



IBM India Software Labs

Tivoli Security Information and Event Manager

Debugging, Troubleshooting and Best practices in TSIEM

Aslam Siddiqui

Boudhayan Chakrabarty



Collection of logs

- **TSIEM has got multiple sub-components like eWAS, TIP, ITDS, DB2 etc and hence multiple types of log files are created on the server side and each of them are present in different directories**
- **On the agent side, i.e., the target event source where you have installed an agent, all the logs are present in a single directory unlike the server side**
- **TSIEM is shipped with a script named as diagnostics which helps in collecting logs from ALL the different components of TSIEM which are present on the server side**
- **We would be covering this script in detail in our upcoming slides**



Installation Logs

- **When Tivoli Security Information and Event Manager components are installed, the installation process creates log files.**
- **The installation program creates log files in three locations:**
 1. **The installation graphical user interface (GUI) logs are called TSIEM_install-*.log. These logs can be found in the home folder of the user who installs Tivoli Security Information and Event Manager:**
 - **On Windows, it is located in the C:\Documents and Settings\Administrator directory.**
 - **On AIX and Linux, it is located in the root (/) directory .**

Installation logs contd...

2. The main log file of the installation engine is located in %TSIEM_HOME%_uninst\TSIEMInstall\plan\install\MachinePlan_localhost\logs. The name of the main log file starts with MachinePlan_localhost_ and is followed by a timestamp (for example, C:\IBM\TSIEM_uninst\TSIEMInstall\plan\install\MachinePlan_localhost\logs MachinePlan_localhos_[INSTALL_0112_15.32].log).
 3. When the installation program calls a subprogram, the resulting logs are written to %TSIEM_HOME%\log (for example, C:\IBM\TSIEM2010\log).
 4. Agent installation log files are written to %TSIEM_HOME%\InstallCeA.log (for example, C:\IBM\TSIEM\InstallCeA.log).
- These installation logs can be helpful in resolving any problems that are encountered during installation.



Message Logs

- **Message logs are text files in which the operations of the system are recorded.**
- **The following types of messages are recorded by default:**
 - **Informational messages - Indicate conditions that are worthy of noting but that do not require you to take any precautions or perform an action.**
 - **Warning messages- Indicate that a condition has been detected that you should be aware of but does not necessarily require that you take any action.**
 - **Error messages- Indicate that a condition has occurred that requires you to take action.**



Message Logs

- **Message logs are text files in which the operations of the system are recorded.**
- **The following types of messages are recorded by default:**
 - **Informational messages - Indicate conditions that are worthy of noting but that do not require you to take any precautions or perform an action.**
 - **Warning messages- Indicate that a condition has been detected that you should be aware of but does not necessarily require that you take any action.**
 - **Error messages- Indicate that a condition has occurred that requires you to take action.**



Trace Logs

- **Trace logging provides you with additional information relating to the condition of the system at the time a problem occurred.**
- **In contrast to message logs, in which records are made of noteworthy events that have occurred, trace logs capture transient information about the current operating environment when a component or application fails to operate as intended.**
- **Trace logging is not enabled by default because in some circumstances it can cause large amounts of data to be collected in a short amount of time and might result in significant performance degradation.**
- **It is not recommended to enable trace logging without the recommendation of a support professional since enabling this might generate a very high amount of logs which can very quickly fill up your disk space and can also affect your system performance**

Types of Trace logs

- **The following logging and tracing levels are provided in Tivoli Security Information and Event Manager:**
- **Off - No events are logged.**
- **Severe - Task cannot continue, but component can still function.**
- **Warning - Potential error or impending error.**
- **Info - General information outlining overall task progress.**
- **Config - Configuration change or status.**
- **Fine Trace information: General trace.**



Types of Trace logs Contd...

- **Finer Trace information** - Detailed trace as well as method entry, exit, and return values.
- **Finest Trace information** - A more detailed trace that includes all the detail needed to debug problems
- **All** - All events are logged. If you create custom levels, All includes your custom levels and can provide a more detailed trace than Finest.
- **When a certain log level is set, higher levels are logged as well; for example, Info also includes Severe and Warning.**
- **The default log level for all Tivoli Security Information and Event Manager application components is Info.**
- **To enable tracing, set the level to Finer.**

Configuring the log settings

- **Message logging is enabled by default. Enable trace logging only at the direction of an IBM Support representative**
- **You can change the settings of the Message/IBM Service logging by executing the steps given below:**
 - 1. Start the Tivoli Integrated Portal and log in as the Tivoli Integrated Portal administrator (tipadmin by default), if necessary.**
 - 2. Click Troubleshooting > Logs and Trace to open the Logging and Tracing page.**
 - 3. Click the name of the server that you want to configure (for example, server1).**
 - 4. Click JVM Logs to view the configuration options.**
 - 5. Select the Configuration tab.**
 - 6. Scroll through the panel to display the attributes to configure.**



Configuring the log settings Contd...

- 7. Change the appropriate configuration attributes and click Apply.**
- 8. Click IBM Service Logs to view the configuration options.**
- 9. Select or clear the Enable service log check box to enable or disable logging. The service log is enabled by default.**
- 10. Set the name for the service log in the File Name field. The default name is activity.log. If the name is changed, the run time requires write access to the new file, and the file must use the .log extension.**
- 11. Specify the number of megabytes to which the file can grow in the Maximum File Size field. When the file reaches this size, it wraps, replacing the oldest data with the newest data.**
- 12 Save your configuration changes by clicking on Apply**
- 13. Restart Tivoli Integrated Portal service.**

How to Enable Trace logging

- **Trace logging is disabled by default. This should be enabled ONLY at the direction of an IBM Support Representative since it can affect system performance**

You can follow the steps given below for doing this:

- 1. Start the Tivoli Integrated Portal and log in as the Tivoli Integrated Portal administrator (tipadmin by default), if necessary.**
- 2. Click Troubleshooting > Logs and Trace to open the Logging and Tracing page.**
- 3. Click the name of the server that you want to configure (for example, server1).**
- 4. Click Diagnostic Trace.**



How to Enable Trace logging Contd...

5. Click the Runtime tab.
6. Select the Save runtime changes to configuration as well check box if you want to write your changes back to the server configuration.
7. Change the existing trace state by changing the trace specification to the desired state.
8. Configure the trace output if a change from the existing one is desired.
9. Click Apply.

You do not have to restart any service for the above changes to come to effect



Diagnostics script

- In the TSIEM server installation directory you would find a script named as diagnostics. bat (diagnostics.sh on Unix based installations of TSIEM)
- This script is capable of collecting logs from all the different sub components of TSIEM that are present on the server side.
- Double click this diagnostics. bat file as the administrative user on a Windows TSIEM server for collecting the logs
- On an Unix based installation, execute the script diagnostics.sh as the root user
- On executing this script, a zip file named as TSIEM_logs_YYYYMMDDhhmmss.zip would be created in the same directory from where you have executed the script (TSIEM home directory)



Diagnostic script-how does it work?

- **Diagnostics.bat or diagnostics.sh script in turn reads a file named as doagnostics.xml which is present in the same installation directory (TSIEM home directory) and collects the logs from the different sub-components of TSIEM and zips them up together**
- **In some specific circumstances, you might see that even after a successful installation of TSIEM, the home directory of TSIEM does not contain this script**
- **In such a case, copy the two files diagnositics.bat (or diagnostics.sh on a Unix based installation) and the file diagnostics.xml from the TSIEM installation media onto the TSIEM installation directory and you can execute it for collecting the logs**
- **Be advised that this script works only on the TSIEM server and NOT on the TSIEM agent. We would be covering the method to collect logs from the agent machine in our next slides**

Contents of diagnostics zip file

■ On un-zipping the file **TSIEM_logs_YYYYMMDDhhmmss.zip** that was created on executing the diagnostics script, you would find the following directories:

1.coi

2.de

3.ia

4.middleware

5.sim

6.tip



Content of these folders

- **coi** - This folder contains important information about the installation of TSIEM together with any FP that might have been installed. Different folders would be present in this folder referring to the different stages of the installation. Generally we look into this folder **ONLY** when we are sure that the issue is related to a faulty installation.
- **de** - This folder contains the Deployment Engine related logs. Different folders/logs contain information about how exactly the installation was done and what were the options that were selected during the installation.
- **ia** - Another folder containing installation related logs etc. Important log files to look out for would be `tsiem_install.log`, `TSIEM_install_trace_stderr.log`, `TSIEM_install_trace_stdout.log` etc

Content of these folders Contd...

- **middleware** - One of the most important folder is this one. This contains all the logs files from the middleware that we have in TSIEM 2.0. These include DB2 diag log file and the ldap (TDS) idsadm.log and the ldapinst logs. These log files help us in understanding any issues with the back-end DB2 and TDS that we might be facing like authentication error etc.
- **sim** - The most important folder we would say. This contains ALL the TSIEM server based logs starting from actuator logs for each and every event source together with their individual agent id. Any collect failure/mapping failuer, this is the place where we look into. Another important file would be the bbbin.log
- **tip** - any GUI based issue, we look into this folder. An important log file worth mentioning here is the SystemOut.log file. This contains most of the report distribution error information.
- Ofcourse there are quite a lot of other log files and directories that are present in the above six different folders which we look into for advanced troubleshooting.



Agent Logs

- **Agents are the Point of Presence (PoP) consisting of the Actuator and the Collect script that you install on a target machine for gathering audit events**
- **Agent logs are stored in the directory {TSIEM Agent Directory}/sim/actuator/logs.**
- **This directory is also present on the server side of TSIEM since for local collects like the Windows event collect, DB2 etc of the TSIEM server itself, an agent is used internally**
- **These log files help us in resolving issues related to collect failure etc where we are using an agent to do the collect**



General Troubleshooting

- **We would now be covering some of the known requirements that we have seen from people using TSIEM as well as some of the known issues that people face while using this product and ways to resolve them. We would be covering them under the following headings:**
- **Modifying the different users that are created by TSIEM 2.0**
- **Syslog collect issues:**
- **Agent/Agent-less collect troubleshooting**
- **Upgrades:**
- **Continuity report**

Users and Groups created by TSIEM

- **Accounts created at the OS Level:**
- **cifadmin**
- **cifdbadm**
- **idsinst**
- **itdsadm**
- **Groups created at the OS Level:**
- **cifusers**
- **DB2ADMNS**
- **DB2USERS**

Users and Groups created by TSIEM Contd...

- **The following users and groups are created while installing TSIEM 2.0:**
- **itdsadmin->LDAP database admin**
- **cn=root-> ITDS admin**
- **cifdbadm-> Database admin**
- **tipadmin-> TIP admin**
- **cifowner-> Security server user**

Modifying the password for users

- The password of the cifadmin account can be modified by whatever provisioning mechanism your company has in place for managing Windows OS account.
- The passwords stored by TSIEM can be changed either via a GUI by using the 'Log On' tab on the relevant Windows service properties panel, or you can do it through the command line using the 'sc.exe' tool (note the space after the '=' sign - this is not a typo):
 - `sc config CEAgent password= newpasswd`
 - `sc config InSightTomCat password= newpasswd`

Modifying the password for users Contd...

- On all TSIEM Enterprise Servers, any cifadmin account credentials stored for InsightIndexer[StandardSrv] services must be updated.

sc config InSightIndexerSTANDARDsrv password= newpasswd

- where STANDARDsrv is the host name of the Standard Server as defined in “IBM Tivoli Security Information and Event Manager Indexer[StandardSrv]” service.
- The passwords stored by TSIEM in the Windows Scheduled task for TSIEM Daily Restart can be modified using the ‘schtasks.exe’ tool.

schtasks /Change /TN “IBM Tivoli Security Information and Event Manager Scheduled

- **Restart” /RP newpasswd**

The above password change operations must be performed on each TSIEM Server that shares the cifadmin credentials.

Modifying the password for users Contd...

- The password of the cifdb2admin account can be modified by whatever provisioning mechanism your company has in place for managing local Windows OS account. The passwords stored by TSIEM can be changed either via a GUI by using the 'Log On' tab on the relevant Windows service properties panel, or you can do it through the command line using the

'sc.exe' tool (note the space after the '=' sign - this is not a typo):

```
sc config CFINST-0 password= newpasswd
```

```
sc config DB2GOVERNOR_CIFCOPY password= newpasswd
```

```
sc config DB2REMOTECMD_CIFCOPY password= newpasswd
```

- However, there is also an LDAP account named 'cifdb2admin', defined in the ITDS server that is deployed on the TSIEM Security Server. It is strongly recommended to keep the password of these 2 accounts the same.
 - Modify the DB2 SelfAudit Event Source property (the one that audits TSIEM DB2 instance) via the TSIEM Console and save the new credentials of cifdb2admin local OS account. When the cifdb2admin OS account password is changed on one TSIEM server, it is recommended to perform the same password change and the service logon credential changes (indicated above) on the cifdb2admin OS accounts defined on the remaining TSIEM servers in a Security Group.

Modifying the password for users Contd...

- The password of the db2adminitds account can be modified by whatever provisioning mechanism your company has in place for managing local Windows OS account.
- The passwords stored by TSIEM can be changed either via a GUI by using the 'Log On' tab on the relevant Windows service properties panel, or you can do it through the command line using the 'sc.exe' tool (note the space after the '=' sign - this is not a typo):

```
sc config DB2IDS-0 password= newpasswd
```

```
sc config DB2GOVERNOR_IDSCOPY password= newpasswd
```

```
sc config DB2REMOTECMD_IDSCOPY password=  
newpasswd
```

Modifying the password for users Contd...

- The password of the idsinst OS local account can be modified by whatever provisioning mechanism your company has in place for managing local Windows OS account. When the OS account password of idsinst is modified, the corresponding encrypted version of the password must be updated in the ITDS configuration file on the TSIEM Security Server. The change to the configuration file requires the ITDS Server Instance to be stopped prior to running the command. Use the following ITDS commands to stop the ITDS instance and to update the idsinst password:

```
ibmslapd -k
```

```
idscfgdb -w newpasswd
```

- The idscfgdb and ibmslapd commands are located in [ITDS_LDAP_HOME]\sbin folder (where ITDS_LDAP_HOME is by default located in C:\Program Files\IBM\ldap\v6.1).
- To start the ITDS instance, use the Windows service control tool (sc.exe) command `sc.exe start idsslapd-idsinst`

Modifying the password for users Contd...

- **The password of the cn=root LDAP account must be changed using the ITDS command `idsdnpw` on the TSIEM Security server. This command modifies the cn=root password in the LDAP repository and updates the ITDS configuration file with the corresponding encrypted version of the password. The change to the configuration file requires the ITDS Server Instance to be stopped prior to running the command. Use the following ITDS commands to stop the ITDS instance and to update the cn=root password:**
- **`ibmslapd -k`**
- **`idsdnpw -u cn=root -p newpasswd`**
- **The `ibmslapd` and `idsdnpw` commands are located in `[ITDS_LDAP_HOME]\sbin` folder (where `ITDS_LDAP_HOME` is by default located in `C:\Program Files\IBM\ldap\v6.1`). To start the ITDS instance, use the Windows service control tool (`sc.exe`) command**
- **`sc.exe start idsslapd-idsinst`**
- **After changing the cn=root password on the ITDS server, the `blrec.val` of all TSIEM Servers in the TSIEM Security Group (including the TSIEM Security Server itself) must be modified to make the new password known to the TSIEM Servers. Any TSIEM Server of which the `blrec.val` that is not updated will not be able to change passwords of the TSIEM users and will not be able to create new TSIEM users.**



Modifying the password for users Contd...

- The password of the `cn=cifdb2admin` LDAP account can be modified by whatever provisioning mechanism your company has in place for managing LDAP accounts, or with the ITDS tool as described below:
- In batch mode you create a file containing the modification instructions, and pass it to `ldapmodify`: for example, create a file named `modme.txt` with the following contents
- `dn: cn=cifdb2admin,cn=cif,o=ibm`
- `changetype: modify`
- `replace: userPassword`
- `userPassword: newpassword`

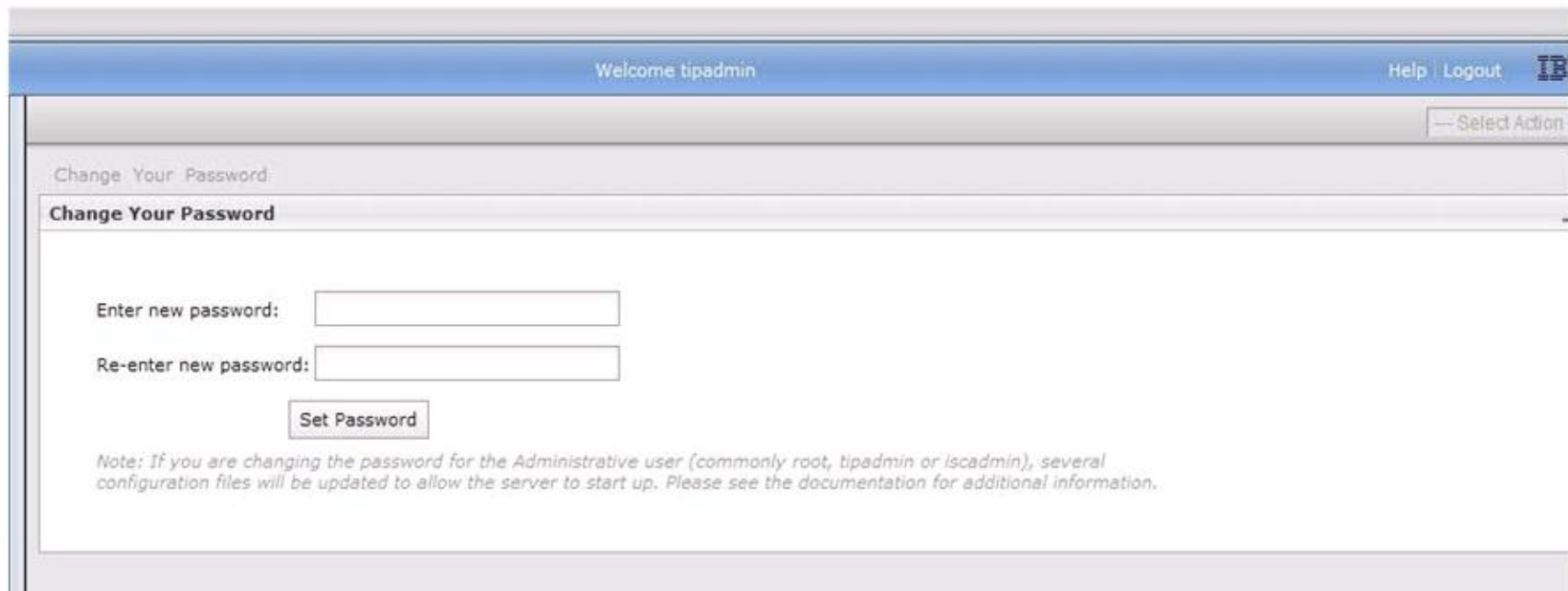
and execute it with

- `ldapmodify -D "cn=root" -w rootpwd -f modme.txt`

Note that there is also a local OS account named 'cifdb2admin'. It is strongly recommended to keep the password of these 2 accounts the same. There is also an interactive mode of doing the above and is part of ITDS administration which is outside the scope of this presentation

Modifying the password for users Contd...

- For changing the password for tipadmin, please log in first as the tipadmin user in the TSIEM console and in there go to "Settings -> Change your password" . In there you would be presented with a screen like the one shown below:



The screenshot shows a web browser window with a blue header bar containing "Welcome tipadmin" on the left and "Help | Logout" on the right. Below the header is a navigation bar with a "Select Action" dropdown menu. The main content area is titled "Change Your Password" and contains two text input fields: "Enter new password:" and "Re-enter new password:". Below the fields is a "Set Password" button. A note at the bottom of the form reads: "Note: If you are changing the password for the Administrative user (commonly root, tipadmin or iscadmin), several configuration files will be updated to allow the server to start up. Please see the documentation for additional information."

Make the changes to the password in this screen and you should be done.



Syslog Collect issues

- Time stamp not properly parsed out of events - This is seen if the locale of the server and the locale of the target machine are not the same. The splitter tool is used by syslog at Server side to get information and construct the event record.
- It means that the event timestamp format is dependent on the Server locale. The function that we were using till now was dependent on the Local setting. We have changed our code post FP 04 to make it independent of the Local setting. This allows us to get the proper timestamp.
- For this, after installing FP 04, execute the following steps:
 - 1.- Set the Syslog event source property field 'Language code for audit trail' with the following value:

en_US
 - 2.- Schedule a new collect to the Syslog event sources.
 - 3.- Execute a manual load of the chunks collected by the previous step to verify that problem has been solved.

Remote collect fails

- **Most common reason for this is the JRE not defined on the target machine. Check the event props file (from the logs collected in the diagnostics zip file) which would be present in the directory sim/server/logs/ and you would get something like the one given below (below example is for the ITDS event source):**

<Date/time stamp> Collect server audit logs

```
../bin/getitdslogs1.sh[53]: java: not found
```

<Date/time stamp> ERROR: Failure collecting server audit logs. Error code 127

```
../bin/getitdslogs2.sh[53]: java: not found
```

<Date/time stamp> ERROR: Failure collecting server error logs. Error code 127

<Date/time stamp> Collect admin audit logs

```
../bin/getitdslogs3.sh[55]: java: not found
```

- This would mean that the SSH collect is not able to find the required JRE directory on the target machine in the path that has been defined. You can define the location of the JRE directory in the Event Source properties under the heading JRE binaries path. This specifies the path to the Java Runtime Environment bin directory, such as C:\j2sdk1.5\bin for Windows systems or /opt/IBMJava2-150/jre/bin for UNIX and Linux systems. The default value is "" (empty). If the path is not specified in the PATH environment variable, then this option must be specified. Otherwise, it can be left blank. For SSH collect this option must be specified. If not specified and the PATH environment variable does not contain the path with the executable files for the JRE, then the collect fails.

Agent/Agent-less Collect Troubleshooting

- **Over View of the Collect process**
- **Logs involved**
- **Stages where collect may fail**
- **Troubleshooting**

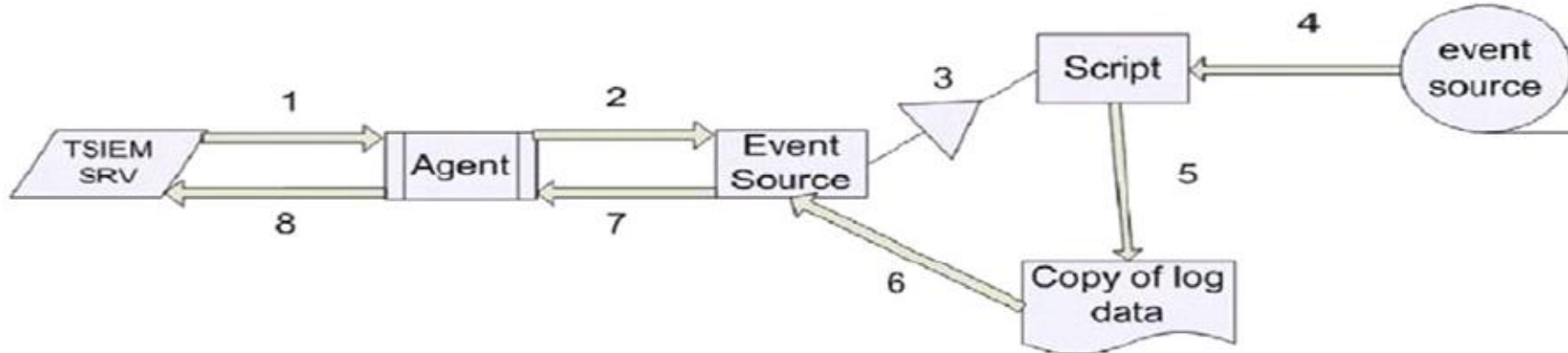
Collect Process Overview.

• Collect Process Overview

Tivoli software

IBM

Lesson 1: TSIEM Generic ExtendIT tool data flow



1. Collect command issued by server
2. Agent invokes an TSIEM Event Source (actuator)
3. Event Source executes the collect script
4. Collect script reads the event source log data
5. a Copy is made of the log data that should be archived
6. TSIEM event source reads and compresses the copy and creates the chunk
7. Agent encrypts the chunk
8. Agent sends the chunk to the server through CSSL

Stages where collect may fail

- Connection fails.
- Collect User has inadequate permission (Audit Trail/TEMP).
- Collect Script fails.
- No Events to collect.

Logs to check for troubleshooting

- **Cesystem log**
- **CeAudit log**
- **Bbbin log**
- **Auditctl log**
- **Agent log**
- **Actuator logs**
- **Client logs**



Dynamic Tracing

Dynamic Tracing is simply setting the verbosity of logging to a high level. The trace files are checked for every minute, so a restart is not required. This level of logging allows for deeper look at what each component is doing. This can be very helpful during troubleshooting.

- Turning on dynamic tracing

On the agent system

1. Create a file named tracing in the {tsiem_home}/actuator/run directory.

Dynamic Tracing Continued...

- In the tracing file place the component name and set it equal to yes.
Component = yes

Component	Log File	On Server	On Actuator
bbbin	bbbin.log	yes	no
auditctl	auditctl.log	yes	no
agent	agent.log	yes	yes
actuator	actuatorXXX.log	yes	yes
bart	bart.log	yes	no
marge	Std out	yes	yes



Connection Failures

Verifying that the Agent and TSIEM server are communicating

CESSYSTEM Log

<20100331 08:25:37 utc> P259M902V0.0.1L775A4S0E44:Crypt: *Ready to receive* messages over secure channel with agent '12.1.105 on itimtargetsystem1d:5992'

<20100331 08:25:37 utc> P259M902V0.0.1L789A4S0E45:Crypt: Secure channel with agent '12.1.105 on itimtargetsystem1d:5992' fully active

CEAudit log

<20100331 08:21:36 utc> P259M902V0.0.1L962A3S8E10:Crypt: Protocol violation: message from 12.1.105 on itimtargetsystem1d:5992 and no secure channel



Connection Failures

**Verifying ssh connections are good.
TSIEM ships with a tool to test ssh connections. It
is located in the {tsiem_home}/bin directory.**

```
chksshconn.sh -h <host_name> -p  
<SSH_server_port> -u <user_name> -k  
  <private_key_file_name>
```

**An alternative to the above is using ssh this:
ssh -2 -p <port> -i <private_key_file_name>
 tsiemssh@<Audited_system>**

Connection Failures

Some common connection errors (this not an exhaustive list):

- 1. Agent not running**
- 2. SSHd not running**
- 3. Agent/SSHd unable to bind to ports
(Default: SSHd 22 Agent 5992)**
- 4. Agent and or target is not reachable**
- 5. SSH keys bad**
- 6. Agent certificate bad.**



Connection Failures

- **To recreate ssh keys (Linux):**

1. Switch to the cfiaadmin user

2. su - cfiaadmin

3. Generate the encryption keys

4. ssh-keygen -t rsa

5. When prompted for a location to save the the key:

/opt/ibm/tsiem/sim/server/run/SSHKeys/audhost-tsiem.ppk

6. When prompted for a passphrase, leave it blank.

7. Change to /opt/ibm/tsiem/sim/server/run/SSHKeys/

8. cd /opt/ibm/tsiem/sim/server/run/SSHKeys/

9. Transfer the public key (audhost-tsiem.ppk.pub) to the Linux system to be Audited.

10. scp audhost-tsiem.ppk.pub

tsiemssh@<Audited_System>:/home/tsiemssh/.ssh/authorized_keys

11. Initiate a connection to the Audited (target) server using the following commands.

```
ssh -2 -p 22 -i ./audhost-tsiem.ppk tsiemssh@<Audited_system>
```

Connection Failures

To create new Agent Certificate:

1. On the TSIEM server under the Audit Machine generate a new install password.
2. On the agent system, start the agent with the new password:
`./start-client [<password>]`

Connection Failure

To recreate ssh keys (Windows):

1. Run the PuTTY Key Generator, puttygen.exe. Do not change any of the parameters.
2. Click Generate to start the key generation process.
3. Leave the passphrase field empty, and click Save private key
4. Save the private key in the appropriate directory.

Server system is the agent system

```
%TSIEM_HOME%\sim\Server\run\SSHKeys
```

agent system

```
%TSIEM_HOME%\sim\Actuator\run\SSHKey
```

When you save the private key to a file, use a file name that clearly identifies the purpose for the key, such as agent_system_user_name.ppk. When you add the audited system to Tivoli Security Information and Event Manager, specify this private key file name for the SSH KeyFile event source property.

5. Save the public key to a text file, such as agent_system_user_name.ppk.pub. To connect to an audited system running the OpenSSH daemon, copy the generated public key from the Public key for pasting into OpenSSH authorized_keys file field in the PuTTY Key Generator to a text file.
6. Transfer the public key file to the audited system.

Collect Failures

- User Permissions to the Audit Trail:
The user the agent runs as must have access to the audit trail directory/files and any other directories defined in the Event Source properties.
- Recommended user that the agent should run as.
Windows - administrator
Linux/AIX - root



Collect Failures

- On Windows system where a user other than the Domain Administrator is being use UAC should be disabled.
- If the logs show permission errors the audit trail directory, collect directory and temporary directories should be checked.
- For ssh collects the ssh users will need to be given explicit permissions to the audit trail directory, collect directory and temporary directories



Collect Script Failures

Collect failures and success are recorded in the Auditctl log

<20110120 17:08:38 utc> P259M189V0.1.99.4L2680A4S8E55:AudCont: ACCreateChunklogCallback, error reply received from Audit Actuator SERVER01 IBM Tivoli Identity Manager 4.6 - 5.0 through SSH(18.1.116) code 90032 caused by request 80020 to Audit Controller

<20110120 17:08:39 utc> P259M189V0.1.99.4L1823A4S0E230:AudCont: received log from eventsource SERVER02 IBM Tivoli Access Manager for e-Business through SSH(18.1.122) on Main_Srv(12.1.1) (SERVER0202:2011 01 20 12:08:36)



Collect Script Failures

Knowing how to manually run a collect script can help show exactly why and where the scripts fails.

To manually run a collect script The event source properties need to be passed to the script on the command.

For instance this is how the DB2 collects script would be started manually.

```
../bin/genact-main "/tmp/TEMPFILE1" "/tmp/TEMPFILE2" "/tmp/TEMPFILE3"  
"/tmp/TEMPFILE4" "../bin/viper2.cfg" "/home/db2inst1/sqllib/security/auditdata"  
"db2audit.instance.log" "/home/db2inst1/sqllib/security/auditdata" "db2audit.db.*.log"  
"db2inst1" "props"
```


Collect Script Failures

- Parameter/variables from the Event Sources Properties Page

```

TEMPFILE1="/tmp/TEMPFILE1"
TEMPFILE2="/tmp/TEMPFILE2"
TEMPFILE3="/tmp/TEMPFILE3"
TEMPFILE4="/tmp/TEMPFILE4"
OPTION1="../bin/viper2.cfg"
OPTION2="/home/db2inst1/db2log"
OPTION3="db2audit.instance.log"
OPTION4="/home/db2inst1/db2log"
OPTION5="db2audit.db.TOOLSDB.log"
OPTION6="db2inst1"
PROPSFILE="props"

```

? _ □
Event Sources

Event Sources > Event Source Details > Advanced

*Name:

IBM DB2 for the SIM Serve

Properties:

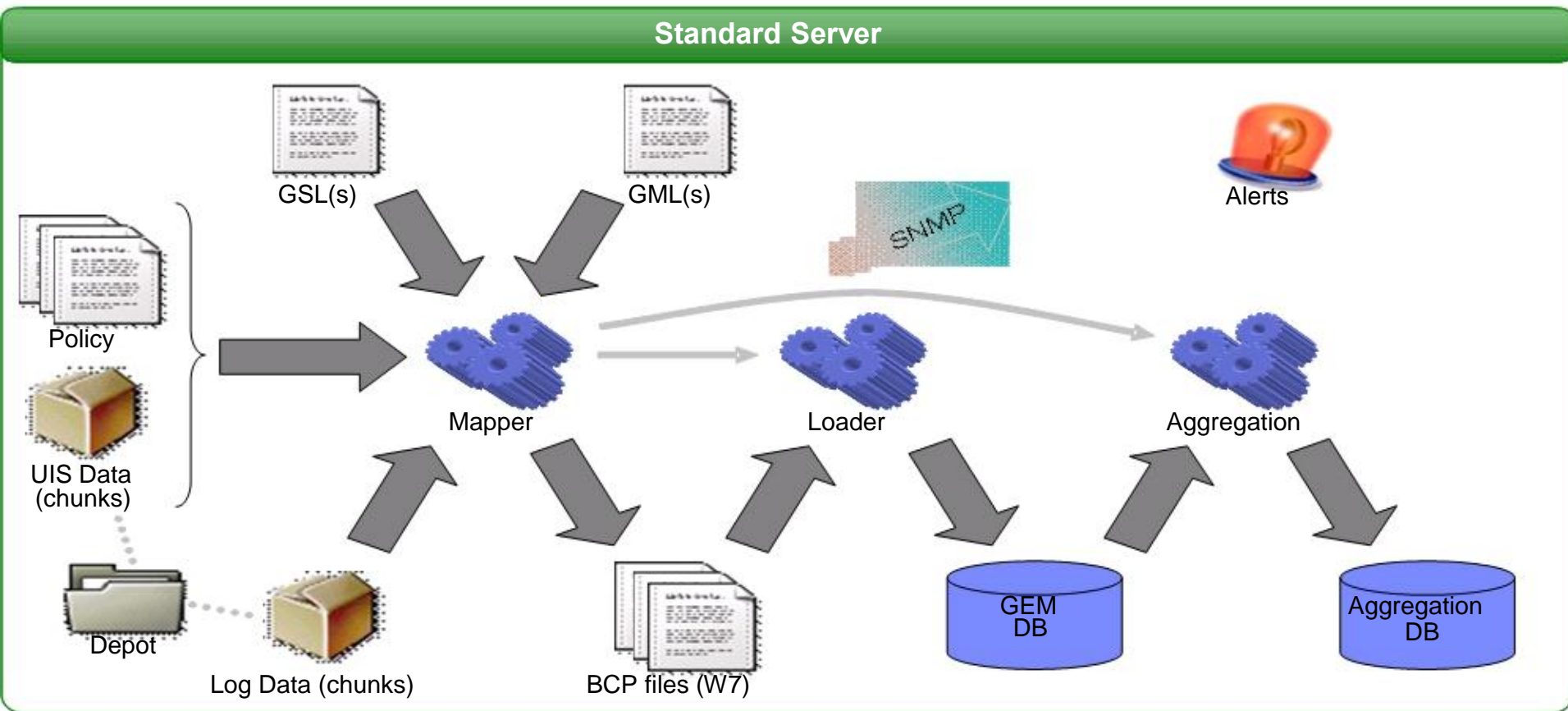
Name	Value
Audited Machine	boygeorge.tivlab.austin.ibm.com
Type	IBM DB2 9.5 - 9.X
Agent	boygeorge.tivlab.austin.ibm.com
Collect Directory	<input type="text" value="/tmp"/>
Instance Archive Path	<input type="text" value="default"/>
Instance Archive File Pattern	<input type="text" value="db2audit.instance.log"/>
Database Archive Path	<input type="text" value="default"/>
Database Archive File Pattern	<input type="text" value="db2audit.db.*.log"/>
Instance Name	<input type="text" value="cifdbadm"/>
Text Encoding	<input type="text" value="ISO-8859-1"/>
Language code for audit trail	<input type="text"/>

Reporting Database Load Problems

- **Over of the Load process.**
- **Stages the load can fail in.**
- **Logs involved.**
- **Reporting Database Status.**
- **Load Time.**
- **Recreating a Reporting Database.**

Reporting Database Load Problems

- **Load Process Overview**



Reporting Database Load Problems

Stages a load can fail in

Pre-Map

- **Bulk Loading**
- **Writing the BCP Files**
- **Post Processing**

Reporting Database Load Problems

Mainmapper logs

The logs are located in the

{tsiem_home}/sim/server/log directory

They are named as follows:

Mainmapper-<GEM_DB_Name>.log

All of the mapping activity is defined by a code the begins with CIF

[Mar 31, 2010 12:41:24 AM] INFO: *CIFJG0540I*: Starting to map chunk(s)

[Mar 31, 2010 12:30:04 PM] INFO: *CIFJG0011I*: Processing chunk:

G:\IBM\TSIEM\sim\depot\timintdev1.109\06N50L0

[Mar 31, 2010 2:24:29 AM] INFO: *CIFJG0541I*: Finished mapping

All these CIF codes are listed at the following URL.

<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tsiem.doc/tg/MessageListing.html>



Reporting Database Load Problems

The CIF codes can be used to look up any message in the log. They will take on the form These CIF messages code can give insight in to why the load failed and offer responses to correct the problem.

CIFDZ0002E

**Failed to configure the serviceName service
Explanation**

An error occurred during the configure step of the service installation.

Administrator response

Check server documentation for error message specified. Ensure that all parameters for the service configuration were passed correctly. Verify that machine has enough free disk space for a new service installation. Try to reinstall service manually. If the problem persists, contact IBM Software Support.

Reporting Database Load Problems

SQL Errors

The mainmapper logs will also contain sql exception if they are thrown.

DB2 SQL Error: SQLCODE=-1035, SQLSTATE=57019,
SQLERRMC=null, DRIVER=3.57.110

The SQLCODE can offer valuable insight in the problem and can be looked up at.

<http://publib.boulder.ibm.com/infocenter/iseriess/v5r3/index.jsp?topic=%2Frzala%2Frzalaco.htm>



Reporting Database Load Problems

DB2 diagnostic logs: The db2diagnostic file is another valuable source for information on what is happening with DB2 and the load process. It will messages that look similar to the following:

```
2011-01-05-09.39.13.278000-300 E1866968F748    LEVEL: Severe
  PID      : 8104          TID : 7468      PROC : db2bp.exe
  INSTANCE : CFINST      NODE : 000
  EDUID    : 7468
FUNCTION: DB2 UDB, database utilities, sqlubConnectDatabase, probe:1258
MESSAGE : SQL1035N The database is currently in use.
DATA #1   : SQLCA, PD_DB2_TYPE_SQLCA, 136 bytes
sqlcaid : SQLCA  sqlcabc: 136  sqlcode: -1035  sqlerrml: 0
          sqlerrmc:
          sqlerrp : sqlubCon
sqlerrd : (1) 0x00000000  (2) 0x00000000  (3) 0x00000000
          (4) 0x00000000  (5) 0x00000000  (6) 0x00000000
sqlwarn  : (1)  (2)  (3)  (4)  (5)  (6)
          (7)  (8)  (9)  (10) (11)
          sqlstate: 57019
```


Reporting Database Load Problems

db2diag.log is generated in one of two ways:

1. The TSIEM diagnostic script is executed.
2. Run db2support
db2support . -d CIFDB -c

db2support gathers a lot of diagnostic data that can be used to get a look at how the db and db2 are configured and performing.



Reporting Database Load Problems

Reporting Database Status

Part of resolving a load error can involve getting the current db status and resetting the status

To get the current status of the reporting db in question:

From a db2 CLI prompt

```
db2=> connect to cifdb user <cifowner>
```

```
db2=> "select dbistatus from eprisedb.metadbinstance where  
dbiname='<gemdb_in_question>'"
```

The returned status code can be used with the follow table to identify the problem.

Reporting Database Load Problems

Code	Description
0	unknown
1	not loaded
2	not loaded
3	cleared
4	loaded
5	loading
6	clearing
40	Error loading while starting server
41	Error starting mapper
42	Other error while clearing
43	The mainmapper was called with an invalid argument list
44	The mainmapper could not open the mapper.cfg file
45	Invalid chunk logs specified for the mainmapper
46	The mainmapper could not open the log file
47	The mainmapper could not find a submapper
48	The mainmapper could not create a file with chunk logs for the submapper
49	The submapper could not find the message file
50	The submapper reported an error
51	The bcp process returned an error
52	Error during postprocessing
53	Error during policy processing
54	Error during aggregation
55	Error during merging of policy and grouping
56	The mapping process resulted in no mapped events
57	The database was too small
58	No log data was selected for loading
59	Other error while loading
60	Insufficient disk space during loading

Reporting Database Load Problems

Once a load problem is resolved or if the status was not updated during load, it may be necessary to manually update the db status:

From a CLI prompt

```
db2=> connect to cifdb user <cifowner>
```

```
db2=> update eprisedb.metadbinstance set dbistatus=4 where  
      upper(dbiname)=upper('gem')
```

```
db2=> commit
```



Reporting Database Load Problems

Changing the load time: Once a load problem is resolved it may be necessary to manually update the last load time to load only the events that necessary.

From a db2 CLI prompt

```
db2=> connect to cifdb user <cifowner>
```

```
db2 "update eprisedb.auditgemdb set constructtime = '2011-01-24-05.00.00.000000'  
where gemdbix=(select DBILOADEDGEMDBIX from eprisedb.metadbinstance  
where dbiname='<gem_db_in_question>')"
```

NOTE: Time is in UTC

Reporting Database Load Problems

In some situations it may be required that the reporting db be recreated

A number of reasons can lead to this, the db is just unrecoverable and/or the amount of time necessary to perform other actions is not available.

To recreate the reporting db and preserve the Event Sources:

```
cmd /c ..\bin\delgemdb.bat CIFDB cifowner <cifpwd> EpriseDb <GEMDBname>
```

```
cmd /c ..\bin\addgemdb.bat CIFDB cifowner <cifpwd> EpriseDb <GEMDBname>  
125 empty
```

Fix Pack Installation

It is recommended that TSIEM be updated with Fix Packs (FP) as they are released

The current Fix Pack is FP008 . It can be downloaded from the TSIEM Customer Support site. Complete installation instructions are in the FP Readme.

NOTE: Before installing any FP make a complete back up of the TSIEM installation.

Fix Pack Installation

Installation Considerations

- Stop and start all services as stated in the Readme.
- On Windows make sure there are no actuator.exe process running.
- In a clustered environment the Security Server must be installed first.

Fix Pack Installation

- **Known issues**

Stopping actuator.exe processes

In rare situations, the SIM service on Windows servers might not kill the actuator.exe processes when the service is stopped.

If these processes are not stopped, the fix pack installation might fail. You can kill the processes manually using the Task Manager. After the processes have been killed, restart the installation of the fix pack.

Upgrading DB2 9.7

- **Why upgrade**

- **DB2 9.7 resolves a problem with physical disk space not being not being returned to for use only container space.**
- **Upgrading resolves a few security vulnerabilities.**
- **New versions of DB2 contain performance enhancement.**
- **DB2 Autonomics**

Upgrading DB2 9.7

- **Before Upgrading.**

- Make a complete backup of the TSIEM environment.
- Have a recovery plan. If the upgrade fails a full restore must be performed.
- TSIEM 2.0 Fix Pack 4 must be installed first.
- If using the manufacture refresh (2.0.0.4) FP4 is already applied.
- In a clustered environment mixed DB2 versions are not supported. Standard servers and the Enterprise server must be upgrade.

Upgrading DB2 9.7

- **Known Upgrade Issues**

- After upgrading you might get an error like the following when running DB2 commands.

- SQL1046N The authorization ID is not valid. SQLSTATE=28000

- This is resolved by changing the login user for both of the below services from db2admin to cifdbadm.

- DB2 - CIFICOPY - CIFINST-0

- DB2 Governor (CIFICOPY)

Upgrading DB2 9.7

- **Known Upgrade Issues**

- After upgrading you might get an error like the following when running DB2 commands.

```
[20101119 06:43:08 utc] INFO: CIFAD0044E: STATUS: Synchronization run has failed. Exception: CIFWI0411E: unable to execute sql:  
REVOKE INSERT, UPDATE, DELETE ON EPRISEDDB.FAP_DIRTY_FLAG FROM  
USER CIFDBADM  
DB2 SQL Error: SQLCODE=-558, SQLSTATE=42504,  
SQLERRMC=CIFDBADM;CIFDBADM;CONTROL, DRIVER=3.59.81
```

This is resolved by executing the following two command.

```
REVOKE control ON EPRISEDDB.FAP_DIRTY_FLAG FROM USER CIFDBADM
```

```
REVOKE INSERT, UPDATE, DELETE ON EPRISEDDB.FAP_DIRTY_FLAG FROM  
USER CIFDBADM
```

Continuity Report

- **Overview**

Regulatory compliancy requires that a report be available that proves that collected data was archived and is complete.

Log Continuity is the mechanism in TSIEM that creates this report.



Continuity Report - How does it look

Dashboard
History
Continuity
Activity
Investigate
Retrieval

Portal > Log Manager > Continuity Report

Log Continuity Report

Continuity Audit

location

- Grouping Windows
- WINDOWSAM
- IBM DB2 8.1 - 9.1
- STUDENT
- IBM Tivoli Compliance Insig...
- STUDENT
- IBM Tivoli Compliance Insig...
- STUDENT
- IBM Tivoli Directory Server
- STUDENT
- Internet Information Server (IIS)
- STUDENT
- Microsoft Windows
- STUDENT
- WINDOWSAM

Last day, 01:00 12 February - 00:59 13 February, 2008

hour
day
week
month
year

Log File Detail

#	Size	Start date	Time	End date	End time	Machine	Eventsource	Eventsource type
4	3kB	February 12, 2008	23:45	February 13, 2008	00:00	STUDENT	IBM Tivoli Compliance Insi...	IBM Tivoli Compliance Insight Man...
4	3kB	February 12, 2008	23:45	February 13, 2008	00:00	STUDENT	Internet Information Server (IIS)	Internet Information Server (IIS)
5	77kB	February 12, 2008	23:45	February 13, 2008	00:00	STUDENT	IBM DB2 8.1 - 9.1	IBM DB2 8.1 - 9.1

Help

This page shows informati
current completeness of lo
in the chunk depots.

In the chart, every rectang
a separate chunk log and e
with rectangles represents
source.

To change the time period
viewed audit information, c
corresponding tab in the lo
corner of the graph (altern
the corresponding label on

To move to an adjacent tim
an orange arrow to the left
time period label.

To toggle the grouping type
corresponding tab next to l

To obtain detailed informati
chunk log, hover the mous
the corresponding rectang

The list represents log chu
to filtering criteria. To filter
column, click the funnel-sh
the header of the column. I
dialog that opens, select th
criteria and click Start Filter

To regenerate the tables, c
'Regenerate report' in the /
section of the Extra Inform

Continuity Report

- **How it works**

The continuity reports is created using data from the Log Management Database (LMDB). Specifically the *chunk continuity tables* are used.

A process /module called the chunk continuity report generator (CCRG) is responsible for updating these tables.

The CCRG uses the chunk headers to determine the status and completeness of the chunks in the depot.

Continuity Report

Five messages that can be on the report

1. Corrupted log set
2. Failed collect, not collected yet
3. Delayed collect, possible data loss
4. Missing log set
5. Missing logs



Continuity Report

- **Why a log set may be incomplete**

Collect failure - Event source did not transfer any chunks to the server. Errors indicating why possible causes for this will be recorded in the auditctl logs.

Sublogs/chunks in the depot are corrupt.

Questions/Comments

