



# **VRUM 11.1 Troubleshooting Guide**

**Version 1.0**  
**04/16/2010**

## Table of Contents

<b>AMD</b>	4
<b>1. AMD performance related issues &amp; AMD restarts</b>	4
❖ Understanding the performance constraints of the AMD	5
❖ True AMD performance vs. AMD performance estimates provided in AMD install guide	6
❖ Existing options to overcome AMD performance overload situation	6
❖ Communicating the AMD overload situation to the customer	7
❖ Nice to know	7
<b>2. Common SSL (HTTPS) decryption issues</b>	8
❖ Signs of SSL decryption not functioning properly	8
❖ Common problems	9
<b>3. XML and SOAP decodes</b>	12
❖ Typical XML structure	12
<b>4. RedHat OS related topics</b>	13
<b>5. Regular expressions</b>	14
❖ Multiple reasons stand for common use of regular expressions AMD	14
❖ There are two types of regular expressions in use – POSIX Basic and POSIX Extended	14
❖ Best practices & nice to know	15
<b>VRUM report servers (VAS/AWDS) specific issues</b>	16
<b>1. Common issues on VAS</b>	16
❖ Lack of application performance & availability metrics	16
❖ VAS 11.1 GA re-installation	17
❖ Known Watchdog service issue on Windows 2008 Server	18
<b>2. Common issues on AWDS</b>	19
❖ Sudden increase of AWDS database after upgrade to CVA 11.1 from CVA 10.x release	19
❖ Things to remember about AWDS 11.1	19
<b>3. Troubleshooting common VAS/AWDS database issues</b>	20
❖ When TempDB shrink task fails	20
❖ How to recover forgotten “delta” DB user password	21
❖ How to recover forgotten “superuser” password	21
❖ BulkInsert issues	21
❖ Database FAQ	23

<b>4. VTCAM (Citrix) common issues .....</b>	<b>24</b>
❖ VTCAM constrains .....	24
❖ Troubleshooting common issue with missing information from VTCAM agent.....	25
❖ Things to remember about VTCAM in 11.1 .....	27
<b>5. Windows Server related topics.....</b>	<b>28</b>
❖ Memory limits for Windows releases .....	28
<b>TBD topics .....</b>	<b>29</b>
❖ VRUM report servers (VAS/AWDS) specific issues.....	29
❖ AMD .....	29
❖ General topics .....	29

# AMD

## 1. AMD performance related issues & AMD restarts

- ❖ In an ideal situation AMD should work 24/7 with no service interruption except for AMD reconfiguration and/or software maintenance on AMD (product upgrades).
- ❖ In reality AMDs operating at customer environments experience events that eventually lead to AMD restart(s). In most cases there are two major reasons for those AMD restarts.
  - 1) Due to overload circumstances
  - 2) Due to a product (AMD) code related problems.
- ❖ Investigations that leads to a determination of the root cause behind the AMD restart – i.e. either (1) or (2) cause – is considered one of most challenging efforts in VRUM world.
  - AMD restart in rtm.log will typically be prefixed this way:
    - No free packet buffers size=XXXX or
    - Could not allocate additional memory for XXXX sessions
  - Both messages indicate insufficient AMD resources (CPU or memory) to perform further packets analysis.
  - The first one (“No free packet buffers size=XXXX”) is typically result of AMD incapable of analyzing incoming packets fast enough to free the packet buffers queue (incoming packets arrive faster to the buffer than AMD is able to analyze and remove from the buffer). A stronger (CPU horsepower) machine will likely overcome this problem.
  - The later one (“Could not allocate additional memory for XXXX sessions”) is caused by AMD running out of memory. Lack of memory can either be due to too much traffic (overload) or due to a memory leak in core AMD engine (or in some particular AMD decode). That is when a core dump file (/usr/adlex/rtm/bin/core\*) and the AMD logs (/var/log/adlex/rtm.log, rtm\_perf.log) play a major role in making a determination one way or another.
  - The AMD restarts root cause determination process typically consists of the following steps:
    - Customer Support checking if the restarts is not a known (product) issue already fixed by a newer (post GA or post latest service pack AMD build)
    - Customer Support checking the performance statistics of the AMD (key AMD resources – CPU & memory – utilization as well as traffic input rate volumes (kpps) and the AMD decode breakdown – a share of different decodes use in analyzing the total traffic on AMD input (from SPAN ports).
    - CVA development team analyzing the core dump files and the logs seeking for some possible code related issues – like unsupported traffic scenarios or a potential memory leak.

## ❖ Understanding the performance constraints of the AMD

Once the investigation performed led to a conclusion that the root cause behind AMD restart is due to AMD overload situation the role of L1 support and FTS is now to communicate this to the customer. At this point both Customer Support team and development team made the determination that neither known nor new product issues (including a memory leak) exist in the AMD code – i.e. AMD is working as designed.

That means AMD only restarts because of overload situation. Here are a couple of guidelines that should help understand the performance constraints of the AMD and help formulate the response back to the customer.

- Actual workload of the AMD strongly depends on the nature of traffic – which typically is a mix of different protocols (http, oracle, XML, MQ, etc)
- AMD performance also depends on the configuration of the AMD decodes – the more sophisticated analysis enabled (like recognition of HTTP custom application errors) - the more horsepower and resources is needed on AMD to do the job timely.

For example, an AMD configured with HTTP decode that is analyzing HTTP custom (application) errors – in such case the AMD is forced to analyze the whole content of HTTP packets (that is the actual application payload) – while with this feature turned off, the AMD is only analyzing the headers of HTTP packets and not the payload – that means way lower memory consumption and a fewer horsepower to handle the job. In that case AMD can handle a lot of http traffic, but with app errors feature enabled, the performance of the HTTP decodes goes down dramatically. That is the payoff of having the extra feature.

- AMD has a fixed upper memory limit – ca 3 GBs of RAM for the core analysis engine (“rtm” service). The limitation comes from a 32-bit OS architecture and adding more RAM to the AMD will not help resolve the problem, since “rtm” service will NOT be able to use this extra memory.

Typically AMDs are equipped with 4 GBs of RAM – the remaining 1 GB of RAM is then utilized by:

- rtmgate (tiny http web server) on the AMD –the component hosting raw data files for VAS/AWDS
- AWDS aggregators (v2page, page2trans)
- other Linux native services & OS functions

Adding more RAM to the system can only leverage the swap memory utilization by those additional tasks/services, but it will not increase upper memory limit for the “rtm” (core) AMD engine. As long as AMD restarts are due to lack of memory in “rtm” engine, the bottle neck is here and more RAM won’t help.

This fixed 3 GBs (per process) 32-bit architectural limitation will be overcome with the introduction of a 64-bit AMD that will be available beginning with Vantage 11.5 release (Summer 2010). Vast majority of the memory related issues will be addressed by 64-bit AMD and unlimited RAM size that could be utilized. Note one thing. The 64-bit AMD will still have a limited performance in the particular decodes, better performance than in case of a 32-bit AMD, but still limited.

## ❖ True AMD performance vs. AMD performance estimates provided in AMD install guide

AMD performance estimates provided in the AMD install guide - that is “how much traffic of a given decode (Oracle DB, HTTP(s), XML, Oracle Forms) AMD can sustain” - contain numbers that only provide some laboratory results achieved for the decodes in a specific traffic profiles (described in the guide). Obviously there is no magic formula that could be used to precisely tell what true capacity an AMD in the specific customer environment can achieve. Again, that depends on the mix of the protocols and the share of those protocols in total volume as well as the monitoring configuration (more detailed analysis -> more power required -> less volume of traffic can be processed simultaneously and without AMD restarts, delays, packet drops, etc). The numbers in the guide are not absolute numbers – i.e. one cannot say: you promised the AMD can handle XXX Mbps of HTTP while my AMD can barely stand half of that volume and then it fails (restarts). Real life implementations can vary and the same AMD with the same decode can reach different performance factor in different environments.

Vantage 11.5 will come with some improvements in reporting on current resource utilization of the AMD (as well as other VRUM components – VAS & AWDS). This way the customers/FTS can take proactive approach to monitor and address upcoming performance troubles in advance and also prevent the overload situation by not enabling more software services to be monitored if the CVA setup is already maxed up.

## ❖ Existing options to overcome AMD performance overload situation

- Acquire another AMD and enable load sharing mode on the both AMDs. This scenario requires for both AMDs to receive (a copy of) the very same traffic on input (same traffic from SPAN ports), only one AMD will analyze ½ of ALL the incoming sessions and the second AMD – the remaining ½ of the entire traffic. This is a very flexible mechanism and allows for maximizing the utilization of the two AMDs (hardware). It is also possible to perform a “prove of value” of this load-sharing setup having only one AMD available at a time (i.e. to prove that adding another AMD will actually resolve the problem) – simply set-up this AMD in a load sharing mode and observe if nor restarts occur during a day/times when the AMD restarted previously when not in load sharing mode. If no restarts occur that means the 2<sup>nd</sup> AMD will be good enough to leverage the workload of the existing one.

Example settings to set load balancing between two AMDs:

AMD1 [/usr/adlex/config/rtm.config]	AMD2 [/usr/adlex/config/rtm.config]
sess.accept.filter.enabled=true sess.accept.filter.fractions=2 sess.accept.filter.id=0	sess.accept.filter.enabled=true sess.accept.filter.fractions=2 sess.accept.filter.id=1

- Acquire another AMD and distribute the workload between the AMDs by separating software services to be monitored by different AMD in a set.
- Simplify the decodes configuration – disable more sophisticated analysis like HTTP application errors reporting, HTTP frames recognition, etc
- Limit the number of monitored software services to the key ones customer needs/wants to monitor – remove those (from the monitoring configuration) that customer can sacrifice.

## ❖ Communicating the AMD overload situation to the customer

This part is equally challenging and demanding. It is about:

- Understanding the product/architecture limited capabilities
- Performing analysis of the AMD workload situation and come up with numbers indicating high resource utilization in conjunction with input packet rates and decode share in total traffic (75% ssl, 25% XML, etc)
- Explaining why the numbers calculated (decode performance vs. input traffic rates) can differ from the estimates provided in product documentation (AMD install guide)
- Discussing the options available to overcome the performance situation.

## ❖ Nice to know

### ➤ 1-minute reporting interval (zdata files being created every 1 minute)

Increasing the frequency of the reporting period from default 5 minutes to 1 minute for example adds additional overhead on AMD and it also multiplies by 5 the number of data processing cycles on the VAS. In fact it may in turn have result quite opposite to the desired. In case the VAS will get behind with too frequent data processing, net result for the customer will be a delay in presenting the data – that is in a total contradiction to near a real time reporting (like every 1 minute). The larger customer environment the more visible this effect can be. Basic question is this: what value would customer have with a delayed data presentation with 1 minute sampling vs. having an up-to-date statistics every 5 minutes?

### ➤ Monitoring traffic behind a load balancer

Often times AMD is placed to analyze traffic behind a load balancer and in front of web servers. User recognition behind a load balancer is **essential** in such situations. Otherwise the load balancer will be presented as just one big/fat client, AMD measurements can be impacted by this – small number of pages with a very long page load time will be reported. Also impact on AMD performance will be significant. There are number of ways to distinguish individual users' traffic behind the load balancer, i.e. break down the aggregated load balancer traffic on the back-end side generated on behalf of users on front-end.

Most common ways to break down traffic behind a load balancer are:

- a) Track users by names : extract sessionIDs behind a load balancer and link it with user name (recognition method) on the front-end side
- b) Identify users by their IPs (username = its IP address) –extract real client IP from the back-end (behind a load balancer) traffic, by extracting it (with a regex) from HTTP header field called: **X-Forwarded-For**  
Example regex: %0d%0aX-Forwarded-For:%20\[0-9.\]\*\)

On top of this, you can configure AMD to replace load-balancer client IP with real (end user) client IP:

The screenshot shows the 'Rule Configuration' window with the 'Edit Rule' tab active. Below the tab, it says 'Software service: SacWis; Analyzer: HTTP'. A horizontal menu contains several tabs: 'Services', 'URL Monitoring', 'User Name Recognition', 'URL Auto-Learning', 'Character Encoding', 'Responses', 'Custom Metrics', 'HTTP Options' (which is highlighted with a red box), and 'Options'. Below this menu, the 'Client IP Address Extraction' section is shown. It contains five radio buttons: 'Off', 'Use Global', 'Header Regex', 'Header Tag', and 'Try to Convert User Name to IP Address' (which is selected and highlighted with a red box). Below the radio buttons is an empty text input field.

## 2. Common SSL (HTTPS) decryption issues

### ❖ Signs of SSL decryption not functioning properly

➤ /var/log/adlex/rtm\_perf.log:

#### RT SSL DECR:

RT     decr:

RT     session decrypted (ok=)858548

RT     **session non-decrypted (f=)215060**

#### AL Alarms

AL **High number of SSL decode failures (75.5%)** - check if all decryption keys are valid and properly assigned

---

➤ /var/log/adlex/rtm.log file flooded with messages like:

- L3 2010-03-15 09:43:10.574 0@ssldecr/sslpktproc.cpp:288 **SSL DECR ERROR processDataPkt packet s=300858471 considered lost - giving up session decoding.** MAX\_PENDING\_PKTS: 10, Happened at packet from 213.149.223.21(2684) to 193.41.205.114(443), server: 0, time 1268646190.574460
  - L3 2010-03-14 14:08:22.420 0@ssldecr/sslrecproc.cpp:1582 **SSL DECR ERROR processCIntKeyX no cipher set 1**, last timestamp seen: 1268575702.420249
  - L3 2010-03-15 09:43:10.791 0@ssldecr/sslrecproc.cpp:745 **SSL DECR ERROR processCipherChange** server: 0 decrCtx.hasError, last timestamp seen: 1268646190.791661
- 

➤ **Large number of “Other SSL errors” on VAS**

TCP errors	
- Connection refused errors:	278
- Connection establishment timeout errors:	3
- Client not responding errors:	645
- Server not responding errors:	158
HTTP errors	
- HTTP client errors (4xx):	1684
HTTP unauthorized errors (401,407):	0
HTTP not found errors (404):	1598
HTTP client errors (category 3):	0
- HTTP server errors (5xx):	75
HTTP server errors (category 1):	0
HTTP server errors (category 2):	0
SSL errors	
- SSL error 1:	33
- SSL error 2:	18
- Other SSL errors:	761249



## ❖ Common problems

### ➤ SSL decryption card not initialized after reboot – AMD unable to decrypt ANY ssl traffic

```
RT      SSL DECR:
RT      config: eng=nitroxlips(native) status=OK keyOK=0 keyFail=18
```

AMD requires the SSL card to be in authenticated mode. That is when AMD process can gain access to RSA private keys stored in the card. It happens many times when AMD is rebooted (the whole box) that end user forgets to log-in to AMD (Linux) console and launch the SSL card configuration utility and authenticate user (unlock access to the keys). Status says “OK” – meaning the SSL card itself is OK and also the proper system driver is loaded but the keyFail<>0 indicates the AMD is not able to retrieve the key information from card.

Refer to AMD install guide for details on how to log-in (authenticate) to different SSL cards.

### ➤ Encryption / key exchange algorithm not supported by AMD

rtm\_perf.log : high number of “key exchange errors” ~= number of non-decrypted sessions

```
RT      SSL DECR:
RT      config: eng=nitroxlips status=OK keyOK=1 keyFail=0
RT      decr:
RT      session decrypted (ok=)651
RT      session non-decrypted (f=)4855
RT      key exchange errors (x=)4849
```

This is typical in situations where in customer’s SSL traffic there is a lot encrypted sessions by unsupported key exchange / encryption algorithms. There is a set of SSL key exchange algorithms that AMD does not support (never will) like Diffie-Hellman one. When you see a high number of key exchange errors, launch **rcon** utility and execute „**SHOW SSLDECR CIPHERS**” command. In result you’ll get a list like that:

```
+ NULL-MD5 id=01 kex=RSA sig=RSA enc=UNKNOWN dig=MD5 ref=0
+ NULL-SHA id=02 kex=RSA sig=RSA enc=UNKNOWN dig=SHA ref=0
* EXP-RC4-MD5 id=03 kex=RSA_EXP sig=RSA enc=RC4 dig=MD5 ref=0
+ RC4-MD5 id=04 kex=RSA sig=RSA enc=RC4 dig=MD5 ref=0
+ RC4-SHA id=05 kex=RSA sig=RSA enc=RC4 dig=SHA ref=0
+ DES-CBC-SHA id=09 kex=RSA sig=RSA enc=DES dig=SHA ref=0
+ DES-CBC3-SHA id=0A kex=RSA sig=RSA enc=DES3 dig=SHA ref=1411
- EXP-DH-DSS-DES-CBC-SHA id=0B kex=DH sig=DSS enc=DES dig=SHA ref=0
- DH-DSS-DES-CBC-SHA id=0C kex=DH sig=DSS enc=DES dig=SHA ref=0
- DH-DSS-DES-CBC3-SHA id=0D kex=DH sig=DSS enc=DES3 dig=SHA ref=0
- EXP-DH-RSA-DES-CBC-SHA id=0E kex=DH sig=RSA enc=DES dig=SHA ref=0
- DH-RSA-DES-CBC-SHA id=0F kex=DH sig=RSA enc=DES dig=SHA ref=343
- DH-RSA-DES-CBC3-SHA id=10 kex=DH sig=RSA enc=DES3 dig=SHA ref=123
```

The list contains methods supported by AMD and more important – a list of algorithms not supported but present in the traffic. Lines prefixed with a PLUS sign indicate a supported algorithm and lines with a MINUS sign indicate a non supported one respectively. A non-zero value of **ref** counter at the very end of each line indicates whether or not SSL sessions using given algorithm are present in the SSL traffic on the wire.

All algorithm names starting with DH (Diffie-Hellman) are NOT supported by AMD (and never will be).

➤ **High SSL packets loss rate – typically a SPAN port issue**

SSL decode is very sensitive regarding the completeness of traffic for the entire SSL session. Especially if some packets are lost during the SSL handshake phase when ssl key exchange occurs and encryption algorithm is selected. Also if some packets are lost later on (during the session) further decryption of the remaining SSL content on that session will not be possible.

If an SSL packet is lost, it results with “packet error” (explained below) message in rtm.log. If a packet is lost during SSL handshake some other errors may also occur. All sessions affected by one of errors described below will be reported as “-1” error type and later reported in “Other SSL errors” bucket on VAS. Note that there may be several error messages per one TCP session, but only one “-1” error will be reported.

Error types reported by AMD [in rtm.log]:

- SSL DECR ERROR processDataPkt packet s= considered lost - giving up session decoding (“packet error” )

This message shows up when a SSL record (no matter SSL handshake or SSL session data) cannot be read from the packet stream. The root cause of this situation is a missing packet in the TCP (SSL) stream. In order to address out-of-order packet arrival AMD waits 10 more packets for arrival of the missing one, and in case the missing packet does not arrive, AMD stops processing of that SSL session and throws this error to the rtm.log.

- SSL DECR ERROR processCIntKeyX no cipher set

This is derived error from previous one and stands for a missing SSL record during SSL handshake. This message shows up when AMD sees “Client key exchange” SSL record which carries an encrypted PreMasterSecret key, but has insufficient data to perform decryption using a private key. It can happen when a public key (included in the server's certificate) has not been seen. Client Key Exchange is the point when the decryption should take place; anyway, for this session we did not see server certificate nor other required server messages. Therefore the key cannot be decrypted that results in the error message. This error is categorized as “-1” = “Other SSL error”.

- SSL DECR ERROR processCipherChange

Another error derived from packet error. This error means: “server change cipher” message arrived, but there's not enough data to obtain a MasterSeretKey. Again, SSL decryption is impossible in such case.

➤ **Incorrect RSA private key (despite customer claiming the key is OK FOR SURE)**

Often times customer provides an outdated RSA private key for SSL decryption for a given server. The key itself comes from the right SSL server however it is no longer in use by this server, i.e. it has changed since the last time it was exported to a PEM file.

Here is a method to prove the key provided is not the same one as used by the SSL server today.

SSL server IP	192.168.171.151
SSL server tcp port	443
RSA private key* name	/var/tmp/priv_key.pem

(\*) The private key must be in PEM encoded format and not password protected.

See manual for details how to extract RSA private key from SSL web servers.

- 1) The private RSA key test requires a public key – this key can be extracted from SSL server's certificate. The certificate can be extracted from SSL traffic that AMD monitors. Here is way to extract server's certificate and save it into a file in a DER format:

```
[root@amd]# rcon
>$ ssldecr certs 192.168.171.151:443 "/var/tmp/"
>$ Wrote 1149 bytes to /var/tmp//cert_192.168.171.151:443_1.der.
Wrote 862 bytes to /var/tmp//cert_192.168.171.151:443_2.der.
2 certificates dumped.
>$ exit
```

- 2) Create a simple text file with current time – this information will be encrypted with the public key:

```
[root@amd tmp]# date > input.txt
```

- 3) Encrypt the input.txt file with a public key from extracted server's certificate:

```
# openssl rsautl -encrypt -inkey "cert_192.168.171.151:443_1.der" -certin
-keyform DER -in input.txt -out output.bin
```

- 4) See if the file is really encrypted (confirm prompt for viewing the file in a binary format):

```
[root@amd tmp]# less output.bin
"output.bin" may be a binary file. See it anyway?
```

- 5) Decrypt the output.bin file with a server's RSA private key provided by customer:

```
# openssl rsautl -decrypt -inkey priv_key.pem -in output.bin -out output.txt
```

Decrypted output.txt file should be **the same** as input.txt file.

```
[root@amd tmp]# cat output.txt
Tue Apr 13 15:40:05 CEST 2010
[root@amd tmp]# cat input.txt
Tue Apr 13 15:40:05 CEST 2010
```

### 3. XML and SOAP decodes

#### ❖ Typical XML structure

XML Request	XML Response
<pre> POST http://www.ab.com/page.html HTTP/1.0 User-Agent: Mozilla/Gecko [en] (WinNT; I) Host: www.adlex.com Accept: image/gif, image/x-xbitmap, image/jpeg, , */* Cookie: user=adlex;  &lt;?xml version="1.0" encoding="UTF-8" ?&gt; &lt;SaleRequest&gt;   &lt;NewTransaction&gt;     &lt;ClientInfo&gt;       &lt;ClientName&gt;Client 1&lt;/ClientName&gt;     &lt;/ClientInfo&gt;     &lt;VendorInfo&gt;       &lt;VendorName&gt;Vendor 1&lt;/VendorName&gt;     &lt;/VendorInfo&gt;     &lt;ProductDesc&gt;H12QW1&lt;/ProductDesc&gt;     &lt;Amount&gt;23&lt;/Amount&gt;     &lt;Price value="dollar"&gt;23&lt;/Price&gt;     &lt;TransID&gt;2005-07-26_0001&lt;/TransID&gt;     &lt;CorrID&gt;QWER12345-111&lt;/CorrID&gt;     &lt;UserName&gt;John Smith&lt;/UserName&gt;   &lt;/NewTransaction&gt;   &lt;NewTransaction&gt;     &lt;ClientInfo&gt;       &lt;ClientName&gt;Client 2&lt;/ClientName&gt;     &lt;/ClientInfo&gt;     &lt;VendorInfo&gt;       &lt;VendorName&gt;Vendor 2&lt;/VendorName&gt;     &lt;/VendorInfo&gt;     &lt;ProductDesc&gt;H12QW2&lt;/ProductDesc&gt;     &lt;Amount&gt;81&lt;/Amount&gt;     &lt;TransID&gt;2005-07-26_0002&lt;/TransID&gt;     &lt;CorrID&gt;QWER12345-112&lt;/CorrID&gt;     &lt;UserName&gt;John Smith&lt;/UserName&gt;   &lt;/NewTransaction&gt; &lt;/SaleRequest&gt; &lt;/xml&gt; </pre>	<pre> HTTP/1.1 200 Ok Date: Wed, 01 Dec 1999 16:00:37 GMT Server: Apache/1.2.6 Last-Modified: Wed, 01 Dec 1999 16:00:37 ETag: \"350ca-6398-363ace72\" Content-Type: text/html  &lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;SaleResponse&gt;   &lt;NewTransaction&gt;     &lt;ClientInfo&gt;       &lt;ClientName&gt;Client 1&lt;/ClientName&gt;     &lt;/ClientInfo&gt;     &lt;VendorInfo&gt;       &lt;VendorName&gt;Vendor 1&lt;/VendorName&gt;     &lt;/VendorInfo&gt;     &lt;UserName&gt;John Smith&lt;/UserName&gt;     &lt;TransID&gt;2005-07-26_0001&lt;/TransID&gt;     &lt;CorrID&gt;QWER12345-111&lt;/CorrID&gt;     &lt;TransStatus&gt;OK&lt;/TransStatus&gt;     &lt;TransRespCode&gt;0xx23200&lt;/TransRespCode&gt;   &lt;/NewTransaction&gt;   &lt;NewTransaction&gt;     &lt;ClientInfo&gt;       &lt;ClientName&gt;Client 2&lt;/ClientName&gt;     &lt;/ClientInfo&gt;     &lt;VendorInfo&gt;       &lt;VendorName&gt;Vendor 2&lt;/VendorName&gt;     &lt;/VendorInfo&gt;     &lt;UserName&gt;John Smith&lt;/UserName&gt;     &lt;TransID&gt;2005-07-26_0002&lt;/TransID&gt;     &lt;CorrID&gt;QWER12345-112&lt;/CorrID&gt;     &lt;TransStatus&gt;Error XXX&lt;/TransStatus&gt;     &lt;TransRespCode&gt;0xx23244&lt;/TransRespCode&gt;   &lt;/NewTransaction&gt; &lt;/SaleResponse&gt; &lt;/xml&gt; </pre>

## 4. RedHat OS related topics

- ❖ Primary OS for Agentless AMD is Red Hat Enterprise Linux 5
- ❖ Only a 32-bit version of RedHat Enterprise Linux 5 is currently supported.
- ❖ Support for a 64-bit version of RedHat 5 is coming in Vantage 11.5 release (Summer 2010)
- ❖ AMD supports RedHat 5.x – only the core version number (5) matters. The minor version number (.x) refers to RH5 revision/update and in general it is only a refresh of the RH 5 with all up-to-date updates to system components. Any customer can reach the same RH 5 “latest/greatest” version level provided the RH automatic update service (yum) is running and (2) the AMD is hooked up to network with Internet access connectivity (to obtain the updates).
- ❖ Customers must obtain the Red Hat Enterprise Linux 5 operating system from Red Hat.
- ❖ Customers obtaining Red Hat Enterprise Linux 5 need to purchase a license (key). RedHat sells different OS type of license depending on the **number of physical CPU sockets** installed in the AMD server’s motherboard:
  - a) not all sockets needs to be active, but RedHat will still count the number of CPU sockets available onboard
  - b) for machines with **up to two CPU sockets** purchase Red Hat Enterprise Linux 5 **Desktop** Platform (32-bit) with “**Workstation with Basic Subscription**” license type.
  - c) for machines with more than two CPU sockets use Red Hat Enterprise Linux 5 **Advanced Server** Platform (32-bit) with “**Standard Subscription**” license type.

## 5. Regular expressions

### ❖ Multiple reasons stand for common use of regular expressions AMD

- Consolidate URLs based upon common parameters or their values but still retain detailed parameter based URL monitoring level
- Extract portions of long strings to be used later for user identification (username from cookie)
- Shorten monitored long URLs by hiding session identification information from URL string to create legible report output
- Define flexible operation boundaries in XML monitoring or extract user names embedded in long multipart strings

### ❖ There are two types of regular expressions in use – POSIX Basic and POSIX Extended

#### ➤ Basic POSIX form is used in:

- SOAP and XML decodes : transactions matching
- MS Exchange decode : user names
- SAP GUI decode
- HTTP decode : user recognition, HTML frames

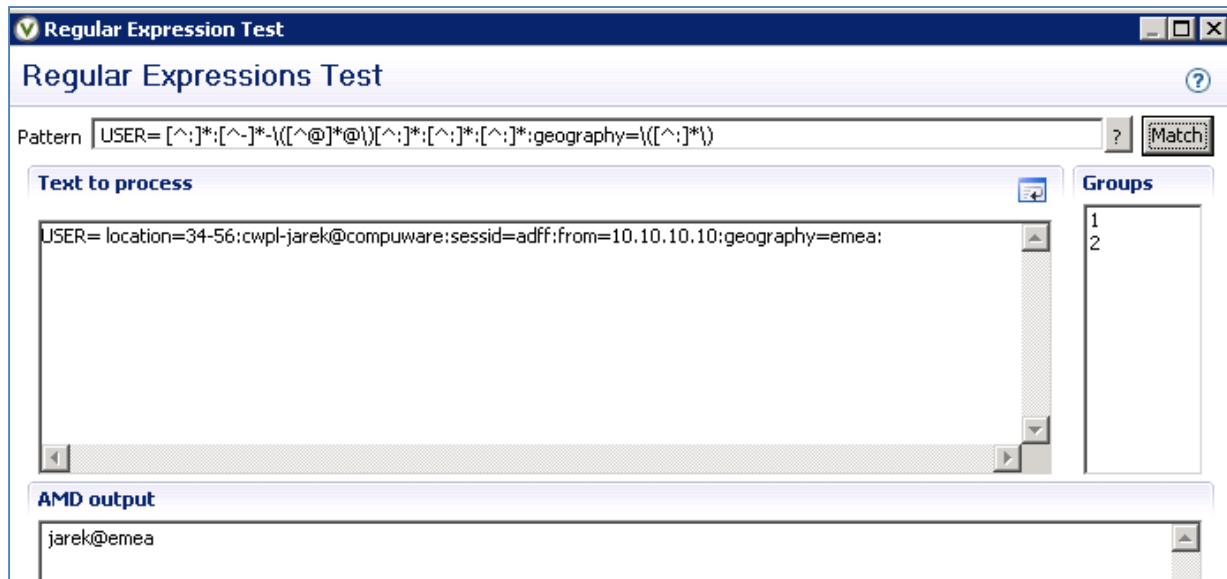
#### ➤ Extended POSIX form is used in:

- HTTP decode: URL monitoring, URL parameters for monitored URLs
- XML decode : extracting URL part that will be added to transaction name
- Syslog : VPN mappings
- Oracle Forms decode : transaction title
- SMTP decode : user name extraction
- XML over HTTP decode :
  - transactions (formerly business transactions)
  - custom metric (pulls out only numerical values)
  - asynchronous transactions matching (correlation tag)

Both forms can do the same job however they are not interchangeable in AMD.

For example a regex pattern in basic form : `^[^@]*-\\([^@]*\\)` and its equivalent in extended POSIX form : `^[^@]*-([@]*)` will give the same result: a word “jarek” when applied to “cwpl-jarek@compuware” string.

Use „Regular Expression Test” in VCA EUE Console to test your regex in a given context.



The example was taken from HTTP user recognition tab HTTP header therefore **basic** regex notation.

#### ❖ Best practices & nice to know

- Regular expressions are very computing intense operations therefore poorly designed pattern often degrades AMD's performance
- Avoid using all matching dot-asterisk (.\* ) in front or in the middle of pattern instead use caret-in-brackets to escape unwanted characters
- Remove the session-id part from reporting, for example:  
<http://gdansk.pl/sessionid-0a568/getArticle/todaynews.jsp>  
lame pattern: `(http://gdansk.pl/).*(getArticle.*)`  
good practice pattern: `(http://gdansk.pl/)[^/]*(getArticle.*)`
- Use Unicode notation not only for URLs but the whole HTTP header (for example : do not use a space character but instead %20 )
- Do not assume input stream ends with end-of-line character - take care of it yourself by closing patterns with **%0d%0a** sequence
- Well written pattern in the example below intended to extract the value of REMOTE\_ADDR filed from HTTP header ensures that the search starts and ends at new line mark. The space between colon and the actual value is Unicode encoded which ensures that it will remain intact through all layers of back and forth conversions from EUE console to rtm process

snippet from HTTP header as input string	ID=34ffff;%0d%0aREMOTE_ADDR: 10.10.10.10%0d%0acontent-type
regular expression	%0d%0aREMOTE_ADDR:%20\([^%0d%0a]*\) %0d%0a
result of the regex pattern matching	10.10.10.10

## VRUM report servers (VAS/AWDS) specific issues

### 1. Common issues on VAS

#### ❖ Lack of application performance & availability metrics

Website Status: URLs - 4/1/10 09:35 CEST											
Software services Servers URLs Sites Reporting Groups Sta											
Time range: Thursday, 4/1/10 (Today) << 4/1/10 00:00 - 4/1/10 09:35 >>											
Page: 1 2 3 4 5 6 7 8 9 10 11 out of 27 >> (Number of entries: 525)											
Find:											
	Page Name/URL		Usage			Performance			Availability		
			Pages	Unique users	Slow pages	Application performance ▲	Affected users	Page load time	Pages stopped	Errors	Application responses
	https://.../elenco_polizze.aspx		1	1	0	-	0	4.58 s	0	0	0
	https://...onali/preferiti.aspx		1	1	0	-	0	2.61 s	0	0	0
	https://.../dati_personali.aspx		5	4	0	-	0	2.14 s	0	0	0
	https://...erazioni_veloci.aspx		4	3	2	-	0	11.7 s	0	0	0
	https://...ici_e_giroconti.aspx		2	1	0	-	0	1.52 s	0	0	0
	https://...giroconti_step2.aspx		3	1	0	-	0	2.6 s	0	0	0
	https://...titoli_conferma.aspx		1	1	0	-	0	964 ms	0	0	0
	https://..._conto_corrente.aspx		3	3	0	-	0	2.53 s	0	0	0

Check if the report is not run for non-business hours by any chance as Application performance and Availability metrics are only calculated for business hours. Check business hours settings on VAS (main menu): Settings->Report Settings->Business Hours

### Business Hours Configuration

Business Days

☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Business Hours

to

Holidays

☒ Exclude Holidays from Business Days [View Holidays](#)

OK

Refresh

Click on “View Holidays” to see a list of hard-coded non-business days recognized by VAS and you can also change the default calendar from USA calendar to match the geographical location of your customer.

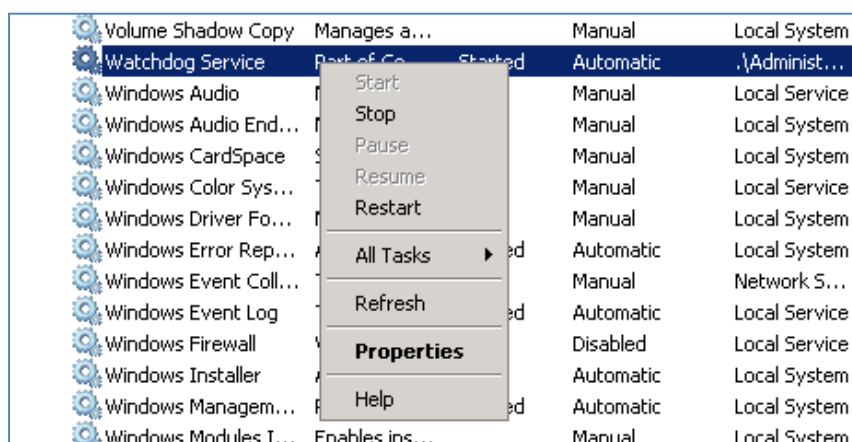




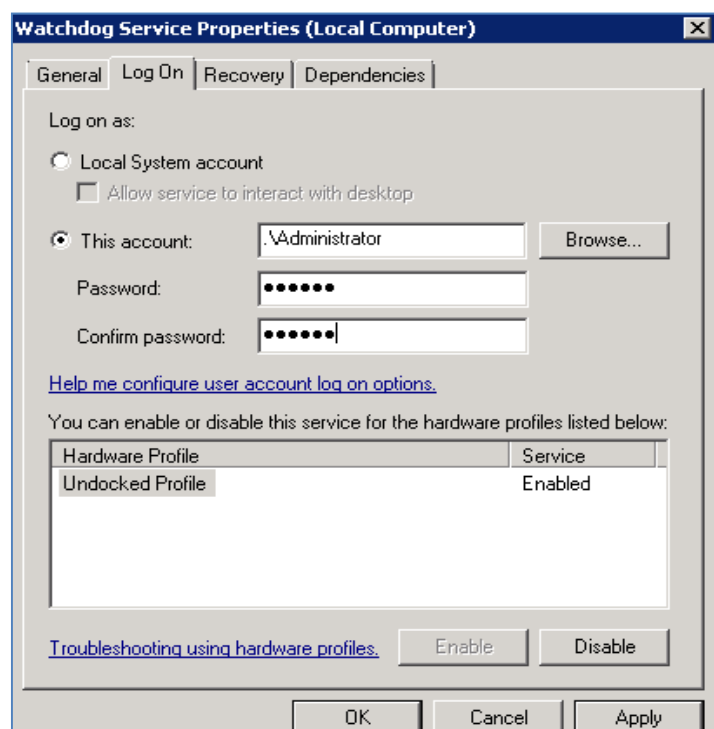
## ❖ Known Watchdog service issue on Windows 2008 Server

Problem	Occasionally Watchdog service (watchdog_nt.exe) crashes in Windows 2008 after running for days.
Reason	Watchdog service is not run under administrative privileges (under Administrator account)
Solution	Set-up Watchdog Service to be run “as administrator”

1) Go to system services, right click on “Watchdog Service”, choose Properties:



2) Switch to “Log On” tab and change from “Local System account” to run as Administrator:



Expected result:

Volume Shadow Copy	Manages a...	Manual	Local System
<b>Watchdog Service</b>	Part of Co...	Automatic	<b>.\Administrator</b>
Windows Audio	Manages a...	Manual	Local Service

## 2. Common issues on AWDS

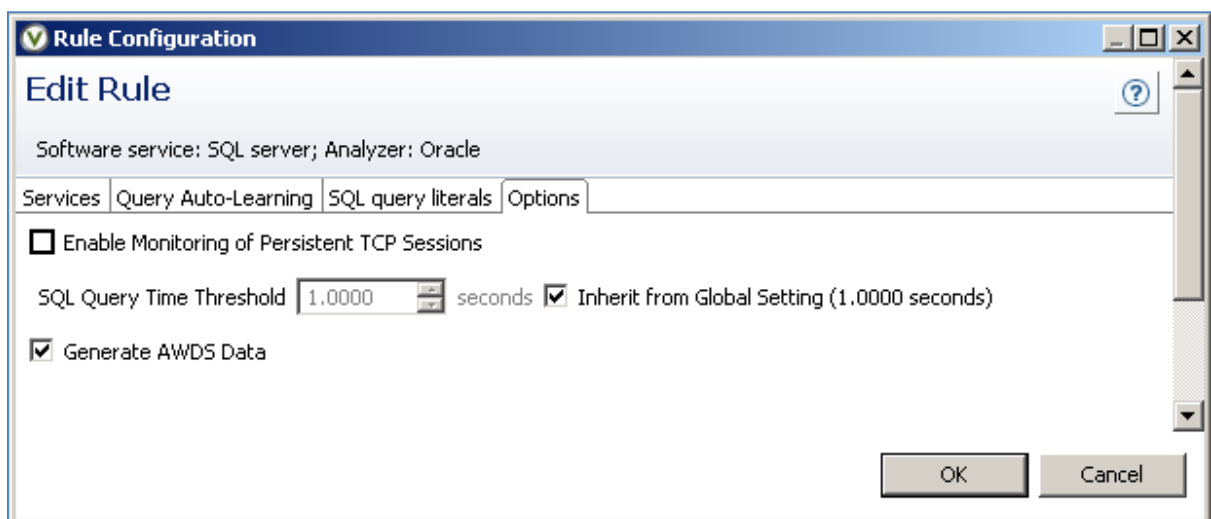
### ❖ Sudden increase of AWDS database after upgrade to CVA 11.1 from CVA 10.x release

Likely a root cause is DB increase due to database decodes (TDS, Oracle) data that are now reported on AWDS. Even though none configured the DB-based software services to report AWDS data after upgrade, this feature can be propagated from a former (10.3) Monitoring configuration settings (user-defined applications) where reporting of “page & hit data” (that is AWDS data) was enabled by default for ALL user-defined software services.



The screenshot shows a window titled "Data Generation" with a tabbed interface. The "Options" tab is selected. It contains four checkboxes: "Enable VAS data" (unchecked), "Enable page and hit data" (checked), "Enable header data" (unchecked), and "Enable all URLs in VAS data (affects all entries for this application and server)" (unchecked).

VRUM 10.x ignored this setting for non-http software services, but it makes a difference in VRUM 11.1, since non-http data can now be presented in AWDS. In order to disable reporting of SQL queries data in AWDS database, edit rule for DB-based software services and disable “Generate AWDS data” in the Options tab:



The screenshot shows a "Rule Configuration" window titled "Edit Rule". The "Software service" is "SQL server" and the "Analyzer" is "Oracle". The "Options" tab is selected. It contains the following settings: "Enable Monitoring of Persistent TCP Sessions" (unchecked), "SQL Query Time Threshold" set to "1.0000" seconds with "Inherit from Global Setting (1.0000 seconds)" checked, and "Generate AWDS Data" checked. "OK" and "Cancel" buttons are at the bottom right.

### ❖ Things to remember about AWDS 11.1

- **Long-term data reporting was moved to VAS**
  - daily and monthly aggregates were removed
  - only data for last 8 days (today and – 7 days) are available in AWDS database now
  - resolutions available: 1 period, 1 hour, 6 hours, 1day
- **Predefined DMI reports were converted**
  - predefined DMI reports are not installed automatically (apart from “Advanced Web Diagnostics” section)
  - DMI reports can be imported manually from “\config\dmireports-examples” directory this way:  
Report-> Import/Export-> Import reports from specified XML file

### 3. Troubleshooting common VAS/AWDS database issues

#### ❖ When TempDB shrink task fails

- User is getting a red status on “Shrinks tempdb and db transaction log” task in a system status report

		System	Java Version	java.runtime.name=Java(TM) SE Runtime Environment; java.vm.version=10.0-b19; java.vm.vendor=Sun Microsystems Inc.; java.vm.specification.name=Java Virtual Machine Specification; java.runtime.version=1.6.0_05-b13; java.vm.specification.version=1.0; java.vm.info=mixed mode;
		System	Server IP	btsdecvrs01/172.19.5.75
	Yes	Task scheduler	Daily report generation	Daily report generation execution failed at 6/10/09 04:23
	Yes	Task scheduler	Shrinks tmpdb and db transaction log. Works only on MS SQL Server	Shrinks tmpdb and db transaction log. Works only on MS SQL Server execution failed at 6/10/09 03:00
	Yes	Task scheduler	RTMDailyDataStore	Executed successfully at 6/10/09 00:09
	Yes	Task scheduler	DBDailyMaintenance	Executed successfully at 6/10/09 00:23
	Yes	Task scheduler	SynchConfigTask	Executed successfully at 6/10/09 11:20

Problem is due to an obsolete SQL “sa” user password stored in a VAS/AWDS database. SA user privileges are required for the shrink task to be performed. Follow these steps to resolve it:

- 1) Make sure you can log in to SQL Server (using SQL Management Studio) as DB administrator, i.e. "sa" user
- 2) In VAS/AWDS main menu (in GUI), choose Tools->Diagnostics->Console and execute the following command:

**SET DB SUPERUSER sa <current\_sa\_password>**

- 3) Stay in the diagnostics console and execute "TASKS EXECUTE" command
- 4) On the following screen, select to execute "Shrinks tempdb and db transaction log. Works only on MS SQL Server" task and press "Run tasks" button.
- 5) On the following screen, press "Start manual tasks" to finally trigger execution of the tempDB and AWDS database log shrink process.
- 6) Stay in the same report and periodically re-run "TASKS SCHEDULE STATUS" command until the manual tempDB shrink task completes its execution, hopefully with a successful end.

- **Is it possible to turn off or disable the tempDB shrink job on the VAS /AWDS?**

Yes, it is possible, however the procedure will have to be repeated each time a new version of VAS/AWDS is installed.

#### Solution:

- 1) Edit \config\tasks-100-hcbs.xml file and remove (or comment out) MsSqlShrinkDB task section:

```
<task ID="MsSqlShrinkDB" name="Shrinks tempdb and db transaction log. Works only on MS SQL Server"
periodType="DAY" period="1" timeLine="SERVER" offsetTime="03:00" timeout="03:00">
<command ID="0" name="Shrinks tmpdb and its transaction log" timeout="02:00">
  <class>adlex.delta.server.repository.scheduledTasks.MsTempdbShrinker</class>
</command>
<command ID="1" name="Shrinks database transaction log file" timeout="03:00">
  <class>adlex.delta.server.repository.scheduledTasks.MsLogShrinker</class>
</command>
</task>
```

- 2) Save the file and restart VAS/AWDS server.

## ❖ How to recover forgotten “delta” DB user password

Current “delta” DB user password is kept in encrypted form in VAS\AWDS config file : \config\repository.properties

```
JDBC_USER=delta
JDBC_PASSWORD_ENC=796A157C3F22E7E16D6A9F3EABB23DAA
```

In order to decrypt the password go to Tools->Diagnostics->Console and execute command:

```
PSWD DECRYPT 796A157C3F22E7E16D6A9F3EABB23DAA
```

## ❖ How to recover forgotten “superuser” password

Report user accounts and their (encrypted) passwords are kept in “wslastused” table in VAS/AWDS database.

### ➤ One way to recover forgotten “superuser” password:

1) Go to Tools->SQL Query Tool and obtain current “superuser” password by this SQL query:

```
select password from wslastused where row_id=1
```

2) Now you need to decrypt the password:

Go to Tools->Diagnostics->Console and execute command:

```
PSWD DECRYPT <PASSWORD>
```

### ➤ Another way is to RESET superuser’s password back to default (blank/no password):

1) Go to Tools->SQL Query Tool and obtain current “superuser” password by this SQL query:

```
update wslastused set password='E1B5A91BA9D93FC88331EA29E1F9D2CD' where row_id=1
```

2) Restart VAS/AWDS server.

## ❖ BulkInsert issues

BulkInsert is a method used to improve database operations on VAS/AWDS when processing data from AMDs. The difference is HUGE between the bulkInsert mode and regular (PreparedInserter) mode.

If you run VAS/AWDS server together with MS SQL Server on the same machine you don’t need to do anything to enable the mechanism. However, in case, SQL Server is located on a separate machine, then both servers require special configuration to enable BulkInsert mode.

### ➤ Here is an evidence in server.log file (right after VAS/AWDS start) indicating problems with BulkInsert.

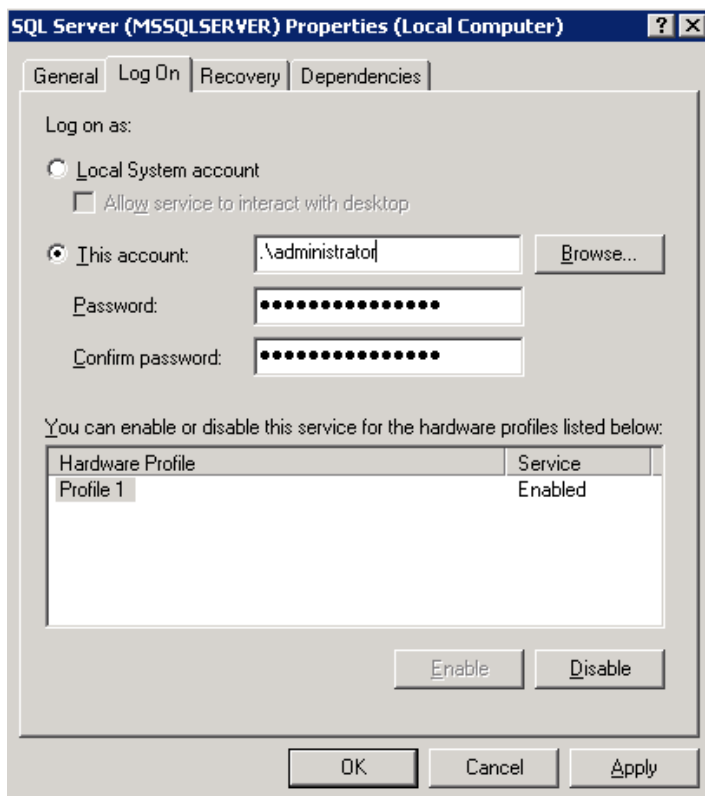
```
E  HLOG  10-04-08 07:27:39.722  BulkInsertTest Cannot open temporary file for bulk load into BulkInsertTest
E  ADM   10-04-08 07:27:39.738  java.io.FileNotFoundException: e:\BulkInsertTest_0.txt (The device is not ready)
T  HLOG  10-04-08 07:27:39.738  BulkInsert made 0 records instead of 80. All inserts will be made by PreparedInserter
T  HLOG  10-04-08 07:27:39.738  On remote SQL you must: .....
```

➤ **Procedure to enable BulkInsert on VAS/AWDS and remote SQL Server**

1) Both VAS/AWDS and SQL Server services on both machines need to be run under the same user account in the system (Windows) with administrative privileges. The goal is for SQL Server service to have access to a shared folder on VAS/AWDS without any prompt for a user name & password.

The administrator (or other administrative user account) password must be **the same** on both machines.

2) Reconfigure both VAS/AWDS and SQL Server (MSSQLSERVER) system services to run under the same administrative account. **Restart SQL Server** service after this change.



3) Do the same (step #2) on VAS/AWDS (change the “Log On” settings for “Vantage Analysis Server” or “Advanced Web Diagnostics Server” services respectively, but do not restart VAS/AWDS service at this time yet).

4) Share “C:\Program Files\Compuware\[VAS|AWDS]\temp” folder as “bulkinsert\$” in read-only access for everyone. The \$ at the end will make the share hidden. SQL server will need access to this folder.

5) Configure **bulk.read** property in VAS/AWDS:

/ATSConbbase on VAS => “Advanced Properties Editor”, locate **RtmJob.bulk.read** property and set this value:  
**\\<IP\_OR\_DNS\_NAME\_OF\_AWDS\_SERVER>\bulkinsert\$\**

On AWDS : scroll down to the very bottom of the /ATSConbase page and add this new property:  
**RtmJob.bulk.read** with a value **\\<IP\_OR\_DNS\_NAME\_OF\_AWDS\_SERVER>\bulkinsert\$\**

6) Now restart VAS/AWDS and check if BulkInsert works – there should be no complains about it in server.log.

## ❖ Database FAQ

- Storage period, reporting periods, trends

/ATSConbase -> Advanced Properties Editor:

**PCS\_STORAGE\_PERIOD** = 10 (default) – defines number of days Intraday data will be kept in VAS database – that is for today and last PCS\_STORAGE\_PERIOD-1 days before today.

Extending storage period beyond 10 days obviously requires more database space. Intraday data occupy the most space within the DB. In order to estimate size of Intra data for day in current DB, access:

ATSConbase -> Database Status report and locate “Samples” row (the top one entry in the list – an aggregated one)

Calculate DB growth factor:

$DB\_DAILY\_FACTOR = \text{Size of "Samples" [GBs]} / \text{current value of PCS\_STORAGE\_PERIOD}$

Estimated database size grow will be:  $(NEW\_STORAGE\_PERIOD - CURRENT\_STORAGE\_PERIOD) * DB\_DAILY\_FACTOR$

**PCS\_REPORTING\_PERIOD** = 10 (default) - defines number of days used for normal (baseline) and average data calculations – this is subject data use during overnight’s ‘Daily report generation’ task. It is not recommended to extend the default period when PCS\_STORAGE\_PERIOD is extended. Typically last 10 days is good enough to provide comprehensive data for averages and baselines.

Extending REPORTING PERIOD will have an impact on duration of ‘Daily report generation’ task and at worst case scenario (very probable) the task will not be executed timely and so not all averages will be available. Also the longer reporting period is the less representative value baselines will contain - towards a simple fixed threshold value. In result baselines would not follow a trend in changing traffic circumstances.

**DAILY\_TRENDS\_LEN** = 31 (default) – defines number of days with **daily** trends stored in database (the last N days trending charts).

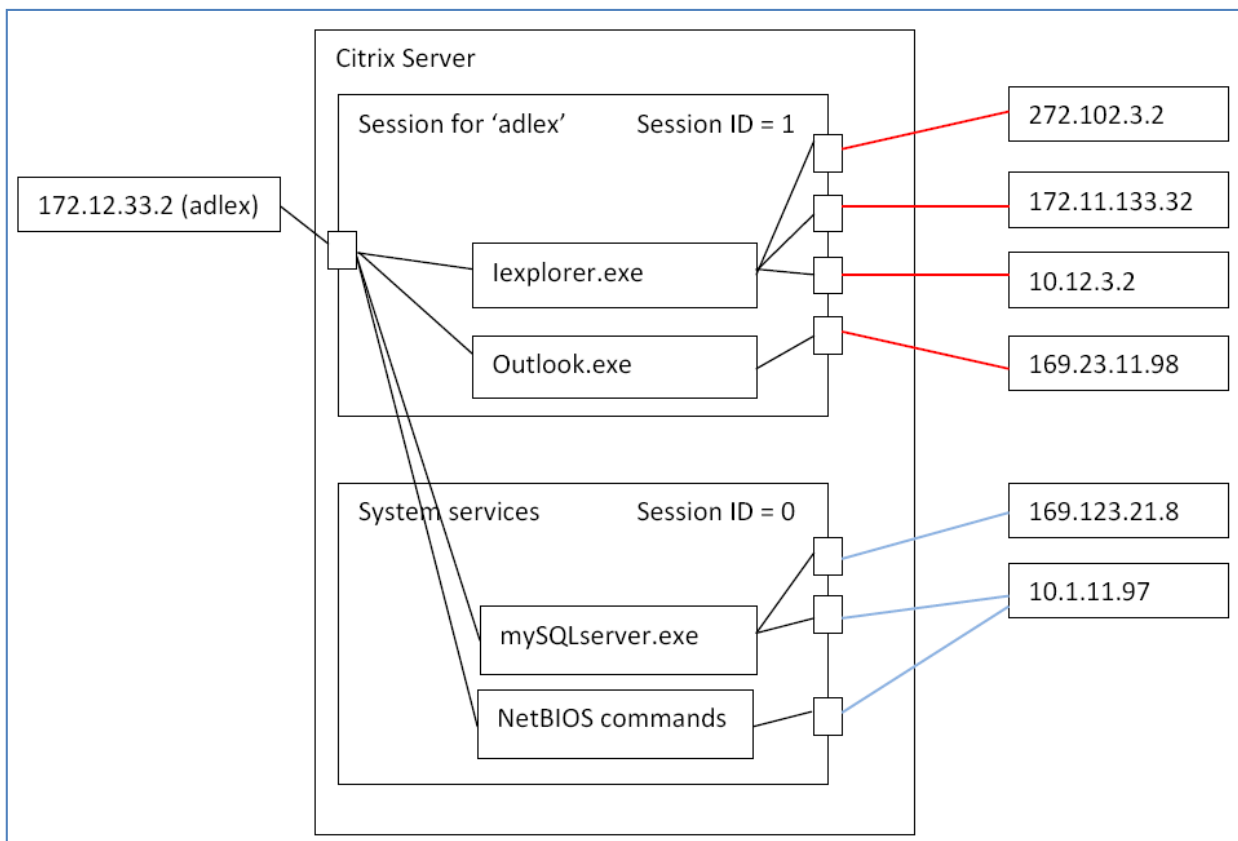
If you extend PCS\_STORAGE\_PERIOD over 30 days make sure to adjust this property accordingly to the rule:

$DAILY\_TRENDS\_LEN \geq PCS\_STORAGE\_PERIOD$

## 4. VTCAM (Citrix) common issues

### ❖ VTCAM constrains

Main purpose of VTCAM application is to associate system network connections with remote (Citrix) user sessions and send that information to another machine for later processing. The machine that gets this information is able to identify which user, from which IP was connecting with which computers during remote session. Each time a user connects with the Citrix machine Windows creates a new session for that user. Each user session is assigned unique ID, called 'Session ID'. All applications run by remote user also have assigned the same 'Session ID'. Using 'Session ID' VTCAM is able to identify which application was run by which user and match that information with network connections. Unfortunately not all network connections can be connected with particular user. When user is using application that runs as a system service it has not the user 'Session ID' it has the System 'Session ID' and VTCAM is not able to assign it to any user. On the picture below only connections marked red color will be reported for user 'adlex'. For other connections VTCAM is not able to recognize user.



### ➤ Here is a receipt on how to verify if a Windows application can be supported by VTCAM

1. Download sysinternals process explorer utility: <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>
2. Launch it on the Citrix/Windows Terminal Server console
3. Right click on any column to add "User Name" column
4. Search for the process that represents the application in question
5. You can verify the process by examining its tcp connections in Right Click -> Properties -> TCP/IP:
  - If the process is in lower tree with proper username in "User Name" column - it is supported
  - If the process is on upper tree with system user name - it is NOT supported



## ❖ Troubleshooting common issue with missing information from VTCAM agent

### ➤ Tracing VTCAM events received by AMD

VTCAM agent provides three types of information from Citrix server to the VRUM AMD:

- logon events on Citrix server (remote Citrix users log on to Citrix server)
- back-end sessions mapping – information about the sessions Citrix users originate from Citrix servers towards the back-end software services (back-end servers/applications)
- basic performance statistics of the Citrix server alone (CPU, memory, disk utilization)

The information is provided to AMD by means of UDP protocol on port 514. This activity can be sniffed by a packet trace utility (tcpdump) on AMD side – packet trace must be set-up on the AMD communication interface (not on the sniffing interfaces), but there is a more convenient way – enable VTCAM debug mode on AMD:

`/usr/adlex/config/rtm.config: map.trace=true`

Then restart **RtmGate** service on the AMD. The debug log is then stored in `/var/log/adlex/rtmgate.log` file.

Here is the syntax of the VTCAM events provided to the AMD with description and examples.

ID	Type	Description, syntax & example
1	Logon event	<p>End user logs in to a Citrix server. Maps real user IP with user name.</p> <p>&lt;1 USER_IP USER_NAME&gt;</p> <p>T MAP 09-07-13 01:41:16.489 CitrixParser: parsing line=&lt;1 192.168.204.154 DOMAIN\username&gt;</p>
2	Back-end session mapping	<p>Links Citrix back-end (BE) session (on behalf of Citrix user) with user name on Citrix srv. This mapping is needed to add user name to a session the AMD sees between Citrix server (Citrix IP being client IP) and back-end application server (server IP)</p> <p>&lt;2 PROTO CITRIX_IP CITRIX_PORT BE_SRV_DEST_IP BE_SRV_DEST_PORT CTX_USER_IP CTX_USER_NAME&gt;</p> <p>T MAP 09-07-13 12:18:24.136 CitrixParser: parsing line=&lt;2 1 192.168.200.35 1045 192.168.200.22 389 192.168.204.154 DOMAIN\username&gt;</p> <p>&lt;user name&gt; can be omitted if the session is originated from Citrix server console</p>
3	CTX perf metrics	<p>Basic CTX server performance stats</p> <p>&lt;3 CTX_SRV_IP &lt;MIN&gt; &lt;AVG&gt; &lt;MAX&gt; ..... &gt;</p> <p>&lt;min&gt; &lt;avg&gt; &lt;max&gt; for each performance counter, i.e.</p> <ol style="list-style-type: none"> <li>a. CPU utilization</li> <li>b. Physical disk utilization</li> <li>c. Memory utilization</li> <li>d. Total session</li> <li>e. Active session</li> </ol> <p>T MAP 09-07-12 08:20:01.237 CitrixParser: parsing line=&lt;3 192.168.2.43 0 0 0 0 0 11 11 11 1 1 0 0 0&gt;</p>

➤ If you are missing Citrix performance statistics on VAS reports

Citrix Status: Servers - 17-09-09 13:05 CEST

Software service: NABS Citrix

Time range: torsdag, 17-09-09 (Today) << 17-09-09 00:00 - 17-09-09 13:05 >> Show: All

Server name	Server IP address	Software service	Usage	Network	Affected users	Average CPU utilization	Average disk utilization	Average memory utilization	Average number of open sessions	Average number of active sessions
10.74.134.110	10.74.134.110	NABS Citrix	6	99.4 %	1	-	-	-	-	-

User: csc@vant11-se-vmvas:80 (en) Report generated: 17-09-09 13:09 CEST Version: Vantage Analysis Server 11.0.1.102

- 1) Start VTCAM manger by selecting Programs → Compuware → Vtcam on the Start menu.
- 2) Make sure VTCAM agent is configured to provide those performance statistics to your AMD at first.

VTCAM Manager

VTCAM IP address: 172.18.130.215

Data receivers

Performance data receiver

IP address: 172 . 18 . 133 . 18 : 514 port

- 3) Often times Citrix servers have multiple NICs configured with multiple IP addresses assigned.

One of those IPs needs to be selected in VTCAM configuration :

VTCAM Manager

VTCAM IP address: (Not Set)

Data receivers

Performance data receiver

IP address: 172 . 18 . 133 . 18 : 514 port

This IP address MUST correspond with the IP of this Citrix server in VCA Configuration Console:

Rule Configuration

Edit Rule

Software service: Citrix RDP; Analyzer: ICA (Citrix)

Services Options

☒ Enabled

Rule Description

Services

IP Address	Ports	Main Server IP ...	NL
172.18.130.215	1494		

OK Cancel

- 4) Check if VTCAM provides Citrix server performance stats to your AMD – enable VTCAM debug mode & examine rtmgate.log for MAP events type #3
- 5) Check if (a) AMD produces /var/spool/adlex/rtm/ctxdata\* files and (b) VAS processes these data (server.log).

## ❖ Things to remember about VTCAM in 11.1

### ➤ VTCAM on Windows 2008 Server R2

VTCAM support for Windows 2008 is available starting with SP1 for VRUM 11.1 (SP1 is available on Frontline). Both 32-bit and 64-bit of Windows 2008 Server R2 are supported.

### ➤ Reboot Citrix server immediately after VTCAM installation on it

Remember to reboot the Citrix server **right after** VTCAM installation - otherwise network connectivity with the Citrix server will be significantly impacted / limited or even no longer possible until the server is rebooted.

## 5. Windows Server related topics

### ❖ Memory limits for Windows releases

<http://msdn.microsoft.com/en-us/library/aa366778%28VS.85%29.aspx>

## TBD topics

### ❖ VRUM report servers (VAS/AWDS) specific issues

- Common Data Mining problems
- Vantage EUE Configuration Console issues
- Server Farm configuration issues
- Expected differences per analyzer between previous and current release
- VRUM integration with LDAP

### ❖ AMD

- Oracle Forms decode
- Microsoft Exchange decode
- Oracle database decode
- Packet tracing

### ❖ General topics

- CVA supported hardware
- Current – 2 releases support policy
- Licensing issues