OpenText™ Database Activity Monitoring

Software Version 24.4.0

Admin Guide

opentext™

Legal notices

Copyright 2023 - 2024 Open Text

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that OpenText offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- View information about all services that Support offers
- Submit and track service requests
- Contact customer support
- Search for knowledge documents of interest
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in.

Contents

Introduction

This manual is targeted for the person responsible for evaluating, installing, and maintaining OpenText™ Database Activity Monitoring (DAM) in a company. Typically, in this document refers to this person as the administrator.

Abbreviations

Information about the abbreviations used in this guide is given in the table below.

Abbreviations	Definition
DAM	Database Activity Monitoring
DSIM	Installation Manager
DSPL	Preload Library
DSTAP	Log Analysis Motor
DSTOOL	General Agent Commands
LDAP	Lightweight Directory Access Protocol

Agent Installations

Agent installation stages are explained separately for Linux and Windows below:

- DAM Agent Installation on Linux, below
- DAM SQL Agent Installation on Windows, on page 55

DAM Agent Installation on Linux

Determining the Installation Package

The relevant package should be selected according to the server where the agent will be installed. During package selection, the part starting with `release xxx` contains the name and version of the compatible operating system. Following this value, infrastructure information and agent version are specified.

An example of the package is given in below figure. Version may vary for each release.

Ad	Değiştirme tarihi	Tür	Boyut
release-aix72-ppc-3485.zip	7.04.2021 09:38	Sıkıştırılmış Klasör	4.354 KB
release-el6-3485.zip	7.04.2021 09:40	Sıkıştırılmış Klasör	3.030 KB
release-el7-3485-dbg.zip	7.04.2021 09:41	Sıkıştırılmış Klasör	5.508 KB
release-sl12-ppcle-3485.zip	7.04.2021 09:42	Sıkıştırılmış Klasör	3.811 KB
release-sl15-3391.zip	28.01.2021 10:07	Sıkıştırılmış Klasör	3.116 KB
release-sun113-sparc-3485.zip	7.04.2021 09:43	Sıkıştırılmış Klasör	3.741 KB

Determination of Operating System Version

A ssh connection is made to the relevant server and the version is determined with the following command.

```
# uname -a
```

```
[root@oracle-test ~]# uname -a
Linux oracle-test 4.1.12-124.15.2.el7uek.x86_64 #2 SMP Tue May 22 11:52:31 PDT 2018 x86_64 x86_64 x86_64 GNU/Linux
```

OpenSSL Version Check

 Linux agent supports OpenSSL 1.0.2+ versions. Users can check OpenSSL version with the following command.

```
# openssl version
```

```
[root@oracle-test ~]# openssl version
OpenSSL 1.0.2k-fips  26 Jan 2017
```

Opening the Agent Package

Agent packages should be sent to the Linux server in .zip format. The package should be unpacked with the following command.

```
# unzip release-e17-3485.zip
```

```
[root@oracle-test Dataskope]# ls
release-el7-3485.zip
[root@oracle-test Dataskope]# unzip release-el7-3485.zip
Archive:  release-el7-3485.zip
   creating: release-el7-3485/
  inflating: release-el7-3485/configure.sh
  inflating: release-el7-3485/deploy.list
  inflating: release-el7-3485/deploy.sh
  inflating: release-el7-3485/deploy_defaults.sh
  inflating: release-el7-3485/deploy_dsim.sh
  inflating: release-el7-3485/deploy_dspl.sh
  inflating: release-el7-3485/deploy_dsplth.sh
  inflating: release-el7-3485/deploy_dstap.sh
  inflating: release-el7-3485/deploy_dstool.sh
  inflating: release-el7-3485/deploy_tools.sh
  inflating: release-el7-3485/dsim-chkconf.sh
  inflating: release-el7-3485/dsim-logrotate.conf
  inflating: release-el7-3485/dsim-method.sh
  inflating: release-el7-3485/dsim-smf.xml
  inflating: release-el7-3485/dsim-systemd.service
  inflating: release-el7-3485/dsim-upstart.conf
  inflating: release-el7-3485/dsim.conf
  inflating: release-el7-3485/dsim.signed
  inflating: release-el7-3485/dsim_server.pfx
  inflating: release-el7-3485/dsplno32.signed
  inflating: release-el7-3485/dsplno64.signed
  inflating: release-el7-3485/dstap.conf
  inflating: release-el7-3485/dstap.signed
  inflating: release-el7-3485/dstool.signed
  inflating: release-el7-3485/gencert.sh
  inflating: release-el7-3485/libdspl.so.signed
  inflating: release-el7-3485/libdsplth.so.signed
  inflating: release-el7-3485/postfilter.conf
  inflating: release-el7-3485/postfilter.list
  inflating: release-el7-3485/uninstall.sh
[root@oracle-test Dataskope]#
```

Granting Executable Authorization to Installation Files

Executable authorization should be given to the `.sh` files in the package using the following command. For this, the following commands should be run respectively.

```
# cd release-e17-3485
```

```
# chmod +x *.sh
```

```
[root@oracle-test Dataskope]# cd release-el7-3485/
[root@oracle-test release-el7-3485]# chmod +x *.sh
[root@oracle-test release-el7-3485]# []
```

Determination of Network Interfaces to be Listened

As a working principle, DSTAP listens to all packets reaching the selected network interfaces and filters the ones related to the database. At this stage, to optimise the resources to be used by the agent, only the necessary (database accessible) network interfaces should be selected. With the following command, the active network interfaces on the server are determined and the network interfaces related to the database are noted by evaluating with the server administrator. In the following example, eth0, eth1 and lo interfaces will all be listened.

```
# ifconfig -a
```

```
[root@oracle-test release-el7-3485]# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.64  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 00:0c:29:bc:12:02  txqueuelen 1000  (Ethernet)
        RX packets 45291994  bytes 6282953652 (5.8 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39318514  bytes 8918789700 (8.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:bc:12:16  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 0  (Local Loopback)
        RX packets 281308  bytes 58032355 (55.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 281308  bytes 58032355 (55.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
# ip addr
```

```
[root@oracle-big-server release-4818-el7]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:fd:29:9b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.74/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 52:54:00:6e:44:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN group default qlen 500
    link/ether 52:54:00:6e:44:5f brd ff:ff:ff:ff:ff:ff
[root@oracle-big-server release-4818-el7]#
```

Pre-Installation Configuration

The necessary parameters must be defined before installation. The deploy.sh file included in the agent package is run with the following command and the settings about how the agent will work are made.

```
# bash deploy.sh
```

Press y.

```
[root@oracle-test release-el7-3485]# ./configure.sh

Following configuration will be used:
  * Network devices list: lo,eth0
  * Messages transport   : 1 (file)
  * Infraskope Server IP: 0.0.0.0
  * DSIM control-if port: 8765
  * DSIM server cert pwd: 1234qqqQ!!
  * Start DSTAP on boot : yes
  * Enable DSPL library : no

Would you like to modify default deployment settings? [y/N]: y
```

Defining Network Interfaces

The noted network interface names are entered separated by commas.

```
Here's list of your network devices:
eth0      (192.168.1.74   / )
lo        (127.0.0.1      / )
virbr0    (192.168.122.1  / )
Enter comma-separated list of network devices to work on (for example: lo,eth0). You can also use * to inc
lude all and -dev_name to exclude specific device (for example: *,-virbr0  means use all except virbr0). O
r press [ENTER] to use default(*): eth0,lo,virbr0
```

Determining Log Transmission Mode

The agent can transmit logs in two different modes. The transmission mode is selected according to the need. Details about transmission modes are given in the below.

- **File**: Logs are collected and compressed on the server and stored in different files. These files are labelled with a time tag.

- **Syslog** (Not Recommended): Logs are collected and sent to the server via the Syslog protocol.

```
Select message transport type (1=file, 2=syslog) or press [ENTER] to use default(1):
```

Defining DAM Server IP Address

If Syslog is selected as the log transmission method, the server IP address must be defined. If File is selected as the log transmission method, the IP address can be left blank.

```
Enter IP address of the Infraskope Server or press [ENTER] to use default(0.0.0.0):
```

Defining the DSIM Transport Port

The DSIM component is used to run the functions required for remote management of the agent on the database. These functions and their details are described in . Port can be left as default 8765. If it is required to communicate over another port, the relevant port is entered.

```
Enter port number for dsim control interface or press [ENTER] to use default(8765):
```

Defining the Password of the DSIM Certificate

The DSIM component executes commands from the remote server over a secure channel. For this reason, it uses the `dsim_server.pfx` certificate included in the installation package. Users can continue by entering the password of this certificate. When a new certificate is created, the password entered in this field is used again.

```
Enter password for dsim server certificate file or press [ENTER] to use default(1234qqqQ!!):
```

Automatic Start of DSTAP

By default, the DSTAP agent is started automatically during Linux boot. Depending on the requirements, this setting should be set to "y" or "n".

```
Start DSTAP automatically on system boot and after installation? [Y/n]: y
```

DSPL Active/Passive Selection

DSPL is for monitoring local connections (other than IP protocol) on the server. The details of this feature are described in . This feature is selected as on or off according to the need. The relevant setting must be entered as "y" or "n".

```
Would you like to enable Dataskope Preload Library (DSPL)? [y/N]: y
```

Creation of DSIM Certificate

By default, a certificate named `dsim_server.pfx` is included in each installation package and there is no need to change it for installation. To use a certificate other than the default for security reasons, a new certificate is created by entering "y" in this section. The password of the generated certificate is the same as the password entered in Defining the Password of the DSIM Certificate.

```
Following configuration will be used:
  * Network devices list: lo,eth0,eth1
  * Messages transport  : 1 (file)
  * Infraskope Server IP: 0.0.0.0
  * DSIM control-if port: 8765
  * DSIM server cert pwd: 1234qqqQ!!
  * Start DSTAP on boot : yes
  * Enable DSPL library : yes

New settings written to deploy_defaults.sh
Would you like to generate new client/server certificates for dsim? [y/N]: n
Configure done.
```

Starting the Installation

To start the installation with the configurations made in the previous step, the `deploy.sh` file in the package is run with the following command and "n" is entered. If there are no errors during the installation, the result will be as follows.

```
# ./deploy.sh
```

```
Would you like to modify settings before proceeding? [y/N]: n
Stopping service: dsim
Waiting for dstap to exit...
installing dstap binary to /usr/bin/dstap
Installing dstap configs to /etc/dataskope/
File-based message transport selected
All done.
Detected init system: systemd
Detected OS: RHEL7
Stopping service: dsim
Installing dsim binary to /usr/bin/dsim
Installing dsim configs to /etc/dataskope/ with control port=8765
Please make sure port TCP/8765 inbound is open...
Installing systemd service: dsim
You can now control dsim service with the following commands:
    sudo systemctl start dsim
    sudo systemctl stop dsim
    sudo systemctl status dsim
Starting service: dsim
All done.
Installing libdspl.so to /lib64/libdspl.so
All done.
Installing libdsplth.so to /lib64/libdsplth.so
Installing 32-bit no-op lib to /lib/libdsplth.so
All done.
Updating dstool at /usr/bin/dstool

[root@oracle-test release-el7-3485]#
```

Checking the Installation

After installation, users can view the status of the services. Choose the relevant command for your operating system from the list below, run it, and check its correctness.

OS	Command
Linux el6	`# initctl status dsim`
Linux el7-el8	`# systemctl status dsim`
AIX 7+	`# lssrc -s dsim`

SunOS	# ps -ef | grep dsim
	# ps -ef | grep dstap
Suse	# systemctl status dsim

```
[root@oracle-big-server release-4818-el7]# systemctl status dsim
● dsim.service - Dataskope Installation Manager Service
   Loaded: loaded (/etc/systemd/system/dsim.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2024-09-17 14:08:39 +03; 2min 18s ago
 Main PID: 26118 (dsim)
   CGroup: /system.slice/dsim.service
           └─26118 /usr/bin/dsim


Sep 17 14:08:39 oracle-big-server systemd[1]: Started Dataskope Installation Manager Service.
[root@oracle-big-server release-4818-el7]#
```

Default Directory of Logs

The default directory is /var/spool/dataskope and logs are compressed and stored in this directory.
The file naming format is message-xxxxxxx-xxxxx. When the file is first created, it is named as
"message" and when the file is closed, the name is added according to the timestamp. This directory
can be changed in dsim.conf and dstap.conf if needed according to the server disc structure. After
changing the setting, DSIM and DSTAP must be restarted.

```
[root@oracle-big-server dataskope]# cd /var/spool/dataskope/
[root@oracle-big-server dataskope]# ls
messages                        messages-20240914-1726333974   messages-20240916-1726451901
messages-20240913-1726216106    messages-20240914-1726334034   messages-20240916-1726451961
messages-20240913-1726216166    messages-20240914-1726334094   messages-20240916-1726452021
messages-20240913-1726216226    messages-20240914-1726334154   messages-20240916-1726452081
```

Using DSTOOL

DSTOOL is used to perform some checks related to the agent. DSTOOL is used for purposes such
as clean removal of the DAM agent, checking file integrity and permissions. Commands and their
descriptions can be accessed with the following command.

```
# dstool --help
```

```
noprelink                Disable(blacklist) prelink for given executable
    --obj                  - Path to binary file to add to prelink blacklist

dump                     Dump sections of binary file into separate files named after section names
    --obj                  - Path to binary file whose sections to dump

replay                   Read packets from the trace file and send them to dstap data sink
    --in                   - Path to trace dump file
    -q                     - Quiet mode (do not print every packet info)

svc_type                 Detect startup service management (init) system on current system

svc_add                  Add service to the system and enable automatic startup
    --name                 - Service name
    --cfg                  - Paths to config files for the service, comma-separated for miltiple files

svc_del                  Remove service from the system
    --name                 - Service name

svc_on                   Enable automatic service startup
    --name                 - Service name

svc_off                  Disable automatic service startup
    --name                 - Service name

status                   Check Dataskope components available on current system
dspl_on                  Enable DSPL module (it needs to be already installed on target system)
dspl_off                 Disable DSPL module (does not remove the module itself)
dspl_clean               Disable DSPL module and remove binaries (legacy and new)

check                    Validate cryptographic signature of binary file.
    [--obj=]               - Path to binary file whose signature to check

trace_list               List trace files in folder and print info.
    [--in=]                - Directory or file to scan. Default is CDW
    --trim                 - Trim long filenames. If provided without value, use 10
    --sort                 - Comma-separated list of fields: X_asc/X_desc, where X is:
                             name, start, end, dur, size, count, cli, srv

trace_split              Split trace file into separate files per each TCP session.
    [--in=]                - Path to source trace file
    --minp                 - Skip sessions having less than minp=N packets
    --mins                 - Skip sessions having less than mins=N bytes
    --ips                  - Comma-separated client IPs list to filter. Default=all
    --ports                - Comma-separated client ports list to filter. Default=all
    -f --full-only         - Skip partial and only write full TCP sessions

trace_scramble           Remove sensitive information from the trace file.
    --in                   - Path to source trace file. A .scram file will be added
    --salt                 - Hexadecimal value to initialize random IPs from
    --char                 - Character to replace terms with. Default is *
    -i, --ip               - Replace source/dest IPs in headers with random ones
    -r, --regex            - Treat terms as regex rules. Otherwise use exact match
    -s, --sort             - Sort terms (long > short). Will not affext regex
    --ports                - List if client ports to include/exclude in new file
    [terms...]             - Space-separated terms to scramble. 3+ chars each

-v, --version            Show program version info
```

DSTOOL File Integrity and Permission Check

The integrity, version and permission checks of the executable files required for the DAM agent to run are done with DSTOOL. This control can be achieved with the following command. The output on a reliable server will be as follows.

```
# dstool status
```

```
[root@oracle-big-server release-4818-el7]# dstool status
```

Binary path	Size	Perm	Module	Arch	Bi	Hw	Target	Ver	R	S	Status
/usr/bin/dstool	1,894,336	711	dstool	x86	64	2	EL7	4818	R	✓	☐26893
/usr/bin/dsim	2,634,912	4711	dsim	x86	64	2	EL7	4818	R	✓	☐26118
/usr/bin/dstap	3,889,064	4711	dstap	x86	64	4	EL7	4818	R	✓	■
/lib64/libdsplth.so	27,104	4755	dsplth	x86	64	2	EL7	4818	R	✓	
/lib64/libdspl.so	1,890,560	755	dspl	x86	64	2	EL7	4818	R	✓	
/lib/libdsplth.so	1,828	4755	dsplno	x86	32	2	EL7	4818	R	✓	

```
DSPL status: Disabled
```

Introducing the DAM Agent

DAM Agent does not start any log collection after it is installed with default settings (unless the `postfilter.conf` file is modified). To define log collection policies and for the collector to recognize the agent, the agent must be added to the panel after installation and initial configuration must be made.

Prerequisite

Default Certificate

By default, agents can utilize a generic client certificate. This certificate can be generated specifically for the organization and is protected by a password unique to the organization. If this option is selected during the initial installation, agents can be added to the panel with this certificate.

Adding DAM Agent to the Panel

After the agent is installed on the database server and the DSIM service is verified to be running, is opened, and the agent is introduced with the New Agent button on the DAM panel.

Ref.	Field	Function
1	IP Address	The real IP address of the database server is entered so that the collector and the administration panel can communicate with the agent. The IP address can be any IP address used to access the database server. If port forwarding is used, the IP address of the router must be entered.
2	Port	In the default settings, the access port is set as "8765". For port forwarding or similar needs, the port specified during agent installation may be a value other than the default. In this case, the port specified during installation is entered.
3	Use new default certificate, Client Certificate	The DAM agent and the collector talk over an encrypted channel. When adding an agent via the panel, the default certificate can be used, or a special certificate can be created for that agent. Default certificate usage is explained in detail in Default Certificate.
4	Certificate Password	This is the field where the certificate password is entered for the agent. If a default certificate is selected, it is not necessary to define any password.

New Agent Wizard

Listener Settings

Select the databases you want to collect logs

pcap.devices	*
oracle.enabled	✔
oracle.server_port	1521
mysql.enabled	☐
mysql.server_port	3306
postgre.enabled	☐
postgre.server_port	5432
mssql.enabled	☐
mssql.server_port	1433

CANCEL   < BACK   NEXT >

Field	Function
pcap.devices	Comma-separated list of capture devices.
oracle.enabled	Enable captures on Oracle ports and Oracle parsing engine.
oracle.server_port	Comma-separated list of ports on which Oracle instances are working.
mysql.enabled	Enable captures on MySQL ports and MySQL parsing engine.
mysql.server_port	Comma-separated list of ports on which MySQL instances are working.

Field	Function
hana.enabled	Enable captures on HanaDB ports and HanaDB parsing engine.
hana.server_port	Comma-separated list of ports on which HanaDB instances are working.
mongo.enabled	Enable captures on MongoDB ports and MongoDB parsing engine.
mongo.server_port	Comma-separated list of ports on which MongoDB instances are working.
cassandra.enabled	Enable captures on Cassandra ports and Cassandra parsing engine.
cassandra.server_ port	Comma-separated list of ports on which Cassandra instances are working.
vertica.enabled	Enable captures on Vertica ports and Vertica parsing engine.
vertica.server_port	Comma-separated list of ports on which Vertica instances are working.
db2.enabled	Enable captures on DB2 ports and DB2 parsing engine.

Field	Function
db2.server_port	Comma-separated list of ports on which DB2 instances are working.
couchbase.enabled	Enable captures on Couchbase ports and Couchbase parsing engine.
couchbase.server_port	Comma-separated list of ports on which Couchbase instances are working.
teradata.enabled	Enable captures on Teradata ports and Teradata parsing engine.
teradata.server_port	Comma-separated list of ports on which Teradata instances are working.
elastic.enabled	Enable captures on Elasticsearch ports and Elasticsearch parsing engine.
elastic.server_port	Comma-separated list of ports on which Elasticsearch instances are working.
netezza.enabled	Enable captures on Netezza ports and Netezza parsing engine.
netezza.server_port	Comma-separated list of ports on which Netezza instances are working.

Field	Function
gauss.enabled	Enable captures on GaussDB ports and GaussDB parsing engine.
gauss.server_port	Comma-separated list of ports on which GaussDB instances are working.
sybase.enabled	Enable captures on SybaseSQL ports and SybaseSQL parsing engine.
sybase.server_port	Comma-separated list of ports on which SybaseSQL instances are working.
Msg.file.max_age	Maximum file age in minutes before rotation.
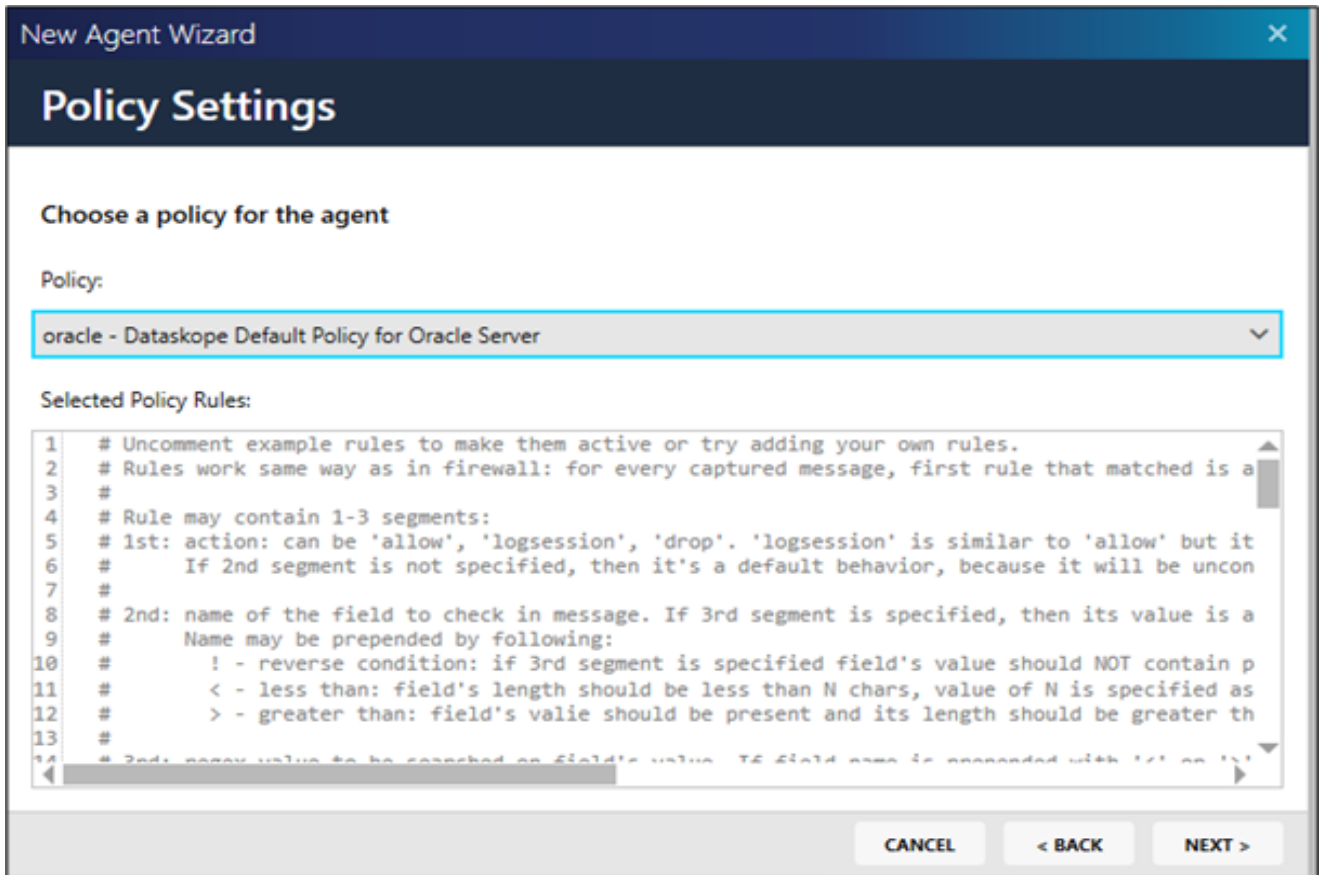
Policy Settings: agent logs or does not log the queries sent to the database according to the specified policies.

Field	Function
Cluster Name	If the database server configuration is designed as "Failover", this information should be given to the cluster. For example, if there are two SQL Database servers and they work in active/passive mode, the common name of these two servers (Cluster Name) should be entered in the relevant field.
Suppress Inactivity Event Minutes	To generate an alarm if the DSTAP agent is inactive for a certain period. If the DSTAP agent appears to be switched off for the time entered here in minutes, an alarm is generated. Event ID:2020
Max Idle Minutes	If the collector cannot collect logs from the relevant agent for the specified time, an alarm is generated. After how many minutes this alarm is desired to be generated, this value should be entered in minutes.
Idle Threshold Minutes	When the agent becomes inactive, an alarm is generated after the specified time. This value should be entered in minutes after how many minutes the related alarm is desired to be generated.
Suppress File Info Event Minutes	This is the event information that is sent whether the agent message files are accumulated on the relevant

	database server or not. This value should be entered in minutes if the related alarm is desired to be generated accordingly.
Suppress Status Event Minutes	It is the event where agent health status information is received in detail. This value should be entered in minutes if the relevant alarm is desired to be generated accordingly.
Tag	Allows adding a tag for distinctive use.

DAM Agent Detailed Information Screen

Detailed information of the desired agent can be accessed through the panel. Since server information can be displayed in this area, agent configuration can be done more accurately.
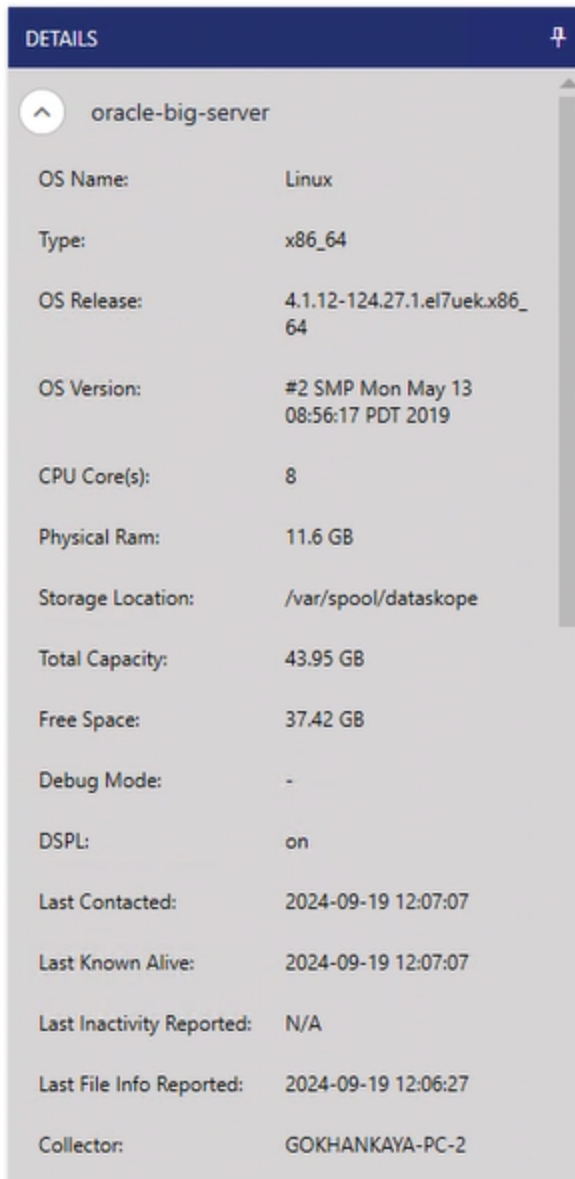
Menu	Function
General Information [OS Name, Type, OS Release, OS Version, CPU Cores, Physical RAM]	The detail screen displays the operating system name, type, version, number of cores and physical memory information of the server.
Storage Location	On the detail screen, it is displayed in which directory on the server of the relevant agent to extract the message files. The default directory is `/var/spool/dataskope` directory.
Total Capacity	From the detail screen, the total size of the directory where the agent will extract the message files for the relevant server can be displayed.

Free Space	From the detail screen, the total remaining size of the directory where the agent will extract the message files for the relevant server can be displayed.
DSPL	The DSPL status of the agent for the corresponding server can be displayed.
Last Contacted	The last time the agent contacted the collector can be displayed.
Last Known Alive	The last time the agent transmitted status information can be displayed.
Last Inactivity Reported	Used to show the last time the agent was inactive.
Last File Info Reported	Used to show when the agent last transmitted the file information in the logging directory.
Collector	Shows the hostname of the machine where Collector is installed.

Advanced Configuration of the Agent

DSIM and DSTAP operating states can be displayed, as well as real-time control of DSTAP can be performed and output.
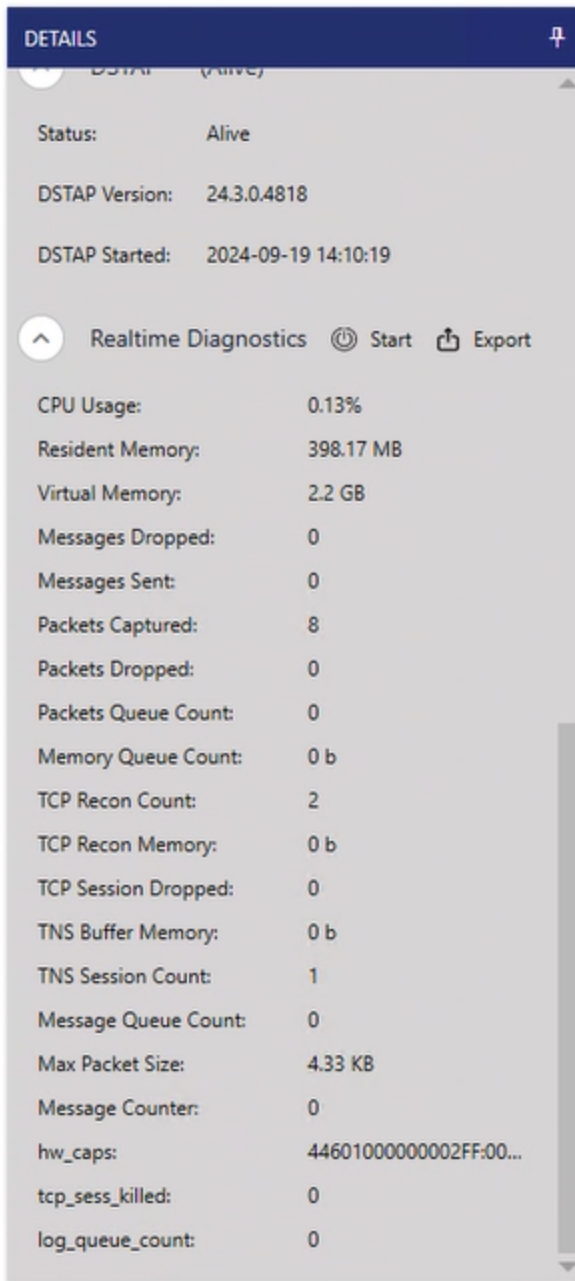
Field	Function
CPU Usages	The CPU status used by the agent in real time can be observed.
Resident Memory	The memory state used by the agent in real time can be observed.
Virtual Memory	In addition to the current memory usage of the agent, it is used to show the memory state that can be used when necessary.

Messages Dropped	The number of messages that are not logged by the agent with the policy can be observed.
Messages Sent	The number of messages logged by the agent with the policy can be observed.
Packets Captured	Shows the number of TCP packets captured.
Packets Dropped	It is possible to observe the number of TCP packets that are somehow not inserted into the log analysis engine by the agent (corrupted packets, etc.) and the number of dropped TCP packets.
Packets Queue Count	The number of packets waiting to be sent by the agent to the log analysis engine can be observed. This situation may vary according to server density.
Memory Queue Count	The number of packets waiting to be processed in memory can be observed by the agent. This situation may vary according to server density.
TCP Recon Count	This value is related to the packet header information sent one time when a connection is made to the database. As the number of connections increases, this value will also increase. If this value is too high (e.g., 1000000) it may cause the agent to stop. This parameter should be checked in case of high memory usage.
TCP Recon Memory	Specifies how much memory the mechanism described in TCP Recon Count. A high value of this parameter may cause the agent to stop. This parameter should be checked in case of high memory usage.
TCP Session Dropped	The number of TCP sessions dropped out by the agent can be observed. The TCP header is dropped when the connection terminates, or when an invalid packet header is encountered (e.g., connections made before the agent starts).
TNS Buffer Memory	Session information sent during the initial connection is held for use in this field. When the session ends, this field is cleared. If there are too many sessions, this value may be high. However, it should not exceed GB.
TNS Session Count	Indicates the total number of sessions since the DAM agent last started. If there are ongoing sessions that occurred before the agent started, they are not counted.

Message Queue Count	The number of messages waiting in the queue can be observed.
Max Packet Size	The maximum package size processed by the agent can be observed.
Message Counter	Linux-based agents have switched to logging in timestamp logic after version 3413. Windows-based agents continue to work in counter logic.
hw_caps	
d_tcp_sess_killed	Shows the number of killed TCP connections.
log_queue_count	Shows the count of log queue

DAM Agent Management Functions

 DAM agents can be managed in detail without depending on the database administrator. Use right-click to reach detailed actions.
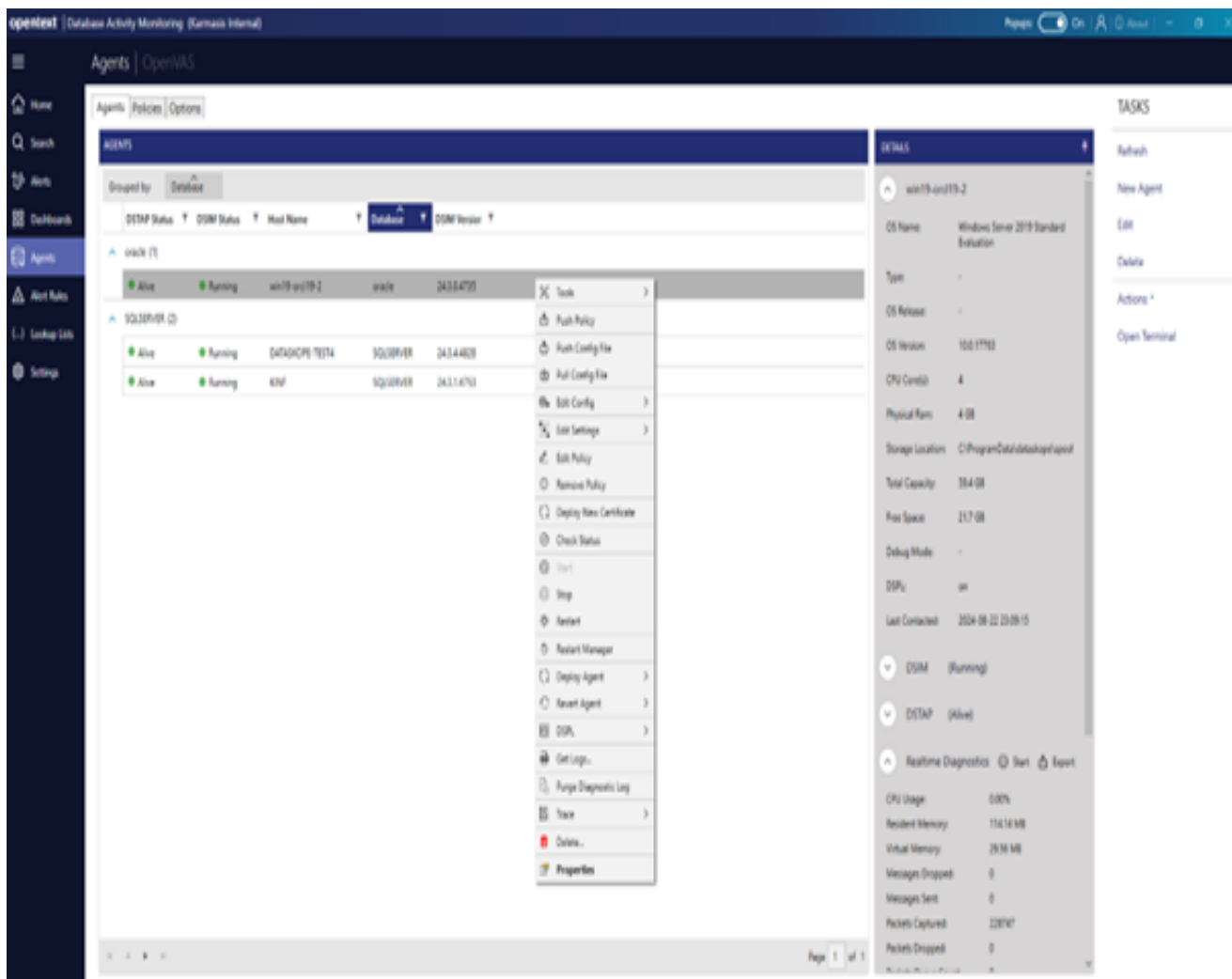
Field	Function
Tools	SSH connection to the server can be made with a username and password. A Read-Only user is sufficient for certain settings and status views of the agent.
Push Policy	A changed policy is normally automatically applied to the agent. However, when this process fails for some reason, policy transmission to the agent can be provided again with the relevant feature.
Push Config File	It allows the agent's configuration files (dstap.conf, postfilter.conf etc.) to be sent to the server. The file is sent after it is selected. It may be necessary to restart the agent according to the content and purpose of the modified file.
Pull Config File	It allows the agent configuration files (dstap.conf, postfilter.conf etc.) to be downloaded from the server.

Edit Config	With the help of this feature, both DSIM and DSTAP configuration editor screen can be opened and the settings that need to be changed or the settings that need to be added can be added to the agent. This feature is more detailed in Linux based agents.
Edit Settings	With the help of this feature, both DSIM and DSTAP setting screen can be opened and the settings that need to be changed or the settings that need to be added can be added to the agent. See DSIM Advanced Settings and DSTAP Advanced Settings for more details.
Edit Policy	Used to assign and edit a policy to the agent. For example, users have created an Oracle policy and applied it to the relevant agents. The point to be considered here is which policy is modified. The change is applied to all agents under the same policy. See Organisation of the Agent's Policy for more details.
Remove Policy	The policy applied to the agent can be deleted and a new policy may be applied.
Deploy New Certificate	This is the certificate required to update agents above 4084 from the old version.
Check Status	The state of the agent can be observed with the corresponding property.
Start	An agent with DSTAP stopped can also be started with the corresponding feature.
Stop	DSTAP can be stopped for some reason with the corresponding feature.
Restart	DSTAP can be restarted with the corresponding feature for some reason.
Restart Manager	This is the DISM restart module.
Deploy Agent	DAM agents can be updated to the upper version of both DSIM and DSTAP through the panel without the need for a database administrator.
Revert Agent	Linux based agents can automatically downgrade both DSIM and DSTAP to a lower version if necessary. Windows-based agents do not have such a feature.
DSPL	DSPL, which is specially developed for Linux-based agents, can be switched on and off via the panel.
Get Logs	All system log files of the agent can be retrieved via the panel.

Purge Diagnostic Log	All system log files of the agent can be reset via the panel.
Trace	It is the module used to monitor the traffic of packets.
Delete	The agent can be removed from the panel with the corresponding feature.
Properties	The features of the agent can be viewed on the panel.

DSIM Advanced Settings

The operating principles of the DSIM service can be changed in the "DSIM Settings". Descriptions of the parameters are explained below.

Menus	Function
log.local.size	The maximum size of the DSIM log file. (Min:1MB, Max:32MB)
log.local.count	The number of rotations of the DSIM log file. (Min:2, Max:10)

log.verbosity	This is the message information to be written to the DSIM log file. (0=debug, 1=info, 2=notice, 3=warning, 4=error, 5=critical, 6=alert, 7=emergency)
msg.storage.location	The directory where the message files will be written. The default is /var/spool/dataskope directory. DSIM must be restarted if changes are made.
ctrl.address	This is the IP address that the DSIM control interface will listen to. If "0.0.0.0" is entered, it can accept commands from all IP addresses. When defining this address, one of the addresses available on the server must be selected. If an IP address that is not on the server is selected, DSIM may not work properly.
ctrl.port	This is the port information that the DSIM control interface will listen to.
ctrl.timeout	This is the information after how many minutes the inactive sessions will be dropped. (Min:1dk, Max:1440dk)
ctrl.max_clients	The number of DSIM connections to be made in parallel. More than this number of clients cannot be connected at the same time. (Min:4, Max:32)
ctrl.proto	This is the TLS protocol version to use.
cert.pass	It is the password of `dsim_server.pfx` certificate.
dstap.path	The default directory information of DSTAP binary files.
dstap.params	Initial parameters can be transmitted to DSTAP. Reserved for future use.
dstap.autostart	Here you can select whether or not to start DSTAP automatically at system start up.
dstap.kill_timeout	If the DSTAP does not close properly, the time in seconds after which a Force-Kill is performed is specified. (Min:5s, Max:120s)
msg.storage.reserve	The minimum space that should remain in the message log directory is determined in MB. When there is less space than the specified value, logging is continued by overwriting the oldest file. Attention! Log loss may occur! (Min:64M, Max:1GB)

msg.file.lock_timeout	It is the information when the message file will be locked.
msg.file.force_delete	Indicates whether a locked message file will be forcibly deleted or not. It is off by default.
watchdog.hang_restart	The number of minutes after which the control interface will restart itself in the event of a pending. (Min:1dk, Max:1440dk)

DSTAP Advanced Settings

The operating principles of the DSTAP service can be changed on the "DSTAP Settings" screen. Descriptions of the parameters are explained below.

Menus (Assigned)	Function
pcap.buffer_size	The size of the pcap temporary buffer memory for each device. (Min:16MB, Max:256MB)
pcap.buffer_delay	
pcap.snap_size	The maximum size for a packet to be captured. By default, it is 80KB. This value must be larger than the largest packet size. (Min:4KB, Max:128KB)
pcp.promisc	

pcap.devices	The information of the devices monitored by DSTAP (can be viewed on the relevant server with the **dstap -l** command output). A new device can be added by separating it with a comma from the setting screen. Then DSTAP will restart itself automatically.
pcap.extra_filter	Extra filter for pcap driver, helps to drop unrelated traffic on early stage.
cpu.queue_reset	Reset the queue after it reaches 8M entries.
pcap.log_drops	It is the information about the reduction of error logs that occur before the packet parsing step. (It may affect performance. It can also be used for error detection. It is not enabled by default.)
pcap.trace.enabled	Enable tracing of pcap packets.
pcap.trace.device	A device to do a trace capture on.
pcap.trace.filter	Filter for trace session.
pcap.trace.max_size	Maximum trace file size to grow.
dspl.enabled	This is the status information whether DSPL is enabled or not during the operation of DSTAP.
tcp.session_timeout	This is the drop time of an inactive TCP session. The relevant value must be entered in seconds. (Min:5dk, Max:600dk)
tcp.session.save_state	Save session state data upon app exit and resume them on restart.
tcp.session.save_template	Save client-specific state data for use with break-in session from same address.
oracle.enabled	This is the status of enabling Oracle port and decomposition mechanism.
oracle.server_port	Oracle ports are listened by DSTAP. If there is a special port, it can be added using a comma.
oracle.names	

Menus	Function
oracle.parse_nums	Parse numeric parameters.
oracle.parse_cursor	
oracle.parse_cur_exec	
oracle.parse_fetch	
mysql.enabled	This is the information about the status of enabling MySQL port and decomposition mechanism.

mysql.server_port	It is the information that MySQL ports are listened by DSTAP. If there is a special port, it can be added using a comma.
postgre.enabled	This is the status information for enabling the PostgreSQL port and decomposition mechanism.
postgre.server_port	It is the information that PostgreSQL ports are listened by DSTAP. If there is a special port, it can be added using commas.
mssql.enabled	This is the status information for enabling MSSQL port and decomposition mechanism.
mssql.server_port	It is the information that MSSQL ports are listened by DSTAP. If there is a special port, it can be added using commas.
hana.enabled	This is the status information for enabling the HANA port and decomposition mechanism.
hana.server_port	It is the information that HANA ports are listened by DSTAP. If there is a special port, it can be added using a comma.
mongo.enabled	This is the status information for enabling the Mongo port and decomposition mechanism.
mongo.server_port	This is the information that Mongo ports are listened by DSTAP. If there is a special port, it can be added using a comma.
mongo.max_docs	Maximum number of documents in query payload to process.
cassandra.enabled	Enable capture on Cassandra ports and Cassandra parsing engine.
cassandra.server_port	Comma-separated list of ports on which Cassandra instances are working.

Menus	Function
cassandra.names	
vertica.enabled	Enable capture on Vertica ports and Vertica parsing engine.
vertica.server_port	Comma-separated list of ports on which Vertica instances are working.
db2.enabled	Enable capture on DB2 ports and DB2 parsing engine.
db2.server_port	Comma-separated list of ports on which DB2 instances are working.

db2.names	
couchbase.enabled	Enable capture on Couchbase ports and Couchbase parsing engine.
couchbase.server_ port	Comma-separated list of ports on which Couchbase instances are working.
couchbase.names	
teradata.enabled	Enable capture on Teradata ports and Teradata parsing engine.
teradata.server_port	Comma-separated list of ports on which Teradata instances are working.
teradata.names	
elastic.enabled	Enable capture on Elasticsearch ports and Elasticsearch parsing engine.
elastic.server_port	Comma-separated list of ports on which Elasticsearch instances are working.
elastic.names	
elastic.max_body	Maximum body length to capture.
netezza.enabled	Enable capture on Netezza ports and Netezza parsing engine.
netezza.server_port	Comma-separated list of ports on which Netezza instances are working.
netezza.names	

Menus	Function
gauss.enabled	Enable capture on Gauss ports and Gauss parsing engine.
gauss.server_port	Comma-separated list of ports on which Gauss instances are working.
gauss.names	
sybase.enabled	Enable capture on Sybase ports and Sybase parsing engine.
sybase.server_port	Comma-separated list of ports on which Sybase instances are working.
sybase.names	
log.local.size	The maximum size of the DSTAP log file.

log.local.count	The number of rotations of the DSTAP log file.
log.verbosity	This is the message information to be written to the DSTAP log file. (0=debug, 1=info, 2=notice, 3=warning, 4=error, 5=critical, 6=alert, 7=emergency)
log.async	
diag.hearthbeat_ interval	The information about sending the statistical health status logs of the agent for analysis at the specified time frequency. The relevant value must be specified in seconds. (Min:1dk, Max:1sa)
diag.log_hearthbeats	This is the status information for enabling health status logs in DSTAP log.
mem.trim.threshold	The shaving mechanism is activated when the memory value assigned to the agent is exceeded.
mem.trim.reserve	This is the information about the size of the shaved memory. (Min:32MB, Max:256MB)
mem.limit.max	It is the maximum memory information that the agent will use. If this value is exceeded, "skip mode" will be activated. The working principle of skip mode is explained in mem.limit.skip_mode.
mem.limit.min	Specifies the level to which memory usage must drop for memory to be reduced to the specified value and for skip mode to be disabled.
mem.limit.skip_mode	Skip mode (1=Dropping TCP sessions, 2=Dropping all packages as in Mode-1, waiting for the memory usage to drop below the minimum, if it does not drop within 60 seconds by default, the agent is restarted)

DSTAP Settings

mem.limit.hold_time	60
tcp.kill.timeout	5000
tcp.kill.max_packets	100
tcp.kill.max_workers	20
tcp.kill.variations	2
tcp.breakin_mode	0
tcp.ip_stats	☐
msg.async_send	☑
msg.transport	1
msg.storage.location	/var/spool/dataskope
msg.file.max_size	2M
msg.file.max_age	1
msg.file.compression	1
cpu.parallel_parsers	1
cpu.queue_size	1M
security.control_iface	☐
replay.enabled	☐
replay.proc	0
replay.verbosity	5
replay.mode	0
ssl.keys	
ssl.sessions.timeout	36000
ssl.sessions.max_count	10000
db.dump_failure	☐
db.dump_max_query	32
diag.bgw_catch	☑
bench.max_stage	0

Unassigned

SAVE   CANCEL

Menus	Function
mem.limit.hold_time	Amount time of in seconds before restarting app if skip_mode=2 and memory limit is reached.

tcp.kill.timeout	Time slice given to TCP kill worker to termice the TCP session.
tcp.kill.max_packets	Number of RST packets to send before giving up.
tcp.kill.max_workers	Max number of parallel workers for killing TCP session.
tcp.kill.variations	Number of SEQ/ACK variations to use per packet.
tcp.breakin_mode	Behaviour for break-in TCP sessions.0=ignore break-in sessions, 1= kill break-in sessions.
tcp.ip_stats	Collect IP stats.
msg.async_send	Synchronous or asynchronous execution can be specified.
msg.transport	It is the information to determine the message creation method. By default, it is file based. (1=local file, 2=syslog)
msg.storage.location	The directory where the message files will be written. The default is /var/spool/dataskope directory. DSTAP must be restarted if changes are made.
msg.file.max_size	Maximum file size for rotation. (Compressed. Raw data will be much larger than seen. (Min:1MB, Max:16MB)
msg.file.max_age	The number of minutes the message file will be created before entering the maximum file size rotation. The default is 10 minutes. If it is desired that the logs reach DAM in a shorter time, this value can be reduced to 1 minute. (Min:1, Max:1440)
msg.file.compression	The degree of compression of the message file. For each value greater than one, the compression mechanism will run slower. The recommended value is 1. (Min:1, Max:22)
msg.file.preallocate	Enables a preliminary field assignment during message file creation. It is switched off by default.
cpu.parallel_parsers	It is determined how many parallel parsers the agent will work with. It can be configured according to server CPU specifications. For example, on a server with 96 cores, this value can be increased to 32.
cpu.queue_size	
security.control_iface	It is the feature that allows DSTAP functions from DSIM to undergo cryptographic verification before execution. It can be enabled for security purposes but may increase CPU usage.
replay.enabled	Enable replay interface.
replay.proc	Replay processor to use. 0=use own processor, 1=use main parallel processor, if parallel parsers are enabled.
ssl.keys	Flat list with comma-separated pairs.

ssl.sessions.timeout	Expiry interval in seconds for saved ssl session id/key.
ssl.sessions.max_count	Maximum number of saved sessions.
bench.max_stage	Testing purpose only. Do not enable it if you do not realize consequences.

Organisation of the Agent's Policy

Users can assign a policy to the agent and this policy can be edited. For example, users have created an Oracle policy and applied it to the relevant agents. The point to be considered here is which policy is modified. The change is applied to all agents under the same policy.

Menus	Function
Policy Name	A name can be assigned to the created policy.
Policy Database Type	It is the information to which database the created policy belongs. It cannot be changed afterward. A new policy must be created to change it.

Rules	
Policy Writing Drop	If it is started with drop, the rule writing must be continued with drop.
Using Policy Lookup List	Policies offer regex support. In addition, DAM lists can be created and used within the policy.
Policy Writing Allow	If it starts with allow, the rule writing must be continued with allow
Test Rule	The correctness of a written policy can be tested using this tool.
Policy Import	A policy written in text format can be uploaded and saved with this tool.

New DAM List
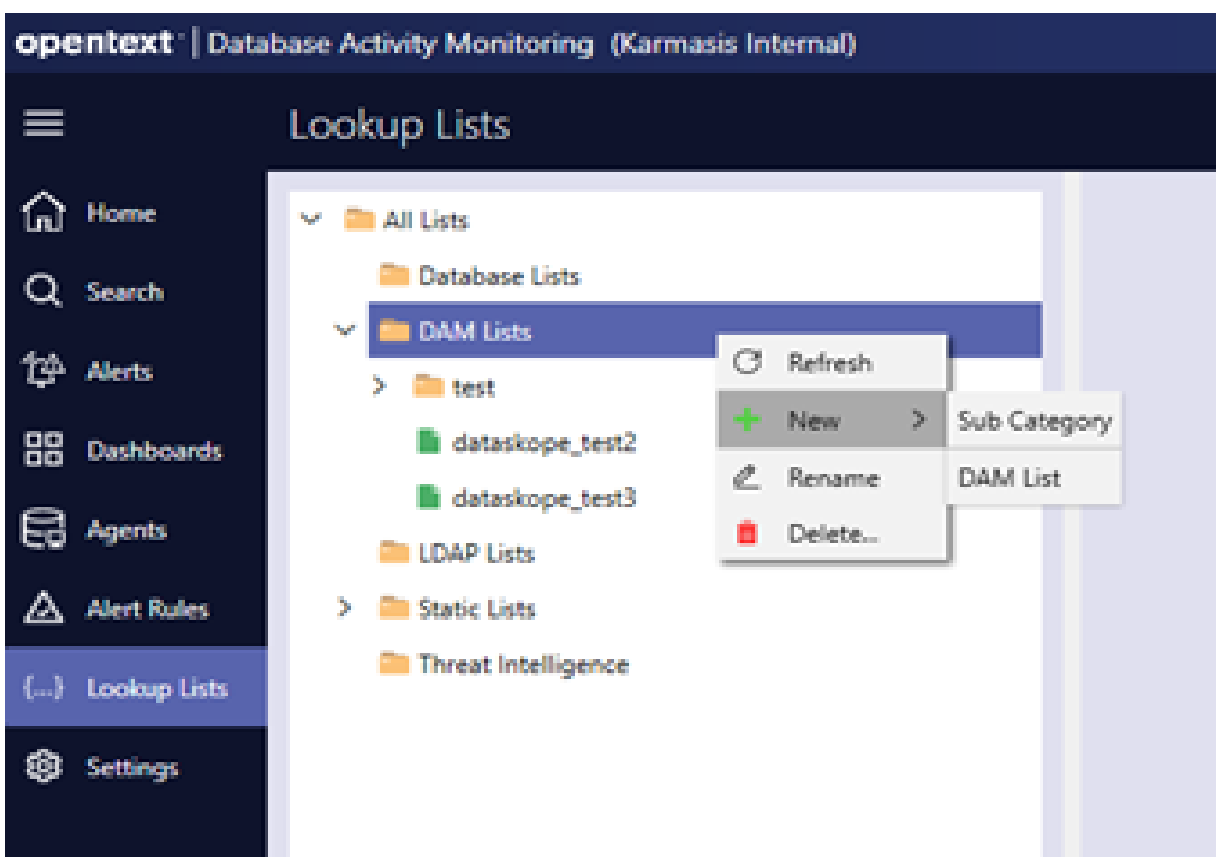
- A new DAM list can be created from the Dashboard **Lookup Lists** section.
- The created list can be given an alias.
- The list elements are defined. Do not define empty elements. Since regex definitions are used here, this may give undesirable results.

Upgrading DSIM to Upper Version

When updating DSIM on Linux-based systems, you must choose and send the `dsim.signed` file.
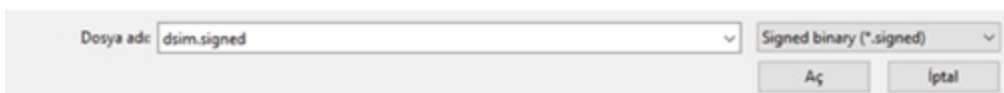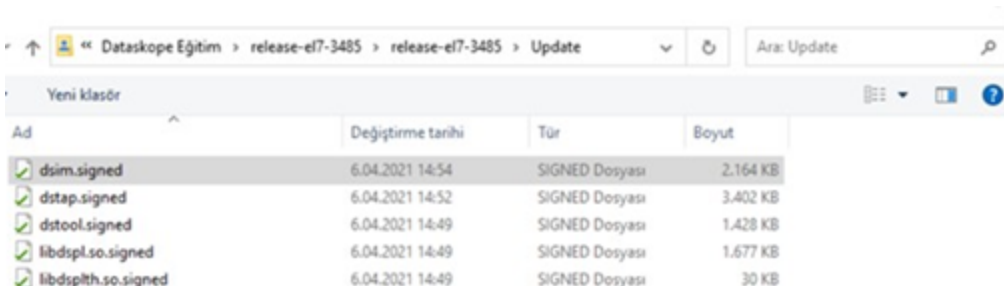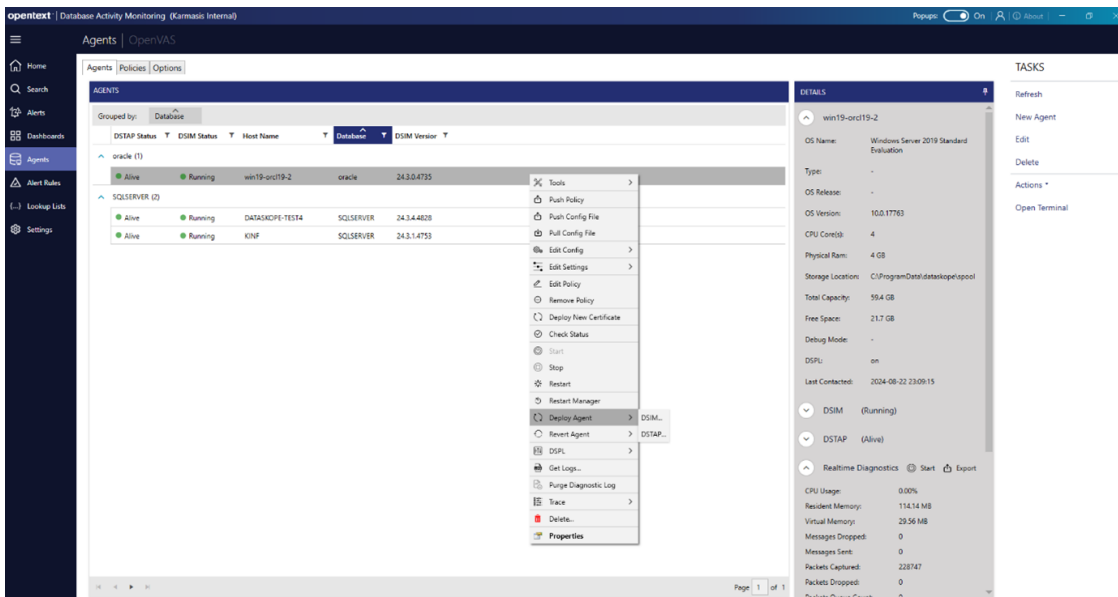
Upgrading DSTAP to Upper Version

When updating DSTAP on Linux-based systems, pick the `dstap.signed`, `dstool.signed`, `libdspl.so.signed`, and `libdsplth.so.signed` files, convert them to `.zip` format, and send them.

Policies

Policies can be viewed and edited through the panel. When the edited policies are saved, if they are assigned to agents, that policy is applied to all relevant agents in real time.
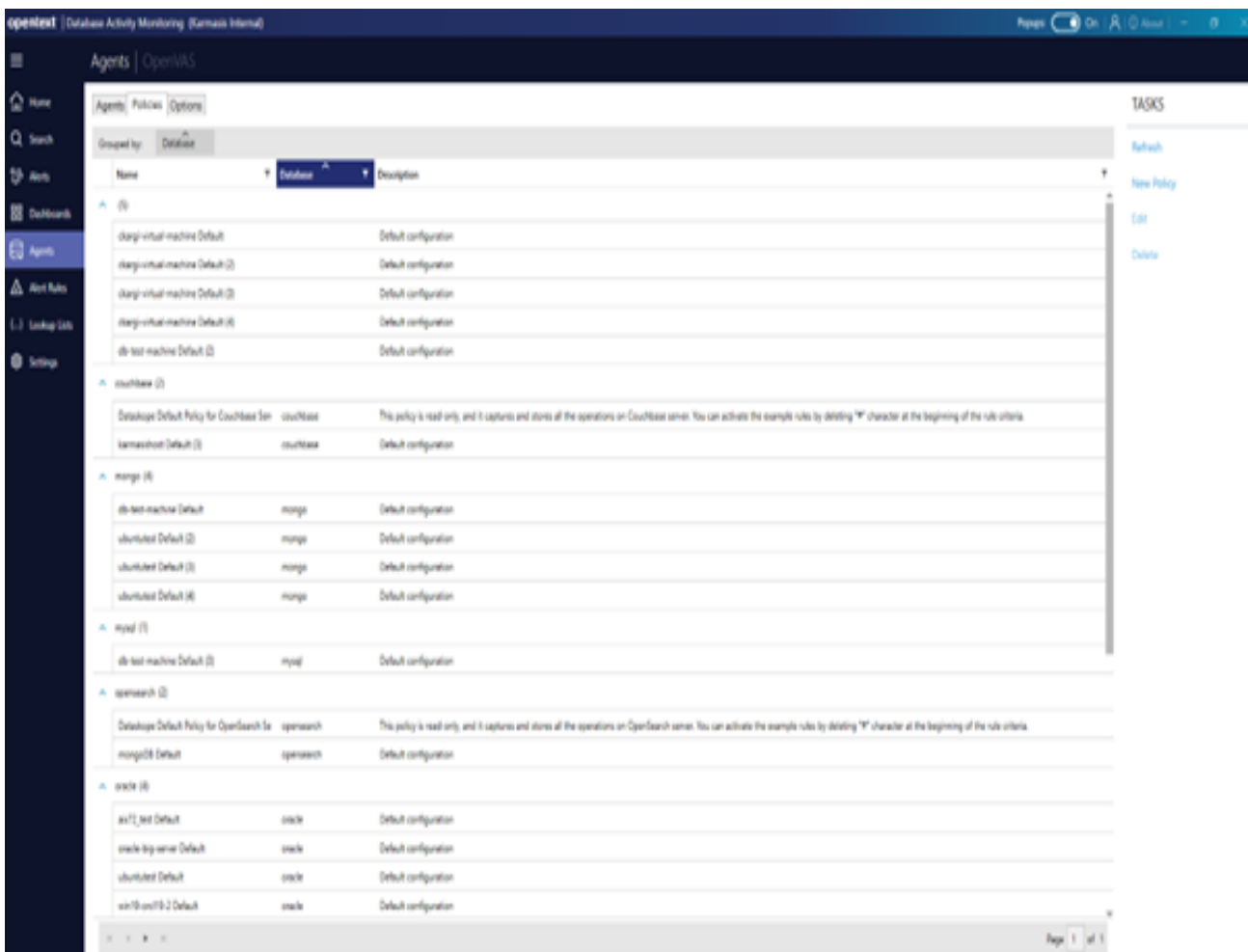
- When creating a policy, drop or allow is used and the spelling is continued by dividing with "|".
  For example, `drop|username|opentext`.

- If many usernames are to be dropped, the spelling should be as follows;
  `drop|username|opentext|dam_test|testdb`

- Many variations can be created by connecting with "+".

  For example,

  ```
  #test#
  #drop user and IP drop|os_user|opentext
  +
  ```

```
drop|db_user|dam_user
+
drop|client_ip|192.168.0.1
```

> **NOTE:** When connecting more than one rule line, the principles of these rules must be the same.
>
> > **EXAMPLE:**
> >
> > - If it is started with allow, it must continue with allow.
> >
> > - If it starts with drop, it must continue with drop.

- The use of a single "#" means a comment line.

- The use of "##" corresponds to match_rule in the logs coming to DAM.

- This is specifically recognised as the name given to the rule written in the line below it and is added to the detail of the relevant log.

- Database resources coming to DAM have both Standard fields and Dynamic fields.

- Dynamic fields are used in the policy. For example, `client_app_name` is a dynamic field and can be used in the policy.

> **NOTE:** Field names may vary depending on the database type. This should be taken into consideration when writing the rules.

- A policy starting with drop should not be continued with allow. For example, the following usage is incorrect, and this rule will not work:

```
#test
##drop query drop|username|opentext

+
allow|client_ip|192.168.0.1
```

DAM SQL Agent Installation on Windows

Pre-Installation Configuration

DAM SQL Agent uses Microsoft SQL Server Extended Events infrastructure. Logs reaching the database are logged by the baykus session. Baykus session is created by the agent within the framework of certain authorizations. For this reason, the following authorization definition must be made on SQL Server, and the following SQL command must be executed with administrator privileges:

SQL Version	Command
SQL 2008 R2	USE [master] CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS WITH DEFAULT_DATABASE=[master] GRANT CONTROL SERVER TO [NT AUTHORITY\SYSTEM]
SQL 2012+	USE [master] CREATE LOGIN DEFAULT_DATABASE=[master] GRANT ALTER ANY EVENT SESSION TO [NT AUTHORITY SYSTEM]

DAM SQL Agent Installation

1. Installation can be done by running the following command with command prompt from the directory where the installation package is located. Installation parameters are defined according to needs.

    # msiexec /i "DAM_SQLAgent.msi" PASSWORD=1234qqqQ!!

    STORAGEPATH=" C: ProgramData Karmasis Dataskope MsgStorage

    OUTPUTMODE="filestorage"

    WEBSERVICEURL="http://192.168.50.10/ElfWebService/default.asmx"

    CREATEDSIMTASK=true

    a. Default certificate password is set.

    b. The directory where logging will be done by DAM SQL Agent is determined.

    c. The method of logging is determined (**filestorage** | **msmq**). Default **filestorage.**

    d. When **msmq** logging is selected, **WEBSERVICEURL** should be entered and **TCP 1801**, **TCP 80** ports should be opened towards Collector machine.

    e. DSIM restart option.

2. Installation can be done by using the installation file from the directory where the installation package is located. Installation parameters are defined according to needs.

a. Go to **\Agents\DAM SQL Agent**

b. Double click on the `damsqlagent.msi`.

c. On the **DAM SQL Agent Setup Wizard** window, click **Next**.

d. On the **Select Installation Folder** window, enter the folder path to install **DAM SQL Agent**, click **Next**.

e. Select **Everyone to Install DAM SQL Agent** for anyone who uses the computer, or for **Just me** for only use yourself and click **Next**.

f. On the **License Agreement** window, choose **I agree**, click **Next**.

g. On the **Confirm Installation** window, click **Next**.

h. On the **DSIM Server Parameters window**, fill the spaces as follows:, click **Continue**.

> **NOTE:** It is recommended not to change the default values in WebServiceURL and Output Mode fields.

i. Click **Close** on the **Installation Completed window**.

Introducing the DAM SQL Agent

DAM SQL Agent does not start any log collection after it is installed with default settings (unless the postfilter.conf file is modified). To define log collection policies and for the collector to recognize the agent, the agent must be added to the panel after installation and initial configuration must be made.

Adding DAM SQL Agent to the Panel

After the DAM SQL Agent is installed on the database server and the DSIM service is verified to be running, DAM is opened, and the agent is introduced with the New Agent button on the DAM panel.
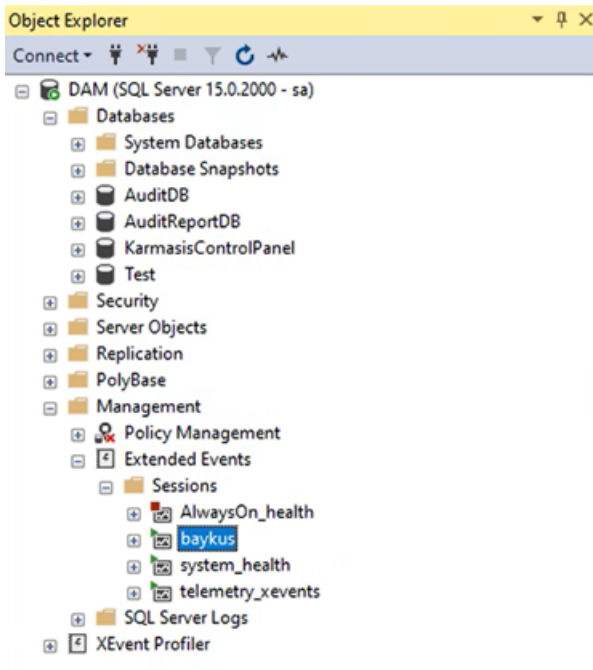
To start agent, right click on the **SQLSERVER** and select **Start**.
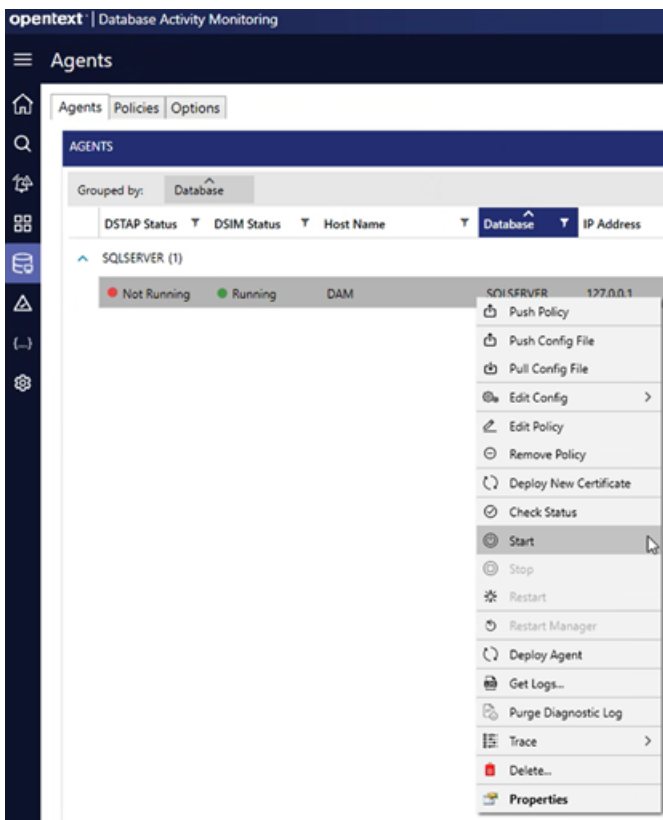
To make sure the DAM SQL Agent is started successfully, go to the SQL Server and check if the baykus events are created

Upgrading DAM SQL Agent to the Upper Version

DAM SQL Agent is updated to the upper version unlike Linux-based agents. As in the screenshot, a .zip file is sent with the relevant feature. The update file must be obtained from OpenText.
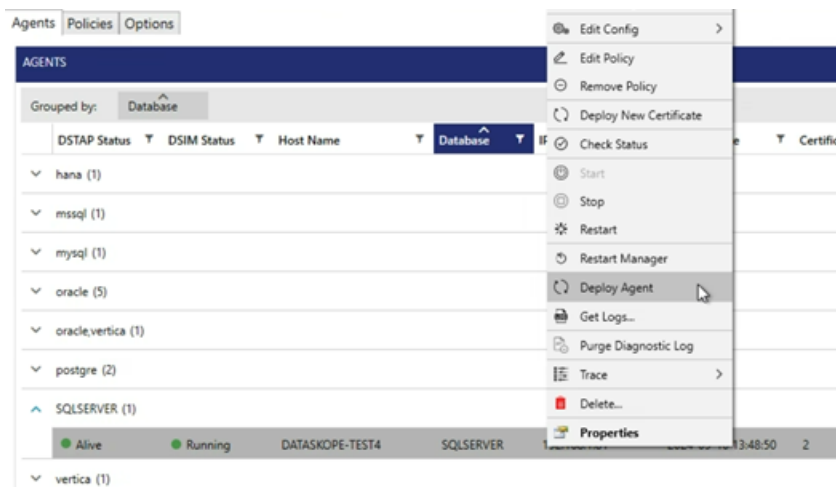
Removing the DAM Agent

Remove from Linux

DSTOOL is used for clean removal of the agent. A clean removal can be performed with the following command.

`# dstool cleanup_host`

```
[root@oracle-test dataskope]# dstool cleanup_host
```

DAM Collector

Installation

1. Go to \InstallMedia\Stage2\ProductComponents.

2. Double click on the DAM_Collector.msi.

3. On the **DAM Collector Setup Wizard** window, click **Next**.

4. On the **End-User License Agreement** window, choose **I accept** the terms in the **License Agreement** and click **Next**.

5. On the **Ready to Install** window, click **Install**.

6. When you see the **Installation Completed** window, click **Finish** to close.

Configuring the DAM Collector

As a default setting, the DAM Collector writes the Dump and LongQuery logs to the installation path, which can lead C disk to rapidly exceed its capacity. To avoid this issue, it is recommended to change the path for the log files.

1. Go to the installation file path **C:\Program Files\OpenText\DAM Collector** on the machine.

2. Open the settings.yaml file with text editor.

3. Fill the following areas with relevant disk path. For example:

```
 94    DumpsPath: K:\DumpsPath
 95    LongQueriesPath: K:\LongQueriesPath
 96    EnableCompressedQueryHashField: false
 97    EnableQueryHashField: true
 98    ExtractTablesAndColumnsFromQuery: true
 99    RestartOnHung: false
100    ProcessDumps: false
101    DebugMode: false
```

Introducing the DAM Collector to DAM Agent

1. Open Agents page on Dashboard. Right click to the agent and select Properties. (Or select the agent and then click the Edit button on right side of the page).
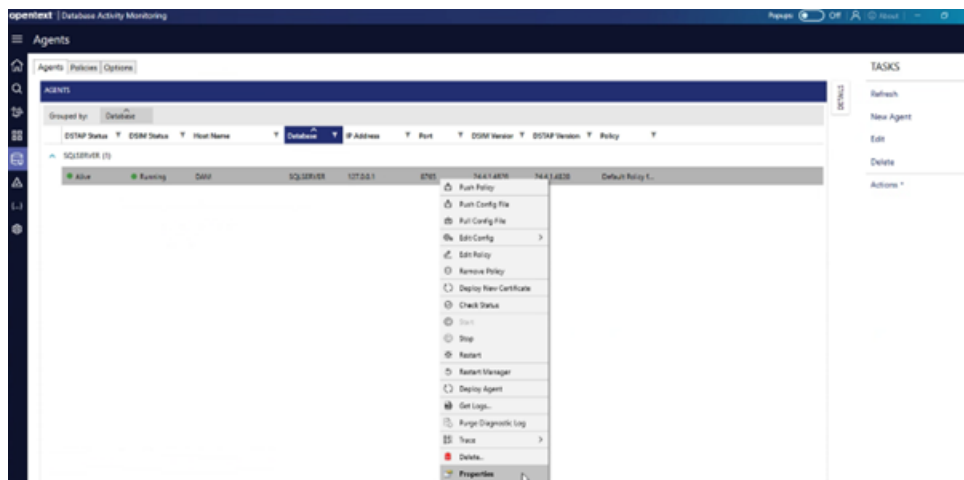
2. Select the Collector you want to add and click Save button.