranunit), B(ALL=All, US=User, USRGRP=Usergroup), INT=hourly

3. Hourly aggregation starts after stats file is downloaded from TIM. Data from base tables is distributed into hourly aggregated tables: TS_ST_'A'_'B'_INT.

4. Daily/Weekly/Monthly aggregations occur 3 minutes after midnight. Data from base tables are distributed into TS_ST_'A'_'B'_'C' tables. Where: C(DLY=daily, WLY=weekly, MLY=monthly).

5. Aggregations start from "Last Aggregated Row(LAR)" indicating when the last aggregation was executed. This column is updated in all INT, DLY, WLY and MLY tables after the aggregations complete.

6. All TS_ST_*_*_* tables are used to generate the SLA, Performance and Quality reports, where you can query for statistics by business transaction, transaction, usergroup or user and for specific timeframe (daily, weekly, etc)

7. Use the "Domain > Data Retention Settings" page, to configure how long the statistic data should be kept.

In 9.1:

8. Stats and Defects aggregation improvement: Stats Files are downloaded concurrently. In pre 9.1, these were downloaded 1 by 1 serially.

9. Performance improvement: Daily stats aggregation runs on a different JVM, this behavior is controlled by the new property "dailystats.aggregateInSeparateJvm=true" in tess-default.properties.

No data in Performance Report, No data from yesterday, Stats aggregation errors.

Checklist:

In the TIM:
1. TIM is responsible for the Stats generation, select "Configure Tim Trace options", enable "Trace statistics"; you should see entries like below when TIM is creating the hourly statistic files:

Fri May 30 12:00:00 2014 21572   StatsMgr: Next interval is May 30 13:00

Fri May 30 12:00:00 2014 21572   StatsMgr: Writing interval 53889CF0 - Fri May 30 11:00:00 2014

Fri May 30 12:00:00 2014 21572   StatsMgr: thread "stats 2014-05-30-15-00" is starting

Fri May 30 12:00:00 2014 21572   StatsMgr: writing stats to file /etc/wily/cem/tim/data/staging/stats/2014-05-30-15-00.1401462000.stats

Fri May 30 12:00:00 2014 21572   StatsMgr: sizeof PR_STATS_HISTOGRAM24 = 320.

Fri May 30 12:00:00 2014 21572   StatsMgr: sizeof PR_STATS_RECORD   = 1032 + variable-length part.

Fri May 30 12:00:00 2014 21572   StatsMgr: wrote stats to file /etc/wily/cem/tim/data/staging/stats/2014-05-30-15-00.1401462000.stats, size=1040

Fri May 30 12:00:00 2014 21572   StatsMgr: statistics records written: 1

Fri May 30 12:00:00 2014 21572   StatsMgr: renaming /etc/wily/cem/tim/data/staging/stats/2014-05-30-15-00.1401462000.stats to /etc/wily/cem/tim/data/out/stats/2014-05-30-15-00.1401462000.stats

Fri May 30 12:00:01 2014 21572   ThreadMgr: thread "stats 2014-05-30-15-00" has completed

2. Go to http://YourTIM/cgi-bin/wily/packages/cem/tim/unsupported, select "View the Tim getDownloadFileNames script log" or open the /etc/wily/cem/tim/logs/getDownloadFileNames.log file, you should see entries confirming that the above file has been downloaded.

In the TIM collector:
3. Go to the Setup > Services, Select "Stats Aggregatoin Service", ensure it is Up and running. Try to restart the TIM Collector server.

4. Review the TIM_COLLECTOR logs for possible WARN or ERROR messages:
a) Check that the hourly stats file has successfully been downloaded: you should see entries like below:

5/30/14 12:01:03.893 PM EDT [INFO] [StatsCollector.Thread1] [Manager.com.timestock.tess.services.collectors.StatsCollector] Downloading stats for 2014-05-30 11:00

5/30/14 12:01:03.934 PM EDT [INFO] [StatsCollectionPool.Thread1] [Manager.com.timestock.tess.services.collectors.StatsDownloadTask] Processing file 'apmr5b3-2014-05-30-15-00.1401462000.stats' from monitor 'apmr5b3' (192.168.101.14); length = 1040...

5/30/14 12:01:03.935 PM EDT [INFO] [StatsCollectionPool.Thread1] [Manager.com.timestock.tess.services.collectors.StatsDownloadTask] Processed 1 records in 0 secs

And, stats processed and saved into the db:

5/30/14 12:01:03.955 PM EDT [INFO] [StatsCollector.Thread1] [Manager.com.timestock.tess.services.processors.StatsProcessor] Inserting interval stats for 30-May-2014 11:00

5/30/14 12:01:06.842 PM EDT [INFO] [StatsCollector.Thread1] [Manager.com.timestock.tess.services.processors.StatsProcessor] Interval aggregation completed; 5 rows processed

5/30/14 12:01:06.843 PM EDT [INFO] [StatsCollector.Thread1]
[Manager.com.timestock.tess.services.processors.StatsProcessor] Statistics processing finished.

b) If you see the message "[Manager.com.timestock.tess.services.processors.StatsAggregator] Last hourly aggregation did not complete after xxx seconds. Daily aggregation will retry tomorrow" or "[Manager.com.timestock.tess.services.processors.StatsAggregator] Last hourly aggregation is still running. Waiting 120 secs before next check. Daily aggregation won't start before hourly aggregation is completed ", try to restart the TIM Collector.

c) Check how long the daily and hourly aggregations take, typically for 200K rows it should take no longer than 10 minutes. You can use the lines' timestamp to validate this condition.

d) If log indicates that EM is processing statistics records from a few days ago instead of yesterday's, daily aggregation is lagging, possibly due to the amount of data in the db (check the data retention settings), performance issue in the TIM collector or that TIM is processing too much defects/stats.

e) Default 128 MB for 'ThreadStackSize' could cause daily stats aggregation and defect aggregation not to start. In the TIM Collector log you might find the message: "[WARN] [DailyAggregation.Thread1] [Manager.com.timestock.tess.services.processors.StatsAggregator] Bad rows processed", it means that stats have not been aggregated and many of the CEM reports will be empty. Open the EM_HOME\config\tess-default.properties in TIM Collector, increase the value to 256 or a higher value.

5. Ensure APM db is accessible, search for JDBC errors

6. Daily Stats aggregation process is JVM heap intensive. Make sure you have allocated enough RAM for its JVM. Starting from 9.1, daily defects aggregation runs from a different JVM. Make sure to keep "dailystats.aggregateInSeparateJvm=true" in tess-default.properties.

What to collect:

1. Go the TIM, /etc/wily/cem/tim/data/out/stats, run ls -l command
2. Go to the TIM UI, select "Collect Tim Log and Configuration files"
3. Zipped content of the TIM_COLLECTOR_SERVER\logs
4. If postgres: POSTGRES_HOME\data\pg_log*
5. apmdb backup: go to EM_HOME\install\database-scripts\windows (or Unix), run dbbackup-postgres.bat/sh [dbserverhostip] [dbinstalldir] [dbname] [dbuser] [dbpassword] [dbport] [dbbackupdir]". For example:
-If postgres,
(Win) dbbackup-postgres.bat 127.0.0.1 "C:\Program Files\CA APM\database" cemdb admin admin 5432
(Unix): dbbackup-postgres.sh 127.0.0.1 /opt/database cemdb admin admin 5432
-If Oracle, you need to use expd/impdp Oracle Tools, see "APM database" section.

Incidents

Important reminders

1. "TIM collection Service" (BizEvent processor) generates the incidents based on the rules set by the user in the CEM UI > Setup > Incident Settings page. BizEvent processor starts every 5 minutes. In the TCS log you will find the below entries:

[INFO] [ServicesCheck.Thread1] [Manager.com.timestock.tess.services.processors.BizEventProcessor] IncidentProcessor started

[INFO] [Thread-40] [Manager.com.timestock.tess.services.processors.BizEventProcessor] IncidentProcessorThread starting

[INFO] [Thread-40] [Manager.com.timestock.tess.services.processors.BizEventProcessor] Checking Pending Incidents

2. The creation of an incident triggers evidence collection script(s) and/or send an email notification.
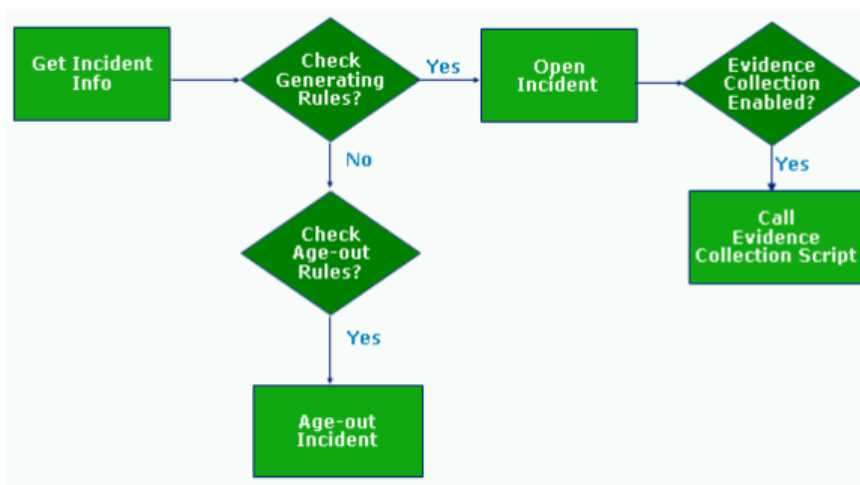
Incidents are not being created

Checklist:

In CEM UI
1. Go to Setup > Incident Settings > Ensure the Incidents settings are correct. For testing purpose, you could try to set "Generate an incident if number of defects per Evaluation Interval is equal or greather than" = 1 and reduce the "Impact settings" too 100, 250 and 500 respectively.
2. Check that "TIM Collection service" is collecting and processing all defects from the TIMs as expected, see "Defects" section.
3. Review the TIM collector logs; you should see an entry like below when an incident is created:
5/30/14 11:35:32.271 AM EDT [DEBUG] [pool-13-thread-1]

[Manager.com.wily.apm.tess.isengard.CEMIncidentPublisher] Sending 1 INCIDENT_CHANGED messages to the MOM using reverse proxy.

What to collect:

1. Go to the TIM UI, select "Collect Tim Log and Configuration files"
2. Zipped content of the TIM_COLLECTOR_SERVER\logs
3. apmdb export, go to EM_HOME\install\database-scripts\windows (or Unix), run configexport.sh/bat [dbhostIP] [dbname] [dbuser] [dbpassword] [dbport] [dbtype] [datafile]. For example:
-If postgres => configexport.bat/sh 127.0.0.1 cemdb admin admin 5432 Postgres apmdbmyexport.xml
-If oracle => configexport.bat.sh 127.0.0.1 cemdb admin admin 1521 Oracle apmdbmyexport.xml

Real Time Transaction Metrics (RTTM), BTstats, Customer Experience (CE) Metrics

Important Reminders

1. On 7 seconds intervals, TIM collects and aggregates metrics (counts and average) of the business transactions, regardless of whether a defect is detected for it or not and stores the metrics in a BTStats xml, for example: For example: /wily/cem/tim/data/out/btstats/btstats-yyyy-mm-dd-hh:mm:ss.xml There will only be a single entry in the BTStats for a business transaction, regardless of how many times it occurred during that 7 second interval.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<BTStats host="apmr5b3" timestamp="1401482018" version="2">
    <BTlist>
        <BT name="View Profile" maxTime="174" minTime="174" defectCount="1" availabilityDefectiveCount="0" performanceDefectiveCount="1" count="1"
            avgTime="174" id="700000000000000004">
            <Defect count="1" id="700000000000000084" type="1"/>
        </BT>
    </BTlist>
</BTStats>
```

2. "TIM Collection Service > RTTM Service" downloads the BTstats file from TIMs every 7 seconds. This interval is configurable from the EM_HOME\config\tess-default.properties, tim.btStatsPollingInterval_Secs.

3. Collected information is aggregated using Introscope calculators (scripts/BtStats-DefectPercent.js and /scripts/BtStats-AggregatedTree.js) and generated metrics saved in the Smartstor db.

4. RTTM metrics are available from:
a) Investigator, under "<YourTIMCollector>|CEM|TESS Agent|Business Service|..|Business Transaction|…".
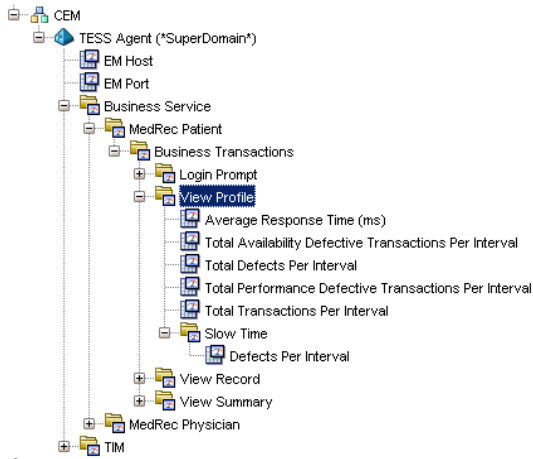
b) Starting from 9.1, RTTM metrics are available from the TriageMap:
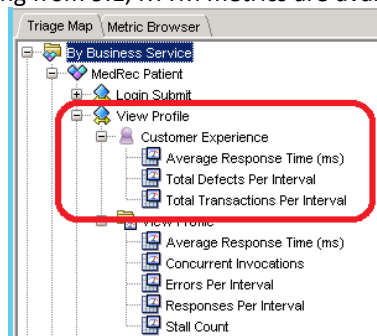
5. You can stop RTTM/Btstats metrics generation and collection from both TIM and TESS UI:
-From TIM, select "Configure Tim Settings", edit BtStats/Enabled, rename it to BtStats/ForceDisabled.
-From CEM UI > Setup > Services > TIM Collection Services > RTTM Collection Service, stop the service.

No TESS Agent, Missing MTTR/BTStats/Customer Experience (CE) metrics.

Checklist:

In the TIM:
1. Check that TIM is running and continuously monitoring the traffic – see "TIM losing statistics data, TIM Restarts."

2. Check the TIM logs and verify that Business Transactions are being monitored as expected. Remember, RTTM/CE metrics are generated from business transaction activity that TIM detects, regardless of whether a defect is detected for it or not.

3. Go to <tm>/cgi-bin/wily/packages/cem/tim/unsupported, select "View the Tim timfiles activity log" or open /etc/wily/cem/tim/logs/timfiles/timfileslog, search for "btstats" to confirm that TIM is collecting and creating the RTTM files and TIM Collector is downloading this information:
Fri May 30 11:35:23 2014 192.168.101.114 listBTstats None OK /wily/cem/tim/data/out/btstats/btstats-2014-05-30-15:35:02.xml,/wily/cem/tim/data/out/btstats/btstats-2014-05-30-15:35:23.xml

In the TIM Collector:

4. Open the TIM Collector log, search for "BtStats", you should see entries like below that confirm that TIM is collecting and processing RTTM files as expected:

5/30/14 11:35:24.049 AM EDT [DEBUG] [TimPollThreadPool.Thread2] [Manager.com.timestock.tess.services.tim.TimIo] Processing 2 files from 192.168.101.14 using http://192.168.101.14/wily/cem/tim/mod_python/timfiles/listBTstats
5/30/14 11:35:24.055 AM EDT [INFO] [TimPollThreadPool.Thread2] [Manager.com.timestock.tess.services.tim.TimIo] File 'apmr5b3-btstats-2014-05-30-15:35:02.xml' read, length=384
..
5/30/14 11:35:44.103 AM EDT [WARN] [BtstatsProcessingPool.Thread2] [Manager.com.timestock.tess.services.processors.BtStatsProcessor] BtStats processing took 20.022 seconds (1 records)

In the CEM UI:

5. Go to "Setup > Monitors", make sure TIMs are synchronized. If possible, try to restart the TIM.

6. Go to the "Setup > Services > Service Configuration", select TIM Collection Service and ensure that "RTTM Collection Service" is running. Try to restart the TIM collector Service.

What to collect:

1. Go to the TIM UI, select "Collect Tim Log and Configuration files"
2. Zipped content of the TIM_COLLECTOR_SERVER\logs

Transaction Discovery (ATD)

Important reminders

In 9.0:
1. "Transaction Discovery Collection" Service (Autogen processor) collects and processes the transaction discovery files generated by TIM on a 5 seconds interval. This feature allows creating business transaction based on actual user transactions with minimal configuration.
2. RegEx cannot be used in the URL path filter of the ATD template, you can specify only *
3. Ensure the Path parameter separator is set to the correct character. If a path parameter separator is specified, everything after the separator character is replaced with a *. For example, if the separator is ";" and the observed path is /login;SessionId=f03z4622;lang-en then TIM reports "/login*" as the URL path. If no path is set, then a new transaction is discovered for each unique session ID.
4. Do not leave this feature turned on as it will cause an overhead on the EM TIM collection server.

In 9.1:
5. TCAP: You can identify transactions based on HTTP Response and Flex in addition to HTTP Request: a) HTML response header and body, b) HTML response tag ("content type filter" must be text/html) and c) Flex request and response ("content type filter" must be application/xml, application/x-amf)

Transactions are not being discovered

Checklist:

In the TESS UI:
1. Go to the TESS UI > Transaction Discovery tab:
- Check that a template has been created and enabled
- Check that Service is running
- For testing purposes, in the Transaction Template, try setting URL Path Filter=/*

In the TIM:
1. Check that TIM is running and continuously monitoring the traffic – see "TIM losing statistics data, TIM Restarts."

2. Go to http://YourTIM, select "Configure Tim Trace Options." enable "Trace HTTP components", put activity on your application again. NOTE: No transaction will be discovered if there is already a Transaction that has the same parameters.

3. Open the TIM log, search for "autogen".
-If the template has not been created or enabled, you will see the below warning:
Fri May 30 22:20:14 2014 21572 ! **Warning:** AutogenConfig: autogen is enbled but there are no templates

-You should see entries like below when Transaction Discovery's definitions have been received by TIM. You then need to validate a possible match, search for "Trace:"
Fri May 30 22:30:10 2014 21572   ConfigFile: writing configuration file
/etc/wily/cem/tim/config/autogenconfig.xml
Fri May 30 22:30:10 2014 21572   ConfigFile: reading configuration file
/etc/wily/cem/tim/config/autogenconfig.xml
Fri May 30 22:30:10 2014 21572   AutogenConfig: New configuration
Fri May 30 22:30:10 2014 21572   AutogenConfig: Enabled: 1
Fri May 30 22:30:10 2014 21572   AutogenConfig: Url Monitoring Enabled: 0
Fri May 30 22:30:10 2014 21572   AutogenConfig: Main components without extensions allowed: 1
Fri May 30 22:30:10 2014 21572   AutogenConfig: Main components extensions: ".asp .htm .html .jsp .php .swe
.fcc .dll .shtml .do .aspx .asmx "
Fri May 30 22:30:10 2014 21572   AutogenConfig: Path parameter delimiter: "(none)"
Fri May 30 22:30:10 2014 21572   AutogenConfig: Template 600000000000000000 "ATD Patient"
Fri May 30 22:30:10 2014 21572   AutogenConfig: app: 700000000000000000 "MedRec"
Fri May 30 22:30:10 2014 21572   AutogenConfig: URL path filter: "/medrec/patient/*"
Fri May 30 22:30:10 2014 21572   AutogenConfig: Content-type filter: "text/html"
Fri May 30 22:30:10 2014 21572   AutogenConfig: Param[0]: type=Url op=Pattern required=0
nametype=ExactMatch name="Port" value="7011"
.

In the TIM Collector:
4. You should see entries like below when a transaction was discovered by TIM and the file successfully processed by the TIM collector:
5/30/14 11:03:35.487 PM EDT [DEBUG] [TimPollThreadPool.Thread7]
[Manager.com.timestock.tess.services.tim.TimIo] Processing 1 files from 192.168.101.14 using
http://192.168.101.14/wily/cem/tim/mod_python/timfiles/listAutogen

5/30/14 11:03:35.512 PM EDT [INFO] [TimPollThreadPool.Thread7]
[Manager.com.timestock.tess.services.tim.TimIo] File 'apmr5b3-autogen-14015054100000695179.xml' read, length=3024
5/30/14 11:03:35.520 PM EDT [DEBUG] [AutogenProcessingPool.Thread2]
[Manager.com.timestock.tess.services.processors.AutogenProcessor] Autogen processing starting of 1 records from monitor apmr5b3
5/30/14 11:03:35.842 PM EDT [DEBUG] [AutogenProcessingPool.Thread2]
[Manager.com.timestock.tess.services.processors.AutogenProcessor] Transaction definition processing took 0.321 seconds (1 records)

5. If not all non-identifying components are discovered, try to clear the browser cache.
6. For HTML, set content type filter equal "text/html" and for Flex, equal "application/xml, application/x-amf"

What to collect:

1. Go to the TIM UI, select "Collect Tim Log and Configuration files"
2. Zipped content of the TIM_COLLECTOR_SERVER\logs

Recording using TIM

Important reminders

In 9.0:
1. "TIM collection Service" (Recording processor) processes the http transaction recording session files generated by TIM on a 5 seconds interval.

In 9.1:
2. New "Content Types" section: users can provide the trusted content-type list in the UI dynamically. In pre 9.1, one needed to manually update "recorder.mainComponentTrustedContentTypes" in tess-default.properties.
3. "Move as component of" list box option: allows moving a recorded transaction across components and transactions sections. In pre 9.1, incorrect pages (i.e.: .gif) could appear as a main transactions incorrectly
4. "Unrecognized transactions" section: transactions that don't match the "content-type" filter or that doesn't belong to any of the recorded main transactions, will appear under this new section. In pre 9.1, this was never displayed.
5. TCAP: Be able to identify transaction based on HTTP response and Flex.

Recording by TIM doesn't work.

Checklist:

1. Check that TIM is running and continuously monitoring the traffic – see "TIM is unable to see the traffic".
2. Go to the TESS UI, select "Setup > Web server filters", ensure the webserver filters are correct.

What to collect:

1. Go to the TIM UI, select "Collect Tim Log and Configuration files"

Recording using Agents

Important reminders

In 9.0:
New "Recording by Agent" feature: mainly for Introscope only deployment, capabilities are similar to the TIM agent. An agent tracer extension and bizrecording.pbd have been created to allow the agent to do a recording, it inspects the HTTP parameters.
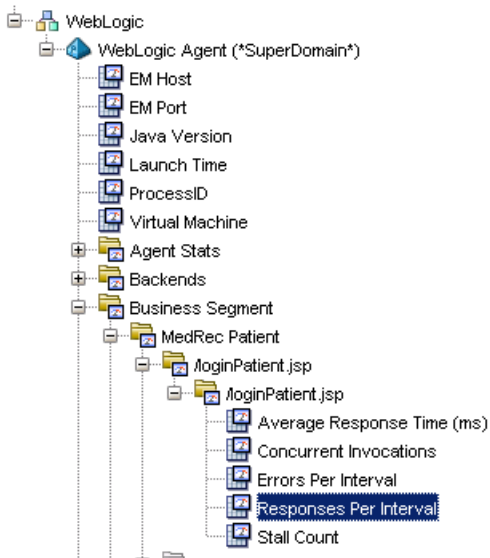
Recording by Agent doesn't work

Checklist:

1. Make sure the bizrecording.pbd is uncommented on the agent typical/full pbl. It is commented out by default. You have restarted the jvm/agent

2. For deployment with Proxy enabled, use Proxy IP as the client IP address for Agent recording.

3. Avoid using ".*" for the agent filter during the recording, as "Recording by Agent" adds a significant overhead on the agent side.

4. For some appservers when inspecting Servlet "Post parameters" it can break the application. To prevent this situation, enable "introscope.agent.bizdef.matchPost = after" in the IntroscopeAgent.profile.

5. If recording is not working, enable DEBUG on the Agent side. You should see entries like below if the URL matches the Recording definitions:

5/31/14 12:13:00 AM EDT [DEBUG] [IntroscopeAgent.Agent] BizRecording component recorded
Name=/patient/viewLoginResult.jsp
Path=/medrec
Date=1401509580218
Address=192.168.101.50
Port=7011
RequestHeader=
POST /medrec/loginPatient.action HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://192.168.101.50:7011/medrec/loginPatient.action
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: 192.168.101.50:7011
Content-Length: 185
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: JSESSIONID=vDdlTJWNf9ZLGbvMvQ03ZVWSK1nlyN77FDNdDQhT0ypB1TQ0Ryhn!726099637

RequestBody=j_id_id3=j_id_id3&j_id_id3:passwordInput=weblogic&j_id_id3:usernameInput=larry@bball.com&j_id_id3:j_id_id19=Submit&javax.faces.ViewState=-576488750838120424:-6115354563459704268
ResponseHeader=
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Expires: Fri, 13 Nov 1981 13:10:00 GMT
Content-Type: text/html; charset=UTF-8
X-Powered-By: JSF/1.2
Cache-Control: no-cache
Cache-Control: must-revalidate
Pragma: no-cache

ResponseBody=null

What to collect:

1. Agent DEBUG logs
2. IntroscopeAgent.profile
3. Application server logs
4. Application server startup script or configuration file.
5. Exact version of the Appserver and JVM version.
6. In case of missing metrics or discrepancy: screenshot from Investigator displaying the Agent | Business Segment node.

CEM to Introscope – Problem Resolution Triage

Important Reminders

1. CE transaction definitions (domainconfig.xml) are sent to the Agents whenever the agents start up or monitors are synchronized. These rules are kept by the Agent in memory and are used to recognize business transactions activity.
2. The agent adds additional performance monitoring information to HTTP response headers (GUID); this enables the correlation of transactions between Wily CEM and Wily Introscope.
3. When the same http request reaches TIM, it adds the CorID and servlet info to the defect.

Transaction Traces are not being generated, missing Introscope link

Checklist:

1. There is a known issue where due to synchronization issue, the agent fails to download Business transaction definitions. Restart the MOM or the specific affected agent.

2. Go to the TESS UI:
- Verify that Business Transactions defintions are correct and being monitored
- Ensure monitors are synchronized.

3. Go to the Agent, ensure that introscope.agent.decorator.enabled=true in the IntroscopeAgent.profile and ServletHeaderDecorator.pbd (java) or/and httpheaderdecorator.pbd (.net) have been enabled in the application typical/full pbl.

4. Go to the TIM, Select "Configure Tim Trace Options.", enable "Trace HTTP components", try accessing to the application, go back to the TIM menu and select "View Tim log", verify that x-wily-info and x-wily-servlet are present: this means that transactions match the definition rules in both TIM and Agent. Take a note of the "guid".
Sat May 31 06:04:07 2014 26709 Trace: Param: Url   Req Port = 7011.
Sat May 31 06:04:07 2014 26709 Trace: Param: Url   Req ClientIP = 192.168.101.113.
Sat May 31 06:04:07 2014 26709 Trace: Param: Url   Req Path = /medrec/loginPatient.action.
..
Sat May 31 06:04:07 2014 26709 Trace: TranSet #24: start TranSetDef=700000000000000003/"Login Submit" at 06:04:07
Sat May 31 06:04:07 2014 26709 Trace: TranUnit #24: start TranUnitDef=700000000000000003/"Login Submit" at 06:04:07
Sat May 31 06:04:07 2014 26709 Trace: TranComp #24: start TranCompDef=700000000000000005/"Login Submit" at 06:04:07
..
Sat May 31 06:04:12 2014 26709 Trace: Param: RespHeader Resp x-wily-servlet = Clear
appServerIp=192.168.101.50&agentName=WebLogic+Agent&servletName=FacesServlet&agentHost=apmw3a4&agentProcess=WebLogic.
..
Sat May 31 06:04:12 2014 26709 Trace: Param: RespHeader Resp x-wily-info = Clear guid=51BC885FC0A8653200758711E3889482.

5. Go to the defectlist.html page >Introscope view: http://YourTESS/wily/cem/tess/app/biz/defectList.html, you should find a "Slow defect" with the above "guid" under the "Request ID" column.

Date and Time	Business Service	Business Transaction	Defect Name	Web Server IP Address	Web Server MAC Address	Application Server ID	Virtual Machine ID	Request Handler ID	Request ID	Transaction Trace
May 31, 2014 6:04:13 AM EDT	MedRec Patient	Login Submit	Slow Time	192.168.101.50	00:50:56:9C:22:E6	192.168.101.50	WebLogic Agent	FacesServlet	51BC885FC0A8653200758711E3889482	No

If "Transaction Trace" column is = "NO", the integration is working but no incident has been opened yet. If there was an incident, open it and check if the transaction tracer is running. If not running, click the "Start Transaction Tracer" button. You can confirm that the transaction is running from the Transaction Tracer Session page: http://YourTESS/wily/cem/tess/app/admin/introscopeEmTranTraceList.html.

NOTE: If an incident has already been opened before the Introscope Integration has been enabled, the Introscope link and "Start Transaction Trace" button in the incident page will not be present. You need to close that incident; all new incidents will include the correct Introscope link.

6. CEM trigger a transaction trace session only for "Slow Time" defects, when an incident has been opened and when the request took longer than the transaction trace threshold defined in the "Setup > Introscope Settings" page.   CEM has access to a special transaction trace method that traces by Business Transaction AND time threshold.

In the TIM Collector log, you should see entries as below:
5/31/14 09:40:41.458 AM EDT [INFO] [DefectLoginProcessingPool.Thread4] [Manager.com.wily.apm.tess.isengard.BizEventTransactionTraceService] Directing the MOM to start transaction trace session for Business Transaction 10
5/31/14 09:40:41.575 AM EDT [INFO] [PO:main Mailman 3] [Manager.TransactionTracer] Started transaction trace for transactions: exceeding 2 milliseconds and with CEM Business Transaction that equals Login Submit

In the Agent log, you should see entries as below:
5/31/14 09:40:43 AM EDT [DEBUG] [IntroscopeAgent.Agent] addEMFilter: {[threshold = 2ms] AND [businesstransactionname = Login Submit]}
5/31/14 09:40:46 AM EDT [VERBOSE] [IntroscopeAgent.Agent] Invoking Business Transaction Match in start_trace() of javax.faces.webapp.FacesServlet
5/31/14 09:40:46 AM EDT [DEBUG] [IntroscopeAgent.Agent] Found business transaction definition as Business Segment|MedRec Patient|Login Submit|Login Submit isIdentifying is## true isResponseBased is## false.
5/31/14 09:41:10 AM EDT [DEBUG] [IntroscopeAgent.Agent] Trace event type: Normal

If the incident hasn't been opend yet, you should still find the sampled trace. Open the Historical Query Viewer, search for the RequestID/GUID. You should see the the Business Transaction under the "Business Segments".
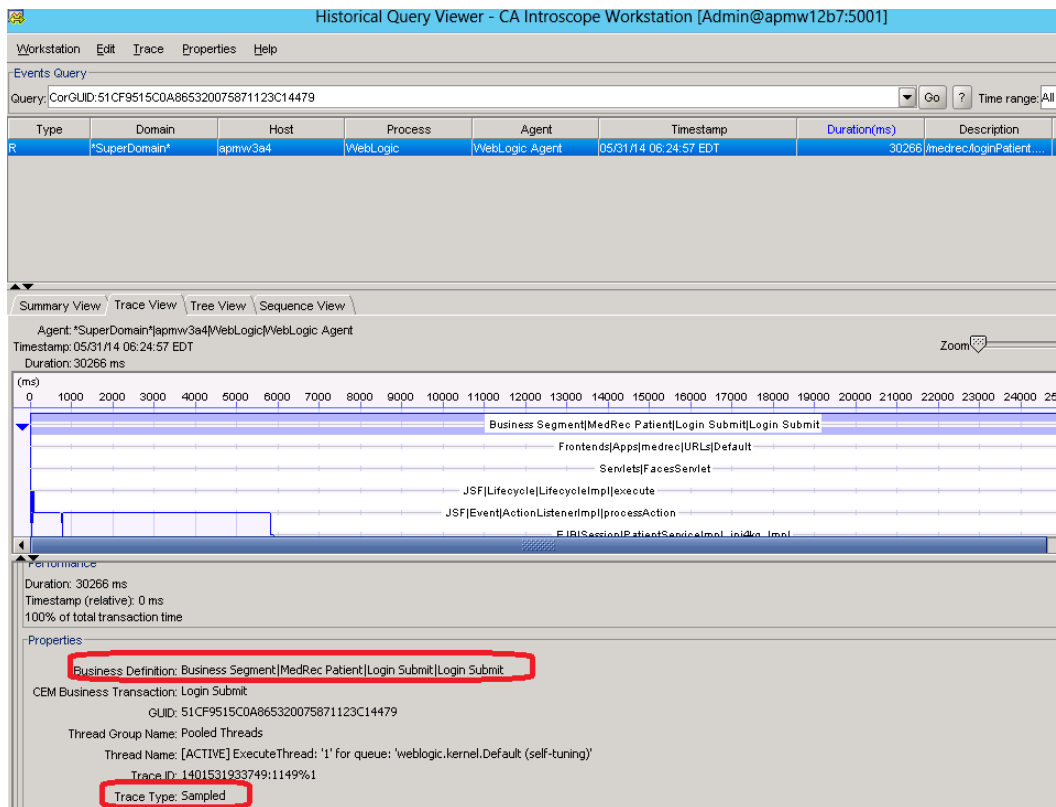
What to collect:

1. zipped content of the AGENT_HOME\logs (DEBUG enabled)
2. IntroscopeAgent.profile
3. Go to the TIM UI, select "Collect Tim Log and Configuration files"
4. Zipped content of the TIM_COLLECTOR_SERVER\logs

No "Business Segment" agent metrics

Checklist:

1. Go to the TESS UI:
- Verify that Business Transactions defintions are correct and being monitored
- Ensure monitors are synchronized.

2. Go to the Investigator, check that the Business Segment" node appears for the monitored agent. If not, it means that no transaction matches the definition rules:
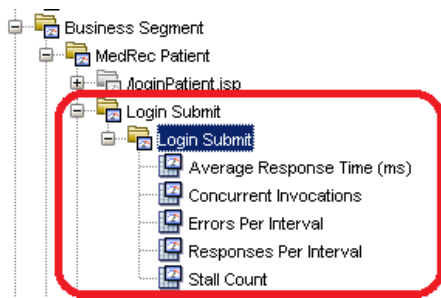
3. You should see entries like below if the agent finds a match based on the user activity.

5/31/14 06:04:09 AM EDT [VERBOSE] [IntroscopeAgent.BizTrxDef] Business Parameter Set found a match to a Business Pattern Rule Set
5/31/14 06:04:09 AM EDT [VERBOSE] [IntroscopeAgent.BizTrxDef] Business Pattern Rule Set Contains the Following Parameters: Pattern Name = Path,Pattern Value = /medrec/patient/viewPatient.action,Pattern Type =PATH,Pattern NameType Operation = LITERAL_NAME_OPERATION,Pattern Action Operation = SIMPLE_MATCH_VALUE_OPERATION,Pattern Case Sensitive Name = false,Pattern Case Sensitive Value = true
5/31/14 06:04:09 AM EDT [DEBUG] [IntroscopeAgent.Agent] Found business transaction definition as Business Segment|MedRec Patient|Login Submit|Login Submit isIdentifying is## true isResponseBased is## false

4. There is a known issue where due to synchronization issue, the agent fails to download Business transaction definitions as expected. Restart the MOM or specific Agent.

What to collect:

1. Zipped content of the AGENT_HOME\logs (DEBUG enabled)
2. IntroscopeAgent.profile
3. Go to the TIM UI, select "Collect Tim Log and Configuration files"
4. Zipped content of the TIM_COLLECTOR_SERVER\logs

CE Reports

Important Reminders

1. Incidents Report: From the Domain page you can enable "Calculate Incident cost" to replace the "Business Impact column" with the "Incident cost column" = (cost per user per minute) x (# of users) x (# of minutes).
2. Defects Report: From the Domain page you can enable "Capture Comprehensive Defect details" to display additional data about query, post parameters, the request and response bodies. NOTE: the request bodies are limited to 1KB and the response bodies to the first 10,000 characters. The size of the request body is configurable from the TIM Settings, "MaxDefectResponseBodySize".

In 9.5.1: Added a new clamp scheduleReports.usersLimitCount=1000

Export Data, Save or schedule a report takes a long time, unavailability of CE reports.

Checklist:

1. Check permissions, if you do not have access to the Business Service you will not get the report as expected.

2. Statistics data are updated once every hour. Apart from the Incident Management reports, you need to wait 1 hour for the Hourly/Aggregation to complete to be able to see data.

3. Check for possible probelms with the Aggregation. A common problem is when 'ThreadStackSize' is too small (128 MB) causing daily stats aggregation and defect aggregation not to start hence many of the CEM reports will be empty. Open the TIM_COLLECTOR\config\tess-default.properties, increase XX:ThreadStackSize to 256 or higher value for both "defects.jvmArgs" and dailystats.jvmArgs entries. You need to restart the TIM Collector. For more information, see "Defect" and "Statistics" sections.

4. Check if the problem is related to the huge number of users, it will affect the EM performance (OOM, become unresponsive), run the below queries to find out the # of active/inactive users:

➔ select count(*) from ts_users where ts_soft_delete='false' and ts_active='true';
➔ select count(*) from ts_users where ts_soft_delete='false' and ts_active='false';

In 9.5.1 a new clamp has been added to prevent this unexpected behavior: "scheduleReports.usersLimitCount" it is set to 1000 by default. In parallel, you could try to reduce the # of users by lowering from TESS UI > Setup > Domain -> Data retention settings, set "Make Users Inactive after".

5. If there are insufficient database connections you might not be able to login, do recording or generate any report. In the EM log, you will see "GenericJDBCException: Cannot open connection" error. In this case, increase the "max_connection" in the <APM_Db_Home>/data/postgresql.conf.

7. Slowness due to huge amount of data in apmd db, see "TEC597519" – how to purge or reduce the size of apmd b and optimize EM data retention

8. Slowness due to EM/Cluster performance issue - see "EM Performance" topic.

What to collect:

1. Zipped content of the logs directory from MOM and collectors, especially from the TIM Collector server
2. apmdb export, go to EM_HOME\install\database-scripts\windows (or Unix), run configexport.sh/bat [dbhostIP] [dbname] [dbuser] [dbpassword] [dbport] [dbtype] [datafile]. For example:
    -If postgres => configexport.bat/sh 127.0.0.1 cemdb admin admin 5432 Postgres apmdbmyexport.xml
    -If oracle => configexport.bat.sh 127.0.0.1 cemdb admin admin 1521 Oracle apmdbmyexport.xml

"Export Data" Tab

Important reminders

In 9.1:
- Added "Export Data" tab to export business statistics, defects and incidents in CSV format.

- Below table comparing PDF (Jasper), CEM Export Tool and New "Export Data tab"

PDF Reports	CEM Export Tool	Export Data Tab
Limited number of predefined reports	A lot of flexibility for inputs, ability to create a large number of different kinds of reports	Easy to use, A lot of flexibility for inputs, ability to create a large number of different kinds of reports
Reports in PDF format – cannot be used/ consumed by other reporting / analyzing tools	Reports in CSV format, can be consumed by other analyzing tools, easy to integrate	Reports in CSV format, can be consumed by other analyzing tools, easy to integrate
Report configurations can be saved	Reports configurations cannot be saved	Report configurations can be saved
Reports can be scheduled to be delivered to emails.	Reports can NOT be scheduled to be delivered to emails.	Reports can be scheduled to be delivered to emails. Note: in tess-default.properties, flexreports.mail.attachment.size=800 . If file size is > 800MB it will be split into multiple files, results are Emailed as zip file.
Number of defects displayed on web UI (Tess > CEM>Incident management > Defect Search) is max 1000 (can be overridden in backend)	All defects can be generated in report.	All defects can be generated in report.
All PDF reports are predefined business reports , measuring business metrics like performance, quality etc	CSV reports are more raw and unprocessed. You can get data like response time, defects count, size etc.	CSV reports are more raw and unprocessed. You can get data like response time, defects count, size etc.
Anyone with access to APM should be able to invoke this.	Only admin can invoke this too.	Anyone with access to APM should be able to invoke this. Data filtered based on user access permissions.

APM database

Important reminders

1. APM support 2 types of databases: postgreSQL and Oracle
   - Postgres: is an open source relational database, comes with APM installer
   - Oracle: the customer has to install Oracle DB, license from Oracle is needed
2. Installation:

- Posgres: APM installer installs the database and creates necessary DB users and APM schema
- Oracle: you need to create the Oracle user before installing APM. The installer creates the APM schema (DB tables) for the user.
3. Free tools to access:
- Postgres: pgAdmin, installed automatically if APM is installed on Windows, otherwise, you can download it.
- Oracle: SQL Developer, you need to download it separately.
4. Script for maintenance are located:
- EM_HOME\install\database-scripts\windows
- EM_HOME/install/database-scripts/unix
5. Available scripts:
- Postgres: dbbackup-postgres, dbrestore-postgres, configexport, configimport, dbupgrade, createdb-postgres, createschema
- Oracle: CreateSchema-database, dbDrop-database, configexport, configimport, dbupgrade, migration
6. Limitations:
- Cross db import/export is not supported. For example: a postgres export file cannot be used for import into Oracle.
- APM schema can be migrated from Postgres to Oracle, however source, destination DB and machine from which the migration is executed need to be in the same time zone. Migration across time zones (for example PST to IST) is not supported.
- APM schema cannot be migrated from Oracle to Postgres.
7. Scripts Examples:

7.1 Backup/Restore scripts: If you need to move the db to a different server

a) For Postgres run dbbackup-postgres.bat/sh [dbserverhostip] [dbinstalldir] [dbname] [dbuser] [dbpassword] [dbport] [dbbackupdir]". For example:

- dbbackup-postgres.bat/sh 127.0.0.1 "C:\Program Files\CA APM\database" cemadmin admin admin_password 5432
- dbrestore-postgres.bat/sh 127.0.0.1 "C:\Program Files\CA APM\database" postgres postgres_password cemRestoreDB admin admin_password 5432 apmdb.backup

b) For Oracle, you need to use expd/impdp Oracle Tools. For example:

Create the Oracle user "oracle_imp_user" (destination user)
Create virtual directory "expdp_impdp_test" for DB dump and set privileges
-CREATE OR REPLACE DIRECTORY expdp_impdp_test AS 'G:\exported_db';
-GRANT READ, WRITE ON DIRECTORY expdp_impdp_test TO oracle_exp_user;
-GRANT READ, WRITE ON DIRECTORY expdp_impdp_test TO oracle_imp_user;
Export/Import:
- expdp oracle_exp_user/passwd1@orcl2 schemas=oracle_exp_user directory=expdp_impdp_test dumpfile=oracle_bckp.dmp logfile=oracle_exp_backup.log;
- impdp oracle_imp_user/passwd21@orcl2 REMAP_SCHEMA=oracle_exp_user:oracle_imp_user directory=expdp_impdp_test dumpfile=oracle_bckp.dmp logfile=oracle_imp_backup.log

7.2 To create/drop Oracle Schema: these scripts call .sql scripts available from EM_HOME\install\oracle\database-scripts:

- CreateSchema.bat/sh -databaseName orcl -databaseType oracle -host 127.0.0.1 -port 1521 -releaseVersion 9.6.0.0 -scriptsDir "C:\Program Files\CA APM\Introscope9.6.0.0\install\oracle\database-scripts" -user cemdb960 -password cemdb960

- dbDrop.bat/sh -databaseName orcl -databaseType oracle -host 127.0.0.1 -port 1521 -releaseVersion 9.6.0.0 -scriptsDir "C:\Program Files\CA APM\Introscope9.6.0.0\install\oracle\database-scripts" -user cemdb960 -password cemdb960

7.3. Import/Export scripts: allow you to export the content of tables specified in configExport.xml and create a fresh new APM db based on transaction definitions and domain setting only. It will not include Defect, report or statistical data

a) configexport.sh/bat [dbhostIP] [dbname] [dbuser] [dbpassword] [dbport] [dbtype] [datafile]:
- configexport.bat/sh 127.0.0.1 cemdb admin admin 5432 **Postgres** apmdbmyexport.xml
- configexport.bat.sh 127.0.0.1 cemdb admin admin 1521 **Oracle** apmdbmyexport.xml

b) configimport.bat/sh:
- configimport.bat/sh -dbhost 127.0.0.1 -dbname cemdb2 –dbport 5432 -databasetype **Postgres** -dbuser admin -dbpassword admin_password –dbscriptsdir <EM_home>\install\database-scripts\windows\ -importfile apmdbmyexport.xml
- configimport.bat/sh -dbhost 127.0.0.1 -dbname cemdb2 –dbport 1521 -databasetype **Oracle** -dbuser admin -dbpassword admin_password –dbscriptsdir <EM_home>\install\oracle\database-scripts -importfile apmd apmdbmyexport.xml

7.4 Upgrade the schema scripts:

- dbupgrade.bat/sh -databaseName apmdb -databaseType **Postgres** -desiredVersion 9.5.3.0 -host 127.0.0.1 -user admin -password admin-password -port 5321 -scriptsDir <EM_home>\install\database-scripts\windows\
- dbupgrade.bat/sh -databaseName apmdb -databaseType **Oracle** -desiredVersion 9.5.3.0 -host 127.0.0.1 -user admin -password admin-password -port 1521 -scriptsDir <EM_home>\install\oracle\database-scripts

7.5 To recreate a Postgres db and schema:

- drop-postgres.bat/sh 127.0.0.1 "C:\Program Files\CA APM\database" apmdb admin admin-password 5432
- createdb-postgres.bat/sh 127.0.0.1 "C:\Program Files\CA APM\database" postgres postgres-password apmdb admin admin-password 5432
- createschema.bat/sh -databaseName apmdb -databaseType **Postgres** -host localhost -port 1521 -releaseVersion 9.5.2.0 -scriptsDir "C:\Program Files\CA APM\Introscope9.5.2.0\install\database-scripts" -user admin -password admin-password

Postgres installation issue, upgrade, connectivity issues

Checklist:

1. Check that postgres is running using: Task manager or "ps -ef | grep postgres" in UNIX.
You should see 6 postgres processes running when no client are connected to it.

2. Try to restart postgres using the "windows services manager" or in UNIX:
su – postgres –c <path_to_bin>/pg_ctl –D <path_to_data_dir>/data start
su – postgres –c <path_to_bin>/pg_ctl –D <path_to_data_dir>/data start

3. Verify the schema version is correct accordingly to the EM version: SELECT ts_db_versions FROM ts_domains

4. Verify that the MOM/config/tess-db-cfg.xml file has the correct database connection information.

5. If Windows: pause the McAfee antivirus service prior to the installation and then resume the service post install.

7. If Solaris: the installer only accepts Solaris 10 as a supported OS.

8. The password for the admin user is sensitive to some special characters. If it contains for example "$", the install will fail.

9. In 64 bits servers you might see "could not execute query: ERROR: language "plpgsql", you can safely ignore this error.

10. Verify maximum shared memory has been configured:
On Linux, configure in /etc/sysctl.conf file similar as kernel.shmmax = 6693928832
On Solaris, when installing as root, configure in /etc/system similar as set shmsys:shminfo_shmmax=6693928832
On Solaris, when installing as non-root, configure in /etc/project by command similar as projadd -U postgres -K "project.max-shm-memory=(priv,7000MB,deny)" user.postgres

11. In an EM cluster environment:
- Ensure that the timezone in all EMs is the same, otherwise the EM will not be able to connect to the db, you will see in the logs "ORA-01882: timezone region not found". To solve the issue add -Duser.timezone=UTC in IntroscopeEnterpriseManager.lax file in all EMs to override the default timezone.
- Add the below line to the <postgres_home>/pg_hba.conf to configure postgres to allow additional connections from the EMs, otherwise the EMs will not be able to connect to the db, you will see the following message in the postgres log: "FATAL: no pg_hba.conf entry for host "<EM IP address>", user "admin", database "apmdb", SSL off"

host   all   all   0.0.0.0/0   md5

12. Search for errors in the logs:
POSTGRES_HOME/data/pg_log
EM_HOME/installer/schematools.log

What to collect:
POSTGRES_HOME\data\pg_log*
POSTGRES_HOME\data\PG_VERSION
POSTGRES_HOME\data*.conf
EM_HOME\install*.log
EM_HOME\config\tess-db-cfg.xml
Output of SELECT ts_db_versions FROM ts_domains

Postgres keeps restarting with OutOfMemory error

Checklist:

Check the postgres log, if you find the below entries:
[14184-cemdb-admin-2013-05-23 13:58:14.248 EDT]WARNING: out of shared memory
[14184-cemdb-admin-2013-05-23 13:58:14.248 EDT]STATEMENT: select count(*) as col_0_0_ from ts_us_sessions_map usersessio0_ where usersessio0_.ts_soft_delete=false

It means that the OOM error is due to high number of ts_us_sessions_map partitions. This issue is fixed in 9.5.1, the logic has been changed to keep ts_us_sessions_map partitions only for last 60 days.

Oracle APM database issues

Checklist:

1. Check the Oracle version is supported and the pre-requisites have been configured. We only support Oracle 10g,11g Enterprise Edition with partitioning option enabled, ensure to set "Optimizer Statistics Gathering" once a day between 8pm – 12 am; if you don't do this, queries will be slow. Also, PROCESSES (Oracle initialization parameter) should be set to 200.

2. Verify the schema version is correct accordingly to the EM version: SELECT ts_db_versions FROM ts_domains

3. If you are using Oracle 11gr2 and above, the property deferred_segment_creation MUST be set to false, otherwise apm db creation will fail with the following error in the EM_HOME\install\schematools.log:
   8/02/13 04:36:47.721 AM EDT [ERROR] [main] [com.wily.apm.dbutil.SqlExecutor] Sql error in file: initdb-oracle-9.5.0.0.sql java.sql.SQLIntegrityConstraintViolationException: ORA-02291: integrity constraint (CEMUSER.FK7591FF002916E672) violated - parent key not found

   To solve this problem connect to sqlplus, run ALTER SYSTEM SET deferred_segment_creation=FALSE scope=both;

4. Search for errors in EM_HOME/installer/schematools.log

What to collect:

EM_HOME\install*.log
EM_HOME\config\tess-db-cfg.xml
Output of SELECT ts_db_versions FROM ts_domains

Integration: EEM

Important reminders

In 9.0:
1. Limitations:
    a) You cannot use the LDA group from the "Access Policies" in the TESS UI, you need to use the EEM UI.
    b) We do not distinguish between Introscope Frontends and CEM business application. If a user is granted permissions to a Business Application Policies for Frontends, the user will also be granted to "CEM Administration" tab in the TESS UI (bug# 79822).

2. EEM failover logic is done on EEM. On the Introscope side, you only enter one of EEM server in realms.xml, see TEC573489.

3. Known issues:
    a) A change made in EEM requires a restart of the EM. Fix in 9.1.5. (BUG# 79780)
    b) Business Application policies restrictions are not applied. Fix in 9.1.2 (BUG# 79822)

4. You can export the users using EM_HOME\install\database-scripts\(window/export)\operators-export.bat/sh, it will generate a safex script. You can then use this file to import the users into EEM.

5. In 9.1:
    Added APM-EEM integration in FIPS mode

Not working, Login takes a long time

Checklist:

1. Is the problem reproducible when connecting directly to the EEM UI? If the issue is not reproducible, then the problem could be related to a performance issue on the APM side, you should review the EM logs.

2. Change the base DN to a location closer to the user and verify if the problem persists.

3. Are you using multiple EEMs, make sure failover is configured on the EEM not APM side, see TEC573489

4. Ensure installation is correct, see <u>TEC593939</u> – How to configure APM with EEM

What to collect:

1. Zipped content of the EM_HOME\log –make sure to enable DEBUG.
2. EM_HOME\config\reamls.xml, server.xml, domains.xml
3. Enable TRACE, reproduce the issue and collect EEM config and log files:
   If you are using EEM v12:
   a) Stop iGateway service
   b) Go to %EIAM_HOME%\config\logger
   c) In the sever.cml file replace level values "info" or "error" with "trace"
   d) Start iGateway
   e) Reproduce the issue
   f) Collect *.logs and *.conf under %EIAM_HOME% folder. Once this is done, reverse the above steps in order to set the logging back to their defaults.

   If you are using EEM v8.4:
   a) Stop iGateway Service (From Command or from Services.msc)
   Net stop iGateway (On Windows Platform)
   S99igateway stop (On *Unix Platform)
   b) Open the iPoz.conf file for editing (this will be located in the iTechnology folder)
   Use the shortcut %IGW_LOC% on Windows Platform and $IGW_LOC on *Unix platforms
   Search for <LogLevel>WARNING</LogLevel>
   c) Replace WARNING with TRACE (this needs to be in upper case)
   d) Save the iPoz.conf file
   e) Restart the iGateway service
   f) Reproduce the issue
   g) Collect igateway logs, iPoz logs and *.conf from \Program Files\CA\SharedComponents\iTechnology folder.
      Once this is done, reverse the above steps in order to set the logging back to their defaults.

4. Export of APM application from EEM: Configuration > EEM Server > Export Application > Select all Objects list – this will allow us to confirm if the problem is related to permissions and recreate the issue in-house.

Application/Services Access Policies not working

Checklist:

1. Verify that the access policy is working in EEM.
   Select Manage Access Policies > Permission Check. Make sure to enable the "Display debug information"option. Enter information to validate the policy.

2. Bug#79780: any change made in the EEM requires a restart of the EM. Fix is included in 9.1.5

What to collect:

1. Zipped content of the EM_HOME\log – please make sure to enable DEBUG

2. Export of APM application from EEM: Configuration > EEM Server > Export Application > Select all Objects list – this will allow us to confirm if the problem is related to permissions and recreate the issue in-house.
3. Screenshot from Permission Check.

Enterprise Manager

Important reminders
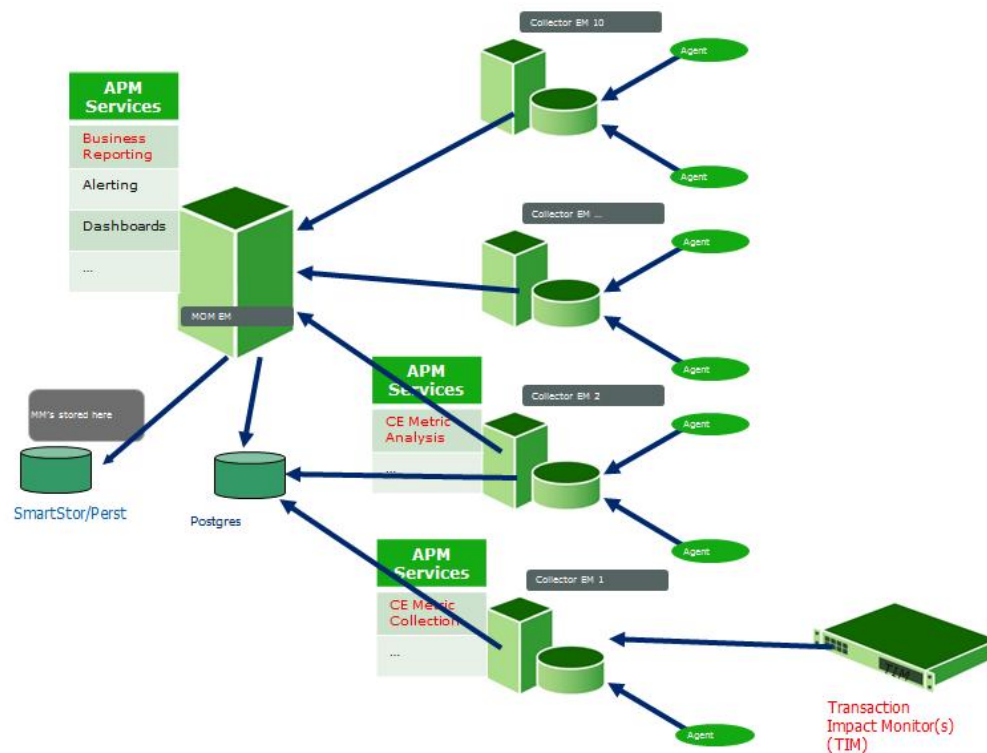
In 9.0:
1. Architectural change: TESS runs inside of the Introscope EM – see TESS section.
2. "TriageMap": it provides a graphical representation of an application in terms of Business Transaction and Frontends to Backends calls. This feature takes advantage of the new multi-threaded calculators support - see TriageMap section.

In 9.1:
1. "LocationMap": it provides a graphical representation of the application elements (Agent, Frontends, called backends) and external data via Catalyst. Although this feature is not location but Agent centric, it is intended to work together with the TriageMap, see "LocationMap" section.
2. "Status Console": it provides active notification/view of the cluster health (EM clamps being reached, important events and denied agents), see "Status Console" section
3. "Collector Data Viewer (CDV)": to address the unavailability to see agent information from other cluster. See CDV section.

4. "Agent controllability" feature: new loadbalancing mechanism – see [Loadbalancing](#) section.
5. Query Paging (large workstation queries can no longer crash the EM): Workstation query results are now sent asynchroneously from collectors to MOM in query pages/blobs (compressed smatstor data without any internal processing). However, in very rare cases, large queries might generate a lot of blobs, requiring a lot of message handling overhead and in some instances freezing the workstation. In this situation, you can buffer the blobs into large/small messages using the below properties however, they do not impact the total amount of data:

   a) Max historical block bytes/count allowed to be batched by any one query:

   -introscope.enterprisemanager.query.max,batching.count.limit=100

   -introscope.enterprisemanager.query.max.batching.bytes.limit=222000

   b) Max bytes batched on a collector at any one time across all queries:

   -Introscope.enterprisemanager.query.max.batching.global.bytes.limit=2220000

In 9.5: Added:
1. Automatic smartstor metadata clean-up – see Smarstor section

EM Performance, slowness, data gaps, frequent MOM/Collector/Agent disconnections, OutOfMemory, Clock-sync issues, EM unable to startup

Checklist:

1. Add the following properties to the MOM and Collectors properties files:

   transport.outgoingMessageQueueSize=6000

   transport.override.isengard.high.concurrency.pool.min.size=10

   transport.override.isengard.high.concurrency.pool.max.size=10

   A restart of the EMs is required for the changes to take effect.

   Increasing the outgoing message queue allows you to have a bigger buffer. Increasing the thread pool size allows you to have more worker threads to send outgoing messages. These important adjustments are required when, sending messages, usually between collectors and MOM, becomes a bottle neck for performance.

2. Ensure you have allocated enough memory. Look at the EM_HOME/logs/perflog,txt. Make sure to set the initial heap size (-Xms) equal to the maximum heap size (-Xmx) in the Introscope Enterprise Manager.lax or EMService.conf. Since no heap expansion or contraction occurs, this can result in significant performance gains in some situations.

3. If the EM is running on UNIX, ensure lax.stdin.redirect in the Introscope_Enterprise_Manager.lax is unset. From ConfigAdminGuide.pdf:

   "Do not run the Enterprise Manager in nohup mode without performing the configuration described above. Otherwise, the Enterprise Manager might not start, or might start and consume excessive system resources."

4. Make sure DEBUG logging is disabled in the IntroscopeEnterpriseManager.properties, depending on the user queries it will affect the EM performance

5. If 9.1+, use the "Status console" to quickly check the Cluster's health:
   - connectivity problem between MOM and collectors
   - Possible EMs' clamps being reached hence preventing you to view the metrics in the Investigator.
   - Disallowed agents, affecting agents and metric visibility, you need to ensure loadbalancing rules has been defined correctly in the MOM/config/loadbalancing.xml – see "Loadbalancing" section.

   Otherwise, you can always check the agent clamp from the Metric Browser, expand the branch

      Custom Metric Host (virtual)
        - Custom Metric Process (virtual)
          - Custom Metric Agent (virtual)(collector_host@port)(SuperDomain)
            - Agents
              - Host
                - Process
                   - AgentName

   looks at the values for : "is Clamped" metric

   To check the EM clamp open the investigator and expand the branch

      Custom Metric Host (virtual)
        - Custom Metric Process (virtual)
          - Custom Metric Agent (virtual)(collector_host@port)(SuperDomain)
            - Enterprise manager
              - Connections

   looks at the values for:

     - EM Historical Metric Clamped
     - EM Live Metric Clamped

   The above metrics should all be 0.

6. Ensure Smatstor db is pointing to a dedicated disk controller and introscope.enterprisemanager.smartstor.dedicatedcontroller=true which allows the EM to fully utilize this setting. Failing to do this, will reduce collector performance by 50%. From SizingGuide.pdf

   "When the dedicated controller property is set to false, the Collector assumes that there is one disk for all Enterprise Manager operations, and therefore uses one disk-writing lock. This means that only one area at a time is written. For example, the Collector will write only to SmartStor or only to the heuristics database that supports the Investigator Overview dashboard.
   Performance disadvantages to having the dedicated controller property set to false are:
   a. Only one I/O task can be running at a time.
   b. SmartStor writes are in shorter segments.
   c. The disk's seek pointer is invalidated after each context switch.

If there is a second disk for SmartStor, but the property is set to false, there is no performance gain by having a second disk for SmartStor.

    d.   Collector sizing recommendations are reduced by 50%."

7. Huge metadata: too much metadata will cause a performance problem as queries will take a long time to be processed, use SmartstorTool to remove periodically any unwanted metric (see TEC609741 – How to remove data using SmartstorTool), especially those where there is no data as each query must examine every metric including the inactive one:

   a) Active metrics / metrics with Data: Check the "Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) | Enterprise Manager | Data Store | Smartstor | Metadata | Metrics with Data" supportability metric. The value should not be higher than 300K in v8.x and 600K in v9.x.

   b) Inactive Metrics / metrics with no data: Starting from 9.5, we have automated this metadata cleanup to remove metrics and agents for which there is no data. This process occurs during reperiodization (midnight) after tier3 data value removal. The only control is by changing tier3 value. You can disable the automated process by setting introscope.enterprisemanager.metadata.autoexpire=false

8. If MOM and collectors are not located in the same subnet, you might experience continuous EMs/Agents disconnections. For transatlantic agent->Em connections it is recommended to use HTTP tunnelling. From SizingGuide:

   "Whenever possible, a MOM and its Collectors should be in the same data centre; preferably in the same subnet. Even when crossing through a firewall or passing through any kind of router, the optimal response time is difficult to maintain. If the MOM and Collector are across a router or, worse yet, a packet-sniffing firewall protection router, response time can slow dramatically."

   Also, ensure to set introscope.enterprisemanager.clustering.manager.slowcollectorthreshold=500. The default value for this threshold is 10000 ms, which is too high for realistic purposes

9. Ensure MOM and collectors synchronize their system clocks with a time server such as an NTP server otherwise EMs will disconnect, in the EM log you will see the following message: "Collector clock is skewed from MOM clock by".
   If it is a virtual environment additional configurations are required to prevent known clock-sync issues:
   http://www.vmware.com/pdf/vmware_timekeeping.pdf
   http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006427
   http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1318

10. Too many incoming traces: open the collector's perflog, check if "Performance.Transactions.Num.Traces" is higher than 500K or increasing rapidly; if so, lower the "introscope.enterprisemanager.transactionevents.storage.max.data.age". Use Historical Event Query to identify what type of trace is causing the problem:

    a) If most are sample events, try disabling transaction sampling on the agent side, set introscope.agent.transactiontracer.sampling.enabled=false
    b) If most are error events, try disabling error detector on the agent side, set introscope.agent.errorsnapshots.enable=false.

c) If most are normal tracers, try reducing introscope.agent.transactiontrace.componentCountClamp.

If you are using CEM, search in the logs for: "[Manager.TransactionTracer] Started transaction trace for transactions: exceeding XXX milliseconds and with CEM Business Transaction that equals ", if you see many entries, for testing purpose, go to the CEM UI > Setup > Introscope Settings" page, reduce the length of the transaction trace session, for example 1, and setting "% of the defect threshold" to 100%. If 9.x Agent, you can disable propagation by setting introscope.agent.transactiontracer.tailfilterPropagate.enable=false

If you are using SPM, turn off boundary tracing on the Agent side, set com.wily.introscope.agent.transactiontrace.boundaryTracing.enable=false. Depending on the implementation; it could cause too many traces or too huge traces affecting both Agent and EM (crash/OOM)

11. If you are using CEM: TESS services should be running on dedicated collectors to prevent any performance and IO contention issues between Stats Aggregation and Smartstor reperiodization. Normal agents should be pointing to separate collectors. You must update the MOM loadbalancing.xml to prevent agents from reporting to the collector you have allocated to for TIM Collection Services and Stats Aggregation.

12. Too many calculators: Calculators are both high CPU and memory intensive. Check if the problem occurs when connecting to a Collector, if not, try disabling the below MOM features:

    - TriageMap: set introscope.apm.feature.enabled=false
    - Any custom virtual agent you might have created in the MOM_HOME\config\agentcluster.xml.
    - If 9.5 and webview is running: charts in Home Page are topN queries and as such can be very expensive, especially in Historical Mode, login into Workstation and disable the below metric grouping from the TriageMapConfigurationsManagementModule.jar management module:
        25 Slowest BTs:Average Response Times (ms)
        25 Worst BTs:Errors & Stalls
        25 Slowest Frontends:Average Response Times (ms)
        25 Worst Frontends:Errors & Stalls

13. Harvest duration spikes:
    a) If harvest duration is high all the time (> 7,500), the EM is overloaded, you need to review the hardware capacity and reduce the # of metrics and calculators.

    b) If harvest duration spikes regularly at 5-min interval, it's related to a volume polling thread which runs every 5 minute to get the disk/dir/file size of data, data/archive, traces.db, log file, and baselines.db set introscope.enterprisemanager.supportability.volumespace.enable=false.

    c) If harvest duration spikes regulary at 1-hour interval and SPM is enabled, you need to disable SOA Deviation: set com.wily.introscope.soa.deviation.enable=false
    Other possible symptoms: Your created calculators will start reporting zero hourly.

    d) If harvest duration spikes at the same time GC duration also spikes: this might be due to a lack of memory: check heap size is enough, huge query or large amount of queries are happening, too many traces.

14. Large/ heavy historical queries:

In 9.0.x: clamp the historical queries to 100k to prevent huge queries from increasing the memory footprint of the collector & mom. By default, it is unlimited:

introscope.enterprisemanager.query.datapointlimit=100000

introscope.enterprisemanager.query.returneddatapointlimit=100000

In 9.1+, the above clamps are still valid for CLW, JDBC and Top-N queries only. For workstation queries, use new clamp "introscope.enterprisemanager.query.maxtransferbytes=" to limit the total memory usage on the EM for historical queries. Queries will stop being processed when the "In Use Memory" exceeds the defined specific value, by default 0 (no limit).

NOTE: If 9.5+, you can make historical queries that fall within the cache to display extremely quickly by increasing "introscope.enterprisemanager.memoryCache.elements", default to 32(8 minutes). Max limit 11520(48 hours). You can specify any value within this range; the value will be truncated to the nearest multiple of 32. Apply the change in both MOM and collector. EMs must be restarted. Increasing this value will increase memory footprint of EMs, setting the cache too big can OOM an EM. It is recommended to increase this value only when using 64bits JVMs.

15. Multiple collectors in the same server: ensure to use 64 bit OS and multiple disks. From SizingGuide:

"a) Run the OS in 64-bit mode to take advantage of a large file cache.
The file cache is important for the Collectors when doing SmartStor maintenance, for example spooling and reperiodization. File cache resides in the physical RAM, and is dynamically adjusted by the OS during runtime based on the available physical RAM. CA Wily recommends having 3 to 4 GB RAM per Collector.

b) There should not be any disk contention for SmartStor, meaning you use a separate physical disk for each SmartStor instance. If there is contention for SmartStor write operations, the whole system can start to fall behind, which can result in poor performance such as combined time slices and dropped agent connections.

c) The Baseline.db and traces.db files from up to four Collectors can reside on a separate single disk. In other words, up to four Collectors can share the same physical disk to store all of their baseline.db and traces.db files."

16. If the EM is unable to start up, open the EM log and search for the below messages:
    a. "Failed to load" message indicates that the problem is related to the Management modules; restart the EM without any management module. Then, introduce them back 1 by 1until you identify the culprit.
    b. "java.nio.channels.CancelledKeyException" message indicates that the problem is related to nio transportation, add transport.enable.nio=false in the EM properties file. You need to restart.
    c. "java.io.IOException: Too many open files" message: Make sure the max open file handle is at least 4096 on both MOM and Collectors. You can check current open file descriptors by using "ulimit -n" against the user who starts EM processes. You might need to increase the maximum number of open files allowed for that user.

17. By design an APM cluster requires an APM db, you should ensure it is always available, otherwise collectors/agents might not work as expected if the APM DB is not available (bug#86473 - Collector hangs/freezes as mailman threads block indefinitely if the APM DB is not available.)

18. Other key supportability metrics to review:
From "Custom Metrics Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent(Virtual)|
Enterprise Manager":

a) Check if "Connection: Number of Historical Metrics" is continuously going up, it is an indication of a possible metric explosion/leak.
b) Check "Connections: Number of Metrics Handled" (Performance.Agent.MetricDataRate column in the perflog), it represents the rate of incoming data. This value should fluctuate around the Performance.Agent.NumberOfMetrics when the system is running properly.
c) Check "Internal|Query:SmartStor Queries Per Interval" (Queries per interval column in perflog.txt), it represents the # of user queries (ie: click on a metric in the investigator), you can identify the user query rate.
d) Check if "Internal:Calculator Harvest Time" is high while "Internal|Calculator:Total Number of Evaluated Metrics" is low, it is an indicator of overshared CPUs, behavior mostly seen on VMs.
e) Check if calculators and alerts are matching too many metrics: "Internal|Calculators: Total Number of Evaluated Metrics" and "Internal|Alerts:Total Number of Evaluated Metrics"
f) Check "Harvest Duration (ms)" (Performance.Harvest.HarvestDuration in perflog), values over 7500 is probably an indicator of an overloaded EM.
g) Check "Tasks:Smartstor Duration (ms)" (Performance.Smartstor.Duration in perflog), values over 7500 is probably an indicator of an overloaded EM.
h) Check "Internal:Number of Connection Tickets" (Performance.Agent.ConnectionThrottleCount in perflog), it represents the number of Agent throttling tickets. There is one ticket per CPU available in the EM. If this value stays at zero for long periods of time (other than at EM startup), then there may be a problem with Agent throttling and the EM should be restarted. This column should be higher than 0 at all times.

What to collect:

Collect the following information from ALL Introscope EMs (MOM and collectors):
1. Zipped content of EM_HOME\logs (include IntroscopeEnterpriseManagerSupport.log and perflog.txt)
2. MOM_HOME\config\agentdomains.xml – will help us confirm if there are virtual agents defined.
3. MOM_HOME\config\loadbalancing.xml
4. Hardware specs of the servers and a general overview of the implementation indicating where the collectors and MOM are
5. Screenshot of the "Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) | Enterprise Manager | Data Store | Smartstor | Metadata | Metrics with Data" supportability metric from all Collectors.
6. If possible, screenshot of MOM > "Status console"
7. Collect a series of threadump from MOM and collector to find out the root cause.

No Live data after an Agent was moved from Superdomain to a custom domain, however metric reports correctly when connecting directly to the collector.

Check list:

1. Ensure domains.xml on MOM and Collectors are the same.
2. TT#80130 - MOM is not properly mapping the Agent to the right domain in the Collector and hence sending wrong query. Workaround:
   a) Clear old Agent using SmartStor tool or
   b) Rename the new Agent for the time being.

What to collect:

Enable querylog on the EM_HOME\config\IntroscopeEnterpriseManager.properties file:

log4j.additivity.Manager.QueryLog=true
log4j.logger.Manager.QueryLog=DEBUG, querylog

Try to reproduce the issue and collect:

1. zipped content of the HOME_HOME\logs folder (debug log is required)
2. EM_HOME\config\domains.xml
3. Screenshots displaying the issue from MOM and collectors

Loadbalancing

Important reminders

In 9.0:
1. MOM only rebalances agents that connect directly to the MOM, based on loadbalancing rules.
2. If an agent prefers any particular Collector: this can be enforced via loadbalancing.xml entry at MOM or agents can connect directly to collectors (by specifying collector IP address in agent profile)
3. Limitations:
-Unable to stop an agent from sending data or redirect the agent to another collector without restarting it.
-MOM down - a single point of failure.
-Loadbalancing.xml is not hot configurable, MOM restart is required for changes to take effect.

In 9.1: Added the "Agent controllability" feature:
1. MOM rebalances all agents connected to any collector in the cluster; load balancing is governed by loadbalancing.xml. The MOM periodically sends loadbalancing.xml to all the Collectors. Agents 9.1 keep the list of EMs to connect in case of failure of MOM and collectors.
2. MOM reads loadblancing.xml every 60 seconds, changes are effective immediately for new agents; for existing agents, they have to wait for the next load balancing operation (10 min by default, introscope.enterprisemanager.loadbalancing.interval - hot property).
3. When the MOM connects to a Collector for the first time, the MOM transfers its introscope.apm.agentcontrol.agent.allowed property value to the Collector, it overrides the value.

4. If the MOM goes down after a Collector has received loadbalancing.xml, the Collector uses the received loadbalancing.xml. If the Collector has never connected to the MOM, the Collector uses its introscope.apm.agentcontrol.agent.allowed property to allow agent connections.

5. introscope.apm.agentcontrol.agent.allowed in collectors decide whether to allow or disallowe those agents if they are not matching any regular expression in loadbalancing.xml,.

7. You can instruct Agents to always connect "first" to a specified collector by using the "Latched=true" flag.

8. If MOM and initial collector are down, the 9.1 agent will use the lookuplist of collectors in memory to identify its available collectors, ensure introscope.apm.agentcontrol.agent.emlistlookup.enabled=true.

Load balancing is not working as expected, Agents getting assigned to excluded collectors, Collector denying agents without any reason, Agent connect to the EM but does not show up, Agents are not acting according to the loadbalancing.xml changes

Checklist:

1. Verify MOM and collector are up and running. If possible restart the cluster, start collectors first and then the MOM. You need DEBUG logs to troubleshoot loadbalancing issues.

2. Make sure loadbalancing.xml definitions are correct. If possible, redefine loadbalancing.xml to use both includes and excludes if applicable. Wrong collector name/ip in loadbalancing.xml will cause the Agents to bounce around. Try using the ip address instead of the hostname. For example, the below message indicates that the agent is connected but in disallowed mode:

   "Connected controllable Agent to the Intro.... Host="test", Process=tomcat, agent name="tomcat", Active="false"

3. Wait for the next reload balancing opearation to complete, remember, MOM reads loadblancing.xml every 60 seconds, changes are effective immediately for new agents; for existing agents, they have to wait for the next load balancing operation (10 min by default, introscope.enterprisemanager.loadbalancing.interval= hot property).

4. Ensure introscope.apm.agentcontrol.agent.allowed property is set to true on the MOM properties file

5. Verify the cluster's health using Status console, you can check collectors' clamps and disallowed agents.

6. The problem could be related to a performance issue in the EM or cluster – see [EM performance](#) topic.

7. Review DEBUG logs and search for errors.

What to collect:

1. Zipped content of the EM_HOME/logs folder (debug log are reaquired) from both Mom and collectors.
2. loadbalancing.xml
3. Screenshot from APM Status console displaying possible clamps, disallowed agents.
4. Agent profile and DEBUG logs from some affected agents.
5. Timeline of different tests, so that we can correlate with log files.
6. Hardware specs of the servers and a general overview of the implementation indicating where the collectors and MOM are

7. Screenshot of the "Custom Metric Host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) | Enterprise Manager | Data Store | Smartstor | Metadata | Metrics with Data" supportability metric from all Collectors.

Smartstor database

Important reminders

1. SmartStor has 3 different maintenance sub-processes that transform metric data into persistent storage flat files. The first SmartStor sub-process store raw files *.spool and converts them to *.data type files. This happens hourly, on the hour. The second sub-process is the transformation of hour long data files into day long data files. This happens at midnight every day. The third sub-process will transform, reperiodize and archive data that is more than one day old according to the tiers defined in the EM properties. This is also part of the SmartStor maintenance running on the EM at midnight.

In 9.1.1.1:
2. If you are upgrading from v8 to v9, you must upgrade the SmartStor database using SmartStorTool, otherwise you might see duplicated metrics under the Frontend and backends nodes. From 9.0.x onwards for TriageMap we created a new metric type for frontend and backend metrics. This new "upgrade" option has been added to 9.0.7.4 and 9.1.1.1.

In 9.5:
3. Added "Automated Metadata Cleanup" - starting from 9.5, we have automated this metadata cleanup to remove metrics and agents for which there is no data. It happends during reperiodization (midnight) after tier3 data value removal. The only control is by changing tier3 value. You can disable the automated process by setting introscope.enterprisemanager.metadata.autoexpire=false

Smartstor Tool

Important reminders

In 8.2.2.0:
1. SS tool bundled with the Introscope EM. If you are using a pre-8.2.2.0 you need to use unofficial version: https://support.ca.com/irj/portal/anonymous/redirArticles?reqPage=search&searchID=TEC533769
2. SmartstorTool does not have an option to delete data for a specific range of time.
3. You cannot use both "-remove_metrics" and "-remove_agents" at the same time.

4. "list_agents" and "test_regex commands" run a historical query to get the matching regex; they need the original or full copy of the original data directory.
5. "remove_agents" and "remove_metrics" commands do prune the metadata files to remove the targeted metrics or agents. These commands work against the metadata files only. You will not see any change until midnight.
6. see TEC609741 – for step by steps instructions about how to remove data using SmartstorTool

In 9.0.7.0:
6. SmartStorTools "Prune" syntax changed in 9.x:
   In v8.2.x, the destination directory argument is "-backup".
   In v9.x, the destination directory argument is "-dest"
7. You can remove and list agents using the agent fully qualified name. For example:
   SmartStorTools.bat list_agents -agents "SuperDomain\|MyServer\|Jboss Agents\|My Jboss" -src "c:\Introscope9.0.5.0\data"
   The capability is available in 8.2.4.0 and 9.0.7.0.

In 9.1.1.1:
9. A new "upgrade" option has been added to migrate Smartstor database v8 to v9

APM Status Console

Important reminders:
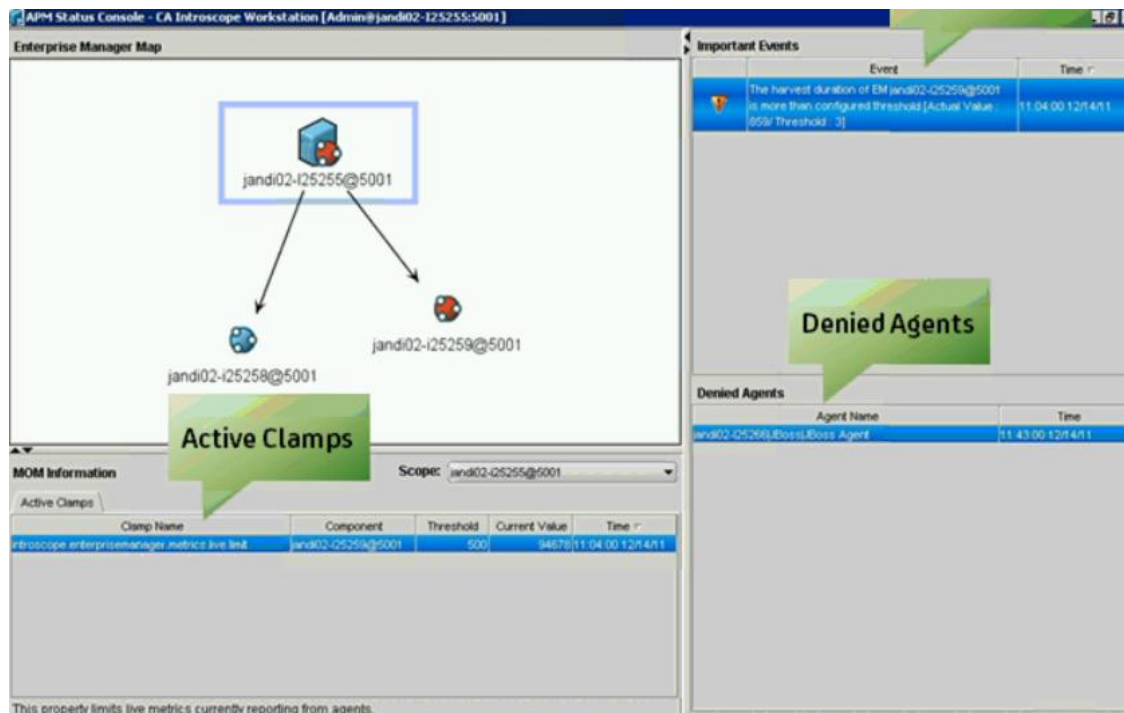
In 9.1:

1. Status console provides active notification/view of the cluster health (EM clamps being reached, important events and denied agents)

2. You cannot modify the denied agents from the UI, for this you need to update the MOM/config/ loadbalancing.xml

3. You cannot modify any clamps from the UI. For this, you need to update the corresponding "clamp id" entry in the MOM/config/apm-events-thresholds-config.xml

4. You cannot modify any event threshold from the UI. For this, you need to update the corresponding "importantEvent id" entry in the MOM/config/apm-events-thresholds-config.xml. It is recommended not to modify these values.

5. Changes in /config/apm-events-thresholds-config.xml, doesn't need MOM restart

6. You can jump from the active clamp to the corresponding supportability metric in the Metric Browser. Not all clamps have supportability metric.

7. Any Admin or user with the "apm_status_console" can access the Status Console.

8. The Status Console shows only the current status, it does not store any history.

9. It is available from workstation only (not webview)

10. For troubleshooting issues on Status Console, see. "EM Performance" and "Loadbalancing section"

Cross-Cluster Data Viewer (CDV)

Important reminders
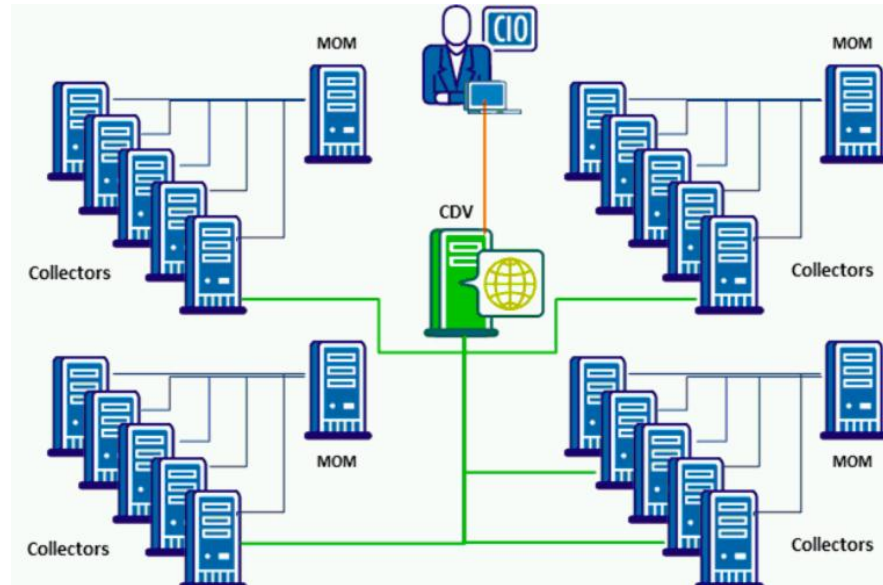
In 9.1:

1. CDV allows to view agents that are connected to collectors in different clusters. CDV is like a MOM with some features disabled.

2. Collectors, CDV and workstation "must be" on the same version.

3. Multiple CDVs can connect to a single collector. You can limit the # of CDV that can connect to a collector. Default value is 5

4. The content of domains.xml of collectors should be present in CDV for the metrics to appear. It supports custom domains.

5. Performance team has tested CDV with 30 collectors

6. introscope.enterprise.manager.cluster.mode it is not a Hot property, invalid values will prevent the EM from starting

7. What CDV doesn't have?
   a. Appmap will be disabled
   b. CDV does not perform load balancing
   c. CDV cannot redirect/connect agents (you will see an exception for agents that try to connect to CDV
   d. APM Model Web Services are disabled in CDV
   e. CDV doesn't require an APM database (postgres/Oracle)
   f. TESS UI and services are disabled

   What CDV has?
   a. Transaction tracing can be performed on agents in different clusters, DI is also supported
   b. Collectors can be added/removed to CDV without having to restart CDV

8. Known issue: CDV makes Javascript calculators disappear from collectors. (BUG# 82239)Fixed in 9.5.
   Workaround: Add to the IntroscopeEnterpriseManager.properties of the CDV
   introscope.enterprisemanager.javascript.hotdeploy.collectors.enable=false

Collector rejects CDV connection, Collector doesn't show up, Collector is connected to CDV but metrics do not show up.

Checklist:

1. Check for any clock synchronization issue - collector system clock must be within 3 seconds of the CDV clock setting

2. The behaviour of CDV is to disconnect any slow collector, you should confirm if this is the case. Check if the collector can connect successfully to a MOM.

3. Check introscope.enterprise.manager.clustering.mode=CDV (not hot property)

4. Check the list of collector connections in the CDV properties file is correct

5. Check if the max # of CDVs clamp has been reached for the collector, see supportability metric "Custom Metric Agent | Enterprise Manager | Connections | Cross-Cluster Data Viewer Clamped". If the value is 1 you need to increase Introscope.enterprisemanager.collector.cdv.max in the COLLECTOR_HOME\config\apm-events-threadhods-config.xml.

6. Ensure that all domains definitions from all collectors are present in the CDV domain.xml. If there are many collectors, you need to merge the content.

What to collect:

1. Zipped content of EM_HOME\logs from collector(s) and CDV
2. EM_HOME\config\apm-events-threadhods-config.xml
3. Domains.xml from CDV and problematic collector(s)
4. Screenshot of the below EM supportability metrics from the collector: "Custom Metric Agent | Enterprise Manager | Connections | Cross-Cluster Data Viewer Clamped" and "Number of cross-cluster data viewer"

LDAP Authentication

Login takes a long time, unable to authenticate

Checklist:

1. Ensure installation is correct, see TEC595290

2. Do you have the same problem using the user used for the binding defined in the EM_HOME\config\realms.xml?

3. Do you have the same problem when using other third party utilities such as "Apache directory studio"?

4. Is the user profile located far from the baseDN defined in the EM_HOME\config\realms.xml. If this is the case, change the base DN to a location closer to the user.

What to collect:

1. Zipped content of the EM_HOME\log – please make sure to enable DEBUG.
2. EM_HOME\config\reamls.xml, server.xml, domains.xml
3. Screen shots of user/group attributes from LDAP server.
4. Which LDAP version you are using?
5. LDAP logs

Triage Map

Important reminders

In 9.0:
1. This feature requires 9.x agents and consists of 2 parts: Tree nodes and Map:
   a) The triage Map tree, nodes grouped by Business Service and Frontends. Metrics are generated using calculators based on Application frontends and Business Transaction metrics from the Metric Browser.
   b) The map is generated using appmap.pbd, appmap-ejb.pbd and appmap-soa.pbd.
2. The "Triage map" tab is only available when connecting to the MOM not the collectors.
3. You can disable triage map from the agents by setting Introscope.agent.metrics.enabled=false.
4. You can see historical data for the map topology and metrics, but we do not store any historical info of the alert threshold definitions.
5. By default, the window historical data covers 3 days (Introscope.apm.data.timeWindow) and we preserve all apm data in db for 365 days. You can change the aging and pruning using Introscope.apm.data.preserving.time in the EM properties file.
6. Edge data is sent by agent to the EM for processing when: a) agent sees an edge, b) "edge storm" that occurs on every agent restart or every 12 hours. "edge storm" will cause spike in EM and postgres CPU utilization.
7. The below properties control the rate edge data that is sent by agent to the EM:
In the Agent profile:
- Introscope.appmap.queue.size=1000 – control how much
- Introscope.appmap.queue.period=1000 (ms)
- Introscope.appmap.intermediateNodes.enabled=false – set it to true if you need data asap but not recommended.
In the EM/config/APMEnterpriseManager.properties:

- Introscope.apm.query.max.results=20000 – this clamp is intended to limit mainly active users, those who click on appmap and requesting data constantly, not even waiting the 15 seconds data to refresh. If you have users that have a big map but do notus it constantly, you can increase the default value.
- hibernate.jdbc.batch_size=10 – represents how many rows we insert at a time.
In the EM config/IntroscopeEnterpriseManager.properties: Introscope.apm.data.agingTime=1DAY

In 9.1:
8. Expose Customer Experience metrics (RTTM metrics)
9. New Agent Resource metrics (CPU Utilization, Memory consumption, Thread Usage, JDBC Connection): available from Location Map, Triage Map (resource metric indicator) and Metric Browser(Resources tab). Metrics have been pre-configured for Websphere, weblogic and Tomcat, for any other (Jboss, .NET, etc), you need to update the EM_HOME\config\ResourceMetricMap.properties. You must supply absolute paths. For some agents additional extensions need to be installed, for example for Weblogic you need to install PP Weblogic, for Webpshere you need to enable PMI, for Tomcat you need to enable JMX. – see TEC595378 – an example of how to enable thread and JDBC graphs in the Resources tab.
10. New TriageMap Alert Editor:
- It requires Super Domain (Admin) permission
- Triage map alerts are stored in "Triage Map configuration": TriageMapConfigurationsManagementModules.jar
- You can delete orphaned triagemap alerts
- For "schedule downtime Triage Map Alerts" or "create alerts for resource metrics" you need to use MM editor
11. TriageMap can be embedded into a dashboard. This feature is NOT supported within Webview.

In 9.6:
12. New Socket grouping feature: it addresses the display problem when there are a large numbers of components displayed with frontend applications. A new "Triage Map Group" Element has been added as an option in the Manaagement Module (you can only group Backends named "System <x> on port <y>"). These new groups will be visible in the TriageMap and Metric Brower Backends > Socket Groups > YourNewSocketGroup)
NOTE: Most of these changes have been done to Webivew code not Workstation (you can see only Triage Map tree socket folder and children groups, no MM changes, TriageMap changes nor location table)

Missing Application or Business Transaction in Triage Map tree

Checklist:

1. Verify that agents are version 9.x.

2. Creating Business Service and Business Transactions is not enough to be able to see this information in the TriageMap. The business Transaction needs to be observed by the Agent.

3. Look for corresponding Application/BT agent metrics reported under the "Metric Browser" tab
   <Host Name>|<Process Name>|<Agent Name>|Business Segment |< BS > |<BT>
   <Host Name>|<Process Name>|<Agent Name>|Frontends |Apps |<AppName> | <Fontend>
   Ensure CEM Integration is working, see CEM to Introscope section

4. Try to restart the EM or the individual agent/jvm; it could be related to a synchronization issue / agent failing to download BT definitions.

5. Verify summary metrics across agents generated under:
   - Custom Metric Host (Virtual) |Custom Metric Process (Virtual) | Custom Business Application Agent (Virtual) | By Frontend | <App. Name> |Health

- Custom Metric Host (Virtual) |Custom Metric Process (Virtual) | Custom Business Application Agent (Virtual) | By Business Service | <BS> | <BT>
Check the EM log for possible calculator errors.

What to collect:

1. zipped content of the EM_HOME\logs from all the EMs(MOM and collectors) (verbose log is required)
2. zipped content of the AGENT_HOME\logs (DEBUG log is required)
3. Screenshot from Triage Map
4. Screenshot from Metric Browser displaying:
   - Custom Metric Host (Virtual) |Custom Metric Process (Virtual) | Custom Business Application Agent (Virtual) | By Frontend
   - Custom Metric Host (Virtual) |Custom Metric Process (Virtual) | Custom Business Application Agent (Virtual) | By Business Service

   From one of the affected agents:
   - <Host Name>|<Process Name>|<Agent Name>|Business Segment |< BS > |<BT>
   - <Host Name>|<Process Name>|<Agent Name>|Frontends |Apps |<AppName> | <Fontend>

Missing Map for Application or Business Transaction available from Triage Map tree

Checklist:

1. Verify that agents are version 9.x.

2. Check that the application has been enabled with appmap tracers: appmap.pbd, appmap-ejb.pbd and appmap-soa.pbd, for most of the cases, jsp, servlet, ejb get detected, however, if this is not the case, you need to create a custom pbd.

3. Information is built based on the apm database, check apm db connection status and look for DB errors in EM log files.

4. Run a sql query in combination to "apm_owner" and "apm_edge" tables to find any map edges stored for that application (owner).

5. It could be related to long duration statements due to
   a. DB performance issues:
      - Check postgres DB logs at <pg_home>\data\pg_log to find the slowest queries reported. In the log you should see a message saying that the query took longer than 500 milliseconds. If this is the case, you might consider modifying the property "log_min_duration_statement" (default value : 500).
      - On the EM properties file, change log level of log4j.logger.org.hibernate.* loggers from ERROR to DEBUG.
   b. Size of the map, amount of data

What to collect:

1. Zipped content of the EM_HOME\logs from all the Ems(MOM and collectors) (verbose log is required)
2. Zipped content of the AGENT_HOME\logs (DEBUG log is required)
3. Screenshot from Triage Map
4. Collect Postgres/Oracle logs. For postgres: <pg_home>\data\pg_log
5. Export of the "apm_owner" and "apm_edge" tables

No MTTR/Customer Experience (CE) metrics/icon.

See "Real Time Transaction Metrics (MTTR)" section.

Location Map

Important reminders
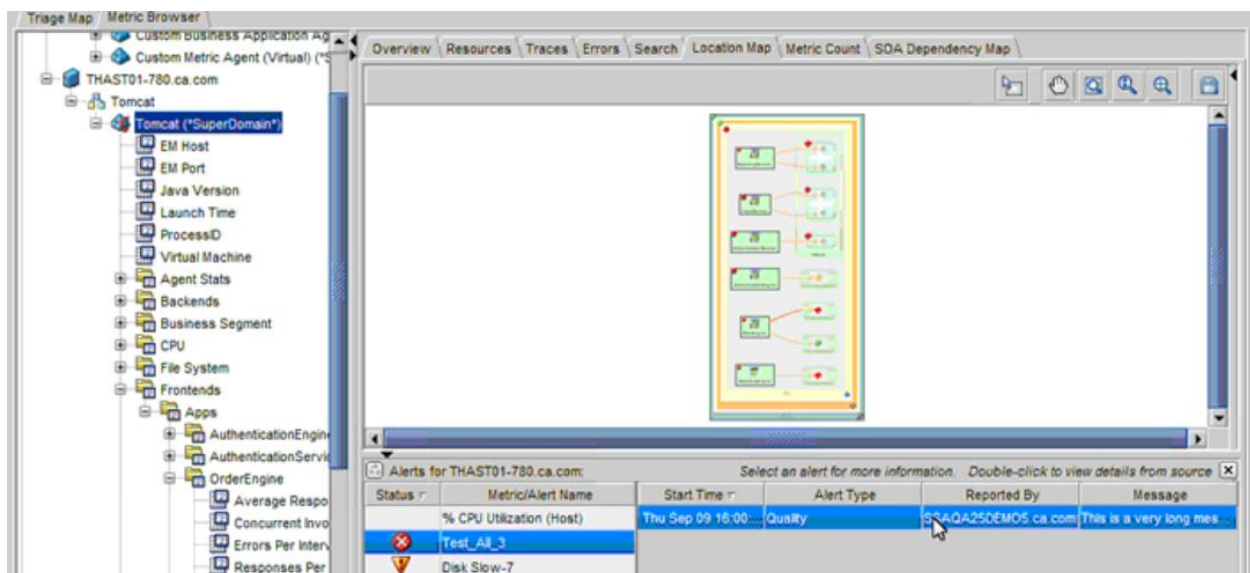
9.1:
1. This feature provides a graphical representation of the application elements (Agents, Frontends, called backends) and external data via Catalyst (database, physical, virtual servers).
2. This feature is not location but Agent centric and it is intended to work together with the TriageMap when troubleshooting a problem.
3. Location Map is available from "TriageMap > Location table" and "Metric Browser > Location Map type viewer)

Location Map missing frontend/backends

Checklist:

1. Information is built based on the metric browser tree > frontends (smartstor data), everything under URLs and backends should show up. By design, it doesn't support custom URL groups, it only considers the "default" node.

2. Review the EM log for any possible clamp issue

What to collect:

1. Zipped content of EM_HOME\logs (VERBOSE log are required)
2. Screenshot from Investigator displaying the Frontends node expanded and from LocationMap showing the missing information.

Location Map is unable to obtain data (physical/virtual server/alerts) from Catalyst

Checklist:

1. Check catalyst data from SSA UI: http://<servername>:7070/ssaweb, navigate CI in question. Make sure it has expected relations and alert.

2. Enable debugging; add the following line to the IntroscopeEnterpriseManager.properties:
   log4j.logger.Manager.Catalyst=DEBUG,logfile
-In debug mode all REST URLs are logged. Note what URLs are used and verify the results in the browser (firefox)

3. If expected alert does not show up verify catalyst and alert filtering settings in EM_HOME\config\Catalyst.properties

4. If database is not found search for the "Insufficient data in database connection string" message. If it exists, note jdbc url in it. Create custom mapfile to fix the problem. Also make sure introscope.agent.appmap.cataystintegration.enable=true in the IntroscopeAgent.profile.

5. If you see timeouts in the EM log increase polling periods.

What to collect:

1. Zipped content of SOI_HOME\logs
2. Zipped content of EM_HOME\logs
3. EM properties file and EM_HOME\config\Catalyst.properties
4. Output of http://<servername>:7070/ssaweb/search

Workstation

Workstation attempts to download a previous version of Java if Java/JRE 7 is installed.

Checklist:

Make sure WebContent\jnlp\workstation.jsp has been updated accordingly:
1. Go to Introscope Enterprise Manager

2. Open
EM_HOME\product\enterprisemanager\plugins\com.wily.introscope.workstation.webstart_9.1.0\WebConten
t\jnlp\workstation.jsp
3. Update the below line:
<j2se version="1.6*&1.6.0_05+"
to
<j2se version="1.7*"
4. Save the file and try again
5. You don't need to restart the EM

NOTE: if you have a mix of workstations using Java6 and Java7 and you need the EM to support those, use the
below line:
<j2se version="1.6*&1.6.0_05+ 1.7*&1.7.0_05+"

Transaction Tracer

Transaction Tracer not displaying full transaction, missing information.

Checklist:

1. Check for possible errors in the EM and agent logs. If you see "transaction trace component limit of <xxx>
   reached" messages in the agent log, increase introscope.agent.transactiontrace.componentCountClamp.

2. If you do not see the expected components, try to set "Lasting longer than" to a lower value, ie: 10
   milliseconds.

3. Check if the components are missing in the investigator tree too.

4. If there are any custom pbds, extensions or formatters created by the Professional Service team, disable them.

What to collect:

1. Zipped content of the EM_HOME\logs
2. Zipped content of the AGENT_HOME\logs and IntrocopeAgent.profile
3. Screenshot from Transaction Tracer displaying the issue.
4. Provide details of which components you are expecting to see.

Query Historical Viewer, no results

Checklist:

1. Does the problem occur using basic filters, such as: type: sampled?

2. Check the EM_HOME log, search for possible exceptions or errors related to the traces database. It could be the case that the db or index is corrupted.

What to collect:

1. Zipped content of the EM_HOME\logs
2. Query detail and what the information you are expecting to see is.
3. Copy of the traces db, zipped content of the EM_HOME\traces folder

Command Line Workstation (CLW)

Important reminders

In 9.1:
5 New CLW commands introduced to support new APM Status Console feature:
-List of active clamps of EM
-list active clamps of EM collectorhost@port
-list active clamps of EM collectorhost1@port1,collectorhost2@port2,etc
-get cluster configuration
-list important events

In 9.5:
New CLW commands introduced to list historical agents
-List Historical Agents
-List historical Agents beteen [time] and [time]
-Turn [off|on] exact metric <metric>

CLW doesn't work, no results

Checklist:
1. Run a small and simple query, for example:
   java -Duser=Admin -Dhost=localhost -Dport=5001 -jar lib/CLWorkstation.jar list alerts matching (.*) in management modules matching (.*)

2. If the problem is related to the high amount of information:
   a) Increase the valued of the EM property introscope.enterprisemanager.workstation.timeout to 120; remember there is a default timeout for the connection between the EM and workstation. For more information, see KB 858.

b)   Increase heapsize, the problem could be related to a lack of memory allocated to the process.

What to collect:

1. Zipped content of the EM_HOME\log
2. Output or screenshot when running the CLWorkstation command and a reference of the time the CLWorkstation command was executed; this will help you correlate the information with the logs.

WebView

Important reminders:

In pre-9.5:
Metric Browser and Console (to display dashboards using Silverlight)

In 9.5:
1. Pure HTML5 and CSS3 (no more Silverlight):
2. Supported browser: IE 8, 9 and Firefox 12, 13, not certified for mobile browser. It is not compatible with IE's "Compatibility View"
3. Document is loaded once, incremental live updates only.
4. Home page layout and queries are fixed by design
5. Data resolution cannot be changed; it is set and locked to sensible values.
6. Webview is not yet localized (English only)
7. Available Features:
–SOA Dependency Map
–Thread Dump typeviewer
–Mgt Modules: Metric Groups, Alert Downtime Schedules
–Dashboards: additional widgets, y-pinning
–Updated links from TESS UI (Defects and Incidents),
–Cross-JVM transaction trace
–URL History ("Bookmarks")
-CEM incidents and defects only.
Not available yet:
- User Preferences
- Charts: Min/Max, Zoom
- Mgt Modules: Calculators editor, SNMP collection, SNMP and shell actions, Dashboard Editor, Report Editor
- Typeviewers: What's Interesting, Change Detector, others
- Dashboard widgets: XML Typeviewers; Application Triage Map; lines, polygons,lens
- Export for events
- Status console, LocationMap
8. Transaction Tracer tab:
- Only available unless the user does not have "Run_Tracer" permission.
- Views: Summary View, Trace View, Tree View. The Sequence View is not supported.
- Filters: No support for the Error, SOA or Mainframe filters, only the Transaction Duration and Parameter filters.
- No support for Transaction Trace features to Export or Save As trace events.

- No support to query for Similar Events or Correlated Events.
- Dynamic Instrumentation is not supported.
9. Pre-instrumentation of webview available. Disabled by default.
10. Known GXT bug: Chart "Y-pinning" does not function in IE 8.

"Long Running Script" Errors

Checklist:

In Windows IE 8, the following message can appear when viewing a graph or dashboard in Webiew:
"A script on this page is causing your web browser to run slowly. If it continues to run, your computer might become unresponsive"

To resolve this issue: upgrade to a supported browser, for example IE 9. The Microsoft Download Center provides a patch to disable the message in IE 8. See http://support.microsoft.com/kb/175500
As a workaround use Firefox 12+.

Slowness, incorrect values, missing information

Checklist:

1. If the problem is related to slowness, compare the result or behavior using an alternative browser, if you are using IE, use firefox instead (recommended browser).

2. If the problem persists, verify the behavior using workstation against the same MOM/EM,

3. Check if the problem is related to the EM/cluster performance – see EM section.

4. If 9.5: Charts in Home Page are topN queries and as such can be expensive, especially in Historical Mode, login to Workstation and disable the below metric grouping from the TriageMapConfigurationsManagementModule.jar management module:
-25 Slowest BTs:Average Response Times (ms)
-25 Worst BTs:Errors & Stalls
-25 Slowest Frontends:Average Response Times (ms)
-25 Worst Frontends:Errors & Stalls

5. Find out if multiple browser sessions were open at the same time. Were those related to TriageMap?

6. Enable debug logging and review EM and Webview logs for possible errors: Open <installdir>/config/IntroscopeWebView.properties, set:
log4j.logger.WebView=DEBUG,console,logfile
log4j.logger.WebServer=DEBUG,console,logfile
log4j.logger.mortbay=DEBUG,console,logfile

7. Clear the cache:
IE – Tools / Internet Options / Browsing History / Delete…
Firefox – Tools / Clear Recent History
Chrome – Ctrl + Shift + Delete

8. Use browser diagnostic tools to diagnose the problem.

IE – Tools / Developer Tools (or F12)
Firefox – Need to install FireBug add-on
Chrome – Ctrl + Shift + J
http://fidder2.com (can see both Requests and Responses, Can be used with any Browser)

What to collect:

1. Zipped content of the MOM/EM logs directory
2. Webview log files
3. If a display issue, screenshot of the problem

Java Agent

Important reminders

In 9.0:
1. Java NIO (buffer and channels) and SSL socket (port and rate metrics) tracing, Deep Inheritance, Support to trace bootstrap classes, Dynamic Instrumentation, New Socket Tracing. NOTE: When using Autoprobe connector all these features will be disabled.
2. Correlation ID over SOAP using additional SOAP Message Transport protocol: HTTP and JMS, this because some apps do not allow us to insert corID in the SOAP message header. NOTE: we are still using handler instead of Tracers for Websphere JAX-RPC 6.1 (server side only). Also: com.wily.introscope.agent.soapheaderinsertion.enabled only works for Java agents.

In 9.1:
3. Lean Agent or New agent mode: New transaction structure used inside the agent allows us to optimize and store relational metrics. The new harvesting strategy requires less synchronization across stack. These agents require Java 5 and 6. New traces (hc2) were created. PBD & PBL refactored (for example SetTracerClassMapping: BlamePointTracerDifferentMethods com.wily.introscope.agent.trace.**hc2**.BlamePointTracer com.wily.introscope.probebuilder.validate.ResourceNameValidator).The New mode is enabled by default. Results: Lower CPU utilization, improved response time and reduced memory utilization.
NOTE: Custom PBDs need to be upgraded to use the new Tracers.
4. Upgrade: new directory structure.
5. In pre-9.1, there have been cases where sockets were not captured on the Frontends, now Sockets are marked as default Backends. You can turn off the new behavior using introscope.agent.configuration.defaultbackends.legacy=false/true
6. New SqlAgent configuration, below default values and meaning:
Intrsocope.agent.sqlagent.sql.turnoffmetric=false – turn off metrics for individual sql statements.
Intrsocope.agent.sqlagent.sql.artonly=false –report only average response time for sql statements.
Intrsocope.agent.sqlagent.sql.turnofftrace=false – turn off transaction tracing for individuals sql statement
Intrsocope.agent.sqlagent.sql.rawsql=false - you can collect SQL bind parameters except for dynamic statements

In 9.1.1:

7. Oracle Java 7 support, however you need to add –XX-UseSplitVerifier to prevent java.lang,VerifyError:StackMapTable error: bad offset. Reason: JSR 202 has made the change in class verification by type checking, thus the method must have StackMapTable attribute. You can use UseSplitVerifier with -Xbootclasspath or -javaagent.

8. Support ORACLE RAC 10gr2, 11i: display format: <SID or Service name><hostname>-<port>(Oracle DB), no change for Stanalone Racle DB

In 9.5.5:

9. Full support of Java7, -Xbottclasspath is not supported with Java7

10. New Socket Clamp(com.wily.introscope.agent.sockets.clamp.level=) and

11. Improvement in Java Agent startup bubble, autoshutdown of Deep Inheritance (introscope.autoprobe.deepinheritance.auto.turnoff.enable=)

In 9.6:

12. Added Smart Instrumentation (Introscope.agent.deep)

Java Agent configuration problem

Checklist:

1. If JVM is IBM J9:
   If you are using JVM 1.5: use AgentNoRedef.jar and IntroscopeAgent.NoRedef.profile.
   If you are using JVM 1.6: use AgentNoRedefNoRetrans.jar and IntroscopeAgent.NoRedef.profile.
   Due to a known issue in IBM JVMs, APM java agents are affected by performance degradations when they attempt to 'redefine' or 'retransform' java classes. Hence, for running APM agents in IBM JVMs we ship a version of the APM agent that has 'redefine' and 'retransform' options disabled. This specialized agent binary is the AgentNoRedefNoRetrans.jar and its corresponding configuration file is IntroscopeAgent.NoRedef.profile

2. Switch from –javaagent to –Xbootclasspath. If the problem persists, the problem is related to a JVM bug. Try upgrading to the latest JVM version or use an alternate JVM. If the problem persists, you need to open a support incident with the jvm vendor.

3. ClassLoading issues: If the appserver fails to startup with the error message: "NoClassDefFoundError: com/wily/introscope/agent/trace/IMethodTracer. The agent requires additional configuration steps:
   a. If Glassfish 3.1.2, open <glassfish_home>\glassfish\config\ osgi.properties and set:
      eclipselink.bootdelegation=oracle.sql, oracle.sql.*, com.wily.*
   b. If Glasfish 3.1.1. open <glassfish_home>\glassfish\osgi\felix\conf\config.properties and set:
      org.osgi.framework.bootdelegation=sun.*,com.sun.*,com.wily.*
   c. If you are using Apache Sling, open the sling.properties, set org.osgi.framework.bootdelegation= com.wily,com.wily*
   d. If you are using Confluence product from Atlassian, add the below system property:-
      Datlassian.org.osgi.framework.bootdelegation=com.wily,com.wily.*,sun.*
   e. If Jboss6.x (you must use Agent 911+) : add -Xbootclasspath/p:%JBOSS6_HOME%\lib\jboss-logmanager.jar –Djava.util.logging.manager=org.jboss.logmanager.LogManager -Dorg.jboss.logging.Logger.pluginClass=org.jboss.logging,LoggerPluginImpl

If you are using JDK 1.6u15 onward, boot.log will not be created; this is due to a Jboss bug affecting agents that perform logging. Workarounds: use JDK 1.6 Update 14 or previous versions OR turn off the logging in the agent profile. You can enable it after the server bootup:

`#log4j.logger.IntroscopeAgent=INFO, console, logfile`

f. If jboss711 or EAP 6.x (you must use agent 911+) : add system property: -Djboss.modules.system.pkgs=com.wily,com.wily.*

If you are using JDK 1.6u15 onward, agent will not start due Jboss bug
https://issues.jboss.org/browse/JBIDE-11338. Workaround: Use JDK 1.6 Update 14 or previous versions OR turn off the logging in the agent profile. You can enable it after the server bootup:

`#log4j.logger.IntroscopeAgent=INFO, console, logfile`

What to collect:

1. Zipped content of AGENT_HOME/logs (DEBUG logs are required)
2. IntroscopeAgent.profile
3. Appserver logs
4. App server config or startup script files.
5. Core dump, if applicable.
6. Exact version of the application server, jvm and OS.

JVM Hangs, Crashes, High CPU, OutOfMemory

Checklist:

1. Use latest agent versions: It is a known issue that 9.1.x agent versions prior to 9.1.1.1 are prone to severe memory leaks.

2. If JVM is IBM J9:
    If you are using Agent 9.1/9.5: use AgentNoRedefNoRetrans.jar and IntroscopeAgent.NoRedef.profile.
    If you are using Agent 9.0x: use AgentNoRedef.jar and IntroscopeAgent.NoRedef.profile.

3. Switch from –javaagent to –Xbootclasspath. If the problem persists, the problem is related to a JVM bug. Try upgrading to the latest JVM version or use an alternate JVM. If the problem persists, you need to open a support incident with the jvm vendor.

4. In case of high CPU, disable manually Platform monitor: you need to move the appropriate OS files (Introscope* and libIntroscope*) out of the /ext directory to another directory.

5. If 9.1+: do not run the agent in mixed mode. You are in mixed mode if you are using any IntroscopeAgentFiles-NoInstaller9.x.x.x<appserver>.<os> packages and you are using:
    a. Websphere Portal, CTG, IBM z/OS, Siteminder Manager, LISA
    b. A custom a PBD still refering to legacy tracers
    c. Agent extension/PBDs created by Professional Service that are not compatible with 9.1 agent new mode.
        In any of the cases above, please apply one of the below recommendations:
        i) Use a legacy agent and keep using a previous configuration.
        iI) Disable any customization and above Powerpacks.

iii) Disable above Powerpacks and upgrade custom pbds. If you are using a formatter created by Professional Service, it might need to be upgraded.

NOTE: Upgrading a custom pbd means replacing all references to old tracers by references to the new ones. For example the line:

TraceAllMethodsOfClass: com.abc BlamedMethodTimer "{classname}|{method}:Average time (ms)"

To upgrade the above line, one needs to replace BlamedMethodTimer with BlamedMethodTimerHC which is mapped to a new tracer:

SetTracerClassMapping: BlamedMethodTimerHC com.wily.introscope.agent.trace.hc2.MethodTimer

See "Tracer-Type-Mapping-Legacy-New-Modes.xls".

6. Find out if the problem is related to the instrumentation, open the IntroscopeAgent profile, set introscope.autoprobe.enable=false; you need to restart the jvm. If the problem does not persist, enable instrumentation back and disable some features to isolate the root cause:

    a. Set introscope.agent.reduceAgentMemoryOverhead=true

    b. If 9.1.1.1+ and Oracle RAC as backend you might notice an overhead as we use reflection to get the correct RAC instance name. Add the below agent property:
        introscope.agent.sqlagent.cacheConnectionsURLs=true

    c. If you are using Agent pre-9.5.5 and are experiencing very long delays on application startup and/or sometimes after startup, this might be due to the large number of classes that are loaded by the application, to resolve the problem set introscope.autoprobe.deepinheritance.enabled=false, disabling deep Inheritance will fall back to pre-90 behavior (only 2 levels of class inheritance).

        NOTE: In 9.5.5+: deep inheritance mechanism has been improved and will shut down automatically to prevent this issue. Additional clamps have been added to better control this condition: introscope.autoprobe.deepinheritance.auto.turnoff.*. In the agent log file you will see entries as below when the deep inheritance has automatically been turned off.
        10/17/13 11:02:35 AM CDT [INFO] [IntroscopeAgent.DeepInheritanceHelper] Deep inheritance configuration: max total time spent (ms) 120000 ; max interval time spent (ms): 12000 ; requests in interval: 100
        10/17/13 11:02:35 AM CDT [INFO] [IntroscopeAgent.DeepInheritanceHelper] Deep inheritance is automatically turned off due to large total delay. total time spent (ms) 120001 ; total requests: 161027255 ; interval time spent (ms): 1 ; interval requests: 95

    d. Disable JMX collection: set introscope.agent.jmx.enable=false

    e. If you are using Agent pre-9.5.5 and are experiencing memory consumption: Turn off the socket tracers in toggles typical/full pbd file.
        TurnOn: ManagedSocketTracing
        TurnOn: SocketTracing
        TurnOn: NIOSocketTracing
        TurnOn: NIOSocketSummaryTracing
        TurnOn: NIOSelectorTracing
        TurnOn: NIODatagramTracing
        TurnOn: NIODatagramSummaryTracing

        NOTE: 9.5.5+ there is a new socket clamping that applies to all kind of sockets above (IOSockets, NIOSockets, NIODatagra and Managed Sockets): com.wily.introscope.agent.socket.clamp.level=100 (it is not hot deploy)

f. Disable any additional Agent extension such as ChangeDetector, Leakhunter, SPM, custom pbd.

7. If you are using SOA SPM:
    a. Turn off SOA boundary tracing, depending on the implementation; it could cause too many traces or too huge traces affecting both Agent and EM (crash/OOM), set com.wily.introscope.agent.transactiontrace.boundaryTracing.enable=false

    b. If you are using CXF and 9.1.2 onward, set com.wily.introscope.soa.cxf.clearoldheaders=all to prevent duplication of corID in the SOAP header and a possible break of the application.

    c. Switch from default SOAP to HTTP header insertion: some app/platform doesn't allow us to insert our corID in the SOAP header thus affecting the application: add the below properties:
    com.wily.introscope.agent.soapheaderread.enabled=false
    com.wily.introscope.agent.soapheaderinsertion.enabled=false
    com.wily.introscope.agent.httpheaderread.enabled=true
    com.wily.introscope.agent.httpheaderinsertion.enabled=true

    d. If you are using application servers that use SOAP handlers and depend on the SOAP engine and API being used (for example: Websphere JAX-RPC server side): By default we prepend on the client and append on the server, however, in some situations, this could break the application; to prevent this, append on the client and prepend on the server: com.wily.prependhandler=false and soa.wily.introscope..soa.server.appendhandler=false

8. If you are using CEM:
    a. Temporally disable the integration, the problem could be related to the BizTrxHttpTracer, as it matches all the requests with the CEM transactions definitions, depending on your implementation and defintions, it could cause a high overhead on the agent side. In addition, disable TriageMap since it uses the same logic as BizTrxHttpTracer, set introscope.agent.appmap.enabled=false.

    b. If you are using Recording by Agent (enabled bizrecording.pbd), you might notice additional delays in response time. Also, be aware that for some appservers when inspecting Servlet "Post parameters" a break of the application might occur. To prevent this, use "introscope.agent.bizdef.matchPost = after" in the IntroscopeAgent.profile. - see "Recording using Agent" section.

9. If 9.1+, switch to Legacy mode; that will revert to old tracer definitions that leverage the traditional "pre-APM 9.1" transaction blame stacks as opposed to the new transaction structure. Open the IntroscopeAgent.profile, add Introscope.agent.configuration.old=true and update directive list with the legacy plbds available from /wily/examples/legacy.

What to collect:

1. Appserver exact version. In case of SPM is used, confirm soap stack version.
2. Zipped content of AGENT_HOME/logs (DEBUG logs are required)
3. IntroscopeAgent.profile
4. Generate a series of 5 thread dumps on the application server for OOM/high CPU situations spaced 5 -10 seconds apart.
5. Appserver logs
6. App server config or startup script files.
7. Core dump, if applicable.
8. Exact version of the application server, jvm and OS.

9. In case of OOM, collect heapdump. Additional jvm switches will be required for this.
   For Sun jvm, add the following jvm switch: -XX:+HeapDumpOnOutOfMemoryError
10. Enable GC log. Additional jvm switches will be required for this.
    For Sun jvm, add the following jvm switches: -Xloggc:<filename>.log -XX:+PrintGCDetails

Unknown SQL node, unable to monitor SQL statements

Checklist:

1. Check the driver type being used to connect to the application. Only type 2 or type 4 drivers are supported. If the problem is with oracle RAC, we support only ORACLE RAC 10gr2, 11i.

2. Open the Agent log, search for possible ERROR or WARN messages, review the Autoprobe log, check if sql methods are being traced.

What to collect:

1. Zipped content of AGENT_HOME/logs
2. If it is a display issue, provide a screenshot from the Investigator displaying the problem
3. What is the database version?
4. A copy of the driver .jar file?

JMX metric are not being reported, missing metrics

Checklist:

1. Ensure the agent has been installed correctly and instrumentation is working – see "Java Agent configuration problems" topic
2. Open the Agent log, check if the problem is not related to the Agent metrics being clamped.
3. Verify that the configuration is correct:

a) For websphere and weblogic, make sure that introscope startup class has been configured as expected and is pointing to the correct location of the WebAppSupport.jar. See TEC605262
b) For Websphere: if J2EE security is enabled you need to define custom properties (jmxusername,jmxpassword) for the Introscope Custom Service with password information in clear text.
c) For Glassfish and Tomcat, open the startup script and add WebAppSupport.jar to the classpath.
e) For Jboss 4, copy WebAppSupport.jar to <jboss>/server/default/lib directory, copy <Agent>/wily/deploy/ introscope-jboss-service.xml to <jboss>/server/default/deploy.
f) For Jboss7 or Jboss6, move the WebAppSupport.jar to <Agent>\wily\core\ext directory.
g) For Jboss6 EAP, see TEC606597
h) For Jboss7 in Domain mode, see TEC606413

Open the IntroscopeAgent.profile:
- add com.wily.use.platform.mbeanserver=true
- set introscope.agent.jmx.enable=true
- set introscope.agent.jmx.name.filter=
- set introscope.agent.jmx.excludeStringMetrics=true

What to collect:

1. Zipped content of AGENT_HOME/logs
2. IntroscopeAgent.profile
3. Appserver config or startup script files.
4. Exact version of the application server, jvm and OS.

PMI counters are not being reported, inaccurate values, negative values

Checklist:

1. We do not do any calculation we just get the values provided by WebSphere API. Verify if the problem is also reproducible using Webphere Tivoli PMI viewer.
2. Our product was designed to support any PMI modules. User has to configure them in agent profile as follows:
    introscope.agent.pmi.enable.New\ Module=true
   The name of the module is case sensitive. If the name of the module contains a space, then it has to be escaped with a backslash "\". For complete details on how to enable PMI metrics, please refer to the powerpack for WAS Distributed guide.

What to collect:

1. Zipped content of AGENT_HOME/logs
2. IntroscopeAgent.profile
3. Server.xml and websphere log files : System.out, system.err.native_stdout, native_stderr.
4. Screenshot from investigator and Tivoli Viewer displaying the issue.
5. Exact version of the application server, jvm and OS.

Platform Monitor is not working

Checklist:

1. Enable DEBUG logging on the Agent profile, it will give you details of the root cause of the problem.

2. Make sure configuration is supported

3. Explicitly enable platform monitor for your OS in the IntroscopeAgent profile, you need to remove the "#" for your specific OS.

4. Make sure all required OS patches have been applied as recommended in the JavaAgent guide.

5. The Platform monitor gets the CPU statistics information from /proc/stat pseudo-file on linux.
   By design, we parse the stat file for all child threads found in /proc and only select those threads that specify an appropriate parent PID that matches the JVM PID. If it failed to open /proc/<PID>/stat Platform Monitor will not work. (The <PID> is the JVM "main" thread PID).

Steps to check the stat:

1. Run the following: $ ps -eaf

2. Find the PID for your JVM "main" thread

3. cd /proc/PID

4. check to see if you can view or open stat.

"vi or cat stat".

What to collect:

1. zipped content of the AGENT_HOME\logs folder (debug log is required)
2. IntroscopeAgent.profile
3. Exact version of the OS, Appserver and JVM

Leakhunter is not working or not detecting a leak

Checklist:

1. Verify that Leakhunter.pbd has been added to the Agent profile and Leakhunter.jar is in the wily/ext
2. Set sensitivity to 10 (default is 5)
3. Set introscope.agent.leakhunter.timeoutInMinutes from default 120 to 240.
4. Send "Leak" dummyagent to confirm that leakhunter functionality is working as expected.

What to collect:

1. Zipped content of the AGENT_HOME\logs – it will include the leakhunter log.
2. Screenshot from the investigator, in case data reported is incorrect.
3. AGENT_HOME\IntroscopeAgent.profile.

Java Dynamic Instrumentation (DI)

Important reminders

In 9.0:

1. Add instrumentation to diagnose the monitored application from a Transaction Trace session

2. Export dynamic instrumentation from running JVM to PBD. Apply dynamic instrumentation from PBD to running JVM

3. Active instrumentation groups (tracer group) or de-activate them from the Investigator tree.

4. After the temporal instrumentation is removed or transaction tracer stopped, metrics will report 0 values until they age out, this because tracers are no longer in the bytecode.

5. You will only be able to instrument methods available under the "Instrumentable" tab. We don't instrument "java" classeses; those will appear under the "Other" tab.

Java DI is not working.

Checklist:

1. It requires Agent 9+

2. Make sure the jvm is 1.5+ and app has been configured with –javaagent.

3. Open the Agent profile and verify that introscope.agent.remoteagentdynamicinstrumentation.enabled=true (hot property) and DI.pbd has been added to introscope.autoprobe.directivesFille.

4. Make sure wily/ext/DynInstrSupport15.jar is in the Agent /ext directory.=

5. DI creates a Derby database in the /logs directory. To fully enable the Dynamic Instrumentation feature, the user under which the application monitored by the agent is running should have write access to the following directories:<Agent_Home> and <Agent_Home>/logs

6. If you are using Websphere, you must use AgentNoRedefNoRetrans.jar and IntroscopeAgent.NoRedef.profile instead of Agent.jar and IntroscopeAgent.profile

7. DI is not supported on Jboss and Tomcat with jvm 1.5. Only 1.6+ is supported for these appservers.

8. Set "Introscope.autoprobe.dynamicinstrument.forceRedefinition=true" to force the agent to use redefinition API when the JVM is 1.5 or IBM JVM.

9. Only BlamePointTracers are currently supported.

10. Some classes cannot be dynamically instrumented, for example:
    a. The one already SkipClass / SkipPackage in active PBDs
    b. Some special class with no byte code or classes that are automatically generated byte code in runtime.

11. Users who connect to the Enterprise Manager using Java Web Start and proceed to use Dynamic Instrumentation (DI) features in the Workstation will encounter some loss of DI functionality if Java version 1.6.0_18 or later is installed on their machine. For full DI functionality, users should have JRE 1.6.0_17 or earlier installed.

What to collect:

Enable the following log modules to get additional information on DI operations:
log4j.logger.IntroscopeAgent.DynamicInstrumentation.Performance=DEBUG
log4j.logger.IntroscopeAgent.DynamicInstrumentation=DEBUG
log4j.logger.IntroscopeAgent.ADynamicInstrumentationService=DEBUG

Try to reproduce the issue and collect the following files:
-Zipped content of the AGENT_HOME\logs
-IntroscopeAgent.profile

GCMonitor

Important reminders

In 9.1:

1. This feature retrieves GC stats for Sun and IBM J9 1.5 and 1.6 (32 and 64bits on any OS). Jrockit is not supported.

2. JVM Memory is divided into different generations, for Sun JVM see:

http://wwww.oracle.com/technetwork/java/gc-tuning-5.138395.html
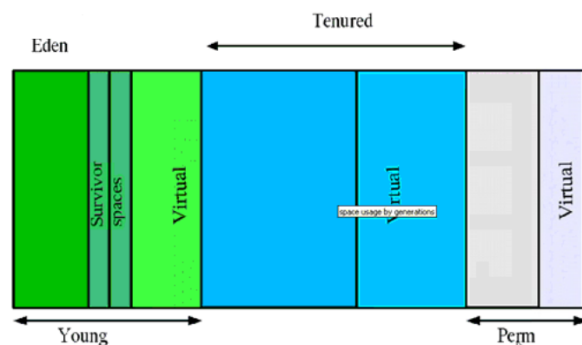
3. We collect this information using Java API Java MXBeans (MemoryMXBean, MemoryPoolMXbean, GarbageCollectionMXBean) instead of reflexion mechanism. Java MXBean is supported by different JVM implementations 1.5 onwards.

4. A "GC Monitor" node is categorized into 2 parts:

a) Garbage collectors: report the algorithms used for garbage collection. For Sun JVM, we monitor "Copy" which is used in the Eden generation and "MarkSweepCompact" used in the Ternured generation. For example, you can see when a gc has occurred: "GC invocation per interval count" and/or how much time it took "GC Time per Interval (ms)"

 b) Memory pool available within a JMV which is divided into different generations, each generation has its own memory. For example, you can see, the "Amount of space used (bytes)"

5. The metrics are reported every heartbeat of 15 seconds against 1 second as reported by previously known field pack.

6. It is enabled by default; to disable it, set introscope.agent.gcmonitor.enable=false (hot property)

7. "Percentage Java of heap used" thresholds are hardcoded: Caution=60, Danger=80. If crossed danger, the Xms and Xmx need to be changed.
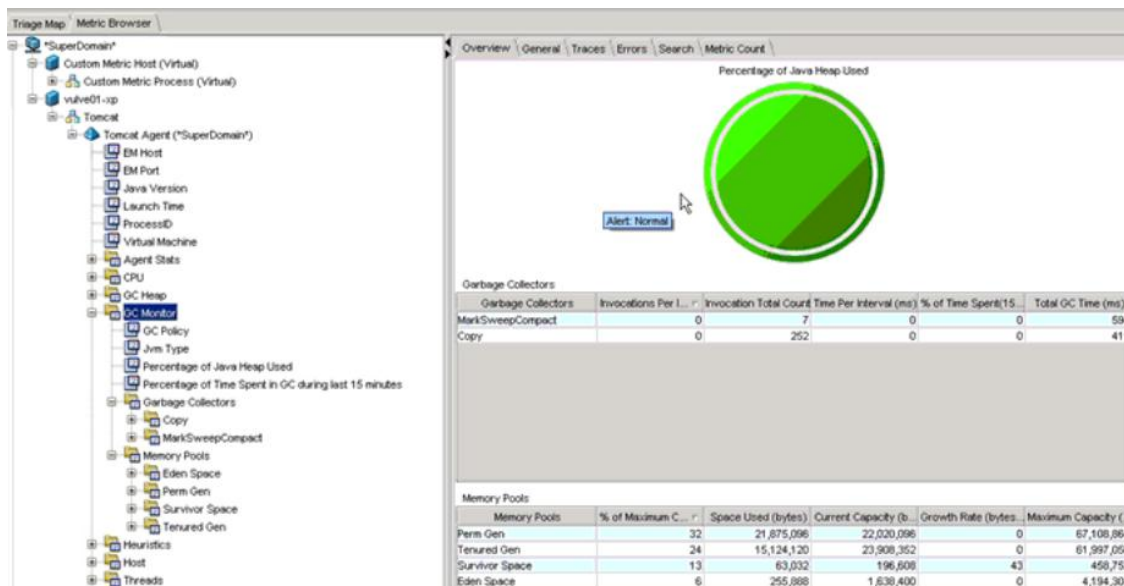
GC Monitor is not working, reporting incorrect values

Applies to: v9.1+

Checklist:

1. Check jvm version. GCMonitor is supported with Sun and IBM jvm only (no Jrockit) 1.5 onward versions.

2. If not working, make sure GCMonitor.jar is available and introscope.agent.gcmonitor.enable=true

3. (If reporting incorrect values) use Jconsole to compare/validate results.

What to collect:

1. Zipped content of the EM_HOME\logs
2. Zipped content of the AGENT_HOME\logs (verbose log is required)
3. (If reporting incorrect values) Collect screenshot displaying results from Investigator and Jconsole

Smart/Intelligent Instrumentation (SI)

Important reminders

In 9.6:
1. No need to create a custom PBD, turned off by default. Instrumentation based on byte code analysis (does not take into account any runtime analysis). It is only available in NEW mode an only for Java agent.

2. By design, deep components in transaction tracer are identified with a "ligjtning bolt" (only available in Webview not Workstation)

3. Deep components can be identified in Error snapshot, they are presented as "class::method"":

Smart Instrumentation is not working

Checklist:

1. SI requires Agent 9.6 in New mode and it is only supported with Java Agent. Ensure JVM is 1.5, 1.6 or 1.7.

2. Make sure introscope.agent.deep.instrumentation.enable=true and introscope.agent.deep.trace.enable=true (hot property). If problem is related with Deep components in Error snapshot, check that introscope.agent.deep.errorsnapshot.enable=true

3. Verify SI supportability metrics: Agent Stats| Sustainability|DeepTracing:Instrumented Methods Count and Agent Stats| Sustainability|DeepTracing:Analyzed Methods Count

4. Check for any problem/unexpected condition in the instrumentation:
   - If class is skipped by any regular PBD, then SI also skip the class
   - If the methods within the class are instrumented by regular tracer then only regular instrumentation is applied, SI will skip the method
   - If the methods within the class are not instrumented by regular tracer, then the skip directive of SI are checked.

5. Try setting Introscope.agent.deep.intrumentation.level=high so more methods are instrumented. It requires appservers restart.

6. Check if clamps have been reached: Introscope.agent.deep.instrumentation.max.methods=1000 (it requires appserver restart), or Introscope.agent.deep.trace.max.components=1000, it doen't require appserver restart.

What to collect:

-Zipped content of the AGENT_HOME\logs
-IntroscopeAgent.profile

ThreadDumps

Important reminders

1. This feature allows Admins or users with appropriate permissions to take a thread dump. In domains.xml, add <grant user="username" permission="Thread_Dump"/>

2. All jvms are supported, no support for .NET agent, and supported only with 9.1 agents.

3. This feature is enabled by default:

On the EM: introscope.enterprisemanager.threaddump.enable=true (hot property)

On the Agent: introscope.agent.threadump.enable=true (hot property)

4 You can enable "Thread > Deadlock" metric to know if there is any thread deadlock. This feature is disabled by default:

Introscope.agent.threaddump.deadlockpoller.enable=false (hot property)

Introscope.agent.threaddump.deadlockpollerinterval=15000 (=15 seconds)

5. You should take a threaddump when you see a stall over period of time, for example more than 10 minutes or when the dead lock metric shows an Increase.

6. If you need to schedule a threadump generation, you can use of the available CLW API:

get Threadump for the agent matching [REGULAR EXPRESSION] for functional

get List of ThreadDump filenames for the agent matcing [REGULAR EXPRESSION]

load ThreadDump [EXACT MATCH] for the agent Matching [REGULAR EXPRESSION]

7. Limitation:

-Saving a threadump as a Text file will truncate it; only the top 10 levels will be saved. Workaround: always refer to the original files generated from the EM_HOME/threadumps

-thread dumps are loaded depending on the agentname. If the agent is renamed then the historical thread dump on the agent will not be accessible anymore.

8. In a cluster, threaddumps are saved in the Collectors
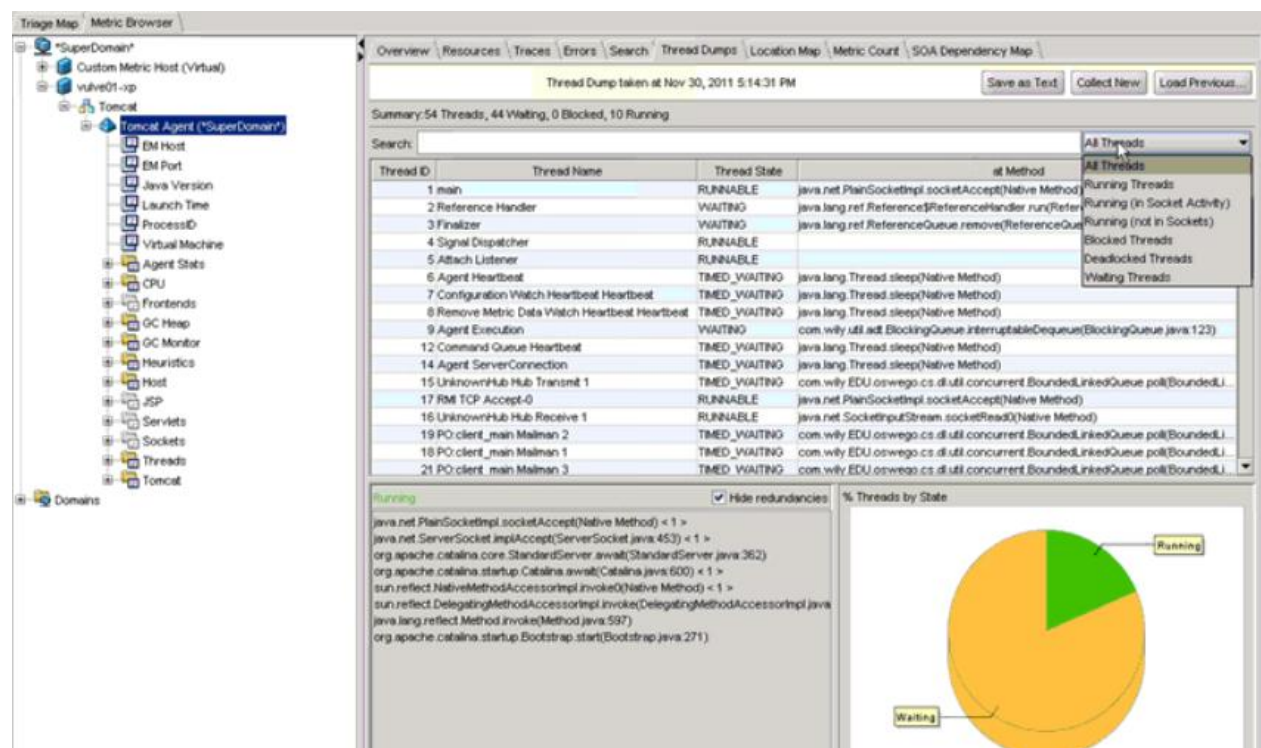
Unable to take threadumps from the Workstation

Checklist:

1. Make sure permissions to take threadumps have been granted to you in the domain.xml. Verify the problem using the Admin user account.

2. In a cluster, threadumps will be saved on the collector server.

3. Make sure the following properties have been enabled:
   On the Agent: intrsocope.agent.threadump.enable=true (hot property)
   On the EM: introscope.enterprisemanager.threaddump.enable=true

4. If the threadump is huge, increase the following property in the agent profile. The limit is 50000
   introscope.agent.threaddump.MaxStackElements=12000

5. It is recommended to leave a gap of 1 minute between two batches of 5 consecutive thread dumps or there will be a strain on performance.

What to collect:

1. Zipped content of the EM_HOME\logs(verbose log is required)
2. Listing content of the EM_HOME\threadumps directory.
3. EM_HOME\config\domains.xml
4. Zipped content of the AGENT_HOME\logs (verbose log is required)
5. IntroscopeAgent.profile

Unable to load a previously taken threadump

Checklist:

1. Has the agent been renamed? Thread dumps are loaded depending on the agent name. If the agent is renamed then the historical threaddump on the agent will not be accessible.

2. Are you able to load any other threadump?

3. Verify if the threadump exists as they are purged periodically
   (introscope.enterprisemanager.threadump.storage.clean.disk.freq.days=1)

What to collect:

1. Zipped content of the EM_HOME\logs(verbose log is required)
2. Listing content of the EM_HOME\threadumps directory.
3. Zipped content of the AGENT_HOME\logs (verbose log is required)
4. IntroscopeAgent.profile

EPAgent

EPAgent is not reporting data or is reporting data incorrectly

Checklist:

1. Enable DEBUG logging in the EPAgent properties file, it will give you the details of the root cause of the problem. If EPAgent is working successfully, you should see lines confirming that EPAgent is sending metrics to the EM.

2. Make sure the EPAgent properties file is pointing to the right EM and that EPAgent plugins are enabled.

3. If the problem occurs when using custom EPAgent plugins, verify first if the problem is reproducible using one of the plugins bundled with the EPAgent package, such as "Disk".
   If the problem only occurs using the custom scripts, professional services need to be involved. Otherwise, disable the line in your script until you identify what the root cause of the problem is.

What to collect:

1. zipped content of the EM_HOME\logs
2. zipped content of the EPAGENT_HOME\logs folder (debug log is required)
3. Introscope EPAgent properties file.

.NET Agent

Important reminders

In 9.0:
1. NativeProfiler in 9.0 to address the following problems: mix of native (c++) and managed code (C#), slow COM transaction between layers, only static instrumentation is possible and limited third party instrumentation engine.
2. Leakhunter .NET using tracers

In 9.1:
3. NET Agent installer changed from InstallAnywhere to InstallShield (.msi). InstallAnywhere has limitations to grant permission, now no manual steps are required for Windows 2008 or Vista.
4. NET agent is able to instrument 32 and 64bits apps
5. Startup bubble: 50% to 80% improvement on startup time:
a) Directive Matching improvement with In-Memory Cache has been implemented. DirectiveMatchingCache is controlled by: introscope.nativeprofiler.directivematching.cache.max.size=5000.
Once this cache limit is crossed "cache has been reached" message will be logged in nativeprofiler log, increasing this value will affect the memory.
b) The ngen monitoring allows the .NET Agent to instrument .net classes in the ngen image cache. This provides better monitoring coverage, but it can impact the startup performance. To prevent this set introscope.nativeprofiler.ngen.monitor.enabled=false.
6. Reduced Perform overhead: previously, perform collection were reported for each agent incurring significant

performance overhead. From 9.1 Perform is a standalone service "CA APM Perfmon Collector Service" (PerfMonCollecotorAgent.exe) which reduces overhead.

7. Support for .NET 4.0 applications

8. "Run Side by Side" feature is supported, which allows multiple versions of CLRs inside the same process and runs them side by side, the following property controls the loading option for profiler: com.wily.introscope.nativeprofiler.monitor.inprocsxs.multiple.clrs. By default "none" means that the first CLR loaded will be instrumented. Valid values are None, V2/v2.0.50727 and V4/v4.0.30319.

Limitations:

a) No separate agent naming for two instances of CLRs in the same host process, for example, if SampleHost.exe process hosts 2 CLR versions side by side and both gets instrumented the agent still appears like SampleHost.exe and SampleHost.exe%1. This is due to a Microsoft limitation.

b) "Run Side by Side" many CLRs will not work when DI is enabled.

c) "Run Side by Side is not applicable to ASAP.NET web application or in other words IIS host applications, it is only supported for standalone apps.

In 9.1.1:

9. Full WCF binding support

11. Support for HTTP/HTTPS communication with EM

.NET Agent Installation problems, instrumentation is not working.

Checklist:

1. Make sure you are using the correct .NET agent installer package. Use 64bit installer in case a 64bit machine and you need to monitor 32 and 64 bit applications.

2. Search for errors in the install log:
   In v8.x or 9.0x AGENT_HOME\wily\install\Introscope_Agent_for_.NET_x.x.x.x_InstallLog.log
   In v9.1 and 9.5: installer log is located in the folder where the .exe installer is. When using .msi, the installer log is located at the %temp% folder

3. Verify that the correct version of wily.Agent.dll has been registered in the GAC (c:\windows\assembly). If not listed, you need to register it manually, drag and drop AGENT_HOME\wily\bin\wily.Agent.dll into C:\Windows\assembly

4. Verify that the below environment variables exist:
   Cor_Enable_Profiling=0x1
   COR_PROFILER={5F048FC6-251C-4684-8CCA-76047B02AC98}
   com.wily.introscope.agentprofile=<install_dir>\wily\IntroscopeAgent.profile
   If you are using .NET 4.0 and Agent 9.0x, ensure the below environment variable is set:
   COMPLUS_ProfAPI_ProfilerCompatibilitySetting=EnableV2Profiler

5. Make sure permissions to the AGENT_HOME have been set accordingly. For example, if you are trying to instrument a Windows service or standalone app, you should run: <AGENT_HOME>\wily\wilypermission.exe <AGENT_HOME>\wily <mytestapp.exe>

6. Verify that the .NET agent is attached to the .NET process using "tasklist /m". For example: If you are trying to monitor IIS: access the application and run tasklist /m
   For 9.1x: "wily.Agent.dll" and "wily.NativeProfiler.dll" should be attached to the process.

For pre-91 / autoprobe instrumentation: "wiily.AutoProbe.dll" and "wily.Agent.dll" should be attached to the .Net process.

7. If CLR is v4, set introscope.nativeprofiler.clrv4.transparency.checks.disabled=true, restart IIS, and try again. The .NET 4 CLR has some additional checks on certain assemblies which may invalidate the instrumented code, thus throwing VerificationException. This agent profile setting will suppress these checks when set to true.

8. It could be the case that the main method of the application has been instrumented however it is not the entry point to the application, set introscope.nativeprofiler.generic.agent.trigger.enabled=true

9. If you are using multiple .NET/CLR version, ensure the correct CLR is monitored, the following property controls the loading option for profiler: com.wily.introscope.nativeprofiler.monitor.inprocsxs.multiple.clrs
By default "none" means that the first CLR loaded will be instrumented.. Valid values are None, V2/v2.0.50727 and V4/v4.0.30319.
Limitation: If you have DI enabled use either V2 or V4 but not both. You cannot use multiple Vs for IIS or when DI is enabled, it is only for standalone apps.

10. Try configuring the agent to instrument all .NET applications by commenting the introscope.agent.dotnet.monitorApplications agent property. This will help you confirm that the problem is related to the application.

11. Look at the Windows Event viewer for Application log Error messages:

    a. APM .NET Agent GUID is **{5F048FC6-251C-4684-8CCA-76047B02AC98}**. If you see an error message similar to:
    "Failed To Co CreateProfiler" ***"The profiler was loaded successfully. Profiler CLSID: '{D6E0BA92-3BC3-45ff-B9CC-B4B5AB7190BC}***

    That indicates that there is another CLR profiler preventing the .NET Agent from probing the .NET process. You need to uninstall it. You can try disabling it from the regedit, search for "COR_PROFILER" or the CLSID. A common situation is with AVICODE application. See "Avicode conflicts with the .NET agent.doc"
    b. You notice the following error in Windows event:
    "System.InvalidProgramException: Common Language Runtime detected an invalid program"
    "…cannot be activated due to an exception during compilation".
    This is a result of windows update: KB2742599 Security Update for Microsoft Windows".
    http://technet.microsoft.com/en-us/security/bulletin/ms13-004
    http://support.microsoft.com/kb/2742599/en-us
    Workaround: turning off WCFRuntimeTracing in the webservices.pbd
    Fix included in 9.5 and 9.1.7

12. Too much instrumentation: Try to disable all or part of the instrumentation:

    a) Disable instrumentation, set introscope.autoprobe.enable=false

    b) Disable Perfmon collection:
       If v8.0, 9.0x: disable perform property in the Agent profile
       If v9.1+: stop the Windows Perfmon collector service.

    c) In the agent profile, instead of monitoring all IIS application pool, which is done by default, only monitor a subset, you can start by monitoring a basic simple standalone application.

    d) If v9.1+, If the problem is related to startup performance, try disabling "ngen monitoring" - it allows the .NET Agent to instrument .net classes in the ngen image cache. This provides better monitoring coverage,

but it can impact the startup performance, set introscope.nativeprofiler.ngen.monitor.enabled=false.

e) In the agent profile, disable Appmap: introscope.agent.appmap.enabled=false

f) In the agent profile, disable bizrecording: introscope.agent.bizRecording.enabled=false

g) In the agent profile, reduce SQL instrumentation:
introscope.agent.sqlagent.sql.turnoffmetrics=true
introscope.agent.sqlagent.sql.artonly=true
introscope.agent.sqlagent.sql.turnofftrace=true

Or turn off the following trace option in the toggles typical/full pbd
#TurnOn: SQLAgentCommands
#TurnOn: SQLAgentDataReaders
#TurnOn: SQLAgentTransactions
#TurnOn: SQLAgentConnections

h) Disable any additional extension (such as ChangeDetector, SPM) or custom PBD.

i) Turn off Socket instrumentation in the toggles typical/full.pbd:
#TurnOn: SocketTracing

j) Turn off SPM instrumentation in the toggles typical/full.pbd:
#TurnOn: WebServicesCorrelationTracing
#TurnOn: WCFServerFaultTracing
#TurnOn: WCFClientFaultTracing
#TurnOn: WCFServerTracing
#TurnOn: WCFClientTracing
#TurnOn: WCFRuntimeTracing

What to collect:

Enable DEBUG: In the logging.config.xml
If the application crashes, enable by code logging, set introscope.nativeprofiler.logBytecode=true and introscope.nativeprofiler.logAllMethodsNoticed=true

Reproduce the issue and collect the below information

1. Install logs:
   If 8.x, 9.0x: zipped content of the AGENT_HOME/install/*.logs
   If 9.1x and 9.5x: installer log is located at the folder where the .exe installer is. When using .msi, the installer log is located at the %temp% folderZipped content of the AGENT_HOME/wily/logs folder
2. AGENT_HOME/wily/IntroscopeAgent.profile
3. The result of "systeminfo" command.
4. The result of "set" command.
5. Exercise the application, then run "tasklist /m", send the output.
6. Scrennshot of the C:\windows\assembly folder, listing the wily.Agent.dll
7. Screenshot of application events from Windows Event viewer

.NET app crash, high CPU, OutOfMemory(OOM), huge native memory usage.

Checklist:

1. Ensure the installation is correct – see ".NET installation" topic

2. Use latest agent versions: It is a known issue that 9.1.x agent versions prior to 9.1.1.1 are prone to severe memory leaks.

3. Memory overhead/leak issues due to frequent disconnection between agent and EM

    Ater 9.1.1.1, there were additional fixes made to help mitigating certain memory overhead/leak issues due to frequent disconnection between agent and EM. Upgrading to the latest 9.1.7 or 9.5.x is recommended.

    Check if loadbalancing is causing the .NET agent connection to be rejected.
    Try to configure the Agent to point directly to the collector.

4. Enable autoConfig at .NET application to allow the applications to be working in optimal mode:
    Default configuration settings are specified in the Machine.config file located in the %SystemRoot%\Microsoft.NET\Framework\versionNumber\CONFIG\ directory.
    Search for autoconfig in it which appears similar to the below which is default true. This change needs a restart of the IIS and do not work immediately.

    > `<processModel autoConfig="true" />`

    Review the below blog for additional details
    http://blogs.msdn.com/b/carloc/archive/2009/02/19/minworkerthreads-and-autoconfig.aspx

5. Too much instrumentation: Try to disable all or part of the instrumentation in order to identify the root cause:
    k) Disable instrumentation, set introscope.autoprobe.enable=false

    l) Disable Perfmon collection:
        If v8.0, 9.0x: disable perform property in the Agent profile
        If v9.1+: stop the Windows Perfmon collector service.

    m) In the agent profile, instead of monitoring all IIS application pool, which is done by default, only monitor a subset, you can start by monitoring a basic simple standalone application.

    n) If v9.1+, If the problem is related to startup performance, try disabling "ngen monitoring" - it allows the .NET Agent to instrument .net classes in the ngen image cache. This provides better monitoring coverage, but it can impact the startup performance, set introscope.nativeprofiler.ngen.monitor.enabled=false.

    o) In the agent profile, disable Appmap: introscope.agent.appmap.enabled=false

    p) In the agent profile, disable bizrecording: introscope.agent.bizRecording.enabled=false

    q) In the agent profile, reduce SQL instrumentation:
        introscope.agent.sqlagent.sql.turnoffmetrics=true
        introscope.agent.sqlagent.sql.artonly=true
        introscope.agent.sqlagent.sql.turnofftrace=true

        Or turn off the following trace option in the toggles typical/full pbd

#TurnOn: SQLAgentCommands
#TurnOn: SQLAgentDataReaders
#TurnOn: SQLAgentTransactions
#TurnOn: SQLAgentConnections

r) Disable any additional extension (such as ChangeDetector, SPM) or custom PBD.

s) Turn off Socket instrumentation in the toggles typical/full.pbd:
   #TurnOn: SocketTracing

t) Turn off SPM instrumentation in the toggles typical/full.pbd:
   #TurnOn: WebServicesCorrelationTracing
   #TurnOn: WCFServerFaultTracing
   #TurnOn: WCFClientFaultTracing
   #TurnOn: WCFServerTracing
   #TurnOn: WCFClientTracing
   #TurnOn: WCFRuntimeTracing

6. Switch to Legacy mode:

   Starting from 9.1.x, the agent supports a "legacy" mode option that will revert to old tracer definitions that leverages the traditional "pre-APM 9.1" transaction blame stacks as opposed to the new transaction structure.

   - Stop all monitored .NET apps.
   - Archive and delete existing log files in the <Agent_Home>/logs directory to prepare for new logs.
   - Back up existing .pbl and .pbd files in the <Agent_Home>/core/config directory.
   - Back up the existing <Agent Home>/core/config/IntroscopeAgent.profile.
   - Copy the legacy .pbl and .pbd files from the <Agent_Home>/examples/legacy directory to the <Agent Home>/core/config directory.
   - Edit <Agent_Home>/core/config/IntroscopeAgent.profile and make the following changes:

   a. Add a new property: introscope.agent.configuration.old=true
   b. Update the agent property introscope.autoprobe.directivesFile to point to the appropriate legacy .pbl and/or .pbd files that have been copied over. For example, replace spm.pbl with spm-legacy.pbl.
        (Note: you can still use the custom xrm.pbd with the BlamePointTracer definition.)
   c. Use default-typical.pbl instead of default-full.pbl.
   d. Disable Appmap: introscope.agent.appmap.enabled=false
   f. Disable bizrecording: introscope.agent.bizRecording.enabled=false

   - Restart the monitored application.
   - Check agent/EM/application/system logs for any errors or unusual messages.
   - Capturing few consecutive dumps upon high CPU and/or memory overhead.

What to collect:

   Enable DEBUG: In the logging.config.xml
   If the application crashes, enable by code logging, set introscope.nativeprofiler.logBytecode=true and introscope.nativeprofiler.logAllMethodsNoticed=true

   Reproduce the issue and collect the below information

1. AGENT_HOME/wily/IntroscopeAgent.profile
2. The result of "systeminfo" command.
3. The result of "set" command.
4. Exercise the application, then run "tasklist /m", send the output.
5. Scrennshot of the C:\windows\assembly folder, listing the wily.Agent.dll
6. Screenshot of application events from Windows Event viewer
7. If the issue is related to WCF/webservices collect investigator screenshot and information about the type of webservice /binding that is used.
8. Use Debug Diagnostics Tool from Microsoft to capture user dump, which contains both heap and thread snapshots. The following KB has both a download link and usage instructions: http://support.microsoft.com/kb/2580960

   Follow the steps described in the below link to capture the performance dumps: http://blogs.technet.com/b/mspfe/archive/2011/12/01/how_2d00_to_2d00_effectively_2d00_capture_2d00_windows_2d00_memory_2d00_dumps_2d00_pt_2d00_1_2d00_using_2d00_debugdiag.aspx

   There are multiple ways to capture dumps on.NET process. One quick way is to bring up Task Manager, find the .NET process with the memory issue, and then right click on the process to select Create Dump File option in its context menu.

   Or, use procdump.exe from Microsoft, it is a free utility included with Sysinternal or other Windows admin toolkit, follow the below steps:
   - Identify the PID (process ID) of the .NET process, e.g. say 6789 for a w3wp.exe process, that is having unusual high CPU.
   - Run the following command to capture 3 dumps with 5 seconds apart: e.g.
     Procdump.exe -ma -s 5 -n 3 6789
   - If the .net app is a 64-bit process, then add -64 to the commandline: e.g.
     Procdump.exe -64 -ma -s 5 -n 3 6789 5. Analyze the dumps.

.NET Dynamic Instrumentation (DI)

Important reminders

In 9.1:
1. "Adding Temporary Instrumentation to all called methods" and "Changing Instrumentation Level" options are not supported, whereas in Java you could instrument all called methods
2. In Java when you select "Make permanent", it creates a pbd and the new instrumentation is applied immediately, whereas in .NET, a new pbd Change_<timestamp>.pbd is created and you need to restart the app to see the new instrumentation.
3. By default this feature is turned off: introscope.agent.remoteagentdynamicinstrumentation.enabled=false
4. In Java DI, you can turn on/off tracer groups from investigator. This is not possible using .NET DI
5. In Java we reinstrument a class, in .NET it is not possible to reload or recompile.
6. New instrumentation will be created under a new node called "Dynamicinstrument" in the investigator.

.NET DI is not working

Checklist:

1. Ensure introscope.agent.remoteagentdynamicinstrumentation.enabled=true (by default = false)

2. Permanent instrumentation creates a PBD under "dynamic" directory. Make sure you have the right permissions on the wily/dynamic folder

3. application/IIS need to be restarted to view permanent Instrumented metrics.

What to collect:

Enable DEBUG: In the logging.config.xml, Reproduce the issue and collect the below information:
Introscope Agent profile
Zipped content of [NETAGENT_HOME]\dynamic*
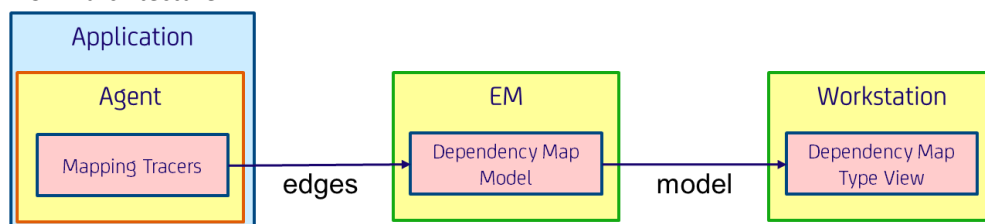Zipped content of [NETAGENT_HOME]\logs*
Screenshot from Transaction Tracer windows displaying the main classes, provide details of which methods you are expecting to see.

SOA Dependency Map

Important reminders

In 9.0:
1. Support for SOA powerpacks (OSB, WPBS, TIBCO, Webmethods, MQ) using single level naming

2. SPM architecture:

- Agent (detects and transmits "dependencies" as edges, caches known dependencies and uses "correlation id" for cross-process dependencies)
- EM extension (incremental construction of model, model is persisted to disk once every hour or when the EM is shutdown under the /data/dependency folder, aging dependencies, remove vertices and edges for umounted agents)
- Workstation dependency map view: display a fragment of the dependency model. By design, the initial view point determined by node in Investigator tree plus 1 level of dependency.

3. In a cluster, collectors hold partial model or connected agents, MOM merges partial nodes.

4. Dependency map clamps to limit the complexity of dependency map model:

On the EM:
- Maximum number of vertices: com.wily.introscope.soa.dependencymap.max.vertices=5000 by default
- Maximum number of edges expressed as a ratio to vertices:
   com.wily.introscope.dependencymap.max.edge.ratio=5 by default (that means 5 * 5000 = 25000 edges.
On the Workstation:
- Maximum number of displayed nodes: com.wily.introscope.soa.dependencymap.ui.view.nodecount=200 by
   default. Drawing the dependency map is very high CPU intensive. If there is a high # of nodes in the
   dependency map it will overload the EM with the # of metric queries. This property cannot be changed when
   using the workstation webstart.

5. Support MQ protocols for showing dependency of Webservices communications in SOA dependency map.

Dependency map is wrong

1. Verify that the agent(s) hasn't been unmounted. If it is a cluster try restarting the MOM, it could be related to
the MOM issue where MOM is not updated with deleted vertices and edges from collectors

2. Enable traces options on the EM and Agent side:
   a. Add com.wily.introscope.soa.dependencymap.readable.enable=true (hot property) in the EM properties file,
      every time the map is persisted in the data/dependency, it will also create a readable form of the dependency
      map in a file called: dependencymap.txt. This will help you narrow down the issue and identify if the problem
      is in the UI, Model or Agent.
   b. Add com.wily.introscope.soa.dependencymap.log.incoming.enable=true. To trace incoming transaction
      bundles from Agent to EM. The output will be found in the EM log file.

3. If the problem is related to MQ protocols not showing in SOA dependency map, make sure to: a) uncomment
webspheremq-extra.pbd in webspheremq.pbd) and that below properties are enabled:
com.wily.introscopeagent.mqheaderinsertion.enabled, com.wily.introscopeagent.mqheaderread.enabled in the
MQMonitor.properties file.

What to collect
1. Agent profile
2. Agent and EM debug logs
3. Zipped content of the data/dependency from MOM, make sure to collect dependency.txt.

SOA Deviation Metrics not generated in Deviation tab, [Harvest Engine Pooled Worker] [Manager] java.lang.NullPointerException

Increase "com.wily.introscope.soa.deviation.max.metric.count". There are 3 SOA deviation calculators; the value
specified for the above property is for all 3 calculators altogether. By default the value is 1000, meaning each
deviation calculator will handle max 333 metrics.

[Manager] Not able to connect to the dependency map remote collector. It might not be fully initialized yet, will retry once again after sleeping 10,000 seconds

-Make sure SOA SPM has been deployed in all the EM (Mom and Collectors).
-Try restarting all the EMs

Oracle Service Bus (OSB) SPM extension

Not working, missing metrics, wrong values

Checklist:

1. Make sure the configuration is supported, confirm the OSB and soap stack version
2. SPM is a prerequisite. Deploy SPM first and then the OSB extension.
3. Verify the installation:
-ensure the agent profile includes OSB-full.pbl or OSB-typical.pbl.
-OSBAgent jar has been copied to the agent ext directory
4. If the problem is a display issue (wrong values or missing, metrics), test the issue using one of the sample apps that come with OSB. This will help us confirm if the problem is app specific.

5. When using lean/new agent with socket tracing enabled on OSB 11.x GC cycles are increased.Workaround: use legacy mode or disable socket tracing.

What to collect:
Exact OSB and soap stack version
OSB startup script
OSB logs
IntroscopeAgent.profile
Listing content of the agent /ext directory
Zipped content of the [AGENT_HOME]\logs
Zipped content of the [AGENT_HOME]\logs (DEBUG log is required)
If the problem is a display issue (wrong values or missing, metrics) send a screenshot from investigator/transaction traces view displaying the issue.

TIBCO BW SPM Extension

Not working, missing metrics, wrong values

Checklist:

1. Make sure the configuration is supported

2. SPM is a prerequisite. Deploy SPM first and then Tibco extension.

3. If the problem is a display issue (wrong values or missing, metrics), test the issue using one of the sample apps that come with TIBCO BW, this will help us confirm if the problem is app specific. for example:

c:\tibco\bw\5.9\examples\activities\soap\soap_over_http\soap_over_http.zip

What to collect:

Exact TIBCO and soap stack version

[TIBCOBW_HOME]\bw*\bin\bwengine.tra

[TIBCOBW_HOME]\tra\domain*\logs*.log*

IntroscopeAgent.profile

Listing content of the agent /ext directory

Zipped content of the [AGENT_HOME]\logs (DEBUG log is required)

If the problem is a display issue (wrong values or missing, metrics) send a screenshot from investigator/transaction traces view displaying the issue.

WPS/WESB SPM Extension

Not working, missing metrics, wrong values

Checklist:

1. Make sure the configuration is supported.

2. SPM is a prerequisite. Deploy SPM first and then WPS/WEBS extension.3. Ensure installation is correct:

- wps.pbd or wesb.pbd has been configured in the Agent profile

-SOAExtensionWPS jar has been copied to the agent ext directory.

What to collect:

Exact WPS/WESB and soap stack version

IntroscopeAgent.profile

Listing content of the agent /ext directory

Zipped content of the [AGENT_HOME]\logs (DEBUG log is required)

If the problem is a display issue (wrong values or missing, metrics) send a screenshot from investigator/transaction traces view displaying the issue.

Powerpack for Weblogic

Negative values

Checklist:
1. Disable custom pbds or any additional extensions from Professional Services
2. Make sure the configuration is supported.

What to collect:

1. collect screenshots from the investigator displaying the issue
2. zipped content of the EM_HOME\logs
3. zipped content of the EM_AGENT\logs
4. IntroscopeAgent.profile
5. Exact appserver version, jvm and OS.
6. Appserver log
7. Appserver startup script
8. Listing content of the AGENT_HOME directory to verify that required PP files are in the appropriate locations.

Powerpack for Websphere

PP for Websphere is not working and trowing exceptions in the Webpshere log

Checklist:
1. Disable custom pbds or any additional extensions from Professional,
2. Make sure configuration is supported.
3. Verify that the powerpack has been installed correctly and required files are in the appropriate locations.

What to collect:

1. zipped content of the AGENT_HOME\logs
2. IntroscopeAgent.profile
3. appserver: pmi-config.xml, sib-service.xml and server.xml
4. Websphere log files: System.out, system.err.native_stdout and native_stderr.
5. server.xml
6. Listing content of the AGENT_HOME directory to verify that required PP files are in the appropriate locations.

Browser Response Time Monitor (BRTM)

Important reminders:
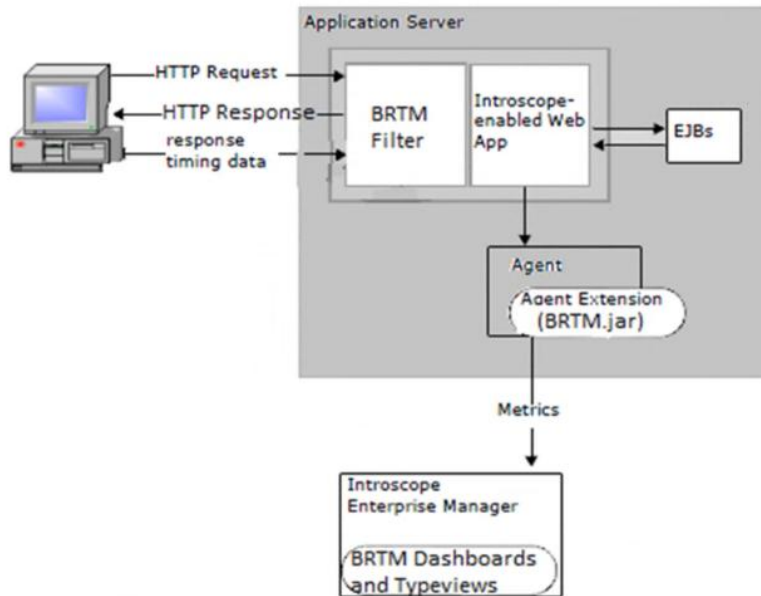
In 9.5:

1. Support manual and automatic insertion of BRTM filter. Automatic only available for Weblogic
2. Support manual and automatic insertion of Javascript snippet.
3. Metric aggregation by URL group
4. Control of instrumented pages using excludelist and includelist agent properties.
5. Provided Metrics:

For latest browsers using web timing API (IE 9+, Firefox7+, Chrome)

-Average Browser Render Time (ms)

-Average Round trip time (ms)

-Responses per interval

For Old browsers:

-Average DOM construction Time (ms)

-Average Page Load Complete Time (ms)

-Average Previous page unload Time (ms)
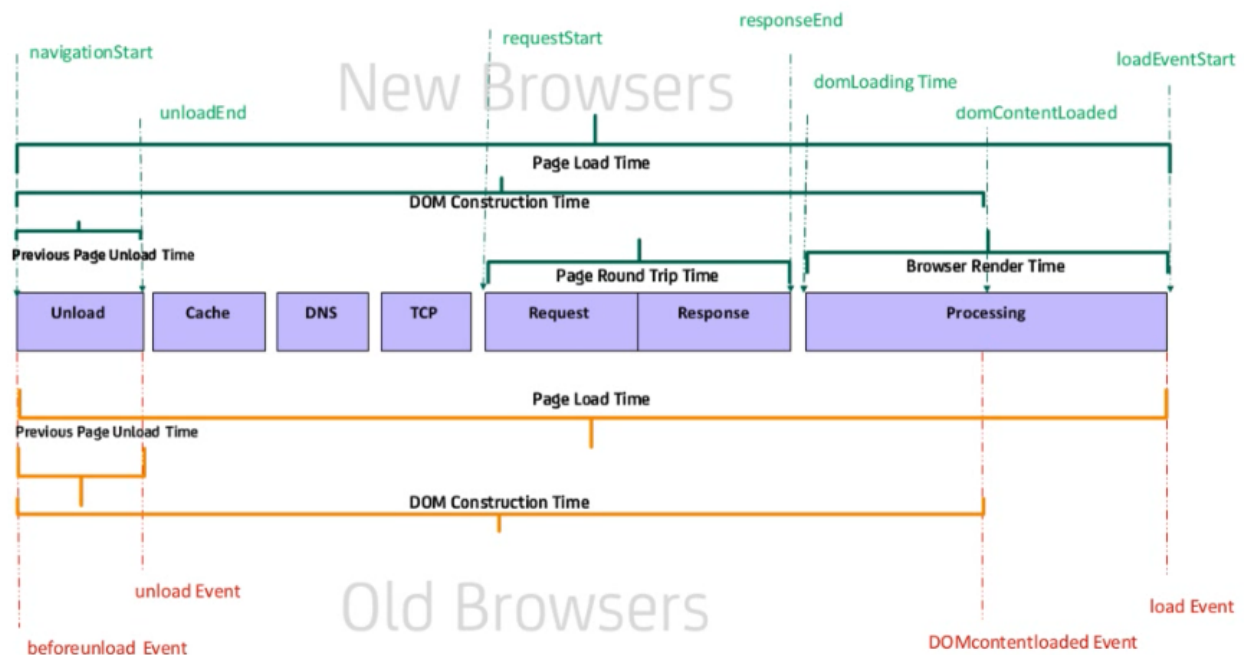
Not working, missing metric

Checklist:

1. Ensure BRTM.jar is available from /wily/core/ext

2. Check BRTM filter is available from the application server class path.
If Tomcat, place BRTMfilter.jar in the <Tomcat>/lib directory
If Websphere, place BRTMfilter.jar in the <WAS>/lib/ext directory
If Weblogic, add BRTMFilter_weblogic.jar in the startup script of the appserver

3. Check BRTM specific pbl and pbd files are included in /wily/core/config and brtm.pbl has been added to
Introscope.autoprobe.directiveFile=…brtm.pbl

4. Check content of SampleIntroscopeAgent.profile is included in the IntroscopeAgent.profile.

5. If manual insertion of BRTM filter, BRTM filters should be listed as a first filter
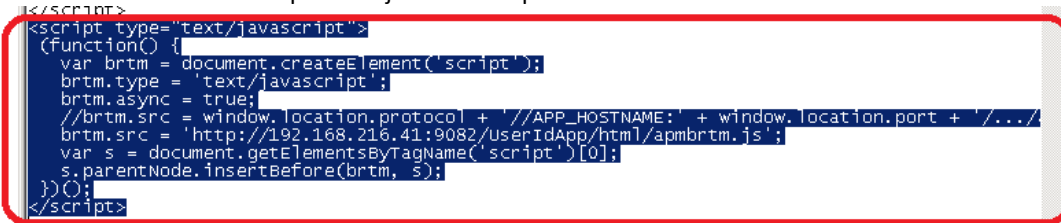If webpshere: check web.xml has a reference to BRTM filter:

With automatic filter insertion, the BTRM filter runs always before all other filters.

6. If manual insertion of javascript sniffer, verify it has correctly been added and make sure brtm.src= is pointing to the correct location of the apmbrtm.js. For example:

```
</script>
<script type="text/javascript">
(function() {
    var brtm = document.createElement('script');
    brtm.type = 'text/javascript';
    brtm.async = true;
    //brtm.src = window.location.protocol + '//APP_HOSTNAME:' + window.location.port + '/.../
    brtm.src = 'http://192.168.216.41:9082/UserIdApp/html/apmbrtm.js';
    var s = document.getElementsByTagName('script')[0];
    s.parentNode.insertBefore(brtm, s);
})();
</script>
```

For dynamic injection, ensure HTML pages content =text/html or the snippet will not be inserted and you will need to use manual insertion. If you are using webphere, set the following web container property to false com.ibm.ws.webcontainertypebysetheader

7. Verify apmbrtm.js is accessible from your browser.

8. Enable debug logging in the Agent, check for possible errors
Open the <WILY_AGENT_HOME>IntroscopeAgent.profile
Set log4j.logger.IntroscopeAgent=VERBOSE#com.wily.util.feedback.Log4JSeverityLevel, logfile
Set log4j.appender.logfile.MaxFileSize=2MB

Below an example on key messages to confirm the configuration and instrumentation are correct:
…
BRTFilter: start. URI: /BRTMTestApp/
…
BRTServletResponseWrapper: shouldWriteJavaScript contentTypeIncludesTextHtml: true(text/html)
BRTServletResponseWrapper: shouldWriteJavaScript m_contentEncoding: null
BRTServletResponseWrapper: shouldWriteJavaScript returns: true
…
BRTFilterBase ReportNewMetrics page unload: 21 round trip: 2 DOM start: 15 DOM ready: 48 page load: 106
BRTFilterBase ReportNewMetrics url: http://myserver:8080/BRTMTestApp/
…

9. "Cannot find BRTA wrapper. Response classname: com.ibm.ws.webcontainer.srt.SRTServletResponse" message in the agent log indicates that the appserver cannot see the BRTM filter. Make sure to add the BRTM filter before you deploy the .war, try redeploying the app.

10. Javascript must be enabled in the browser,

11. Test the behaviour using firefox 7+ or chrome latest versions.

12. Check if the issue is not related to a BRTM limitation: no support for AJAX or JavaServer Faces Applications, support,

What to collect:

1. Exact version of the appserver
2. zipped content of the AGENT_HOME\logs
3. IntroscopeAgent.profile
4. web.xml or start-up script
5. copy of the application config file (web.xml) or startup script
6. appserver logs
7. screenshot when accessing apmbrm.js from the browser

8. screenshot displaying that the snippet.js is part of the HTML page

Powerpack for Webserver
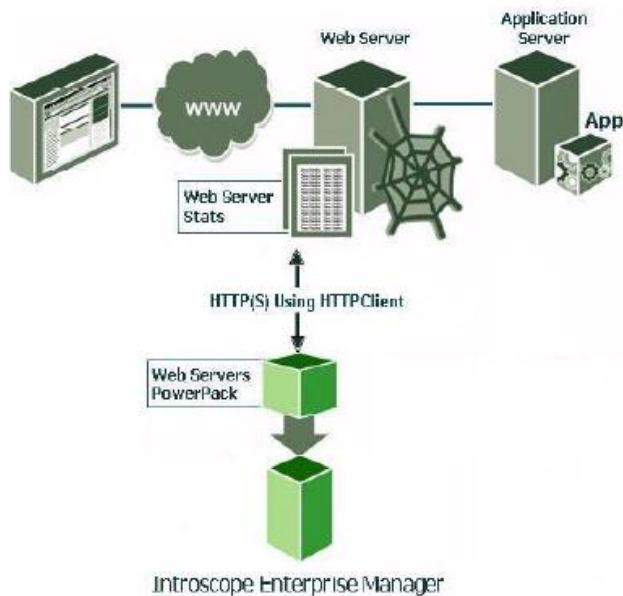
Unable to collect webserver statistics, agent not starting.

Checklist:

1. The powerpack is supported only with Sun JRE version, use latest 1.5 or later 32bit version. You can use 64bits platform.

2. The PowerPack cannot monitor an authenticated web server. Also verify if the web server is fronted by a proxy server? This is not supported and is currently a product limitation.

3. Missing configuration or jar files. Make sure the product has been correctly installed and all jar files are in the correct places.

4. By default, the PowerPack looks for the web server statistics at the following locations: server-status for Apache, iisperfstats for Microsoft IIS, and .perf for Sun ONE. If the web server has been configured to publish its statistics at a location different from the default locations, use the attribute MetricsURL in the WebServerConfig.xml to specify the new location.

5. If the "Availability" metric shows the status as zero in the Investigator, check that the port on which the web server is running is not blocked

6. If SSL:

-What version of SSL or TLS your HTTPS communications are using?
-What cipher are you using?

SSL v3.0 and TLS v1.0 are supported

7. Limitation: Two way authentication or iSSL client authentication is not supported by PP, the same goes for http based URL s, we don t support password protected, there is no existing functionality in code to pass in password when polling a Server URL for performance.

What to collect:

Enable verbose mode on the PP for Werbserverside:
a) Open the <PP_HOME>/config/WebServerAgent.profile:
b) Edit the following lines, replace "INFO" with "VERBOSE#com.wily.util.feedback.Log4JSeverityLevel"
log4j.logger.IntroscopeAgent=INFO, logfile
log4j.logger.WebServerMonitor=INFO, logfile
log4j.logger.AutoDiscoveryEngine=INFO, logfile
log4j.logger.AgentConfig=INFO, logfile
log4j.logger.UpdateMonitorConfig=INFO, logfile

Exact version of Webserver and OS.
Result of executing ServerVersionFinder.bat
Listing content of the PP_HOME
Zipped content of the PP_HOME/config folder
If you are using Apache or IHS, send httpd.conf file
Also add screenshot of results when accessing http://<server-name>/server-status
If you are using IIS,
Also add screenshot of results when accessing http://<server-name>/iisperfstats
If you are using iPlanet: send obj.conf file
Also add screenshot of results when accessing http://<server-name>/.perf

Powerpack for Oracle

Not working

Checklist:

1. Verify that the configuration is listed in the compatibility guides. At the present time Powerpack has not been tested with Oracle 11g. Also, Oracle RAC is not supported. We are not implementing any enhancements to Oracle PP and instead customers are advised to use DPM Insight Lite which has far greater monitoring capabilities and is available as part of APM license.

2. Configuration issue:
- Verify that the user account called ISCOPE_ORCL exists.
- Verify that Oracle PP has been installed correctly and that all files are in the correct places.

What to collect:

1. Exact versions of Oracle database and jre.
2. Zipped content of the PPOracle_HOME/config folder
3. Request Oracle admin person to rerun PPOracleDB_UserPrivileges.sql and to provide us with a screenshot of the result.
4. Request Oracle admin person to connect as ISCOPE_ORCL using Oracle Sql plus and to provide us with a screenshot of the result.
5. PPOracle_HOME/OracleDBAgent.log

MQMonitor

Important reminders

1. There are 2 sets of configurations for monitoring MQ.
- MQ Monitor agent: Agent that remotely accesses the MQ Manager.
- Java Agent: MQ Connections for the Java agent.

In 9.0:
2. MB7 support starts from 907 and onward versions:
3. Auto-discovery feature: Ensure mq.autodiscovery.enabled=true and mq.autodiscovery.que= are the same in both MQMonitor.properties and MQAgent.properties. Set maq.autodiscoery.properteis.update=true in order to get MQdiscovery list and MQMonitor.properties up to date.
4. Support MQ protocols for showing dependency of Webservices communications in SOA dependency map.

Install and configuration, not working

Checklist:

1. Ensure that the configuration is supported.
2. Missing configuration or jar files. Make sure the product has been correctly installed and all jar files are in the correct places.
3. Make sure the right commands have been executed

What to collect:

Enable DEBUG, set log4j.logger.IntroscopeAgent=DEBUG, console, logfile
Try to reproduce the issue and collect:

1. MQ, OS and JVM exact versions.

2. Zipped content of the MQMonitor_HOME\properties folder
3. startMQMonitor.bat (Windows) or startMQMonitor.sh (UNIX)

Unable to monitor Message Broker (MB)

Checklist:

1. Ensure tha the configuration is supported.
2. Missing configuration or jar files. Make sure the product has been correctly installed and all jar files are in the correct places.
3. Make sure the right commands have been executed; some of the commands for MB 6 will not work for MB7.

What to collect:

Enable DEBUG, set log4j.logger.IntroscopeAgent=DEBUG, console, logfile
Try to reproduce the issue and collect:

1. Listing of MQ_Monitor/ext folder
2. MQ_Monitor\properties*
3. MQ_Monitor\properties\startMQMonitor.bat/.sh
4. Execute the following commands, redirect the output to a text file and send it to us.

a) To get to know whether all the required 10 JMS queues are created on the JMS QM
DISPLAY QLOCAL(SYSTEM.JMS.*)
DISPLAY QMODEL(SYSTEM.JMS.*)

b) To view the ACL entry on the configuration manager
mqsilistaclentry <CMGR> -u <USERNAME>

c) To confirm whether the statistics for Message flows on the Execution Groups on the broker are enabled
mqsireportflowstats -s -e <ExecutionGroupName> -j

d) To confirm whether Publish/Subscribe statistics for the brokers is enabled
mqsireportproperties <BrokerName> -e <ExecutionGroupName> -o DynamicSubscriptionEngine -n statsInterval

e) To confirm whether allmqi permission is applied on the Queue Manager of the Configuration Manager
dspmqaut -m <ConfigQMGR> -t qmgr -p <user>@<domain>

f) To confirm whether put permission is applied on the SYSTEM.BROKER.CONFIG.QUEUE queue of the CMP Queue Manager
dspmqaut -m <ConfigQMGR> -t q -n SYSTEM.BROKER.CONFIG.QUEUE -p <user>@<domain>

g) To confirm whether get permission is applied on the SYSTEM.BROKER.CONFIG.QUEUE queue of the CMP Queue Manager
dspmqaut -m <ConfigQMGR> -t q -n SYSTEM.BROKER.CONFIG.REPLY -p <user>@<domain>

h) To confirm whether allmqi permission is applied on the Queue Manager of the JMS QM
dspmqaut -m <JMS_QMGR> -t qmgr -p <user>@<domain>

i) To confirm whether allmqi permission is applied to all JMS pub sub queues (#10) defined in the JMS Queue Manager

there will be 10 jms queues created after running the runmqsc(1st) command......10 refers to the count

dspmqaut -m <JMS_QMGR> -t q -n SYSTEM.BROKER.* -p <user>@<domain>

Application Behavior Analytics (ABA)

Important Reminders
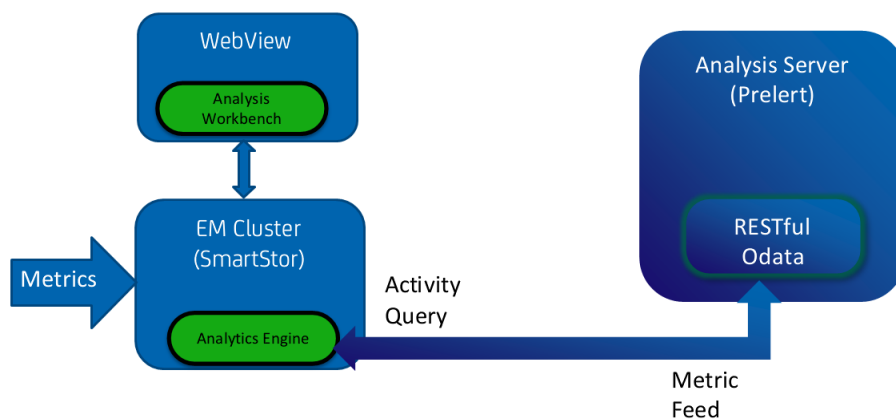
In 9.5:

1. Supported platform:

ABA Windows 2008R2 64bit, RH/CentOS 6.x 64bit

CA Analysis server: 2008R2 64bit, RH/CentOS 6.x 64bit

2. Pre-requisites: Linux (non-root), Windows (admin user)

3. By design:

-ABA is installed only on the MOM not collectors.

-1 ABA can server only 1 MOM.

-Super-domain users only.

4. If Webivew and the EM are on different directories, you need to copy the appropriate install files from Introsocope9.5-ABA-<build>-add-on.(tgz|zip) to the appropriate servers.

5. It is recommended to use "deploy_analytics_hotfix.sh/bat" to install ABA as it will clear the webview cache, do a backup and copy all the corresponding files to the appropriate locations.

No available metrics, missing metrics

Checklist:

On the Enterprise Manager:

1. Review the below supportability metrics from "SuperDomain > Custom Metric Process (Virtual) > Custom Metric Agent (Virtual) > Enterprise Manager > Analysis Server":

-"Metrics received" and "Metrics sent" should match.

-"Metric uploads processed" should be 1; if it is less than one, it means your regex is matching more APM than has been configured to be sent in a single cycle to the CA Analysis Server.

2. Review the regular expressions in EM_HOME/config/Analytics.properties

3. Try to restart the Enterprise Manager

4. Enable debug logging as below in the config/IntroscopeEnterpriseManager.properties, restart required
Add - log4j.logger.Manager.AnalyticsEngine=DEBUG, console, logfile
Add - log4j.additivity.Manager.AnalyticsEngine=false
Look for WARN, ERROR, [Analysis-Server-Worker* and analytics.em

5. Check API connectivity with CA Analysis Server:
-Get metadata
  http://<host>:<port>/prelertApi/prelert.svc/$metadata
-Count all activities
  http://<host>:<port>/prelertApi/prelert.svc/Activities()/$count
-Get a couple activities and make sure evidence is also returned
  http://<host>:<port>/prelertApi/prelert.svc/Activities()?$top=2&$expand=ActivityMetrics
-Get activities with a component metric with Average in the name
  http://<host>:<port>/prelertApi/prelert.svc/Activities()/$count?$filter=(MPQuery+eq+%27%25Average%25%27)
-Get activities within a time window
  http://<host>:<port>/prelertApi/prelert.svc/Activities()/$count?$filter=(LastEvidenceTime+ge+datetime%272013-05-05T00:00:00%27+and+FirstEvidenceTime+le+datetime%272013-05-12T00:00:00%27)

6. Make sure APM and the Analysis Server have the same time or it will impact time range queries from the analysis workbench.

On the CA Analysis Server machine:
1. Verify processes are running:
$ bin/prelert_ctl{.bat} status
$ ps –efH | egrep "apache|java|service"
$ cots/pgsql/bin/pg_ctl status
$ cots/pgsql/bin/psql -l
Should list data "prelert"

2.Verify processes and ports:
Linux:
$ ps -efH | grep prelert
$ netstat -an | grep 8080

Windows:
use task manager and view the list of processes

cmd netstat -an

3. Verify firewall settings to ensure ports used for the product are open.

4. Verify server resources are not exhausted (Linux):
Memory : $ cat /proc/meminfo
Disk ": $ df -h
Free memory and swap - $ free
You should use these commands to sample the system periodically over a period of time

5.Review logs looking for WARN and ERROR messages
+ logs/api/prelertApi.log
should be logging activity requests as well as metrics for analysis
+ logs/ts_feature_detector/ts_feature_detector.log
should be logging every 10K 'points' received
+logs/tomcat/catalina.out
logs/evidence_gatherer/evidence_gatherer.log
should be logging every 1K 'features' identified
+ logs/rate_monitor/rate_monitor.log
logs/engine/engine.log
should be logging every 5 seconds or so, regardless of any 'evidence'
+logs/activity_mgr/activity_mgr.log
Default logging is set to rotate 10 files, each with a maximum file size of 1MB
+Tomcat logs roll daily

6. Restarting CA Analysis Server
First, source your profile.sh so it load the necessary env vars.
ctl/admin/prelert_shutdown(.bat)
ctl/admin/preleret_startup(.bat)
(Windows) Administrative Tools -> Services can also be used

What to collect:

From the Enterprise Manager:
- EM_HOME/config/Analytics.properties
- Zipped content of EM_HOME/logs
- Screenshot of the below supportability metrics: Enterprise Manager > Analysis Server Supportability:
" Metrics received", "Metrics sent" and "Metric uploads processed"

From the CA Analysis Server machine:
-(Linux)Run bin/prelert_top.sh for 10 minutes before capturing the logs
-(Windows) Open up Windows task manager, select the processes tab, click "Show processes from all users", sort by descending memory size and take a screenshot. Then sort by descending CPU usage and take another screenshot. Finally, switch to the performance tab, wait a minute for the graphs to populate and take another screenshot.

-(Windows) Open Administrative Tools -> Event Viewer and export the most recent Windows events for "System" and "Application
-Collect all files and subdirectories in logs/
-(Linux)Collect any files with 'core*' in the name
-Exact OS Version
-Hardware specifications
CPUs, cores, bus speed
NIC cards and speed
Memory installed and available
Disk type (SSD?), size, and free space, swap space

DPM Insight for APM

Missing metrics, installation problems

Checklist:

1. Make sure to use the correct DPM installer depending of your Database version.For example if you are planning to monitor Oracle DB 32bit, make sure to use DPM 32bit.

2. If using Oracle, make sure the DB user has enough permissions to read the DB information, otherwise, you will see this type of errors in the log:
(OraLib.c 929 OraError) Oracle error returned from varchive_dest
(OraLib.c 929 OraError) Error number -942

3. Make sure DPM Integration services are up and running:
-CA Insight Bridge for CA Wily Introscope
-Insight Network Service

4. Go to the DPM configuration page, select "Configuration Insight Agent" tab, click the "Test Connection" button

5. Verify installation is correct, see TEC596866 – How to install DPM Agent 9.5 with DPM 11.6 on Oracle

What to collect:

%uvroot%/agents/<agent name>/*.*
%uvroot%/log/*.*
%uvroot%/../Introscope/logs/*
%uvroot%/../Introscope/conf/*

Integration: Introscope to Siteminder (SMM Agent)
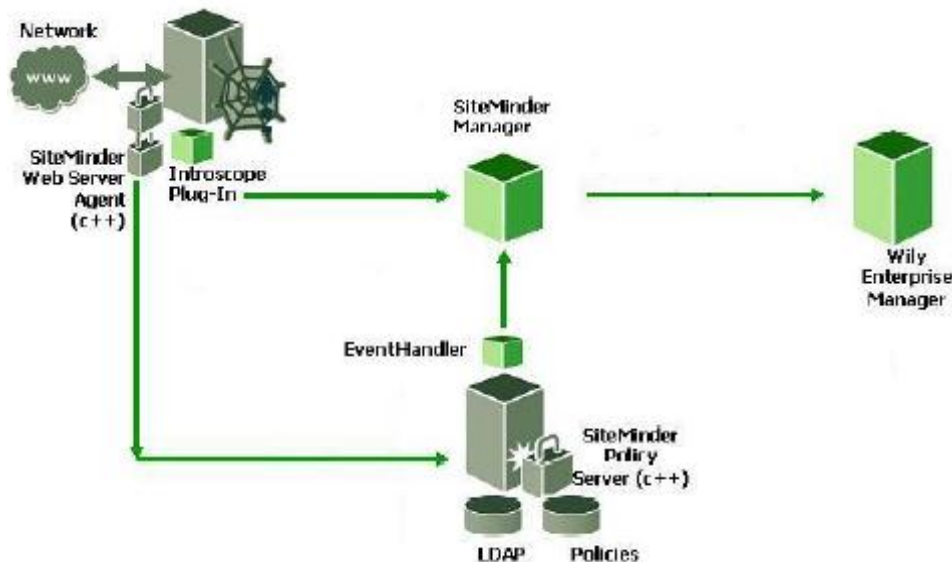
WebAgent or Policy Server no reporting any metric, unable to startup SMM Agent

Checklist:

1. Wily SMM Agent needs to create a shared memory segment of size 10 mb. Ensure shared memory settings have been set as per documentation. You need to reboot the server.
set shmsys:shminfo_shmmax=10485760
set shmsys:shminfo_shmmin=10485760

2. Verify that the shared memory segment has been created, run <SMM Agent>/IntroscopeNativeDataReporter.sh -list or IntroscopeNativeDataReporter.exe -list

If the integration is working you should see entries as below:

Shared File: /<SMM Agent>/SiteMinderManagerAgent/data/IntroscopeAPI.shm
Metric Counters:
Type: PerIntervalCounter Name: SiteMinder|Policy Server|server-VM74163|Caching|PolicyStore:Hits Per Interval
Type: PerIntervalCounter Name: SiteMinder|Policy Server|server-VM74163|LDAPDatabase|userstore|Operations|UserStore:Responses Per Interval
Type: FlucuatingCounter Name: SiteMinder|Policy Server|server-VM74163|Health|High Priority Request Queue:Max Length
Type: AverageCounter   Name: SiteMinder|Policy Server|server-VM74163|LDAPDatabase|userstore|Operations|UserStore:Average Response Time (ms)
Type: FlucuatingCounter Name: SiteMinder|Policy Server|server-VM74163|Health|Request Queue:Current Length
Type: AverageCounter   Name: SiteMinder|Policy Server|server-VM74163|Operations|Authorize:Average Response Time (ms)
Type: PerIntervalCounter Name: SiteMinder|Policy Server|server-VM74163|Database|Operations|PolicyStore:Responses Per Interval
Type: FlucuatingCounter Name: SiteMinder|Policy Server|server-VM74163|Health|Sockets:Max Count
Type: FlucuatingCounter Name: SiteMinder|Policy Server|server-VM74163|Health|Sockets:Currently In Use

Type: FlucuatingCounter   Name: SiteMinder|Policy Server|server-VM74163|Health|Worker Threads:Max Count
Type: PerIntervalCounter Name: SiteMinder|Policy Server|server-VM74163|Operations|Login:Responses Per Interval
Type: AverageCounter   Name: SiteMinder|Policy Server|server-VM74163|Operations|IsProtected:Average Response Time (ms)
Type: AverageCounter   Name: SiteMinder|Policy Server|server-VM74163|Database|Operations|PolicyStore:Average Response Time (ms)
Type: PerIntervalCounter Name: SiteMinder|Policy Server|server-VM74163|Operations|IsProtected:Responses Per Interval
Type: AverageCounter   Name: SiteMinder|Policy Server|server-VM74163|Operations|Login:Average Response Time (ms)
Type: FlucuatingCounter   Name: SiteMinder|Policy Server|server-VM74163|Health|Worker Threads:Currently in Use
Type: FlucuatingCounter   Name: SiteMinder|Policy Server|server-VM74163|Health|Request Queue:Max Length
Type: FlucuatingCounter   Name: SiteMinder|Policy Server|server-VM74163|Health|High Priority Request Queue:Current Length
Type: PerIntervalCounter Name: SiteMinder|Policy Server|server-VM74163|Operations|Authorize:Responses Per Interval
Type: PerIntervalCounter Name: SiteMinder|Policy Server|server-VM74163|Caching|Authorization:Hits Per Interval
Type: PerIntervalCounter Name: SiteMinder|Policy Server|server-VM74163|Database|Operations|PolicyStore:Errors Per Interval

Traces:
Trace Threshold: -1
Connections: 1

If no data is being written into the shared memory segment, the above command will show 0 if no process is connected to the memory segment.

2. The shared memory segment can be corrupted or not created at all.

a) Shut down all processes that are accessing the shared memory segment including WebAgents, Policy Server as Wily SMM Agent

b) Open the <SMM Agent>/SiteminderManagerAgent/data/IntroscopeAPI.log, find out the id of the shared memory, for example:

INFO - Shared memory segment ID: 25

c) Delete the segment using ipcrm -m <shared memory segment id>

d) Clear contents of the <SMM Agent>/SiteminderManagerAgent/data folder

e) Start WilySiteminder agent first so it creates the shared segment properly.

3. Ensure the Installation is correct:

a) Verify libIntroscopeNativeDataAPI.so has been copied from <SMM>/SiteminderManagerAgent to <PolicyServer>/lib and <WebAgent>/bin, check the file size.

b) Verify smm_env.sh has been copied from <SMM>/SiteminderManagerAgent to the the <Policy Server home> and <WebAgent home>/bin

c) Verify the following line has been added to the <Webagent>/ca_wa_env.sh file:
. /<webagent>/smm_env.sh

Verify the following line has been added to the <PolicyServer>/ca_ps_env.ksh file:
. /<webagent>/smm_env.sh

d) For Policy Server, make sure libEventIntroscopeprovider.so has been added to the event handlers list in the Policy Server: First source ". /CA/siteminder/ca_ps_env.ksh", then run <PolicyServer>/bin/XPSConfig
From the menu, select "5-AuditSMHandlers", ensure it is set to <PolicyServer>/lib/libEventIntroscopeprovider.so

c). Verify WebAgent.conf and envvars have been update on the webserver side, for example:
-For apache, you need to open <apache>/conf/WebAgent.conf and add the below lines:

EnableMonitoring="YES"
EnableIntroscopeAgentSupport="YES"
LoadPlugin="<webagent>/bin/libIntroscopePlugin.so"

You also need to add the following line to <apache>/bin/envvars:
<SMM>/SiteminderManagerAgent/IntroscopeNativeDataReporter.sh init

What to collect:

Uncomment the following lines in the smm_env.sh of the webagent and/or policyserver:
  INTROSCOPE_NATIVEDATAAPI_LOGGING=1
 export INTROSCOPE_NATIVEDATAAPI_LOGGING

1. Confirm OS details, Policy Server or WebAgent exact version details
2. Output of ls -la for <Wily SMM>/SiteminderManagerAgent/data folder and zip of all the data present in this folder
3. Output of ./IntroscopeNativeDataReporter.sh -list
4. Output of ipcs -ma
5. Shared memory segment settings for the OS
6. Output of truss -p <Wily SMM process id> > trussout.txt (for Wily SMM hang issues)

Introscope Webservices

Important reminders

Applies to: Introscope v7 and 8

1. Architecture:
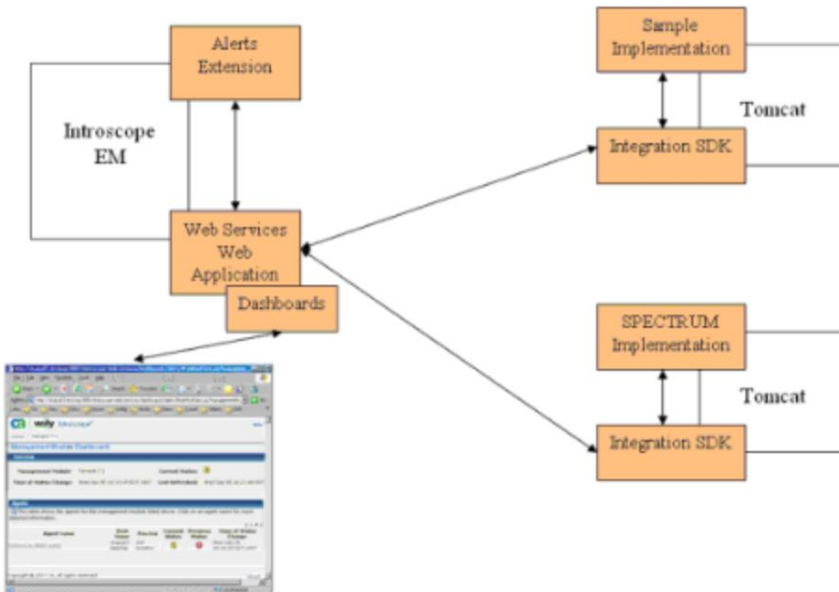
EM components:

a) EM alerts extension: EM_HOME/ext/IscopeAlertsExt-EM.jar
    -comprises of an inventory cache of Introscope objects (agents, alert definitions, metrics) used in a MM.
    -status calculation of each inventory object (when alerts are triggered)
    -sends notifications to subscribers (inventory changes, status changes)
    -can filter management modules which participate using EM property:
    Introscope.alerts.extension.managementmodules.enable (possible values: ALL or include module names)

b) EM Webservices Web application: EM_HOME/webapps/Introscope-web-services.war
    -Polling Web services (query interface):
        MetricsListService: list of agents and metrics
        MetricsDataService: metric data values for agent/metric regular expression and query period
        AlertsPollingService: inventory and status of MM, agents and alert definitions
        EmLifeCycleService: EM availability.
    -Subscription webservices: there are 7 topics on which we publish data, users can subscribe to these topics.
    For example, a user subscribes to a topic status changes so he gets notified whenever this condition takes place:
        Management module add/delete
        Agent discovered/lost in context of a management module
        Alert definition add/delete
        Alert message module status change
        Agent status change
        Alert definition status change
    -Exposes status dashboard for Introscope objects
    -Pre-configured dashboards: Web UI to display status for: MM, Agents, alert definitions:
    http://em:8081/introscope-web-webservices/dashboards/alerts/IScopeView.jsp

Client side for EM Webservices part:
a) Tomcat
b) SDK Web appp: Tomcat_HOME/webapps/instroscope-wssdk-consumer.war

c) SDK dependent libraries: Tomcat_HOME/shared/lib/*.jar
d) Sample usage of the SDK deployed throught Eclipse project (wssdk_sample_build.xml):

2. To enable DEBUG, in the IntroscopeEnterpriseManager.properties, add:
log4j.logger.Manager.IntroscopeWebServices=DEBUG,webserviceslogfile
log4j.appender.webserviceslogfile.File=logs/IntroscopeWebServices.log
log4j.appender.webserviceslogfile=com.wily.org.apache.log4j.RollingFileAppender
log4j.appender.webserviceslogfile.layout=com.wily.org.apache.log4j.PatternLayout
log4j.appender.webserviceslogfile.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
log4j.appender.webserviceslogfile.MaxBackupIndex=4
log4j.appender.webserviceslogfile.MaxFileSize=20MB

3. Verify and collect a screenshot from Webservices Polling and Subscription supportability metrics from Custom Metrics host (Virtual) | Custom Metric Process (Virtual) | Custom Metric Agent (Virtual) (*SupperDomain*) | Enterprise Manager | WebService

Integration: Introscope to NSM
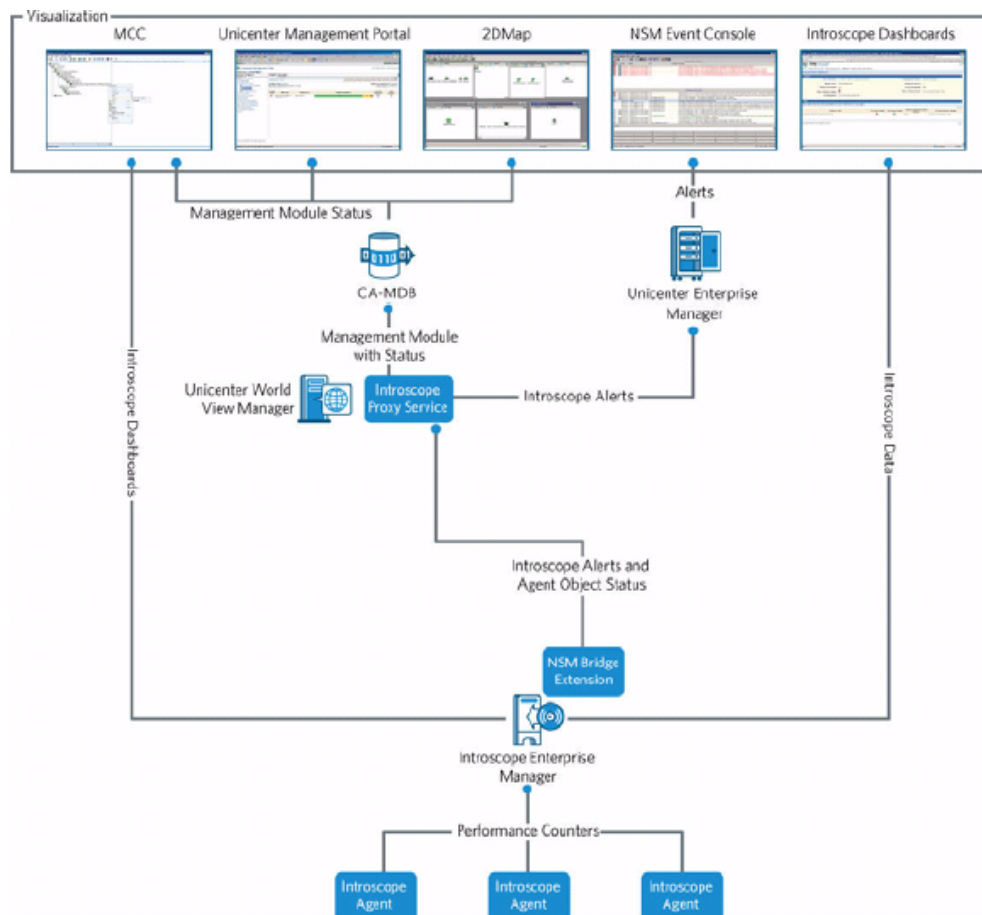
Important reminders

1. Pre-requisites: Windows 2003 and NSM 11.1 SP1 or higher.
2. The integration needs to be installed on the NSM server
3. v9.0 Introscope-NSM integration is NOT supported with EM v8 or 7
4. The integration supports simple alerts not summary alerts.

Introscope to NSM: Events/alerts are not populated into NSM

Checklist:

1. If you have EM v8.x, make sure you have installed Introscope SDK using the Introscope-NSM integration v2.0 installer.
   If you have EM v9, add the below lines to the EM_HOME\config\IntroscopeEnterpriseManager.properties file:
   introscope.alerts.extension.managementmodules.enable=ALL
   introscope.alerts.extension.inventory.updatecheckintervalsecs=60
   Then verify that all Introscope webservices are accessible from the NSM server side:
   http://<EM_hostname>:8081/introscope-web-services/services/AlertPollingService?wsdl
   http://<EM_ hostname>:8081/introscope-web-services/services/MetricsDataService?wsdl
   http://<EM_ hostname>:8081/introscope-web-services/services/MetricsListService?wsdl
   http://<EM_ hostname>:8081/introscope-web-services/services/EmLifecycleService?wsdl

2. Restart the NSM Windows services:
   If the problem lies with MCC or 2DMap, restart "CA unicenter Business Process View Management" and "CA Worldview Severity Propagation Service"
   If the problem lies with Event Console, restart: "CA-unicenter" service

3. Make sure "Apache Tomcat for CA Wily Integration Pack" window service is running.

4. Ensure Tomcat is running and there is no port conflict, verify this in the tomcat stdout log

5. Go to the integration webpage: http://localhost:8082/CA-Wily-Introscope-NSM-IP, select "Introscope EM Host Configuration", click the "Validate Connection" button to verify that the integration is connected to the Introscope EM.

6. Go to the integration webpage: http://localhost:8082/CA-Wily-Introscope-NSM-IP, select the "CA NSM Configuration" tab.
   If the problem lies with MCC or 2DMap, reenter the credentials under NSM WorldView repository section.
   If the problem lies with Event Console, ensure the servername is correct.

7. Run nslookup against the NSM Worldview Server, NSM Event and Introscope EM hostnames from the Integration server to ensure hostname/ip addresses are correct. If there is a firewall between each of the components, for testing purposes, disable them.

8. Go to the Management Module editor, ensure that the Alerts are active and if possible, configure the alerts to send a notification to the workstation consol; this will help you confirm that the alerts are correctly being generated by the Introscope EM.
   Go to the Integration webpage > Monitoring tab, ensure that the correct alerts have been selected.

9. If the problem persists, test the issue using a fresh new simple alert

10. Check for errors in the:
    ISCP_NSM_HOME\apache-tomcat-5.5.25\logs\IcopeNSMLogger.log
    EM_HOM\logs\IntroscopeEnterpriseManager.log

What to collect:

Enable DEBUG logging in the Introscope-NSM side:
a) open the log4j.properties from Integration_HOME\apache-tomcat-5.5.25\webapps\CA-Wily-Introscope-NSM-IP\WEB-INF\classes
b) remove the "#" in all the lines that refer to the wily classes.

Enable DEBUG on the EM side:
a) Open the <EM_HOME>/config/IntroscopeEnterpriseManager.properties:
b) Set:
log4j.logger.Manager=DEBUG,logfile
log4j.appender.logfile.MaxFileSize=200MB

Then, restart the Introscope-NSM service, try reproducing the issue and collect:

1. Exact NSM, OS and integration version
2. Zipped content of the ISCP_NSM_CONNECTOR_HOME\apache-tomcat-5.5.25\logs

3. ISCP_NSM_CONNECTOR_HOME\CAWily_Introscope_NSM_IntegrationPack\
CAWily_Introscope_NSM_IntegrationPack_InstallLog.log.
4. Zipped content of the EM_HOME/logs
5. EM_HOME\config\IntroscopeEnterpriseManager
6. Screenshots of the following pages from the IntroscopeNSM integration webpage (http://localhost:8082/CA-Wily-Introscope-NSM-IP/): a) Introscope EM Configuration tab, b) CA NSM configuration tab and Monitoring tab (expanded nodes).
7. Screenshots of the Introscope Workstation Management Module Editor, displaying the alert definitions.
8. Results of nslookup and ping from :
   - NSM to EM
   - EM to NSM

Integration: Introscope to CMDB

Important reminders

1. Pre-requisites: cmdb 11.2, 12.1 and 12.5
2. v9.0 integration is NOT supported with EM v8 or 7
3. The integration can be installed in a separate server from the EM and cmdb servers

Events/alerts are not populated into CMDB

Checklist:

1. If you have EM v8.x, make sure you have installed Introscope SDK using the Introscope-cmdb integration installer.
   If you have EM v9, add the below lines to the EM_HOME\config\IntroscopeEnterpriseManager.properties file:
   introscope.alerts.extension.managementmodules.enable=ALL
   introscope.alerts.extension.inventory.updatecheckintervalsecs=60
   Then verify that all Introscope webservices are accessible from the NSM server side:
   http://<EM_hostname>:8081/introscope-web-services/services/AlertPollingService?wsdl
   http://<EM_ hostname>:8081/introscope-web-services/services/MetricsDataService?wsdl
   http://<EM_ hostname>:8081/introscope-web-services/services/MetricsListService?wsdl
   http://<EM_ hostname>:8081/introscope-web-services/services/EmLifecycleService?wsdl

2. Make sure "Apache Tomcat for CA Wily Integration Pack" window service is running.

3. Ensure tomcat is running and there is no port conflict; verify this in the tomcat stdout log

4. Go to the integration webpage: http://localhost:8082/CA-Wily-Introscope-CMDB-IP, select "Introscope Configuration", click the "Run Now" button to transfer the data. If you get an error make sure the EM has correctly been registered on the CMDB side and that there is no connectivity issue.

5. Go to the integration webpage: http://localhost:8082/CA-Wily-Introscope-CMDB-IP, select "CMDB Configuration" tab, reenter the credentials to ensure they are correct.

6. Go to cmdb UI > Administration > CA CMDB > MDR Management > MDR List, verify the EM has been registered

7. Run nslookup against the CMDB and Introscope EM hostnames from the Integration server to ensure hostname/ip addresses and correct. If there is a firewall between each of the components, disable them for testing purposes.

8. Go to cmdb UI > Service Desk > CMDB > CI Families > All, search for Introscope entries to confirm that the Introscope information has been received. For example, monitored app database are categorized under "Other Software Database" class

9. Check for errors in the:
    ISCP_CMDB_HOME\apache-tomcat-5.5.25\logs\IscopecmdbLogger.log
    EM_HOM\logs\IntroscopeEnterpriseManager.log

What to collect:

Enable DEBUG on the EM side:
a) Open the <EM_HOME>/config/IntroscopeEnterpriseManager.properties:
b) Set:
log4j.logger.Manager=DEBUG,logfile
log4j.appender.logfile.MaxFileSize=200MB

Then, restart the integration service, try to reproduce the issue and collect:

1. Exact CMDB, OS and integration version
2. Zipped content of the ISCP_CMDB_CONNECTOR_HOME\apache-tomcat-5.5.25\logs
3. ISCP_CMDB_CONNECTOR_HOME\CAWily_Introscope_CMDB_IntegrationPack\
    CAWily_Introscope_Cmdb_IntegrationPack_InstallLog.log.
4. Zipped content of the EM_HOME/logs
5. EM_HOME\config\IntroscopeEnterpriseManager
6. Screenshots from cmdb UI > Administration > CA CMDB > MDR Management > MDR List, confirming the EM registration and configuration details.
7. Screenshots of the following pages from the integration webpage: http://localhost:8082/CA-Wily-Introscope-CMDB-IP : Introscope Configuration, CMDB configuration tabs.
8. Screenshots from cmdb UI > Service Desk > CMDB > CI Families > All
9. Result of nslookup and ping from CMDB to EM and from EM to CMDB

Integration: Introscope to Spectrum

Events/alert are not populated into Spectrum

Checklist:

1. If you have EM v8.x, make sure you have manually installed Introscope SDK.
   If you have EM v9, add the below lines to the EM_HOME\config\IntroscopeEnterpriseManager.properties file:
   introscope.alerts.extension.managementmodules.enable=ALL
   introscope.alerts.extension.inventory.updatecheckintervalsecs=60
   Then verify that all Introscope webservices are accessible from the NSM server side:
   http://<EM_hostname>:8081/introscope-web-services/services/AlertPollingService?wsdl
   http://<EM_ hostname>:8081/introscope-web-services/services/MetricsDataService?wsdl
   http://<EM_ hostname>:8081/introscope-web-services/services/MetricsListService?wsdl
   http://<EM_ hostname>:8081/introscope-web-services/services/EmLifecycleService?wsdl
2. Regarding the "Spectrum Trap Generation workstation Plugin". If you are using EM 9.0.6.2 and higher version, this plug-in is already part of the Introscope Workstation. If you are using a previous EM version, RO28562 replaces "Spectrum Trap Generation workstation Plugin". You can download "RO28562 - WIN - CA APM SNMP ALERT ACTION PLUGIN" from CA Support Online, you need to install it on the EM side to be able to create a "SNMP Alert Acion".
3. Run nslookup against the Spectrum and Introscope EM hostnames from the EM and Spectrum servers respectively. If there is a firewall, disable it for testing purposes.
4. Go to the Management Module editor, ensure that the Alerts are active, if possible, configure the alerts to send a notification to the workstation console, this will help you confirm that the alerts are correctly being generated by the Introscope EM.
5. NOTE: The integration support Introscope simple alerts not summary alerts.
6. If the problem persists, test the issue using a fresh new simple alert.
7. Check for errors in the EM_HOM\logs\IntroscopeEnterpriseManager.log

What to collect:

Enable DEBUG on the EM side:
a) Open the <EM_HOME>/config/IntroscopeEnterpriseManager.properties:
b) Set:
log4j.logger.Manager=DEBUG,logfile
log4j.appender.logfile.MaxFileSize=200MB

Then, restart the Spectrum/tomcat windows service and try to reproduce the issue; collect:
1. Spectrum version.
2. Snapshot from OneClick web Administration page > wily integration configuration
3. $SPECROOT/tomcat/logs/stdout.log from the spectrum oneclick server
4. Zipped content of the EM_HOME/logs
5. EM_HOME\config\IntroscopeEnterpriseManager
6. Screenshots from the Management Module Editor, displaying the alert and SNMP alert action definitions.
7. Output of nslookup from Spectrum to EM and from EM to spectrum

Integration: Introscope to Service Metric Analysis (SMA) /SQM
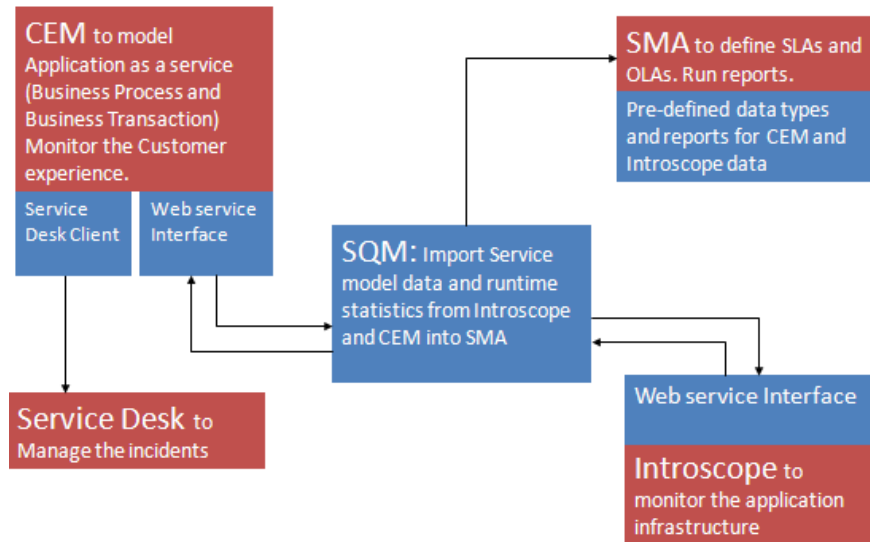
Unable to collect Introscope metrics

Checklist:

1. The incorrect EM SDK webservice being used. Make sure to use the Introscope-web-services.war file from the latest Introscope SDK package.
2. Look for possible error messages in the SQMServer_HOME/logs/SQM.log, SQMServer_HOME/logs/wrapper.log and EM_HOME/logs/IntrocopeEnterpriseManager.log

What to collect:

- Zipped content of the SQMServer_HOME/logs directory
- SQMServer/config/SQM.properties
- SQMServer/Data/CEMimporter.xml
- SQMServer/Data/IntroscopeImporter.xml
- zipped content of the EM_HOME/logs

CEM Web Services

Important reminders

CEM Web Services API provides a mechanism to access CEM data using Standard SOAP Web services, available web services:

http://tesshost:web-services-port/CA/cem/webservices/ConfigurationDataOutService?wsdl
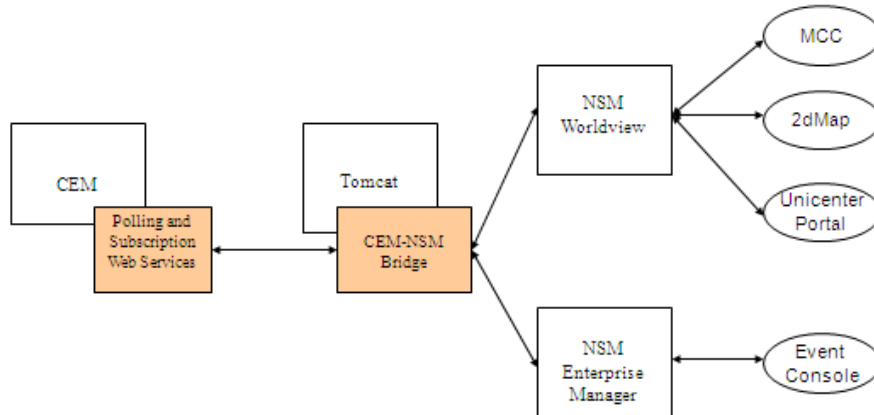http://tesshost:web-services-port/CA/cem/webservices/StatisticsDataOutService?wsld
http://tesshost:web-services-port/CA/cem/webservices/EventsDataOutService?wsdl

In 9.0.5:
Added 10 additional webservice commands for defects.

In 9.1:
Added Webservice "ExportToolDataOutservice" to support the new "Export Data"

Integration: CEM to NSM

Important reminders

1. Pre-requisites: Windows 2003 and NSM 11.1 SP1 or higher.

2. The integration needs to be installed in the NSM server

3. The only difference between the Integration v1.0 to 9.0 is the port number, in v9 integration port is 8081. The Installation and configuration steps are the same in both versions

4. The integration v9 is not supported with CEM 4.x

5. CEM business Services, Business Transactions and User Groups activity can be monitor using NSM MMC and 2DMap. CEM Incidents can be monitor using NSM Event Console.
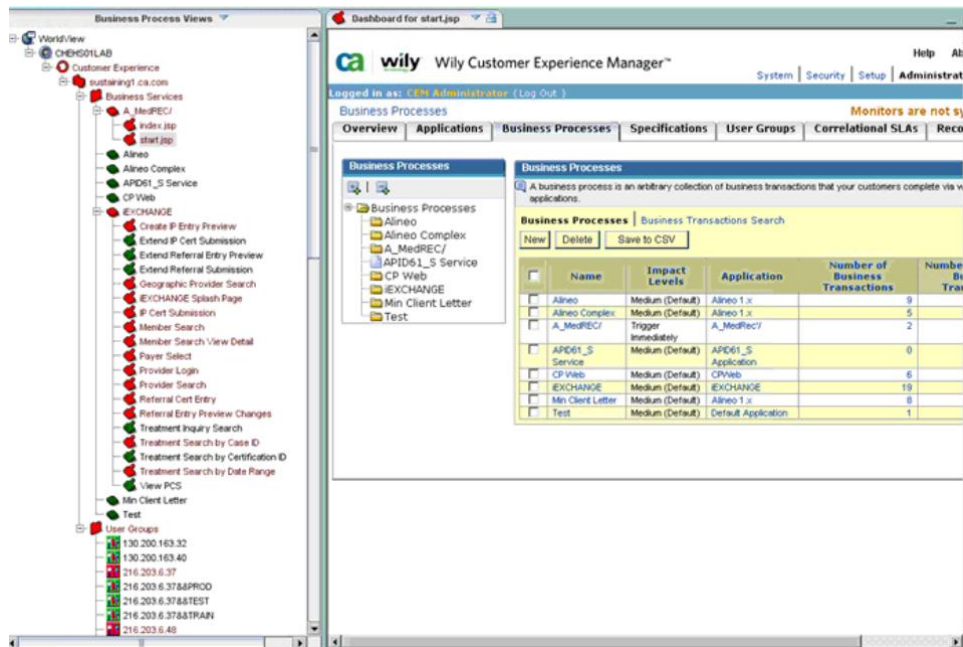
BT, BS, incidents are not populated into NSM.

Checklist:

1. Restart the NSM Windows services:
   If the problem lies with MCC or 2DMap, restart "CA unicenter Business Process View Management" and "CA Worldview Severity Propagation Service"
   If the problem lies with Event Console, restart: "CA-unicenter" service

2. Make sure Apache Tomcat Windows service used for the integration is running.

3. Open the TOMCAT_HOME\shared\classes\cemBridgeConnector.properties and make sure to update the below 2 properties accordingly to the tomcat configuration:
   WEBAPP_CONTAINER_HOST=localhost (servername where the integration/tomcat is running)
   WEBAPP_CONTAINER_PORT=8080 (integration/tomcat port, by default 8080)
   Ensure all tomcat ports are available, you can verify this in the tomcat stdout log

4. Open the TOMCAT_HOME\shared\classes\nsmBridgeConnector.properties, make sure worldview and EM NSM servername are correct.
   NOTE: SetNsmBridgeConnector.bat does NOT validate the worldview password; you can validate the password using "modp" NSM utility as below:
   modp –r worldview_servername –u <user> -n <password>

5. Run nslookup against the NSM Worldview Server, NSM Event and Introscope EM hostnames from the Integration server to ensure hostname/ip addresses are correct. If there is a firewall between each of the components, disable them for testing purposes.

6. Check for errors in the:
   EM_HOM\logs\IntroscopeEnterpriseManager.log
   CEM_NSM_HOME\apache-tomcat\logs\cemNsmIntegration.log, if you see an "unsubscribing" message when an event occurs, it means that the configuration is not correct.

7. Verify that the Business Service and Business Transactions names do not include Unicode characters. If this is the case, you need to replace them with ASCII characters; you also need to remove all created objects in NSM using NSM 2dmap.

What to collect:

Enable DEBUG on the Integration/tomcat side:
a) open <cem-nsm_integration_tomcat>\webapps\cem-nsm-integration\WEB-INF\classes\log4j.properties
b) Add the below lines to the file:
log4j.logger.com.timestock.tess.webservices.api=debug
log4j.logger.com.timestock.tess.webservices.impl=debug
log4j.logger.com.timestock.tess.webservices.muse.extensions=debug

Enable DEBUG on the EM side:
a) Open the <EM_HOME>/config/IntroscopeEnterpriseManager.properties:
b) Set:
log4j.logger.Manager=DEBUG,logfile
log4j.appender.logfile.MaxFileSize=200MB

Then, restart the Introscope-NSM service and try to reproduce the issue, collect:

1. Exact NSM, OS, Tomcat, JRE and integration version.
2. Zipped content of the TOMCAT_HOME/logs directory
3. Zipped content of the TOMCAT_HOME/shared/classes directory.
4. Zipped content of the EM_HOME/logs
5. EM_HOME\config\IntroscopeEnterpriseManager
6. Screenshots of the TESS UI displaying Incidents report activity.
7. Result of nslookup and ping from NSM to EM and from EM to NSM

Integration: CEM to CMDB
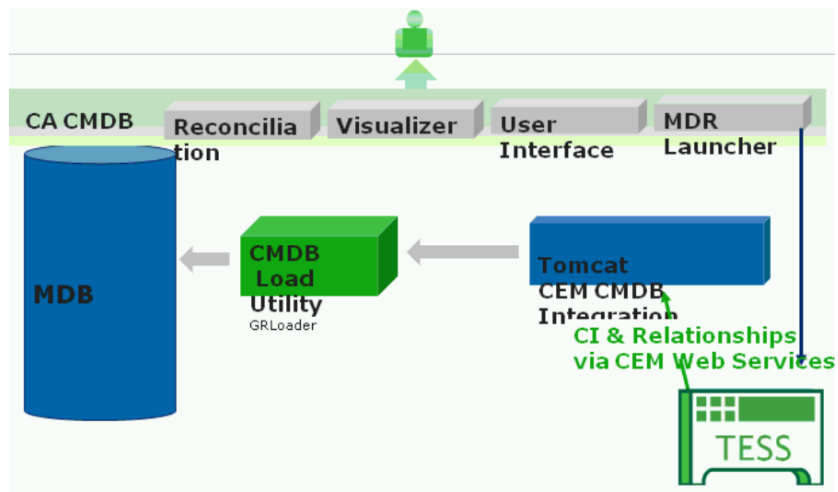
Important reminders

1. Pre-requisites: cmdb 11.2, 12.1 and 12.5.
2. v9.0 integration is NOT supported with CEM4.0 or 4.5
3. The integration can be installed in a separate server from the EM and cmdb servers
4. The only difference between the Integration v1.0 to 9.0 is the port number, in v9 ntegration port is 8081. The Installation and configuration steps are the same in both versions

BT, BS, incidents are not populated into CMDB

Checklist:

1. Make sure "Apache Tomcat for CA Wily Integration Pack"Windows service is running.

2. Ensure tomcat is running and there is no port conflict, verify this in the tomcat stdout log

3. Go to the integration webpage: http://localhost:8082/CA-Wily-CEM-CMDB-IP, select "Introscope Configuration", "Run Now" button to transfer the data,. If you get an error ensure the EM has correctly been registered on the CMDB side and that there is not a connectivity issue.

4. Go to the integration webpage: http://localhost:8082/CA-Wily-CEM-CMDB-IP, select "CMDB Configuration" tab, reenter the credentials to ensure they are correct.

5. Go to cmdb UI > Administration > CA CMDB > MDR Management > MDR List, verify that the EM has been registered

6. Run nslookup against the CMDB and Introscope EM hostnames from the Integration server to ensure hostname/ip addresses are correct. If there is a firewall between each of the components, disable them for testing purposes.

7. Go to cmdb UI > Service Desk > CMDB > CI Families > All, search for CEM entries to confirm that the Introscope information has been received. For example, Business Transactions are categorized under "Enterprise

Transaction" class

8. Check for errors in the:
   CEM_CMDB_HOME\apache-tomcat-5.5.25\logs\CEM-cmdbLogger.log
   EM_HOM\logs\IntroscopeEnterpriseManager.log

What to collect:

Enable DEBUG on the EM side:
a) Open the <EM_HOME>/config/IntroscopeEnterpriseManager.properties:
b) Set:
log4j.logger.Manager=DEBUG,logfile
log4j.appender.logfile.MaxFileSize=200MB

Then, restart the integration service and try to reproduce the issue; collect:

1. Exact CMDB, OS and integration version
2. Zipped content of the CEM_CMDB_CONNECTOR_HOME\apache-tomcat-5.5.25\logs
3. CEM_CMDB_CONNECTOR_HOME\CAWily_CEM_CMDB_IntegrationPack\
   CAWily_CEM_Cmdb_IntegrationPack_InstallLog.log.
4. Zipped content of the EM_HOME/logs
5. EM_HOME\config\IntroscopeEnterpriseManager
6. Screenshots from cmdb UI > Administration > CA CMDB > MDR Management > MDR List, confirming the EM
   registration and configuration details.
7. Screenshots of the following pages from the integration webpage: http://localhost:8082/CA-Wily-CEM-CMDB-
   IP : Introscope Configuration, CMDB configuration tabs.
8. Screenshots from cmdb UI > Service Desk > CMDB > CI Families > All
9. Result of nslookup and ping from CMDB to EM and from EM to CMDB

CEM Siteminder integration

Important reminders

Purpose: In siteminder deployments, if single sign-on(SSO) or expiring cookies are used, the basic cookie approach
does not work because the request headers DO NOT contain the username and static cookie that are required for
the Transaction Identification. In this case, TIM needs to communicate with CA Siteminder to determine/decode
SMSESSION tokens from traffic.

In pre-9.1.1: Based on 4.x SM API, you need to provide a shared secret to communicate with Policy Server. - In the
TESS UI > Plug-in > you provide the Session Cookie Name (SMSESSION) and manually the "Shared Secret".

In 9.1.1: New "Host registration model" (Based on 5.x API): More secure trusted host model for connecting with
Siteminder Policy Servers. In the TESS UI > Plug-in > you provide the Session Cookie Name=SMSESSION, Siteminder
Agent (used for connecting and stablishing trust with the policy server) and Policy server (you enter the

administrator's credentials that are needed to run the <tim_home>/smlib/smreghost.exe to generate <tim_home>/config/SmHost.conf file for the WebAgent)

User/session Siteninder identification not working

Checklist:

1. Select "Configure Tim Trace options", enable "Trace sessions and logins", review logs for possible errors,
2. Ensure configuration of Siteminder plug-in is correct. If you are using "Host registration model", make sure to use an administrator account for the Siteminder Policy registration.

What to collect?

1. Go to the TIM, take a screenshot of the
-"TIM status", If you are using ssl, send a screenshot of TIM Server SSL Status
- "View Tim package statistics" 5 sec or 5 min
2. TIM logs
3. Screenshot from CEM \ Setup \ Plug-Ins \ CA Siteminder Web Access Manager: General, Policy Server and Agents

Integration: CEM to Service Desk

Pre-requisites: Service desk 12.5.

Architecture:

/etc/wily/cem/service-desk/scripts/createIssue.sh

Issues or Incidents are raised from TESS

Important reminders

1. Service Desk provides Help Desk capabilities and workflow.
2. CEM-Service Desk integration does not come with Tomcat, you need to download a supported version.
3. Limitations:
- All the incidents are open in the same request area
- Required fields cannot be populated
- Possible issues with CMDB/MDB

Integration: CEM to Spectrum

Important reminders

1. Spectrum is very similar to NSM. NSM has a better event management. Spectrum has a much easier UI. Spectrum is a network management tool that provides root cause analysis.
2. CEM-Spectrum integration is provided by Professional Services.
3. Uses SNMP Traps to send CEM information to Spectrum
4. Integration Points:
- Event & Alert sharing: Alerts sent from CEM to Spectrum, Spectrum represents application monitored by CEM
- Context Launch: Launch from Spectrum context to CEM.
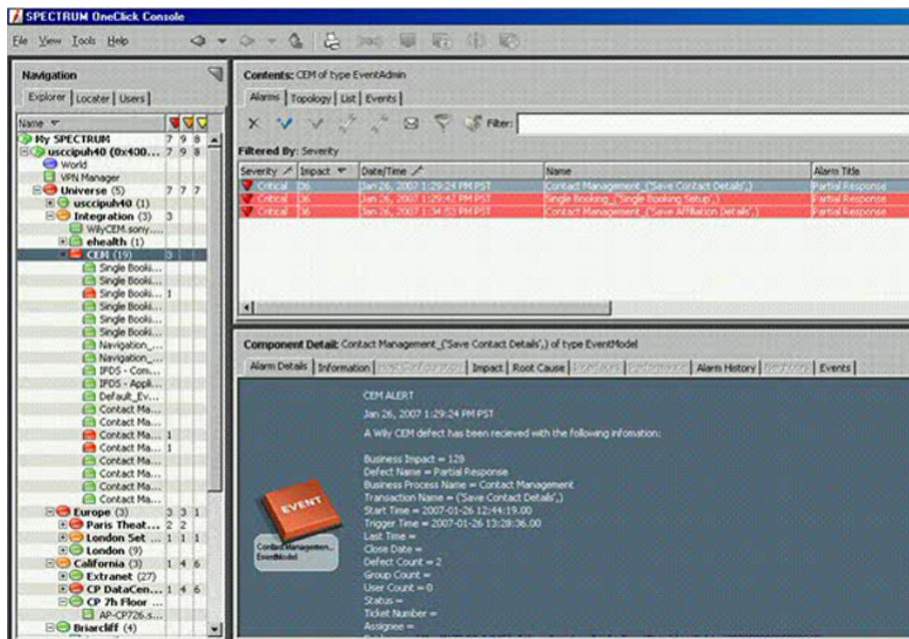
APM Model Webservices

Important reminders

Applies to: 9.0.5 and onward versions
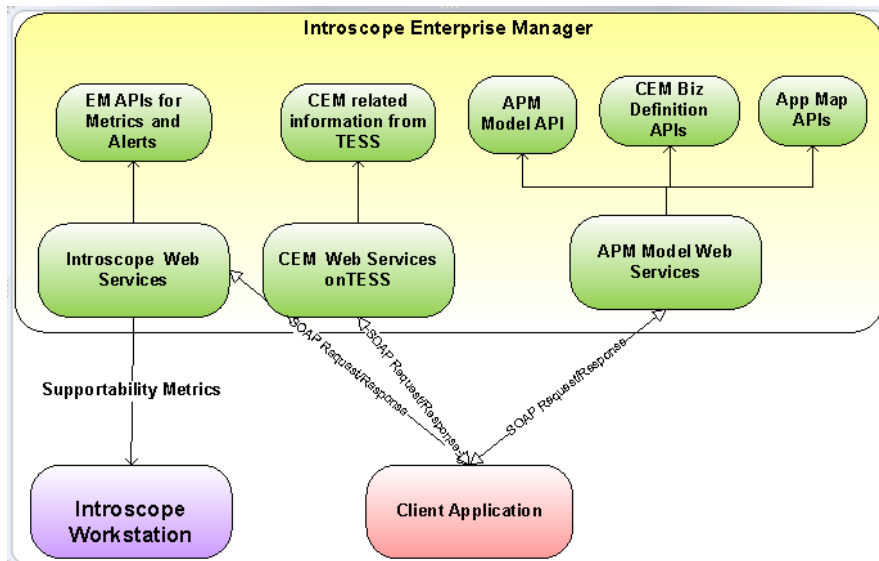
1. Client side sample code is not distributed.
2. Added Webservices API exposes Transaction Model information on: BS, BT, Tx, Edge, Vertex, Owner, EM configuration.
3. How to use the webservices: Generate the stubs from the WSDLs, write a sample wrapper client class and invoke the operations for a given service. Here is an example: apmmodel_sampleclient.zip
4. You can clamp Webservice queries by setting "introscope.apm.query.max.results" in the MOM\config\APMEnterpriseManager.properties

Integration: ADA extension for CA APM

Important reminders
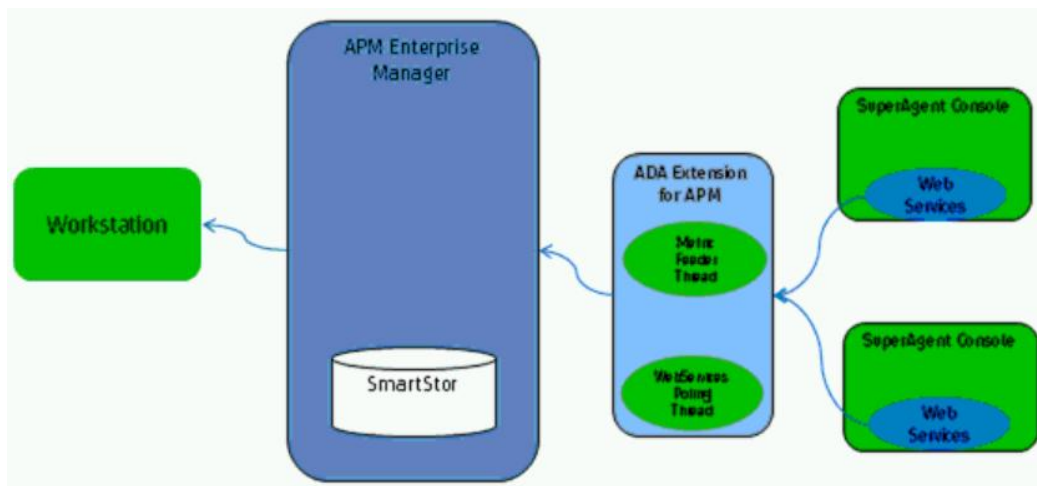
In 9.1:

1. This feature allows you to obtain Network and Server health and below additional Enhanced metrics of Network and Server from ADA/SA (SuperAgent) into Introscope and use a pre-built dashboards to jump into NPC/CAPC
- Data transfer (ms)
- Network round trip time (ms)
- Retransmission delay (ms)
- Server response time (ms)
- Status
We do not show all data status, only the above 4 status.
2. OOB workstation dashboard and typeviews
3. To launch NPC UI (NetQs console) from workstation dashboards, you need to edit the "Object links" of "More info" links in the "Network Status information" dashboard accordingly.
4. Connect to more than one SA console with a single instance of ADA Extension from APM
5. Collect data from SA at every 5 mins, let say it is 10:02, it will collect data from 9:55 to 10:00am. In the workstation, data will not be different for the next 5 minutes.
6. For the dashboard you need to update the Edit Object Link in the "Networks status information" dashboard (network and server overview links)

Not able to see the ADA/SA metrics in workstation

Checklist:

1. Ensure "ADA APM Service" windows service is running

2. Make sure the clocks of "ADA Extension for APM" machine and SuperAgent/ADA machine are synchronized

3. Check if you have the processed data * in SA console > Operation View

4. Collecting data takes time; wait for 10-15 mins.

5. If you are expecting to see Enhancement metrics, make sure to set com.wily.apm.adaconnector.ada_enhancedmetric_enabled=truein ADAConnector.properties. You need to restart the ADA APM Service.

6. Check ADA connector and EM log for errors

7. Check for corresponding problematic/missing metrics in SA/ADA Console.

What to collect:

Enable DEBUG in ADAConnector_HOME/conf ADAConnector.properties, set log4j.logger.ADAConnector=DEBUG, logfile

1. Collect the EM and ADA connector log
2. A copy of /conf/ADAConnector.properties
3. Screenshot from investigator displaying the metric issue
4. Screenshot from SA/ADA Console > Operation View showing the correct data you are expecting to see.

Integration: CA Performance Integration Pack

Important reminders:
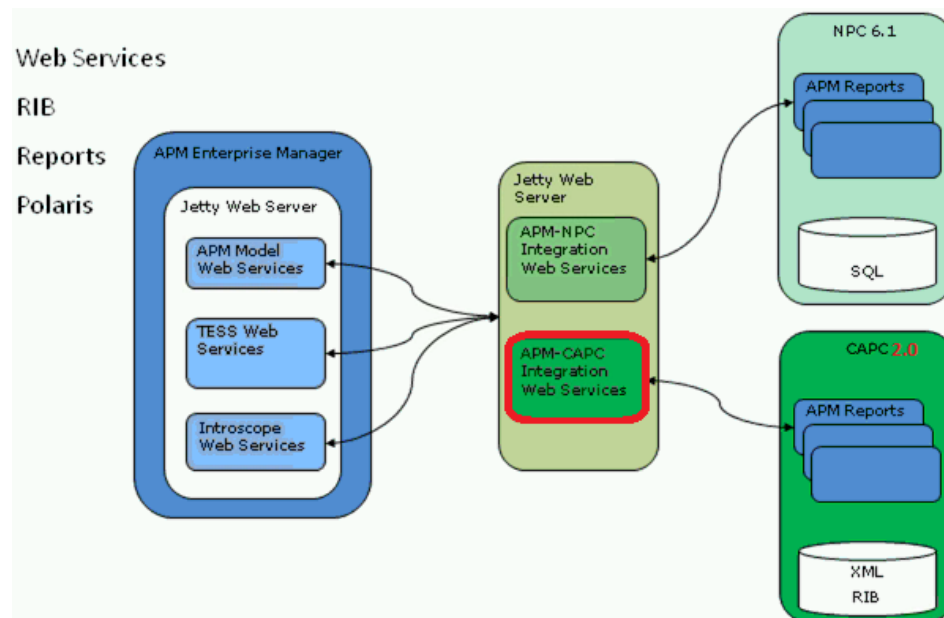
1. Be able to see Application, Business Services & Business Transactions, CE Metrics, CE Incidents and defects in CAPC.

In 9.1
2. Integration support: CAPC 1.0/NPC 6.1
3. Limitation: Only 1 APM data source per NPC instance.

In 9.1.1:
4. Integration support: CAPC 2.0, revised Webservices to support CAPC (ListRIBs, GetRIB,etc), .

No APM report show up on CAPC report menu, "This view request needs at least one APM datasource" message when accessing the APM summary reports

Checklist:

1. Go to the CAPC UI > Admin > Data Sources and verify that the APM datasource has been created. Click on the "Test" button to verify the connectivity. Note: The port # is the one from APM-ADA integration Jetty server.

2. Review CAPCIntegrationPack_HOMElogs\Jetty-service.log and apm-capc-integration.log for possible errors

What to collect:

1. Open the CAPCIntegrationPack\resoureces\log4j.properties, set log4j.logger.ApmCapcWebservices=DEBUG, LOGFILE
2. A copy of the CAPCIntegrationPack\resources\apm-capc-integration.properties
3. Zipped content of the CAPCIntegrationPack_HOME\logs
4. Screenshot from CAPC UI displaying the test connection results.

No data in reports or graphs, "No data to display", "RIB Query error", "Object reference not set to an instance of an object" message

Checklist:

1. Ensure APM is running

2. Verify APM Data Source connection is working. CAPC UI > Admin > Data Sources, Click on the "Test" button

3. Ensure Application TriageMap is enabled:
    CAPC > Reports > APM Application Summary report should match what you see in TriageMap:
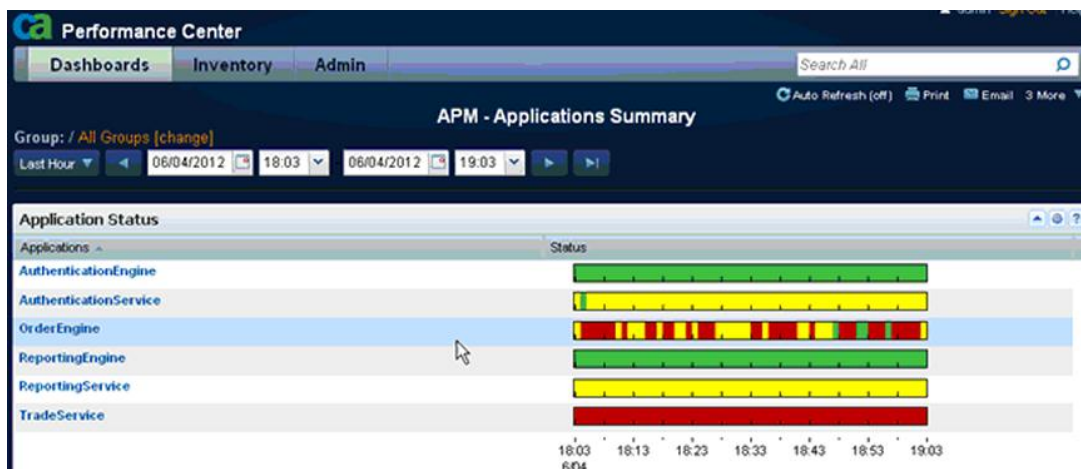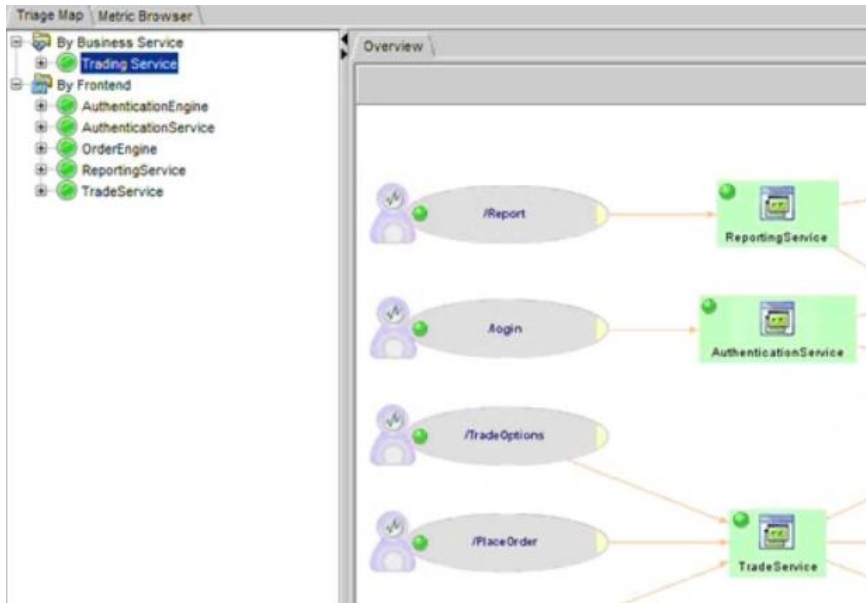
4. Ensure Triage Map Alerts has been created:

The status bar and colors in the APM Summary reports are the representation of the Triage map alerts. Verify that alerts have been configured and are being triggered
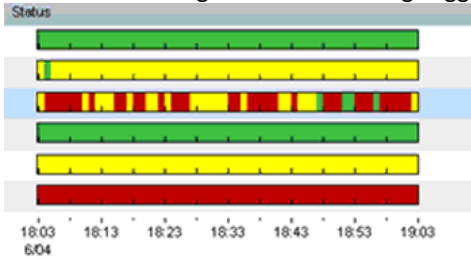
5. Make sure Customer Experience Metrics (RTTM) Collector Service is enabled:

CAPC Metrics graphs are the representation of the "Business Segments" metrics of the BS/BT and 3 of the MTTR metrics.
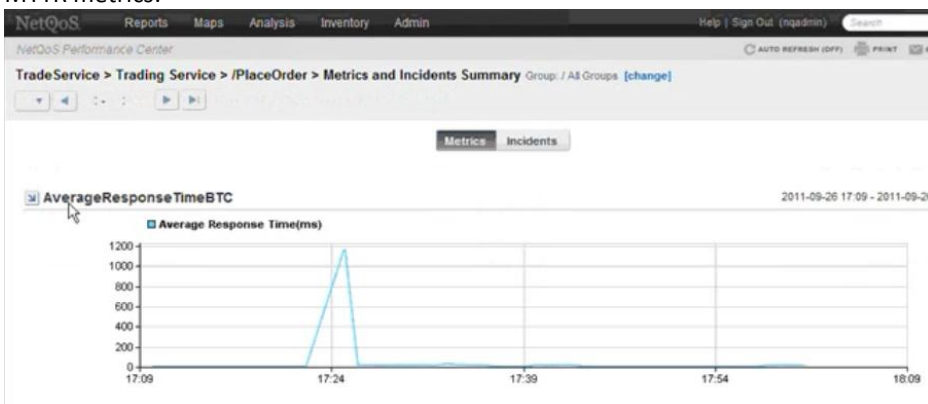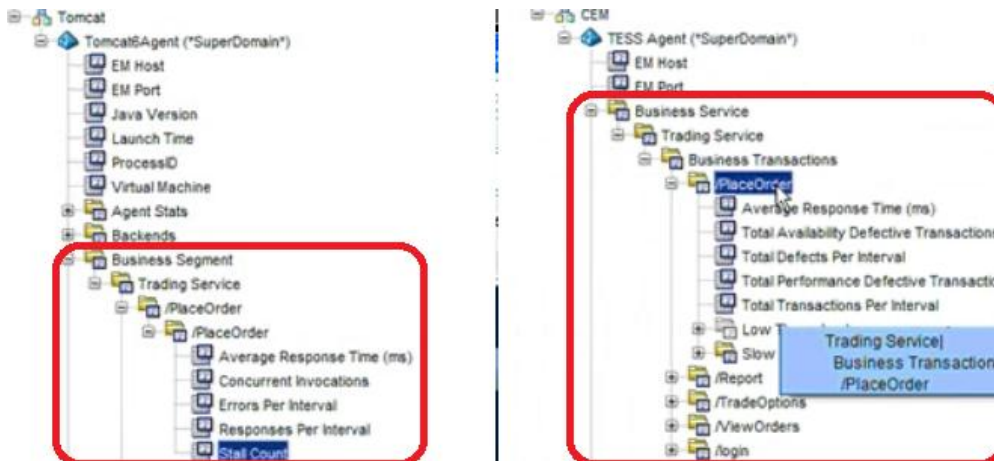
6. Review the apm-capc-integration.properties file in <Integration Home>/CAPCIntegrationPack/resources and verify that you have provided the correct administrator user names and passwords for APM and CEM during the installation. If necessary, you can edit this file and restart the service. Note that if you use https instead of http, there is an optional section titled "Enable HTTPS Support" in the Integration guide which you should follow.

7. Limitation: APM data within CAPC doesn't respect the CAPC grouping permissions: Any user who can see "all groups" have access to the APM pages, users locked down to specific groups will not access to the APM views instead they will get "No data to display" in the view.

8. Review CAPCIntegrationPack_HOMElogs\Jetty-service.log and apm-capc-integration.log for possible errors
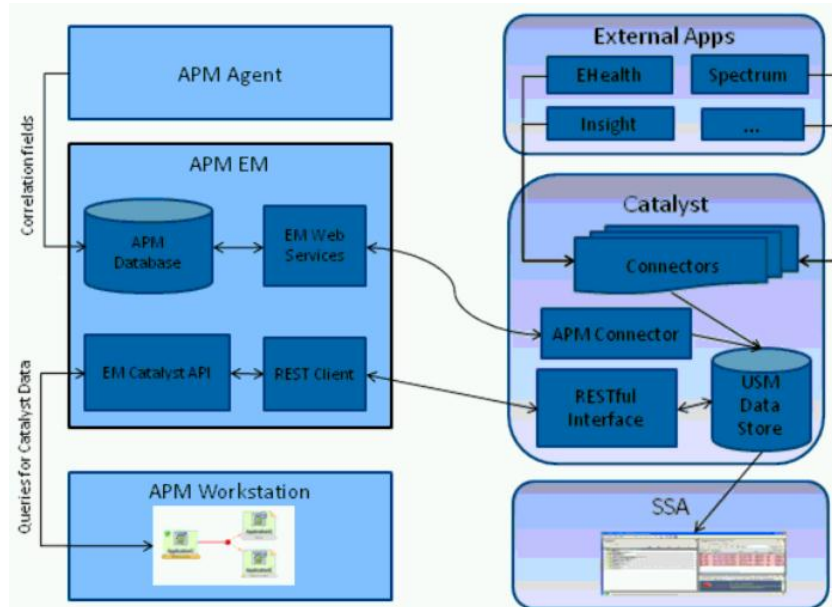
What to collect:

1. Zipped content of the EM_HOME\logs
2. Open the CAPCIntegrationPack_HOME\resources\log4j.properties, set
log4j.logger.ApmCapcWebservices=DEBUG, LOGFILE
3. Go to CAPC_HOME/DM/etc/log4j.xml, uncomment the logger statements for the rib components
(com.ca.im.rib.engine.query, Engine, portal and sorces), it will list the SQL commands sent to APM and the results returned.
4. A copy of the CAPCIntegrationPack_HOME\resources\apm-capc-integration.properties
5. Zipped content of the CAPCIntegrationPack_HOME\logs
6. Screenshot of the problematic APM Summary reports and TriageMap displaying the discrepancy.

Integration to SOI, Catalyst, APM Connector

Important reminders

1. Two types of integration:
   a) We submit data to catalyst via "APM Connector", data is reconciled in Catalyst (USM) using correlated fields.

b) EM retrieves data from Catalyst using REST APIs and displays information in LocationMap. This feature is bundled with the EM – see Location Map section.

APM Connector download location:

https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=b001f6d2-cdb6-4100-90a8-f40a05116d8a&productID=8257

SOI Software: https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=b49e31b4-3de1-4e83-9b67-6f305bdef913&productID=8257

2. Added in 2.0:
    -In addition to simple alerts, the APM Connector support triage map alerts, it requires manual configuration in the EM properties file: Introscope.apm.catalyst.triagemapalert.*

Introscope Alerts are not populated in SOI

Checklist:

1. Make sure windows service "CA SAM Integration Service" is up and running

2. If you are using SOI 3.0, apply patch RO56291 (SOI 3.1), there is a known issue affecting 3.0.

3. Run nslookup to the APM Connector server from the Introscope EM server and to SOI server from the APM connector server.

4. If there is a firewall, for testing purpose, disable it

5. Open <SOI_home>\resources\Configurations\APM_<your severname>.xml, ensure:
    - EMHost= IP address of the Enterprise Manager
    - EMSNMPHostIPAddress= IP address of the Enterprise Manager
    - EMSNMPBindAddress= IP address of the APM connector server

- EMSNMPCommunity and EMSNMPTrapPort should match the vales in the SNMP Alert action.

Open the SNMP Alert action in the Introscope Management module editor, ensure:

SNMP Destination > Trap Port= EMSNMPTrapPort

SNMP Destination > Community= EMSNMPCommunity

SNMP Destination > Host IP = IP address of the APM Connector server

6. If you are using a desktop build on the EM side, the APM Connector will fail to identity the APM version. In this case, you must explicitly set the APM version in their APM_<em_host>.xml as below

    <ConnectionInfo APMVersion="PostAPM906"

    Possible values:PreApm906, APM906, PostAPM906, APM9071, APM91, APM95, APM96

7. Enable TRACE logging and search for errors:
    Open SOI_HOME \resources\Configurations\log4j\APM_log4j.xml
    <logger name="com.ca.wily.apm" additivity="false">
    <level value="INFO" />
    <appender-ref ref="APMConnector" />
    </logger>
    Replace INFO with TRACE.

8. Use the SNMP Alert Action "Test Now" button to verify that the EM is able to send a trap to the APM connector server. This will help you validate the connectivity. In the APM_Connector.log you should see a message like this:

    "Action Test: New SNMP Alert Action, 1.3.6.1.4.1.791.4.4.5: TestDomain, 1.3.6.1.4.1.791.4.4.6: testHost, 1.3.6.1.4.1.791.4.4.7: testProcess, 1.3.6.1.4.1.791.4.4.8: testAgent, 1.3.6.1.4.1.791.4.4.9: TestMetric:metric, 1.3.6.1.4.1.791.4.4.10: 0, 1.3.6.1.4.1.791.4.4.11: http://:8080/console/frameset.do?managementModuleName=Sample&domainName=SuperDomain&dashboardName=Overview, 1.3.6.1.4.1.791.4.4.12: 0, 1.3.6.1.4.1.791.4.4.13: 1, 1.3.6.1.4.1.791.4.4.14: no, 1.3.6.1.4.1.791.4.4.25: 10.130.112.99, 1.3.6.1.4.1.791.4.4.19: true,]]."

    If you don't see the message, use Wireshark utility on the the EM and APM connector servers to confirm that the trap is being sent by the EM and received by the APM connector.

9. For 8.x agents, EPAgents, or any agents that doesn't report any frontend you need to configure an initial alert (sent a trap) to be able to report these agents as Running Software CIs to SOI. In APM connector 2.2 a new property has been added "non9XJavaOrDotNETAgents" to allow the connector to automatically discover these types of agents.

10. Verify that the agent has been added to an SOI Service, this is required to be able to see the Introscope alerts information in the SOI console. If this hasn't been done, below are the steps you need to take:
    a. Go to SOI Service Modeler
    b. From the Menu, select Tools \Create New Service
    c. Locate the agent under the Computer System \ Running Software
    d. Right click, select Add with sub-components
    e. Give a name to the Service and save it

11. Review the SOI_HOME\logs\APM_connector.log, search for errors.

What to collect:

1. Stop CA SAM Integration Services
2. Delete SOI_HOME\logs\APM_connector.log
3. Start CA SAM Integration Services
4. Generate Alerts from Introscope
5. Collect:
   a) Zipped content of SOI_HOME\logs
   b) Zipped content of SOI_HOME\Resources\configurations\
   c) Zipped content of EM_HOME\logs
   d) Zipped content of AGENT_HOME\logs
6. Screen shot of the SNMP alert action and alerts definition from the management module editor.
7. General overview of the implementation indicating where is SOI, APM Connector and Introscope EM

TriageMap Alerts are not populated in SOI

Checklist:

1. Make sure windows service "CA SAM Integration Service" is up and running

2. If you are using SOI 3.0, apply patch RO56291 (SOI 3.1), there is a known issue affecting 3.0.

3. Run nslookup to the APM Connector server from the Introscope EM server and to SOI server from the APM connector server.

4. If there is a firewall, for testing purpose, disable it

5. Open <SOI_home>\resources\Configurations\APM_<your severname>.xml, ensure:
   - EMHost= IP address of the Enterprise Manager
   - EMSNMPHostIPAddress= IP address of the Enterprise Manager
   - EMSNMPBindAddress= IP address of the APM connector server
   - EMSNMPCommunity and EMSNMPTrapPort should match the vales in the
   EM_HOME\config\IntroscopeEnterpriseManager.properties:
   introscope.apm.catalyst.triagemapalert.snmp.destination.trap.port=
   introscope.apm.catalyst.triagemapalert.snmp.community=

6. Ensure introscope.apm.catalyst.triagemapalert.snmp.destination.host.ip has been set equal to the ip address of the SSA/Catalyst connector

7. If you are using a desktop build on the EM side, the APM Connector will fail to identity the APM version.
   In this case, you must explicitly set the APM version in their APM_<em_host>.xml as below
   <ConnectionInfo APMVersion="PostAPM906">

8. Enable TRACE logging and search for errors:
   Open SOI_HOME \resources\Configurations\log4j\APM_log4j.xml
   <logger name="com.ca.wily.apm" additivity="false">
   <level value="INFO" />
   <appender-ref ref="APMConnector" />
   </logger>
   Replace INFO with TRACE.

9. Verify that the frontend/Business Transaction alert has been added to a SOI Service, this is required to be able to see the alerts information in the SOI console. If this hasn't been done, below are the steps you need to take:
    a. Go to SOI Service Modeler
    b. From the Menu, select Tools \Create New Service
    c. Locate the TriageMap agent under the appropriate class:
       Frontends alerts = Transaction Context CI
       Business Transaction alert = Business Transaction CI
    d. Right click, select Add with sub-components
    e. Give a name to the Service and save it

10. Review the SOI_HOME\logs\APM_connector.log, search for errors.

What to collect:

1. Stop CA SAM Integration Services
2. Delete SOI_HOME\logs\APM_connector.log
3. Start CA SAM Integration Services
4. Generate Alerts from TriageMap
5. Collect:
    a) Zipped content of SOI_HOME\logs
    b) Zipped content of SOI_HOME\Resources\configurations\
    c) Zipped content of EM_HOME\logs
    d) EM_HOME\config\IntroscopeEnterpriseManager.properties
6. General overview of the implementation indicating where is SOI, APM Connector and Introscope EM
7. Screenshot from TriageMap displaying the alerts.

Integration: APM with CA Executive Insight
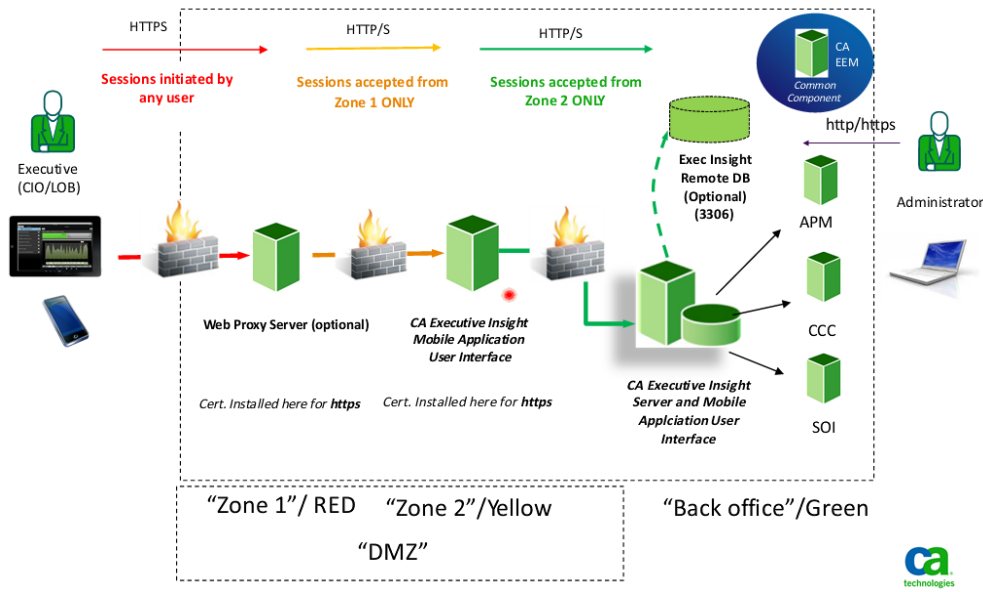
Important reminders

In 1.0, 1.1, 1.2:

1. Ability to expose CA Service Assurance content via mobile platform for anytime/anywhere access: Catalog of business indicators, Business Dashboard and widgets, devices: Apple iPhone, iPad and Android
2. Business indicators via integration with: CA APM, SOI, CSV import to allow non-IT data
3. Collaboration via Annotations: In-context annotating on the charts in the mobile UI
4. Business Indicators Editor: Admin UI on Desktop to manage connectors, categories and indicators.
5. Security integration with EEM: role based security to restrict administrative privileges and access content.
6. Fully localized in Japanese.
7. Known Issues:
   -69046 - Large numbers are not rendered correctly in Biz Indicators details page.
   -69552 - Mobile UI: Count for Biz Indicators list does not update once data is cached. Workaround: It needs a manual refresh
   -70621 - Rotation Issue: annotation creation window with keypad open gets distorted
   -70386 - [sencha] Rotation: Page does not display with correct dimensions
8. Known Limitations (by design):
   -It doesn't support HTTPS.
   -You cannot delete/edit annotations; you cannot apply permissions/rules to annotation.
   -15m resolution in graphs for CEM metrics is irrelevant.
   -Do not support String metrics
   -When switching from Portland to Landscape, the graph takes the full space, this is by design.
   -CEM default frequency is 60 minutes, you cannot lower this value

In 1.3:

1. Business Branded Images: Allow custom images.
2. Gauge Widget (semicircular): New visualization type available in a dashboard.
3. You can use "Bulk Edit" to add an image and set a visualization type to multiple BI simultaneously.
4. Business Indicators via Integration with CA Capacity Command Center (CCC)
5. Internally/Code level: Upgrade to Sencha Touch 2.1 framework

6. Better visualization of indicator having data interval greater than a minute, causing blank graphs. Known issue for CEM graphs.
7. FIPS compliance.

In 2.0:

1. Internet Accessible Deployment (no VPN):
   - New "Mobile Application User Interface" option to be place in DMZ: embedded in a tomcat server.
   - "Server and Mobile Application User Interface", to be used if you don't want to use the Internet option
2. Simplified URL and Admins:
   Mobile UI : http://<host>:8080/exec -> New http://<host>:8080/
   Admin UI : http://<host>:8080/execDesktop -> New http://<host>:8080/admin
3. Universal Web Services Adaptor:
   a. Authentication: Basic, Digest or none
   b. Response formats: XML, JSON, ATOM
   c. Metric and metadata request types
   d. Parameter for filtering data from web services
   e. The GET HTTP execution method
   f. Variables to pass data from one request to another
4. Support for Android Tables (Both 10 and 7 inch running on OS 4.x.
5. Non-Marquee features:
   a. Configure thresholds with decimal values
   b. New property to configure the amount of data collected from CCC: Max allowed=30 days, higher # of days, greater is the performance overhead in case of large number of indicators.
   c. Display of large values in dashboard widgets and detail views (suffixes are specific to locale, i.e: 1M, 5B or 6.5T), not in axis or detail pane.
   d. Change default duration of indicators (useful for indicators where default 1 hour is not appropriate)
   e. Latest aggregate value in a given time range(15m, 1H, 1D,etc)

EI configuration issue, not working

Checklist:

1. Make sure configuration is supported:

   a) Admin UI: Windows 2008 and RHEL 5 64bit support only using MySQL 5.5.8 shipped with the product, IE 8, 9 and firefox 10.x browser with EEM r8.4 and CEM 4.5(web service port 80), Introscope 8.x (port 8081), APM 9.x (port 8081), SOI 3.0 (port 7090), CCC 2.1.0 (port 8081)

   b) Mobile UI:
   Need Webkit browser (Safari on iOS, Chrome, default browser on Android), it will not work in IE or Firefox.
   iOS:
   - Device: iPhone 4, 4S, 5 ; Browser: Safari Browser shipped with iOS 6.0
   - Device: iPad2, iPad2 ; Browser: Safari Browser shipped with iOS 6.0 (iPad1 not supported as it caused crashes)
   - Device: Samsung Galaxy, HTC, Motorola Atrix (blackberry not longer supported) ; Default Android shipped with Android 2.3, 4.1. Only Chrome browser from Android 4.0

2. Limit enforced:
   a) Admin UI:
      Maximum number of categories =50

Maximum number of indicators per group (category/home page) = 25
Maximum number of annotations per indicator = 50
b) Mobile UI:
Maximum number of indicator shown in the All list=250

3. Configuration files:

a) Server and Mobile Application User Interface:

<InstallDir>/config:
-execConfig.properties: Contains various limits
-EEM.properties: Connection information to EEM Server
-masterDbCredentials.properties: Database connection parameters

EEM and DB Passwords are stored encrypted in the config files. If a password needs to be changed, run
EncryptPasswordTool.sh/bat to create encrypted password
b) Mobile Application User Interface:
<installDir/config/execWebUIConfig.properties : contains connection properties for The EI server.

4. Configuration in the database:

Master.Tenant_Connpool : Connection pool parameters (max pool = 40)
Master.Tenant_Dbconfig: Tenant schema Connection details
Tenant.Tenant_settings:
- Biz Indicators Raw Data Retention days (3)
- Biz Indicators Hourly Aggregated Data Retention days (14)
- Biz Indicators Daily Aggregated Data Retention days (730)
- Data Aggregation Service Offset minutes (30)

5. Authentication: after 24 hours, you need to re-enter credentials.

6. You can use DBVisualizer (http://www.dbvis.com) if you need to look at the data in the MySQL db.

7. If MySQLserver is running in a separate server, the user should have access to "execute commands from a remote server"

8. Change <EI_InstallDir>/config/log4j.rootLogger to DEBUG for debug logging in
<InstallDir>/config/log4j.properties, no need to restart. This applies for Mobile Application User Interface available
in v2.0

Server Log files:
<EI_InstallDir>/log/ExecutiveInsightServer.log
<EI_InstallDir>/log/ExecutiveInsight _Install.log
<EI_InstallDir>/log/ei_inst_history.txt -> Useful for upgrade issues.

Mobile Application User Interface Log files
<EI_InstallDir>/log/ExecutiveInsightWebUI.log
<EI_InstallDir>/log/ExecutiveInsight _Install.log
<EI_InstallDir>/log/ei_inst_history.txt -> Useful for upgrade issues.

Integration with CCC not working

Checklist:

Turn DEBUG on in the EI log4j.properties file to see polling details:
Log4j.logger.com.ca.exce.services.BizIndicatorDataFetchService=DEBUG
Log4j.logger.com.ca.exce.services.BizIndicatorDataPersistenceService=DEBUG

Turn DEBUG on in the EI log4j.properties file to see the CCC API calls and results:
Log4j.logger.com.ca.exec.connector.hyperformix.v1.HyperformixConnector=TRACE

Use a browse or any REST API client utility to make the CCC web service calls.
For example, use WizTools.org RESTClient 2.3, against URL: http://server:8181/ccc/api/1.0/Baselines
Select Headers, Body.

Specify JSON as output format to make it easier to view the result output.

Universal Webservices Adaptor issues

Checklist:

Turn DEBUG on in the EI log4j.properties file to see polling details
log4j.logger.com.ca.exec.services.BizIndicatorDataFetchService=DEBUG
log4j.logger.com.ca.exec.services.BizIndicatorDataPersistenceService=DEBUG

Turn TRACE on in the EI log4j.properties file to see the API calls and results
log4j.logger.com.ca.exec.connector.http.v1=TRACE
log4j.logger.com.ca.exec.http.restclient=TRACE

Use a browser or any REST API client utility to make the remote web service calls

Specify JSON as output format to make it easier to view the resulting output

Limitations:
    -only HTTP method GET requests are supported
    -only Basic, Digest authentication methods are supported
    -only XML and Json format responses are supported.

Integration: APM Cloud Monitor Agent

Important reminders

In 9.1.1:

1. Cloud Monitor: monitors synthetic transactions (replicates real user transactions coming from 60+ monitoring stations around the globe), User configured monitors (from simple browser, transactional and various protocols), provides public status pages, provides REST APIs for data retrival.
2. APM Cloud monitor integration goal: makes cloud monitor available in investigator.
3. All data collected via APM Cloud Monitor's RESTful API calls: Metric every 1 min, and (Folder, Monitors, Checkpoints) every 1 hour.
4. Detailed CloudMonitor metrics available in investigator and customized dashboards.
5. Architecture:
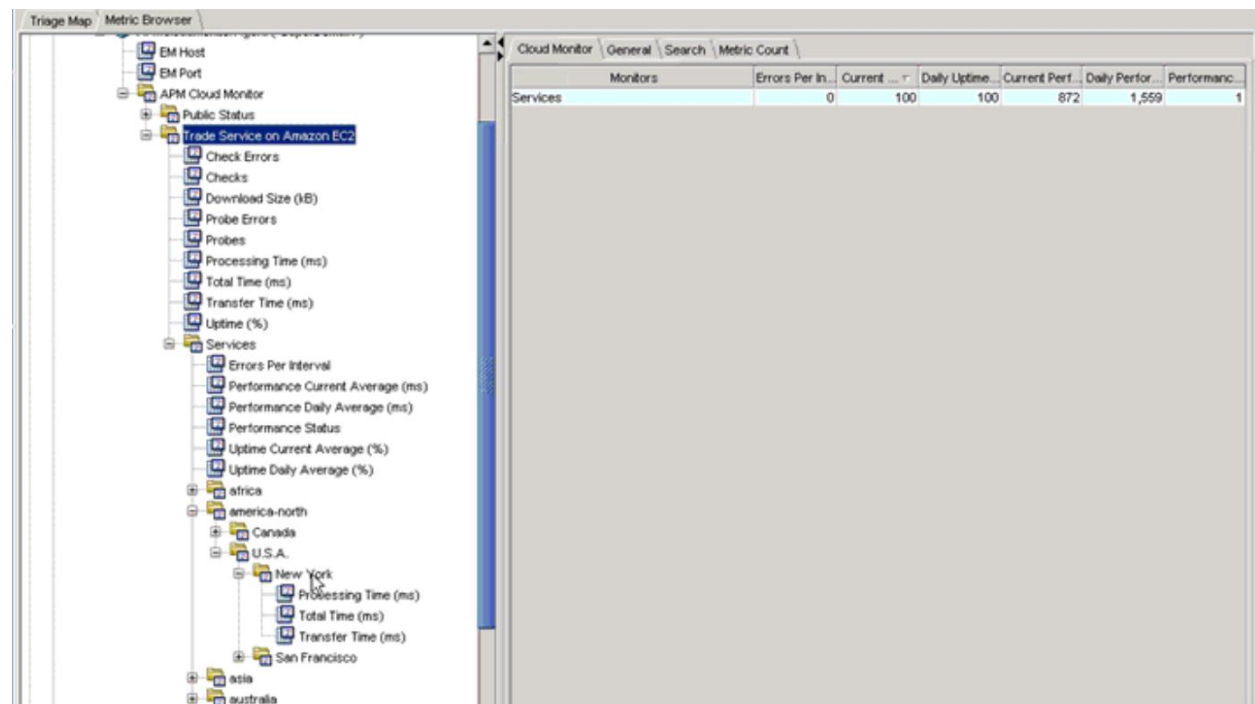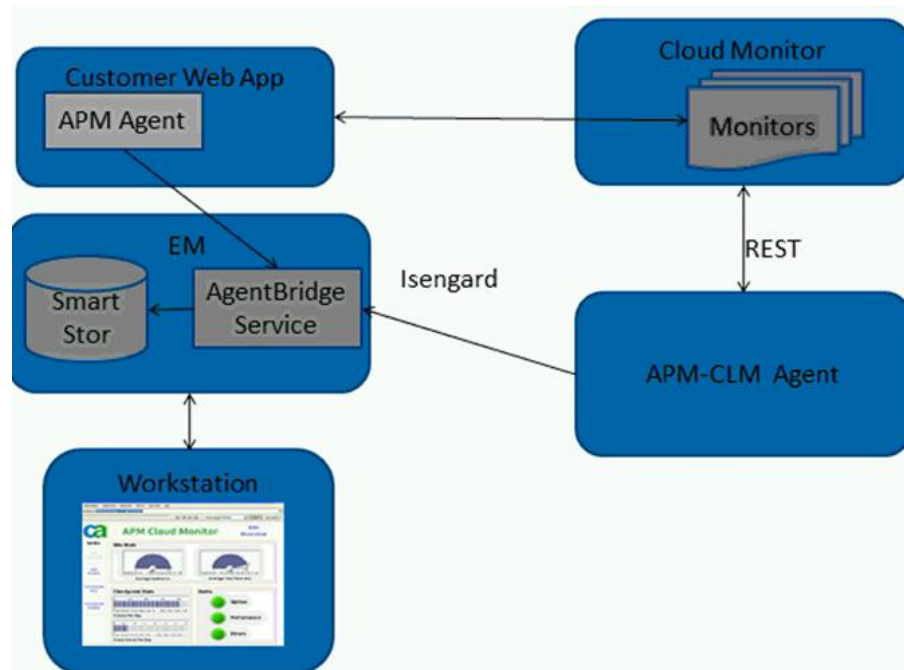
## Not working, missing metric

Checklist:

1. Ensure that the server where the agent is running has internet connection. If proxy is needed, specify proxy settings.

2. Make sure the \conf\APMCloudMonitor.properties file configuration is correct: apmcm.user, apmcm.password, apmcm.url, apmcm.http.method, apmcm,em* parameters.

3. Make sure the cloud monitor properties file configurations and folder count will not exceed the API credit limit. We are not allowed to make more than 5000 API calls a day. The API call acct_credit can be used to check credits.

4. Verify data on CloudMonitor site: http://cloudmonitor.ca.com
And from the APIs at https://api.cloudmonitor.ca.com/1.6/

5. Enable debugging in config/logger.properties file, set
       Log4j.logger.CloudMonitorIntegration.CloudMonitor=DEBUG.
       log4j.logger.CloudMonitorIntegration.EM=DEBUG
Review the log, copy the URLs used and verify the results in a browser, to know if the problem is in the Cloudmonitor or CloudmonitorAgent side.

What to collect:
CMAGENT_HOME\conf\APMCloudMonitor.properties
CMAGENT _HOME\logs*.log
CMAGENT _HOME\install*.log
EM_HOME\log*

Integration: APM LISA Agent

Important reminders
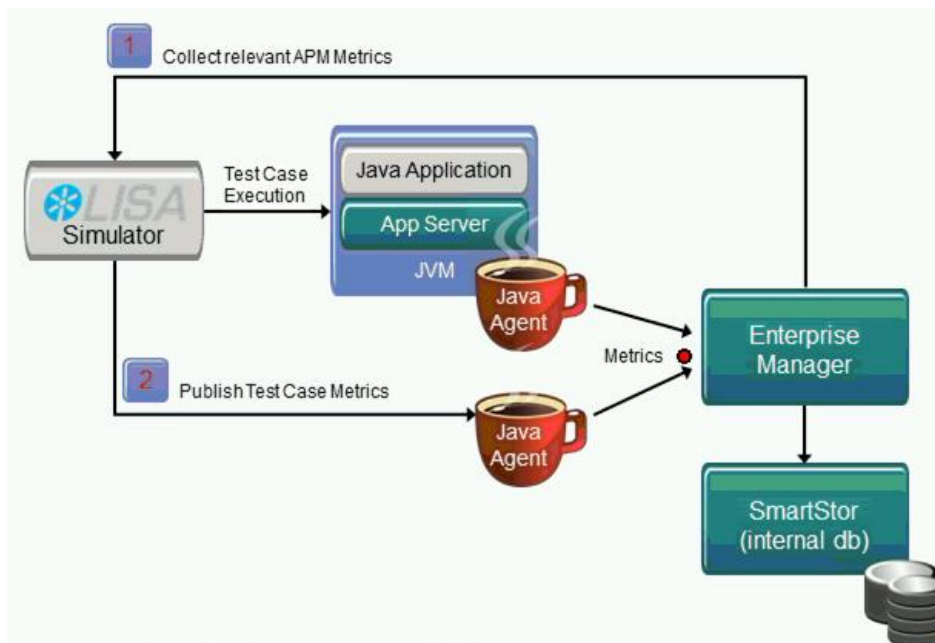
In 9.1.1:

1. LISA itself helps prevent problems before they get to production.

2. Support: LISA 6.0.6

3. Integration option 1: In LISA, you use VSE companion (Wily data source) and collect metrics of your application in production using APM API webservices. This will allow the building of a more accurate model, this information will be used by Development, QA teams to identify any bottleneck/problem.

4. Integration option 2: Use the APM LISA Agent to:

a) Publish results of LISA test case execution into workstation:

b) Publish metric of synthetic transactions (generated from LISA workstation) and real user transactions into worlstation:
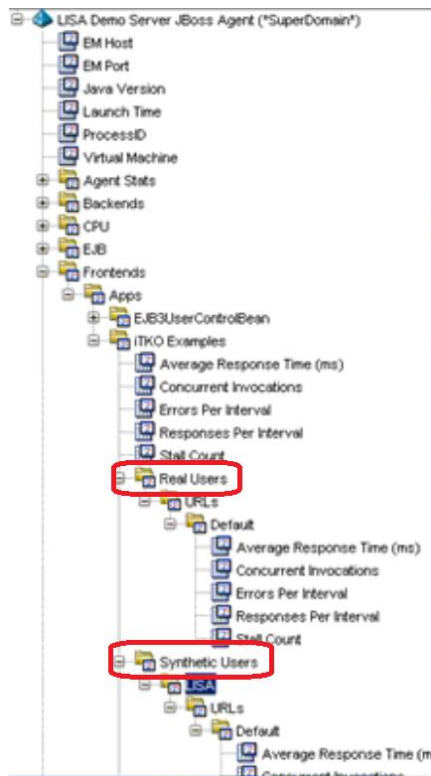
Missing metrics in Investigator, no metrics from LISA test results, no synthetic users

Checklist:

1. Ensure lisa-typical.pbl is added to Introscope.autoprobe.directivesFile and Lisa.jar is in the /ext directory

2. To enable synthetic tracer you need to uncomment the "Introscope.agent.synthetic.header.names=Synthetic_Transaction,x-wtg-info,lisaframeid" property in the IntroscopeAgent.profile

3. LISA tests run under ITR, metrics will not display under investigator, you should use instead Staging document that has all the attributes.

4. Try to restart the LISA server

What to collect:

LISA_HOME\hs_err_.log
LISA_HOME*.properties
LISA_HOME *.vmoptions
LISA_HOME\lisatmp_**.log*
LISA_HOME\.install4j*.log*
Zipped content of the APMLISA_HOME\logs
IntroscopeAgent.profile