CLEONDRIS

Cleondris Technical Implementation Note | TIN-94

Cleondris DMT (Data Manager Tools) Deployment Guide

[Version 2020-03-27]

Cleondris GmbH, Switzerland

March 2020

IMPORTANT

The information given in this technical implementation note represents current internal planning for Cleondris and can be subject to further changes without further notice. As such, this document is subject to change and may be changed by Cleondris at any time without notice. The information is not intended to be binding upon Cleondris to any particular course of business, product strategy and/or development.

Table of Contents

1 Overview

The Cleondris Data Manger Tools (DMT) is a software agent component that allows to distribute the logic of Cleondris software over a cluster of computers. DMT is available for Linux[1] and Microsoft Windows. Specifically, DMT can be used in the following scenarios:

- Deployment of FPE (FPolicy Engines) to Linux and Windows hosts
- Quiescing (during Snapshot backup) of Oracle Databases running on Linux hosts
- Execution of scripts during HCI failover

The communication between a centralized Cleondris appliance (running, for instance, the Cleondris SnapGuard or Cleondris Data Manager software) and an attached DMT agent is over an encrypted SSL connection via TCP port 7683. This port has been assigned by IANA to Cleondris exclusively for this task[2]. Communication is always initiated by the Cleondris appliance.

A common problem of distributed agent setups is an increased management complexity due to the need of keeping the software versions of agents in-sync with the centralized application using them. However, this is not the case with DMT. The installation of DMT is merely a basic container/runtime with the agent infrastructure. The actual application logic is only present in memory and will be pushed by the Cleondris appliance as needed. Therefore, the version of the application logic in the agent always matches the version of the Cleondris appliance that is controlling the agent. Rigorous use of software certificates and a public/private key infrastructure ensures that only software certified by Cleondris can be dynamically pushed into the agent's memory.

2 Installation on Microsoft Windows

2.1 Prerequisites / Requirements

To be able to install the DMT software, the following prerequisites are needed:

- A copy of the DMT installer binary for Windows
- A Windows host (physical or virtual) running a 64-bit copy of Microsoft Windows (Microsoft 7/8/10, Microsoft Windows Server 2008 or newer)
- Administrative access to this machine (i.e., ability to install software, edit config files, start/stop Windows services and access the Windows event log).
- Access to a Cleondris appliance (to be able to test the setup)
- An agent-specific password must be chosen that is shared between the agent and the Cleondris appliance

[1] Linux support is experimental. Please use the Windows version in production setups.
[2] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

2.2 Installation Procedure

- Log into the Windows host using an administrative account
- Download the DMT installer from the Cleondris website (or a local repository, if the host has no Internet access)
- The installer is digitally signed with a certificate issued to "Cleondris GmbH".
- If the signature is missing or has been tampered with, do not execute the installer and immediatelly contact Cleondris support.
- Run the installer
- Carefully read the license agreement and accept it if you agree to it. Otherwise abort the installation and contact Cleondris.
- Whenever possible, accept the default installation path[3]. If you cannot accept the path, please contact Cleondris support, we would like to know why it is not acceptible.
- The installation takes place (the Windows UAC dialog may show up) and automatically starts the DMT service and registers the needed event source and the incoming firewall rule.
- After the installation has finished, all the components are in place, however, the DMT service won't accept connections from outside. You need to setup a configuration first.

2.3 Configuring the DMT agent

To configure the agent, a config file needs to be put in place.

- Either open the configuration directory manually using Windows Explorer[4] or alternatively use the Windows "Start" menu and navigate to "Cleondris → Data Manager Tools → Configuration".
- Please copy the supplied example configuration file "dmt_example.conf" to a new file called "dmt.conf".
- Now edit the "dmt.conf" file, you may need to start your text editor explicitly as an administrator to be able to save the changes.
- At minimum, you need to set a value for the "password" entry (do not forget to remove the hash (#) sign used to comment the example password line).
- For testing purposes, the supplied "ssl_example.crt" and "ssl_example.key" can be used. However, if you plan to the use the DMT agent in a production environment, you *must* generate a custom private key and a SSL certificate for each DMT agent installation. Please use different file names (e.g., "ssl.crt" and "ssl.key") and adapt the "dmt.conf" accordingly, since the supplied example SSL files may be overwritten during a later update of the DMT installation. If you do not use your own SSL private key/certificate, the communication (including the shared password) can be easily decrypted by an attacker that has access to the local network.

[3] C:\Program Files\Cleondris\Data Manager Tools
[4] C:\Program Files\Cleondris\Data Manager Tools\Config

- Everytime you change the config file, the DMT Windows service needs to be restarted. Simply open the Windows Services panel and restart the "Data Manager Tools" service.
- The DMT service logs event messages to the Windows application log. Open the Windows event viewer to verify that the agent has accepted the configuration and is listening on port 7683 for incoming control connections.

2.4 Testing the DMT installation

- Please verify in the Windows event viewer that the agent has properly started up and is accepting incoming connections.
- Open the web GUI of your Cleondris appliance and register the host running the DMT software using the "Setup → Hosts" menu. You must set the "DMT password" field.
- The host will automatically be scanned and is visible in the "Inventory" view.

2.5 Upgrading the DMT agent

The DMT core software (DMT Windows service) is stable and Cleondris only releases very few updates for the core agent infrastructure. However, if you are supplied with a new release of the DMT agent, you can simply proceed like during the initial installation. Simply double-click the installer and proceed with the installation. The Windows installer automatically stops the existing DMT service, replaces all components and then restarts the DMT service. Files not present during the initial installation ("dmt.conf" and your custom SSL private key/certificate) won't be touched by the installer.

Very important: please close the Windows event viewer during an upgrade of the DMT service installation, otherwise the DMT service binary may be locked and Windows Installer asks you to restart the computer after the upgrade.

2.6 Removing the DMT agent

You can remove the DMT agent using the Windows "Uninstall a program" feature. The DMT agent has a complete integration with Windows Installer and is correctly registered in the Installer database.

Please close the Windows event viewer during a removal of the DMT service installation, otherwise the DMT service binary is locked and Windows Installer asks you to restart the computer after the removal.

After the uninstallation of the DMT software, the configuration directory will remain on the computer, since it contains components that were not installed by Windows installer. Typically, this is the "dmt.conf" file and your local SSL key/certificate. You can remove these files (or the complete configuration directory including its parent directory[5]) with Windows Explorer.

[5] C:\Program Files\Cleondris\Data Manager Tools\Config

3 Installation on Linux

3.1 Prerequisites / Requirements

To be able to install the DMT software on Linux, the following prerequisites are needed:

- A copy of the DMT installer package for Linux
- A Linux host (physical or virtual) running a 64-bit copy of one of the following Linux distributions:
  - CentOS 7.x / 8.x
  - RedHat Enterprise Linux (RHEL) 7.x / 8.x
  - Oracle Linux 7.x / 8.x
- Current DMT releases require the "selinux" feature to be disabled on the Linux host.
- Administrative access to this machine (i.e., ability to login via SSH and to install software, edit config files, start/stop services and have access to log files as well as to the systemd journal).
- Access to a Cleondris appliance (to be able to test the setup)

3.2 Installation Procedure

- Download the DMT installer from the Cleondris website and transfer it to the Linux host, e.g., via SCP upload to the "/tmp" directory.
- Log into the Linux host using SSH and become root user ("sudo su –").
- Unpack the archive:

```
# cd/root
# tar xzvf /tmp/cleondris-dmt-installer-2020XYZ.tar.gz
# cd cleondris-dmt-installer
# cat EULA.txt
```

- Carefully read the license agreement – only continue you agree to it. Otherwise abort the installation and contact Cleondris.
- Start the installer and follow the instructions:

```
# sh INSTALL.sh
```

- Please carefully note down the random password that has been created as part of the execution of the installation script, it will be shown to you by the installer. This password is needed when registering the DMT in the Cleondris appliance.
- At the end, do not forget to cleanup and remove the installer files:

```
# rm -f /tmp/cleondris-dmt-installer-2020XYZ.tar.gz
# rm -Rf /root/cleondris-dmt-installer
```

3.3 Testing the DMT installation

- Open the web GUI of your Cleondris appliance and register the Linux host running the DMT software using the "Setup → Hosts" menu. You must set the "DMT password" field based on the password string that was generated during the installation.

- The host will automatically be scanned on a regular basis and is visible in the “Inventory” view.

3.4 Removing the DMT agent

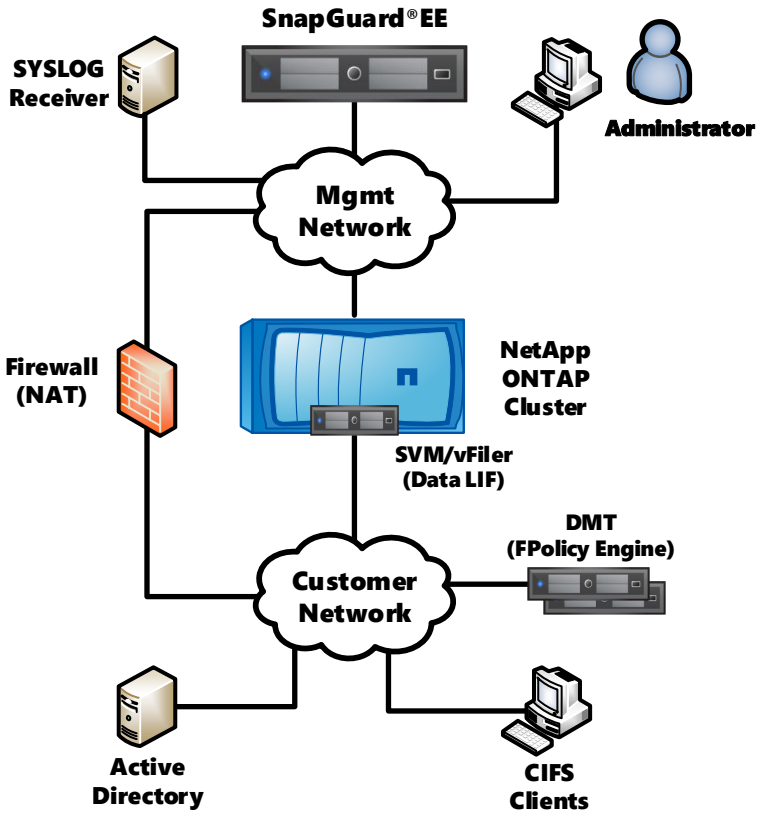
Please login via SSH as root user and execute the following commands:

```
# systemctl stop cleondris-dmt.service
# systemctl disable cleondris-dmt.service
# rm -f /etc/systemd/system/cleondris-dmt.service
# systemctl daemon-reload
# rm -Rf /opt/cleondris/dmt
```

4 NetApp FPE considerations in Provider Setups

Various Cleondris products have support for the NetApp FPolicy feature, and the Cleondris DMT can act as an external FPolicy Engine (FPE).

A typical use case of an FPE running on the Cleondris DMT, are Providers that offer CIFS services via NetApp SVM/vFilers to a larger set of customers. They can use multiple DMT installations (for scalability and traffic separation) to implement per-customer FPEs that run inside the customer networks. The network diagram (showing only a single customer) looks as follows:



To be able to setup the FPE running on the DMT, and to receive firewall events, regular communication between the central SnapGuard instance (running on the Cleondris appliance) and the DMT running inside the customer's network is needed. Also, in case SnapGuard shall be able to resolve CIFS SID/usernames, communication with the customer's active directory must be allowed.

The following table lists the TCP connections where the DMT agent is involed. Source and target columns indicate how a TCP connection is being established, the listed ports always refer to the target.

Source	Target	Protocol	Use
SnapGuard <-> DMT Communication			
SnapGuard	FPolicy Engine running on DMT	SSL via TCP port 7683	FPE configuration, event polling via Cleondris proprietary protocol

SID lookups performed by the FPE running on DMT			
FPolicy Engine running on DMT	AD (Active Directory) Servers	MSRPC/SMB2 via TCP port 445	SID/username lookups
File verification performed by the FPE running on DMT (optional)			
FPolicy Engine running on DMT	SVM Data Interface	SMB2 via TCP port 445	File verification
FPolicy Communication with Clustered Data ONTAP			
cDot ONTAP SVM Data-LIF	FPolicy Engine running on DMT	XML via TCP port 10000-10099	FPolicy Events via NetApp proprietary protocol
FPolicy Communication with 7-Mode Data ONTAP			
7-Mode vFiler Interface	FPolicy Engine running on DMT	SMB1 or SMB2 via TCP port 445	FPolicy Events via NetApp proprietary protocol over CIFS/DECRPC
FPolicy Engine running on DMT	7-Mode vFiler Interface	SMB2 via TCP port 445	Registration for 7-Mode FPolicy via NetApp proprietary protocol over CIFS/DECRPC

- Note 1: if NetApp cDot vScan servers are in use, it is possible to share resources and install DMT on the same hosts (if they are powerful enough).
- Note 2: Syslog events are always delivered by SnapGuard on behalf of the FPE running on DMT. DMT never communicates directly with the Syslog infrastructure.
- Note 3: DMT always uses SMB2 to communicate with AD controllers and 7-mode filers. However, 7-mode filers communicate with AD controllers and FPolicy servers either using SMB1 or SMB2, depending on the setting of the filer option "*cifs.smb2.client.enable*".

5 NetApp 7-mode FPE considerations

When using DMT to run an external NetApp 7-mode FPE (FPolicy engine), certain additional configuration of the Windows system is needed (7-mode FPEs must be running on Windows, Linux is not supported), so that the NetApp ONTAP FPolicy filter can communicate with the external FPolicy engine running inside the DMT.

Please read the following carefully. Performing indicated changes is at your own risk.

- To be able to register as an external fpolicy server, the Cleondris FPE running inside DMT needs to establish an SMB2 connection with the filer. Hence, SMB2 needs to be enabled on the filer (*options cifs.smb2.enable = on*). Also, the filer must be joined to a domain (otherwise it very likely won't be able to receive SMB2 connections) and must be on the same domain as the computer running DMT.

- The credentials for the SMB2 connection used by the FPE have to be set in the per-SVM firewall setup screen in SnapGuard (fields "*7-Mode CIFS Username*" and "*7-Mode CIFS Password*"). Enter a domain user in the format "*domain**user*", alternatively enter a local NetApp account using the format "*user*". Please ensure that the user is member of the local "*backup*" group on the NetApp system. You must enter these credentials, the FPE *never* uses the credentials of the Windows user that runs the underlying DMT software.

- To receive FPolicy screen requests, the filer needs to establish an SMB connection back to the FPE (the filer uses either SMB1 or SMB2, depending on its setting of the "*cifs.smb2.client.enable*" option). Since the DMT runs on Microsoft Windows, it has to use the Windows built-in SMB server (port 445 cannot be shared) to accept this SMB connection. Please note that the FPE tries to guess its main IP automatically, and then tells the filer to establish the SMB connection to this address. To override the IP address where the SMB connection shall be initiated to (i.e., an IP interface on the Windows host which must be accessible from the data interface of the respective 7-mode vfiler), use the optional field "*7-Mode Host override*" in the per-SVM firewall setup screen in SnapGuard. **Optimally, you should use the NETBIOS hostname and not the IP address of the DMT host when setting "*7-Mode Host override*", especially if you have enabled the option "*cifs.netbios_over_tcp.enable*" on the 7-mode filer.**

- After the 7-mode filer has established a connection with the FPolicy server via SMB, it wants to open an SMB pipe anonymously. This behavior cannot be changed, and by default, Windows does not accept anonymous connections to named pipes. You therefore need to change two security settings on the Windows system that runs DMT. Please be aware that this weakens the security of the used Windows computer, but again, this is a restriction of 7-mode FPolicy. Do this at your own risk and in doubt contact your local Windows administrator.
    - Click Start > Administrative Tools > Local Security Policy.
    - Look for "Local Policies" (expand), click "Security Options", scroll down.
    - Set "**Network access: Named Pipes that can be accessed anonymously**" to "**ntapfprq_cdm**" (without the quotes).
    - Activate "**Network access: Let Everyone permissions apply to anonymous users**".
    - Reboot the computer.

- Please note that DMT checks incoming anonymous PIPE connections based on the senders IP address (it must match one of the filers's IP adresses), however, no such statement can be made for other PIPE software running on the Windows host.

- You may need to set the option *cifs.netbios_over_tcp.enable* to *off* in case the 7-mode filer cannot establish SMB connections with the Windows server. However, changing this option may require you to restart the CIFS service on the filer.

- Please ensure that "File and Printer Sharing" is enabled for the network interface on the Windows host running DMT and communicating with the NetApp filer. Also, you need to check the firewall settings for incoming SMB connections (sometimes Windows does not enable the corresponding firewall rules, see https://technet.microsoft.com/en-us/library/ff633412(v=ws.10).aspx).

Cleondris GmbH
Buckhauserstrasse 17
CH-8048 Zürich