

# Voltage Database Activity Monitoring

Software Version 23.4.0

Admin Guide

**opentext**<sup>™</sup>

Document Release Date: December 2023  
Software Release Date: December 2023

## Legal notices

Copyright 2023 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Except as specifically indicated otherwise, this document contains confidential information and a valid license is required for possession, use or copying. If this work is provided to the U.S. Government, consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## 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 .....	5
Abbreviations .....	6
DSTAP Agent Installation .....	7
DSTAP Agent Installation on Linux .....	7
Determining the Installation Package .....	7
Determination of Operating System Version .....	7
Opening the Agent Package .....	8
Granting Executable Authorisation to Installation Files .....	9
Determination of Network Interfaces to be Listened .....	10
Pre-Installation Configuration .....	10
Defining Network Interfaces .....	11
Determining Log Transmission Mode .....	11
Defining Voltage DAM Server IP Address .....	11
Defining the DSIM Transport Port .....	12
Defining the Password of the DSIM Certificate .....	12
Automatic Start of DSTAP .....	12
DSPL Active/Passive Selection .....	12
Creation of DSIM Certificate .....	12
Starting the Installation .....	13
Checking the Installation .....	14
Default Directory of Logs .....	15
Using DSTOOL .....	15
DSTOOL File Integrity and Permission Check .....	16
Removing the Voltage DAM Agent .....	17
DSTAP Agent Installation on Windows .....	17
Voltage DAM SQL Agent Installation .....	17
Introducing the Voltage DAM Agent .....	19
Adding Voltage DAM Agent to the Panel .....	19
Voltage DAM Agent Detailed Information Screen .....	26
Advanced Configuration of the Voltage DAM Agent .....	28
Voltage DAM Agent Management Functions .....	31
DSIM Advanced Settings .....	33

DSTAP Advanced Settings .....	36
Organisation of the Agent's Policy .....	43
New Voltage DAM List .....	45
Upgrading DSIM to Upper Version .....	46
Upgrading DSTAP to Upper Version .....	46
Upgrading Windows Agent to the Upper Version .....	47
<b>Policies .....</b>	<b>48</b>

# Introduction

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

# DSTAP Agent Installation







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

- [DSTAP Agent Installation on Linux](#)
- [DSTAP Agent Installation on Windows](#)

## DSTAP 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.

Ad	Değişirme tarihi	Tür	Boyut
 <a href="#">release-<u>aix72-ppc</u>-3485.zip</a>	7.04.2021 09:38	Sıkıştırılmış Klasör	4.354 KB
 <a href="#">release-<u>el6</u>-3485.zip</a>	7.04.2021 09:40	Sıkıştırılmış Klasör	3.030 KB
 <a href="#">release-<u>el7</u>-3485-dbg.zip</a>	7.04.2021 09:41	Sıkıştırılmış Klasör	5.508 KB
 <a href="#">release-<u>sl12-ppcle</u>-3485.zip</a>	7.04.2021 09:42	Sıkıştırılmış Klasör	3.811 KB
 <a href="#">release-<u>sl15</u>-3391.zip</a>	28.01.2021 10:07	Sıkıştırılmış Klasör	3.116 KB
 <a href="#">release-<u>sun113-sparc</u>-3485.zip</a>	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

Voltage DAM 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 Authorisation to Installation Files

Executable authorisation 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-e17-3485/  
[root@oracle-test release-e17-3485]# chmod +x *.sh  
[root@oracle-test release-e17-3485]#
```

## 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-e17-3485]# 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
```

## Pre-Installation Configuration

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

```
# ./configure.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.

```
Enter comma-separated list of network devices to work on (for example: lo,eth0) or press [ENTER] to use default(lo,eth0): lo,eth0,eth1
```

## Determining Log Transmission Mode

The Voltage DAM 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 Voltage DAM server via the Syslog protocol.

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

## Defining Voltage DAM Server IP Address

If Syslog is selected as the log transmission method, the Voltage DAM 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):
```

Figure 1: Defining Voltage DAM Server IP Address

## 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):
```

Figure 2: Defining the DSIM Transport Port

## 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 with the following commands.

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-test release-el7-3485]# 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 2021-06-08 11:06:22 +03; 2min 41s ago
 Main PID: 8021 (dsim)
    CGroup: /system.slice/dsim.service
            └─8021 /usr/bin/dsim
              └─8046 /usr/bin/dstap -d

Jun 08 11:06:22 oracle-test systemd[1]: Started Dataskope Installation Manager Service.
Jun 08 11:06:22 oracle-test systemd[1]: Starting Dataskope Installation Manager Service...
[root@oracle-test release-el7-3485]# █
```

## 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. 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-test release-el7-3485]# cd /var/spool/dataskope
[root@oracle-test dataskope]# ls
messages
[root@oracle-test dataskope]# █
```

## Using DSTOOL

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

```
# dstool --help
```

```
[root@oracle-test dataskope]# dstool --help
Options:
mkhash          Creates a cryptographic signature of binary file.
  --out          - Path to write hash to
  --obj          - Path to binary file to make signature of
  --pvk         - Path to private key to be used in signature creation

mkver           Creates a version data to be embedded into binary file.
  --out          - Path to write version data to
  --id           - App identity. Allowed values: dsim, dstap, dspl
  --ver         - App version in format: x.x.x.x (where x is a number)
  --os          - Target OS. For example: EL7, SUN113
  --arch        - Target architecture. Allowed values: x86, ppc, ppcle, sparc
  --cfg         - Build configuration. Allowed values: debug, release

mkres           Compile a resource file to be embedded into binary file.
  --in          - Path to resource definition file
  --out         - Path to write compiled resource to

check           Validate cryptographic signature of binary file.
  --obj         - Path to binary file whose signature to check
-q, --quiet    - Perform operation quietly (if possible)

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

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 multiple 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)

-v, --version   Show program version info
-h, --help     Show this help message
```

## DSTOOL File Integrity and Permission Check

The integrity, version and permission checks of the executable files required for the Voltage 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-test dataskope]# dstool status
/usr/bin/dsim... 2,215,736 (4711), dsim-1.1.0.3485-x86-64-EL7-Release, valid, running (8021)
/usr/bin/dstap... 3,483,072 (4711), dstap-1.1.0.3485-x86-64-EL7-Release, valid, running (8046)
/usr/bin/dstool... 1,461,976 (711), dstool-1.1.0.3485-x86-64-EL7-Release, valid, running (24907)
/lib64/libdsplth.so... 30,616 (4755), dsplth-1.1.0.3485-x86-64-EL7-Release, valid, not running
/lib64/libdspl.so... 1,716,480 (755), dspl-1.1.0.3485-x86-64-EL7-Release, valid, not running
/lib/libdsplth.so... 1,852 (4755), dsplno-1.1.0.3485-x86-32-EL7-Release, valid, not running
DSPL status: Enabled:Global
```

## Removing the Voltage DAM Agent

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

```
# dstool cleanup_host
```

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

## DSTAP Agent Installation on Windows

### Pre-Installation Configuration

Voltage 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 authorisations. For this reason, the following authorisation 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 2008 R2+	USE [master] CREATE LOGIN [NT AUTHORITY SYSTEM] FROM WINDOWS WITH DEFAULT_DATABASE=[master] GRANT ALTER ANY EVENT SESSION TO [NT AUTHORITY SYSTEM]

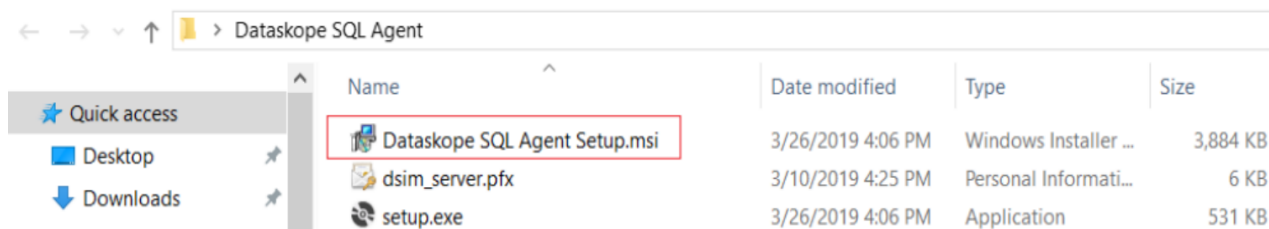
### Voltage DAM SQL Agent Installation

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.

```
# msixec /i Dataskope SQL Agent Setup.msi " PASSWORD=1234qqqQ!!
STORAGEPATH=" C: ProgramData Karmasis Dataskope MsgStorage
OUTPUTMODE="filestorage"
WEBSERVICEURL="http://192.168.50.10/ElfWebService/default.asmx"
```

CREATEDSIMTASK=true

1. Default certificate password is set.
2. The directory where logging will be done by Voltage DAM SQL Agent is determined.
3. The method of logging is determined ( **filestorage** | **msmq** ). Default **filestorage**.
4. When **msmq** logging is selected, **WEBSERVICEURL** should be entered and **TCP 1801, TCP 80** ports should be opened towards Voltage DAM Collector machine.
5. DSIM restart option.



## Introducing the Voltage DAM Agent

Voltage 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 recognise the agent, the agent must be added to the panel after installation and initial configuration must be made.

### Adding Voltage DAM Agent to the Panel

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

New Agent Wizard

### Connection

Enter the connection information to connect to the agent

IP Address: 192.168.1.74 : 8765

Protocol: TLS 1.2

#### Certificate

Use old default certificate  Use new default certificate  Upload certificate

Use old certificate  Use new certificate

Client Certificate:  Browse

Password:

CANCEL NEXT >

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 Voltage 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.

Ref.	Field	Function
5	pcap.devices	Comma-separated list of capture devices.

6	oracle.enabled	Enable captures on Oracle ports and Oracle parsing engine.
7	oracle.server_port	Comma-separated list of ports on which Oracle instances are working.
8	mysql.enabled	Enable captures on MySQL ports and MySQL parsing engine.
9	mysql.server_port	Comma-separated list of ports on which MySQL instances are working.

Ref.	Field	Function
10	hana.enabled	Enable captures on HanaDB ports and HanaDB parsing engine.
11	hana.server_port	Comma-separated list of ports on which HanaDB instances are working.
12	mongo.enabled	Enable captures on MongoDB ports and MongoDB parsing engine.
13	mongo.server_port	Comma-separated list of ports on which MongoDB instances are working.

14	cassandra.enabled	Enable captures on Cassandra ports and Cassandra parsing engine.
15	cassandra.server_port	Comma-separated list of ports on which Cassandra instances are working.
16	vertica.enabled	Enable captures on Vertica ports and Vertica parsing engine.
17	vertica.server_port	Comma-separated list of ports on which Vertica instances are working.
18	db2.enabled	Enable captures on DB2 ports and DB2 parsing engine.

**New Agent Wizard** [X]

## Listener Settings

Select the databases you want to collect logs

db2.server\_port: 50000

couchbase.enabled:

couchbase.server\_port: 4369

teradata.enabled:

teradata.server\_port: 1025

elastic.enabled:

elastic.server\_port: 9200

netezza.enabled:

netezza.server\_port: 5480

CANCEL   < BACK   NEXT >

Ref.	Field	Function
19	db2.server_port	Comma-separated list of ports on which DB2 instances are working.
20	couchbase.enabled	Enable captures on Couchbase ports and Couchbase parsing engine.
21	couchbase.server_port	Comma-separated list of ports on which Couchbase instances are working.

22	teradata.enabled	Enable captures on Teradata ports and Teradata parsing engine.
23	teradata.server_port	Comma-separated list of ports on which Teradata instances are working.
24	elastic.enabled	Enable captures on Elasticsearch ports and Elasticsearch parsing engine.
25	elastic.server_port	Comma-separated list of ports on which Elasticsearch instances are working.
26	netezza.enabled	Enable captures on Netezza ports and Netezza parsing engine.
27	netezza.server_port	Comma-separated list of ports on which Netezza instances are working.

**New Agent Wizard** [X]

## Listener Settings

Select the databases you want to collect logs

elastic.enabled

elastic.server\_port

netezza.enabled

netezza.server\_port

gauss.enabled

gauss.server\_port

sybase.enabled

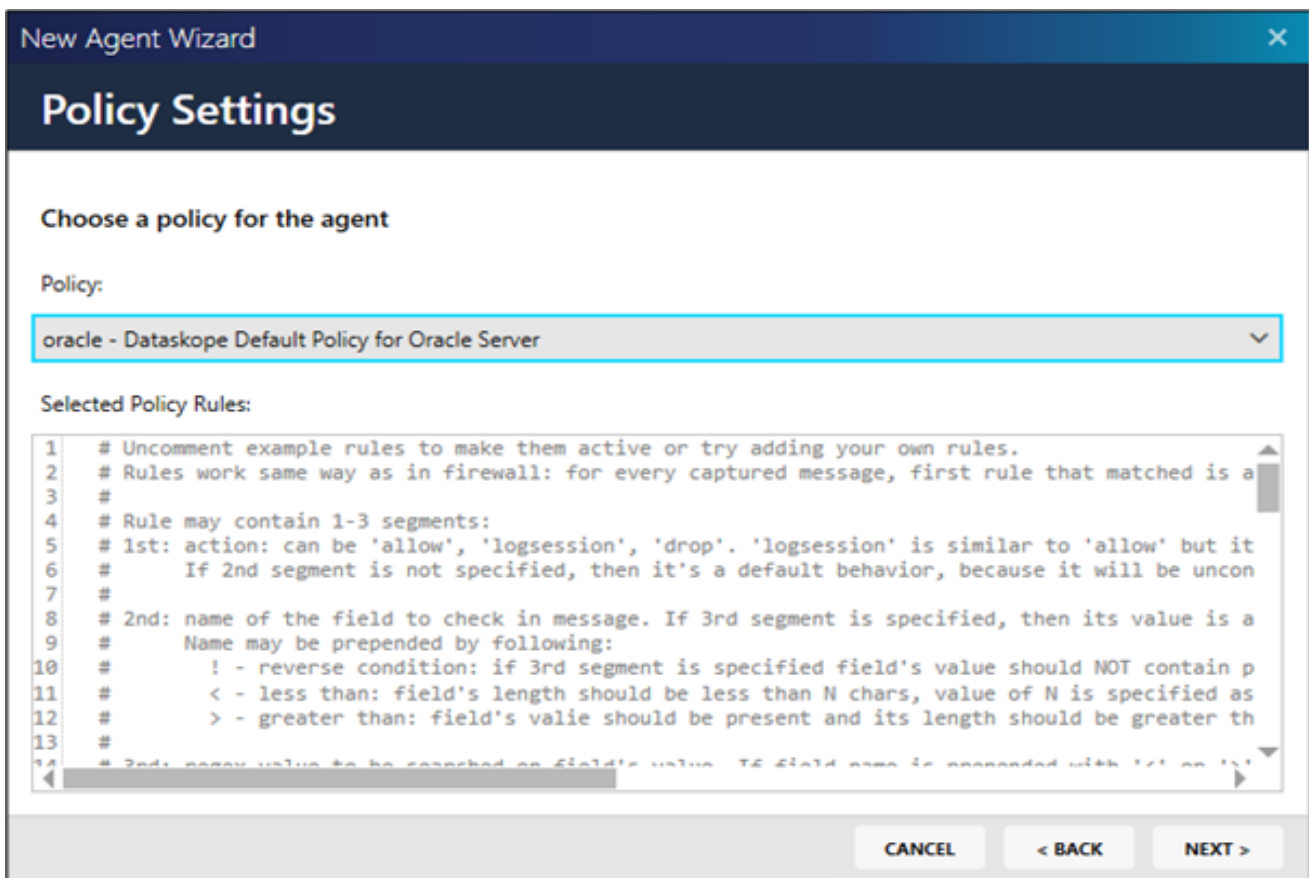
sybase.server\_port

msg.file.max\_age

CANCEL < BACK NEXT >

Ref.	Field	Function
28	gauss.enabled	Enable captures on GaussDB ports and GaussDB parsing engine.
29	gauss.server_port	Comma-separated list of ports on which GaussDB instances are working.
30	sybase.enabled	Enable captures on SybaseSQL ports and SybaseSQL parsing

		engine.
31	sybase.server_port	Comma-separated list of ports on which SybaseSQL instances are working.
32	Msg.file.max_age	Maximum file age in minutes before rotation.



**Policy Settings:** Voltage DAM agent logs or does not log the queries sent to the database according to the specified policies.



Ref.	Field	Function
1	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.
2	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
3	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.
4	Idle Threshold Minutes	When the Voltage DAM 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.
5	Suppress File Info Event Minutes	This is the event information that is sent whether the Voltage DAM 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.

6	Suppress Status Event Minutes	It is the event where Voltage DAM 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.
7	Tag	Allows adding a tag for distinctive use.

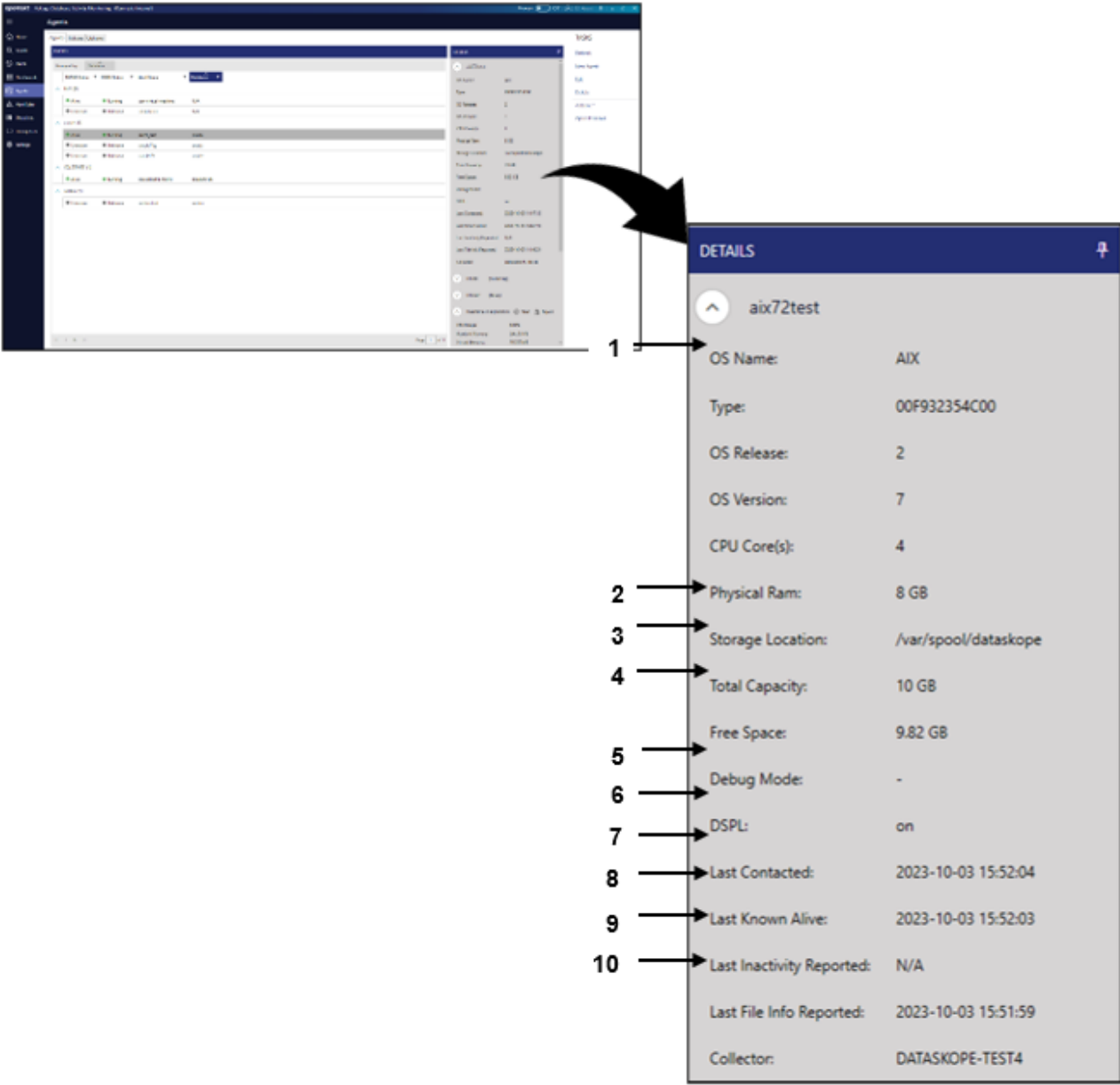
### Default Certificate

A generic client certificate can be defined for agents to use by default. This certificate can be created specifically for the organisation and protected with a password specific to the organisation. If this setting is made during the first installation, agents can be added to the panel using this certificate.

The screenshot shows the 'Agents' configuration page with tabs for 'Agents', 'Policies', and 'Options'. The 'Default Certificate' section is active. It contains two identical forms for different agent versions. The first form is for agents older than version 3.2.0.4084, and the second is for agents of version 3.2.0.4084 and higher. Each form includes a 'Certificate \*' field with the text 'dsim\_client.pfx file selected.' and a 'Remove' button, a 'Password \*' field with masked characters, and 'SAVE' and 'CANCEL' buttons.

### Voltage 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.

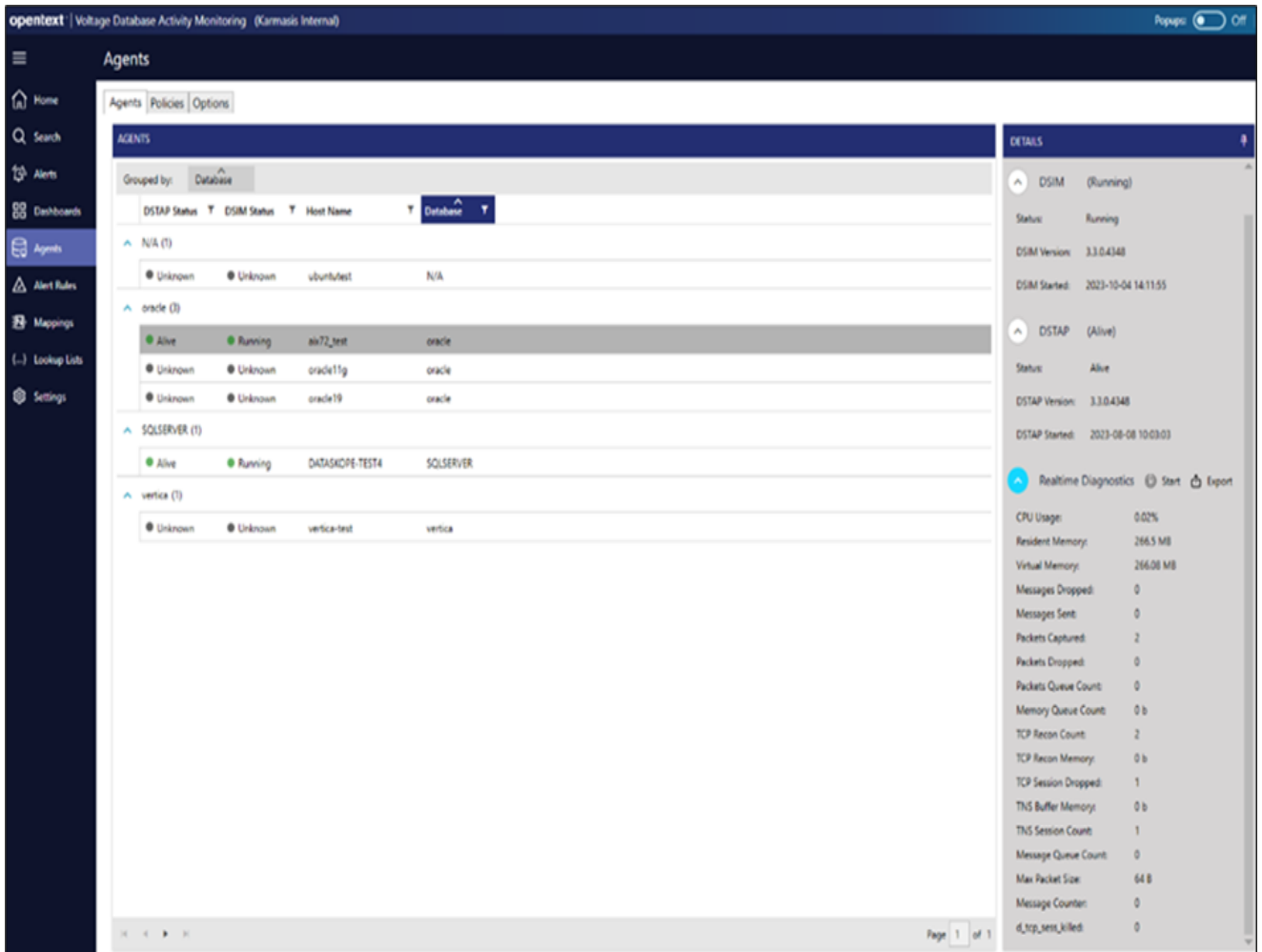


Ref.	Menu	Function
1	General Information [OS Name, Type, OS Release, OS Version, CPU Cores, Physical RAM]	The detail screen displays the operating system name, type, version, number of cores and physical memory information of the server.
2	Storage Location	On the detail screen, it is displayed in which directory on the server of the relevant agent to extract the message files. The default directory is /var/spool/dataskope directory.

3	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.
4	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.
5	DSPL	The DSPL status of the agent for the corresponding server can be displayed.
6	Last Contacted	The last time the agent contacted the collector can be displayed.
7	Last Known Alive	The last time the agent transmitted status information can be displayed.
8	Last Inactivity Reported	Used to show the last time the agent was inactive.
9	Last File Info Reported	Used to show when the agent last transmitted the file information in the logging directory.
10	Collector	Shows the hostname of the machine where Collector is installed.

## Advanced Configuration of the Voltage DAM Agent

DSIM and DSTAP operating states can be displayed, as well as real-time control of DSTAP can be performed and output.

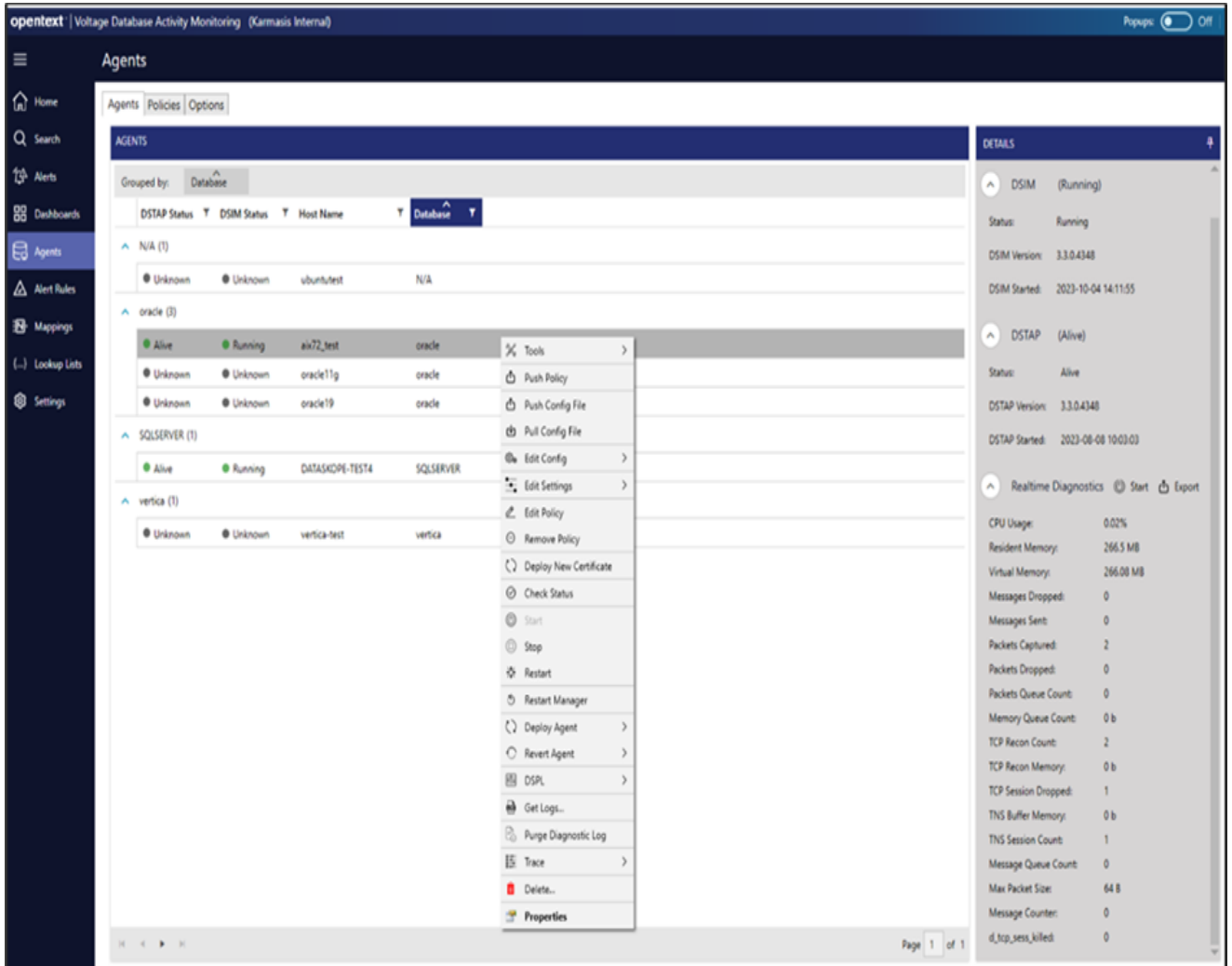


Ref.	Field	Function
1	CPU Usages	The CPU status used by the agent in real time can be observed.
2	Resident Memory	The memory state used by the agent in real time can be observed.
3	Virtual Memory	In addition to the current memory usage of the agent, it is used to show the memory state that can be used when necessary.
4	Messages Dropped	The number of messages that are not logged by the agent with the policy can be observed.
5	Messages Sent	The number of messages logged by the agent with the policy can be observed.
6	Packets Captured	Shows the number of TCP packets captured.

7	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.
8	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.
9	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.
10	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.
11	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.
12	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).
13	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.
14	TNS Session Count	Indicates the total number of sessions since the Voltage DAM agent last started. If there are ongoing sessions that occurred before the agent started, they are not counted.
15	Message Queue Count	The number of messages waiting in the queue can be observed.
16	Max Packet Size	The maximum package size processed by the agent can be observed.
17	Message Counter	Linux-based agents have switched to logging in timestamp logic after version 3413. Windows-based agents continue to work in counter logic.
18	d_tcp_sess_killed	Shows the number of killed TCP connections.

## Voltage DAM Agent Management Functions

Voltage DAM agents can be managed in detail without depending on the database administrator. Use right-click to reach detailed actions.



Ref	Field	Function
1	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.
2	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.
3	Push Config	It allows the agent's configuration files (dstap.conf, postfilter.conf etc.) to be

	File	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.
4	Pull Config File	It allows the agent configuration files (dstap.conf, postfilter.conf etc.) to be downloaded from the server.
5	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.
6	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.
7	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.
8	Remove Policy	The policy applied to the agent can be deleted and a new policy may be applied.
9	Deploy New Certificate	This is the certificate required to update agents above 4084 from the old version.
10	Check Status	The state of the agent can be observed with the corresponding property.
11	Start	An agent with DSTAP stopped can also be started with the corresponding feature.
12	Stop	DSTAP can be stopped for some reason with the corresponding feature.
13	Restart	DSTAP can be restarted with the corresponding feature for some reason.
14	Restart Manager	This is the DISM restart module.
15	Deploy Agent	Voltage DAM agents can be updated to the upper version of both DSIM and DSTAP through the panel without the need for a database administrator.
16	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.
17	DSPL	DSPL, which is specially developed for Linux-based agents, can be switched on and off via the panel.
18	Get Logs	All system log files of the agent can be retrieved via the panel.



19	Purge Diagnostic Log	All system log files of the agent can be reset via the panel.
20	Trace	It is the module used to monitor the traffic of packets.
21	Delete	The agent can be removed from the panel with the corresponding feature.
22	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.

DSIM Settings
— □ ×

---

Assigned

---

log.local.size

log.local.count

log.verbosity

msg.storage.location

---

Unassigned

---

ctrl.address

ctrl.port

ctrl.timeout

ctrl.max\_clients

ctrl.proto

cert.pass

dstap.path

dstap.params

dstap.autostart

dstap.kill\_timeout

msg.storage.reserve

msg.file.lock\_timeout

msg.file.force\_delete

watchdog.hang\_restart

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

3	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)
4	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.
5	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.
6	ctrl.port	This is the port information that the DSIM control interface will listen to.
7	ctrl.timeout	This is the information after how many minutes the inactive sessions will be dropped. (Min:1dk, Max:1440dk)
8	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)
9	ctrl.proto	
10	cert.pass	It is the password of dsim_server.pfx certificate.
11	dstap.path	The default directory information of DSTAP binary files.
12	dstap.params	Initial parameters can be transmitted to DSTAP. Reserved for future use.
13	dstap.autostart	Here you can select whether or not to start DSTAP automatically at system start up.
14	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)
15	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)
16	msg.file.lock_timeout	It is the information when the message file will be locked.
17	msg.file.force_delete	Indicates whether a locked message file will be forcibly deleted or not. It is off by default.
18	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.

The screenshot shows a window titled "DSTAP Settings" with the following parameters and values:

- pcap.buffer\_size: 128M
- pcap.buffer\_delay: 1000
- pcap.snap\_size: 80K
- pcap.promisc:
- pcap.devices: \*
- pcap.extra\_filter:
- cpu.queue\_reset:
- pcap.log\_drops:
- pcap.trace.enabled:
- pcap.trace.device:
- pcap.trace.filter:
- pcap.trace.max\_size: 32M
- dspl.enabled:
- tcp.session.timeout: 86400
- tcp.session.save\_state:
- tcp.session.save\_template:
- oracle.enabled:
- oracle.server\_port: 1521
- oracle.parse\_nums:
- mysql.enabled:
- mysql.server\_port: 3306
- postgre.enabled:
- postgre.server\_port: 5432
- mssql.enabled:
- mssql.server\_port: 1433

Buttons for "SAVE" and "CANCEL" are located at the bottom right of the window.

Ref.	Menus (Assigned)	Function
1	pcap.buffer_size	The size of the pcap temporary buffer memory for each device. (Min:16MB, Max:256MB)

2	pcap.buffer_delay	
3	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)
4	pcp.promisc	
5	pcap.devices	The information of the devices monitored by DSTAP (can be viewed on the relevant server with the <b>dstap -l</b> command output). A new device can be added by separating it with a comma from the setting screen. Then DSTAP will restart itself automatically.
6	pcap.extra_filter	Extra filter for pcap driver, helps to drop unrelated traffic on early stage.
7	cpu.queue_reset	Reset the queue after it reaches 8M entries.
8	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.)
9	pcap.trace.enabled	Enable tracing of pcap packets.
10	pcap.trace.device	A device to do a trace capture on.
11	pcap.trace.filter	Filter for trace session.
12	pcap.trace.max_size	Maximum trace file size to grow.
13	dspl.enabled	This is the status information whether DSPL is enabled or not during the operation of DSTAP.
14	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)
15	tcp.session.save_state	Save session state data upon app exit and resume them on restart.
16	tcp.session.save_template	Save client-specific state data for use with break-in session from same address.
17	oracle.enabled	This is the status of enabling Oracle port and decomposition mechanism.
18	oracle.server_port	Oracle ports are listened by DSTAP. If there is a special port, it can be added using a comma.
19	oracle.parse_nums	Parse numeric parameters.

20	mysql.enabled	This is the information about the status of enabling MySQL port and decomposition mechanism.
21	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.
22	postgre.enabled	This is the status information for enabling the PostgreSQL port and decomposition mechanism.
23	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.
24	mssql.enabled	This is the status information for enabling MSSQL port and decomposition mechanism.
25	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.

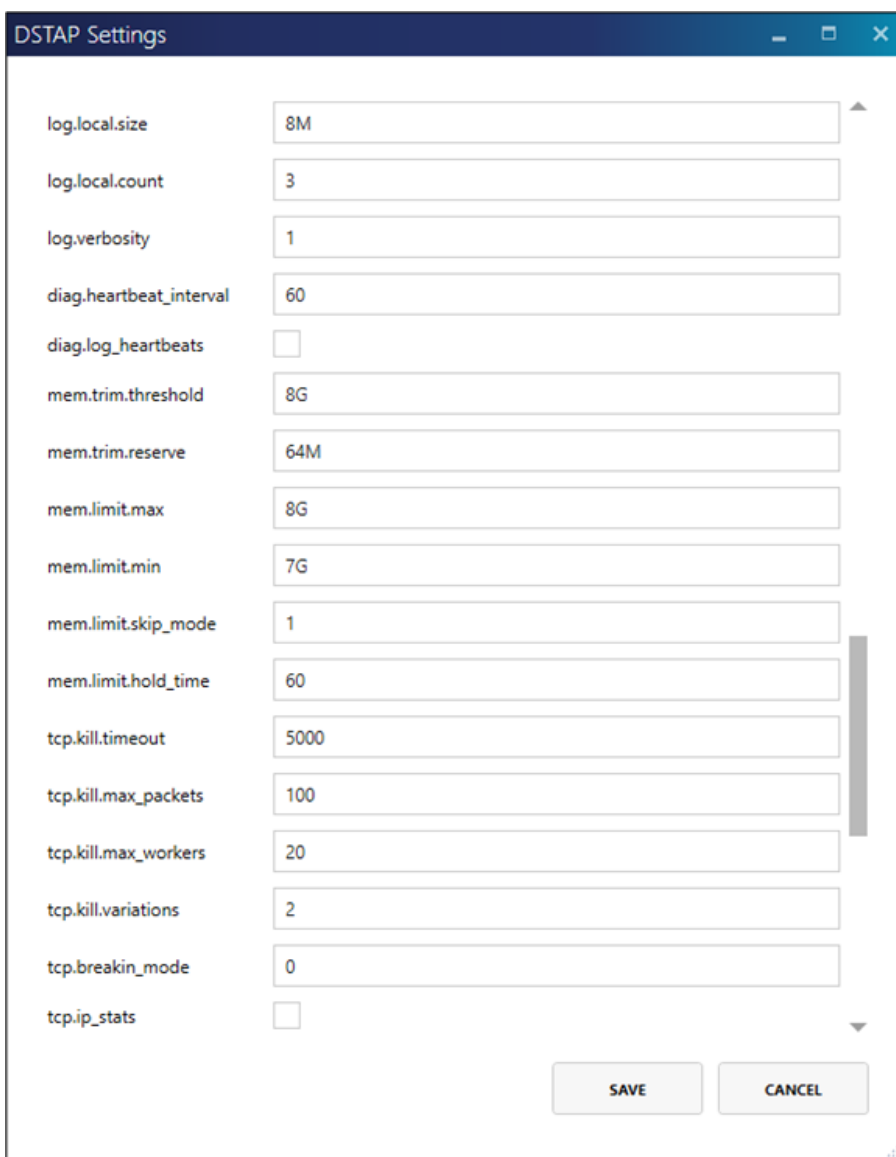
The screenshot shows the 'DSTAP Settings' window with the following configuration options:

- hana.enabled:
- hana.server\_port: 39015
- mongo.enabled:
- mongo.server\_port: 27017
- mongo.max\_docs: 100
- cassandra.enabled:
- cassandra.server\_port: 9042
- vertica.enabled:
- vertica.server\_port: 5433
- db2.enabled:
- db2.server\_port: 50000
- couchbase.enabled:
- couchbase.server\_port: 4369
- teradata.enabled:
- teradata.server\_port: 1025
- elastic.enabled:
- elastic.server\_port: 9200
- elastic.max\_body: 32K
- netezza.enabled:
- netezza.server\_port: 5480
- gauss.enabled:
- gauss.server\_port: 1888
- sybase.enabled:
- sybase.server\_port: 5000

Buttons: SAVE, CANCEL

Ref	Menus	Function
26	hana.enabled	This is the status information for enabling the HANA port and decomposition mechanism.
27	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.
28	mongo.enabled	This is the status information for enabling the Mongo port and decomposition mechanism.
29	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.
30	mongo.max_docs	Maximum number of documents in query payload to process.
31	cassandra.enabled	Enable capture on Cassandra ports and Cassandra parsing engine.
32	cassandra.server_port	Comma-separated list of ports on which Cassandra instances are working.
33	vertica.enabled	Enable capture on Vertica ports and Vertica parsing engine.
34	vertica.server_port	Comma-separated list of ports on which Vertica instances are working.
35	db2.enabled	Enable capture on DB2 ports and DB2 parsing engine.
36	db2.server_port	Comma-separated list of ports on which DB2 instances are working.
37	couchbase.enabled	Enable capture on Couchbase ports and Couchbase parsing engine.
38	couchbase.server_port	Comma-separated list of ports on which Couchbase instances are working.
39	teradata.enabled	Enable capture on Teradata ports and Teradata parsing engine.
40	teradata.server_port	Comma-separated list of ports on which Teradata instances are working.
41	elastic.enabled	Enable capture on Elasticsearch ports and Elasticsearch parsing engine.
42	elastic.server_port	Comma-separated list of ports on which Elasticsearch instances are working.
43	elastic.max_body	Maximum body length to capture.
44	netezza.enabled	Enable capture on Netezza ports and Netezza parsing engine.
45	netezza.server_port	Comma-separated list of ports on which Netezza instances are

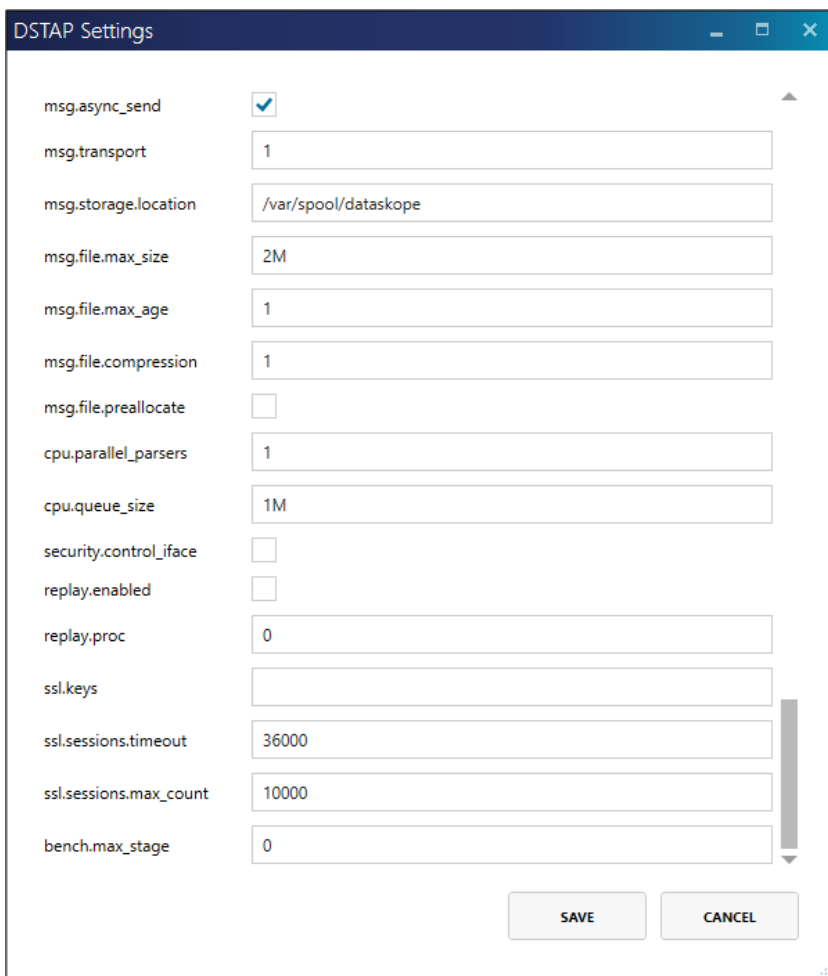
		working.
46	gauss.enabled	Enable capture on Gauss ports and Gauss parsing engine.
47	gauss.server_port	Comma-separated list of ports on which Gauss instances are working.
48	sybase.enabled	Enable capture on Sybase ports and Sybase parsing engine.
49	sybase.server_port	Comma-separated list of ports on which Sybase instances are working.



Ref	Menus	Function
-----	-------	----------



50	log.local.size	The maximum size of the DSTAP log file.
51	log.local.count	The number of rotations of the DSTAP log file.
52	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)
53	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)
54	diag.log_hearthbeats	This is the status information for enabling health status logs in DSTAP log.
55	mem.trim.threshold	The shaving mechanism is activated when the memory value assigned to the agent is exceeded.
56	mem.trim.reserve	This is the information about the size of the shaved memory. (Min:32MB, Max:256MB)
57	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.
58	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.
59	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)
60	mem.limit.hold_time	Amount time of in seconds before restarting app if skip_mode=2 and memory limit is reached.
61	tcp.kill.timeout	Time slice given to TCP kill worker to termice the TCP session.
62	tcp.kill.max_packets	Number of RST packets to send before giving up.
63	tcp.kill.max_workers	Max number of parallel workers for killing TCP session.
64	tcp.kill.variations	Number of SEQ/ACK variations to use per packet.
65	tcp.breakin_mode	Behaviour for break-in TCP sessions.0=ignore break-in sessions, 1= kill break-in sessions.
66	tcp.ip_stats	Collect IP stats.



Ref	Menus	Function
67	msg.async_send	Synchronous or asynchronous execution can be specified.
68	msg.transport	It is the information to determine the message creation method. By default, it is file based. (1=local file, 2=syslog)
69	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.
70	msg.file.max_size	Maximum file size for rotation. (Compressed. Raw data will be much larger than seen. (Min:1MB, Max:16MB)
71	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 Voltage DAM in a shorter time, this value can be reduced to 1 minute. (Min:1, Max:1440)
72	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)
73	msg.file.preallocate	Enables a preliminary field assignment during message file creation. It is switched off by default.
74	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.
75	cpu.queue_size	
76	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.
77	replay.enabled	Enable replay interface.
78	replay.proc	Replay processor to use. 0=use own processor, 1=use main parallel processor, if parallel parsers are enabled.
79	ssl.keys	Flat list with comma-separated pairs.
80	ssl.sessions.timeout	Expiry interval in seconds for saved ssl session id/key.
81	ssl.sessions.max_count	Maximum number of saved sessions.
82	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.

Edit Policy
\_ □ ×

Name \*

Dataskope Default Policy for Windows MS SQL Server - test1

Database \*

SQLSERVER
▾

Description

Rules

```

14 #
15 # NO SPACES ALLOWED IN 1st AND 2nd segment, ONLY IN 3rd SEGMENT (AS A PART OF REGEX).
16
17 #drop EVERYTHING from the program name ending with 'toad.exe'
18 #drop|client_app_name|Toad\.exe$
19
20 #allow SL (SELECT) action for everything else
21 #allow|action_id|^SL$
22
23 #drop capture which has no query field or if it's empty
24 #drop|!sql_text
25
26 #drop capture has query length greater than 1KB
27 #drop|>sql_text|1024
28
29 #allow any query that contains 'select'
30 #allow|sql_text|select
31
32 #deny any query that contains 'into '
33 #drop|sql_text|into
34
35 ##Drop logs based on Client IP & DB User
36 #drop|client_ipaddr|192.168.1.10|192.168.2.11
37 #+
38 #drop|username|service_user1
39
40 ##Drop logs based on Client IP and SQL statement
41 #drop|client_ipaddr|192.168.1.10
42 #+
43 #drop|sql_text|select|update
44
45 ##Drop Infraskope ES Api
46 #drop|client_app_name|Api
47 #+
48 #drop|query|ElaSessionLog
49
50 ##Default Allow Rule for MSSQL DB
51 allow
52

```

TEST RULE

IMPORT

SAVE

CANCEL

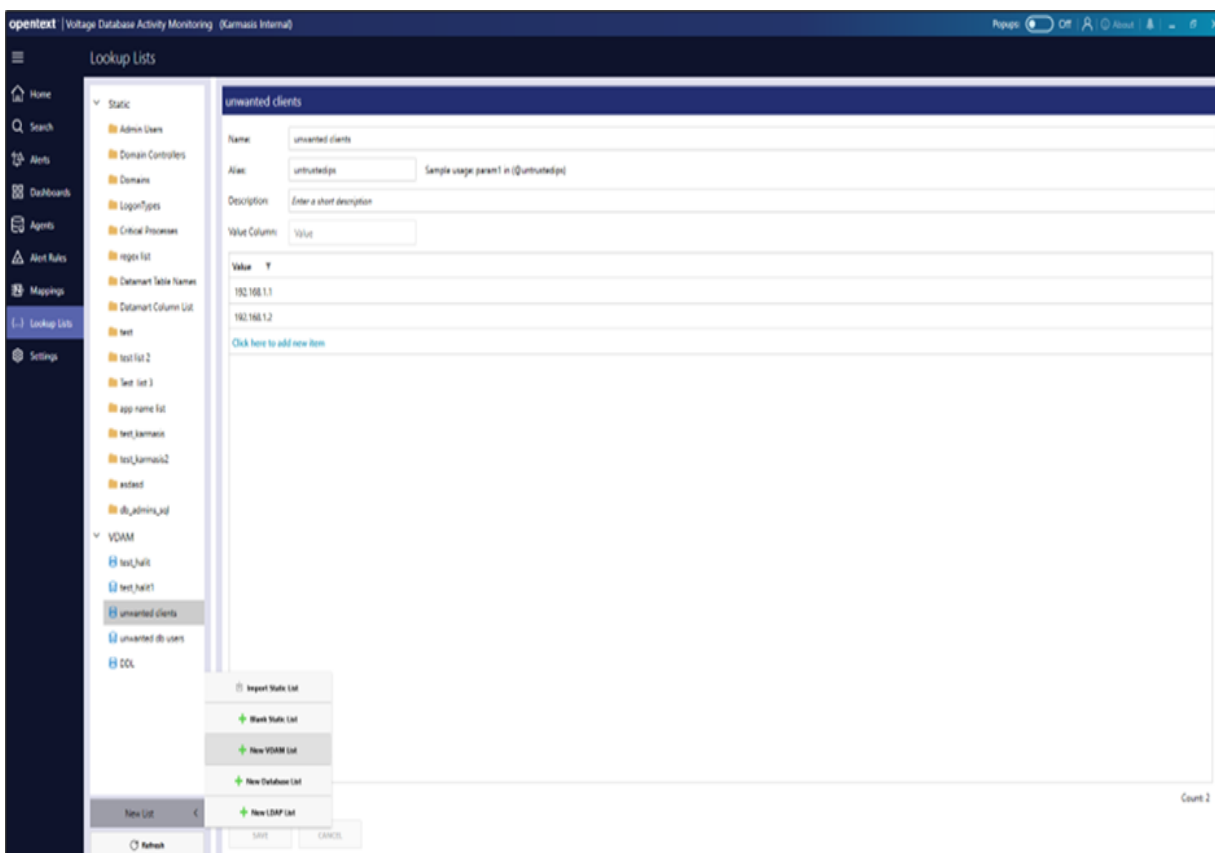
Ref.	Menus	Function
1	Policy Name	A name can be assigned to the created policy.
2	Policy Database	It is the information to which database the created policy belongs. It cannot be changed afterward. A new policy must be created to change it.

Voltage Database Activity Monitoring (23.4.0)

Page 44 of 49

	Type	
3	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, Voltage 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
4	Test Rule	The correctness of a written policy can be tested using this tool.
5	Policy Import	A policy written in text format can be uploaded and saved with this tool.

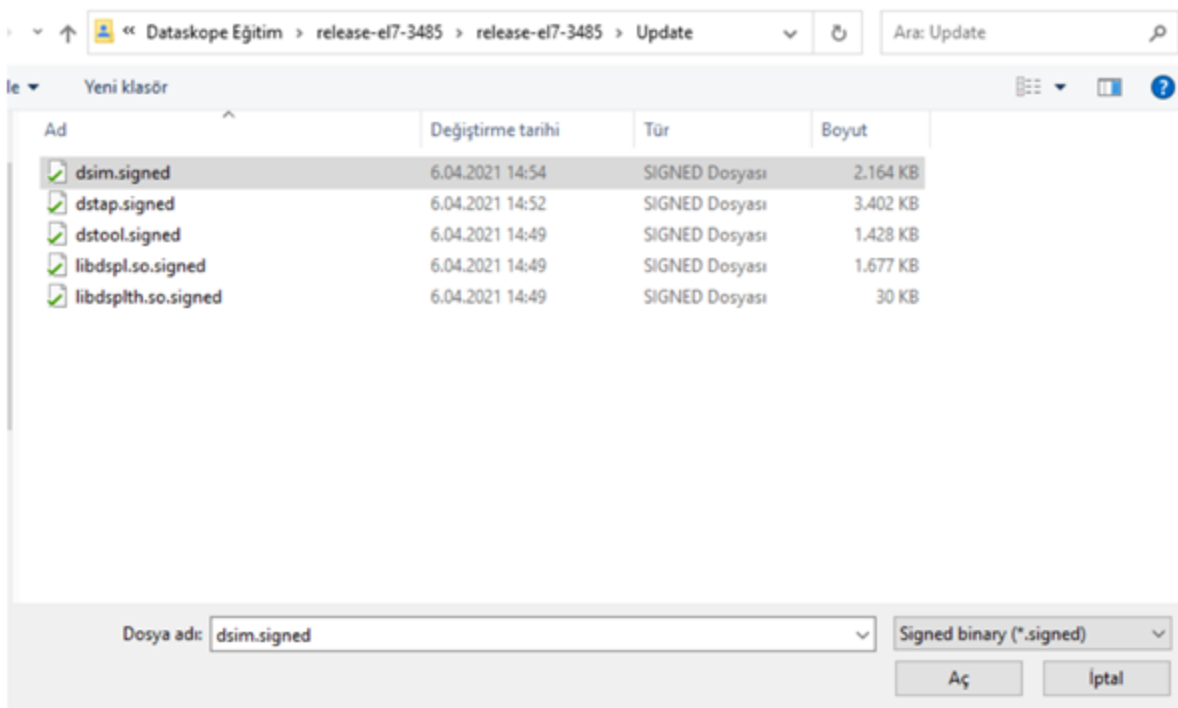
## New Voltage DAM List



- A new Voltage 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, the dsim.signed file must be selected and sent.



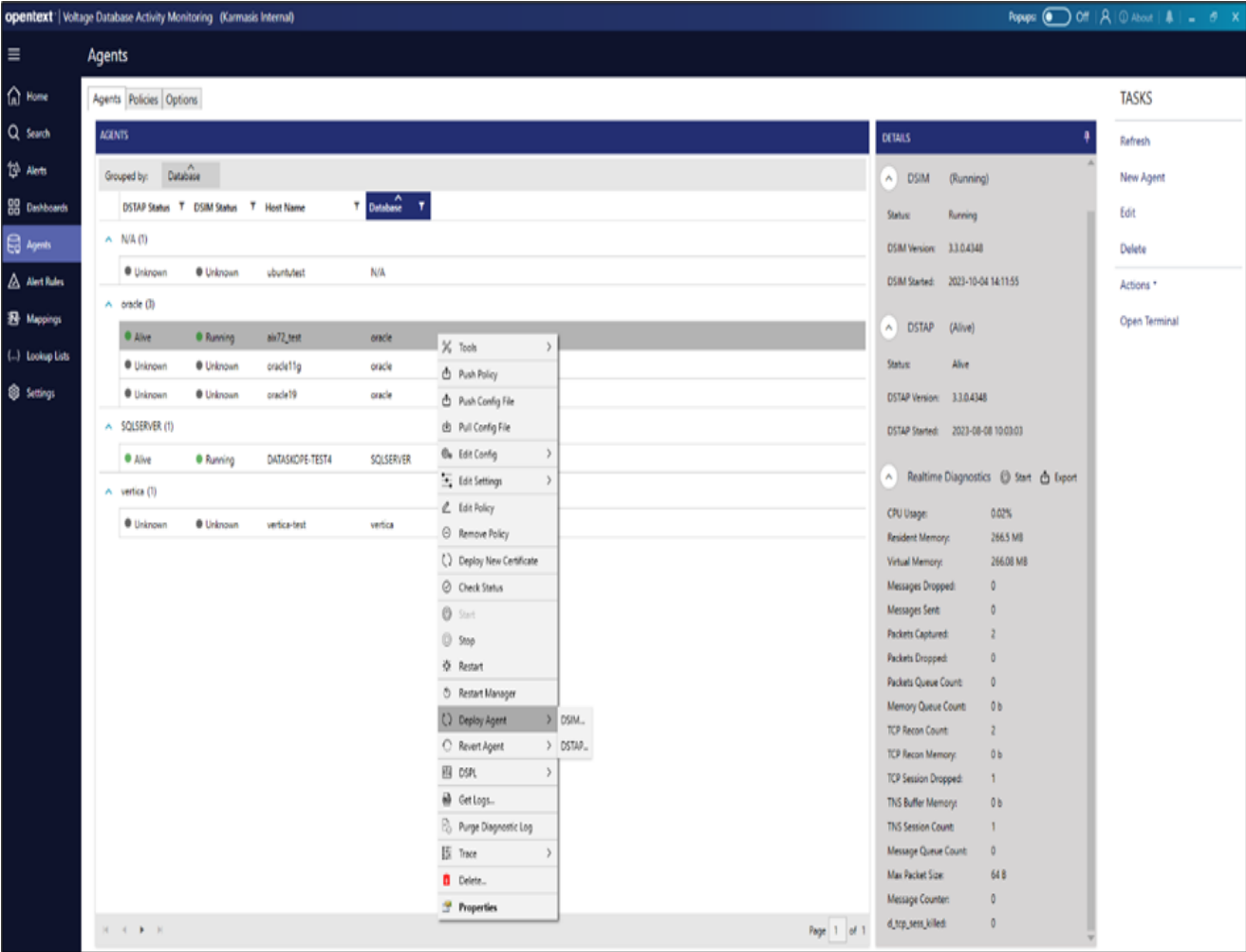
## Upgrading DSTAP to Upper Version

When updating DSTAP on Linux based systems, dstap.signed, dstool.signed, libdspl.so.signed, libdsplth.so.signed files should be selected, converted to .zip format and sent.

Ad	Değiştirme tarihi	Tür	Boyut
<u>dstap.signed</u>	6.04.2021 14:52	SIGNED Dosyası	3.402 KB
dstap.zip	11.06.2021 14:03	Sıkıştırılmış Klasör	2.530 KB
<u>dstool.signed</u>	6.04.2021 14:49	SIGNED Dosyası	1.428 KB
<u>libdspl.so.signed</u>	6.04.2021 14:49	SIGNED Dosyası	1.677 KB
<u>libdsplth.so.signed</u>	6.04.2021 14:49	SIGNED Dosyası	30 KB

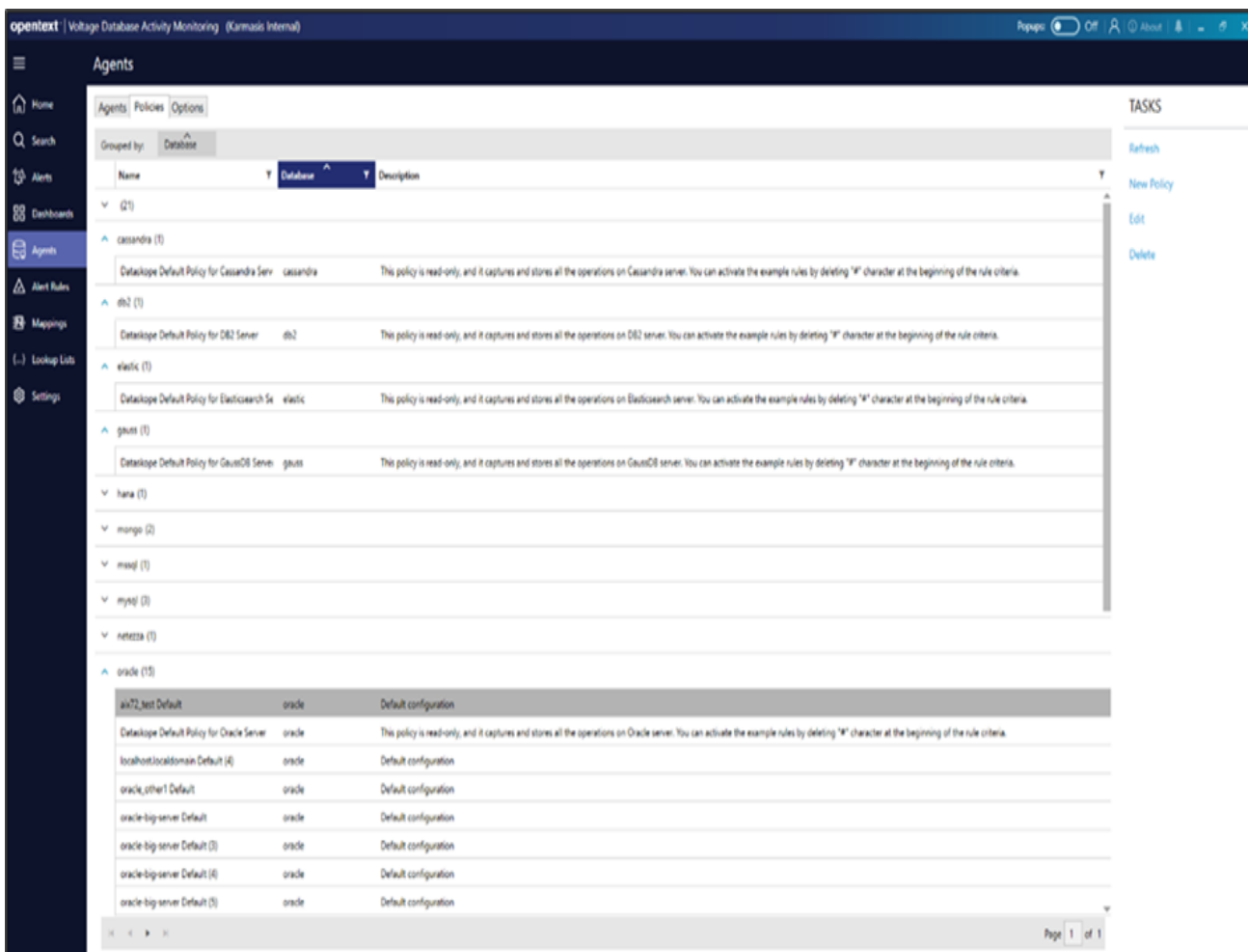
## Upgrading Windows Agent to the Upper Version

Windows 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.



# 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|xxxxxx.
- If many usernames are to be dropped, the spelling should be as follows; drop|username|xxxxxx|yyyyyy|zzzzzz
- Many variations can be created by connecting with "+".

For example,

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



```
drop|db_user|yyyyyy  
+  
drop|client_ip|zzz.zzz.zzz.zzz
```

**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 Voltage 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 Voltage 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|xxxxxx  
+  
allow|client_ip|yyy.yyy.yyy.yyy
```