CLEONDRIS

Cleondris Technical Implementation Note | TIN-95

# SnapGuard Quickstart Guide

**[Version 2020-03-20]**

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 SnapGuard Overview

SnapGuard is a Cleondris software product which helps customers to protect their valuable CIFS data on shared NetApp Data ONTAP systems. The product features a unique FPolicy based CIFS firewall that is dynamically hooked into ONTAP and stops attacks from malicious clients.

SnapGuard can be installed as a virtual appliance (OVA) within an hour and can be attached to NetApp Data ONTAP systems easily. It does not require architectural changes to existing NetApp ONTAP setups.

This quick start document describes the architecture of SnapGuard, the requirements for software hardware and network, as well as the involved communication flows. There is also a section dedicated to the involved workflow when performing an initial SnapGuard setup.

# 2 Architecture

In smaller environments, SnapGuard can be easily deployed as a standalone appliance. However, this kind of deployment is not suitable for large-scale setups with many NetApp Data ONTAP filers or clusters (possibly distributed over different sites), where ten thousand of concurrent CIFS sessions need to be tracked. Therefore, SnapGuard has a built-in tiered architecture that allows to tackle the following problems:

- Adaptation to the workload: scaling with large amounts of concurrent CIFS sessions
- Low-Latency: no impact on CIFS client experience
- High-Availability: system must continuously available, even if parts are failing or being upgraded
- Ease-of-use: centralized manageability of all involved components

The tiered architecture consists of the following components:

**Tier-1**: A central SnapGuard installation, based on the Cleondris appliance, that aggregates the views of all attached NetApp Data ONTAP systems. In smaller setups, this is the only Cleondris software component needed, as the built-in FPolicy engine ("FPE") can be used.

**Tier-2**: Local FPolicy engines ("FPE") that are connected to nearby NetApp filers. Customers need to install the Cleondris DMT software ("DMT", Data Manager Tools) on dedicated servers, which can then host the FPolicy engines. This is the only part of the architecture that relies on low-latency connections.

Thanks to the clear separation between the central SnapGuard server and the assigned FPolicy engines (no low-latency connection required between Tier-1 and Tier-2), the architecture can easily be extended for setups where a customer has many locations, e.g., different branch offices in a country or region.

Many customers start with a standalone SnapGuard deployment for testing purposes or small installations. As the number of attached NetApp ONTAP systems grows, the system can easily be scaled by installing the DMT software on dedicated servers. In case of unexpected growth of the CIFS traffic on a NetApp Data ONTAP cluster, additional Tier-2 FPolicy engines, based on hosts running the DMT agent, can be added at any time.

**Detailed Description of the involed Tiers**

**Tier-1** serves as a single point of management of presence and management for the different locations of the customer. A Tier-1 SnapGuard installation connects to one or more assigned NetApp Data ONTAP clusters and the assigned FPolicy modules. Each SnapGuard installation contains the actual configuration for a complete customer location ("which volumes on which NetApp cluster shall be monitored by which FPolicy modules"). The SnapGuard instance pushes the actual FPolicy configuration to the Tier-2 FPolicy modules, followed by the NetApp clusters which are informed about the volumes to monitor and the assigned FPolicy modules. The central SnapGuard installation regularly checks the status of the FPolicy modules (suspicious activity, dynamic blocking of clients, etc.). It is the responsibility of the  SnapGuard installation to send monitoring events (Syslog, SNMP, E-Mail) to the respective monitoring system. There is no HA needed on this level: Tier-2 (DMT) based FPolicy engines cache all escalation events locally until a "parent" SnapGuard installation is fetching them. In case the central SnapGuard installation is being updated (i.e., unavailable for a couple of minutes), polling of Tier-2 events is suspended and continues once the updated central SnapGuard installation starts again. Hence, even in the case of an unavailable Tier-1 SnapGuard instance, events will never be dropped, only the reporting via Syslog/SNMP/E-Mail may be delayed for a short time.

**Tier-2** is the actual workhorse: one or more FPolicy engines (running as part of a DMT installation) are connected to the nodes of a NetApp cluster and monitor all CIFS activity. Preferably, there is more than one FPolicy engine per NetApp Data ONTAP cluster (or even per SVM). This allows to load-balance the incoming FPolicy requests (scaling with many CIFS sessions). Multiple FPolicy engines per cluster also allow HA requirements to be fulfilled (the ONTAP cluster is automatically load-balancing requests to all available FPolicy engines, if an engine fails then ONTAP sends requests to the remaining connected FPolicy engines). In theory, a set of FPolicy engines can be shared between different clusters (in case the load per cluster is not very high). Typically, a single FPolicy engine should be planned per 1000 concurrent CIFS sessions, no matter whether these CIFS sessions are targeting one cluster or are the sum of connections hitting different clusters (which share a common set of FPolicy engines).

# 3 Required Software Components

All SnapGuard components run on virtual or physical hardware. SnapGuard (Tier-1) is typically installed as a virtual appliance on VMware ESX, however, it can be installed on pre-existing CentOS or RHEL 7 server as well. The FPolicy engines (Tier-2) are dynamically deployed. For this to work, the target servers (physical or virtual servers) need to have an installation of the Cleondris DMT software ("Data Manager Tools").

The DMT software is available for Windows Server (64-bit) and Linux (64-bit).

- In case of NetApp cDot clusters ("Clustered Data ONTAP"), DMT agent installations on both Windows and Linux are supported (the nodes of the NetApp cluster send messages using a proprietary message protocol via multiple TCP connections to the FPolicy engine running on the DMT agent).
- In case a legacy NetApp 7-Mode system needs to be monitored, the respective FPolicy module must be deployed on a DMT agent running on a Windows machine (the monitored NetApp controller is using a CIFS connection to report FPolicy events to the FPolicy engine).

Please refer to the following table for deployment options:

| Tier | Software | Deployment Options |
|---|---|---|
| Tier-1 | SnapGuard | • Cleondris Virtual Appliance on ESX<br>• RHEL/CentOS 7.x/8.x 64-bit (virtual or physical) |
| Tier-2 | DMT | • Windows Server 2008+ (64 bit)<br>• RHEL/CentOS 7.x/8.x 64-bit (virtual or physical) |

The Cleondris virtual appliance is distributed by Cleondris as an .OVA file (less than 600MB). The image is based on Linux, however it includes a console based configurator (similar to the yellow ESXi console interface), therefore no Linux knowledge is needed to install or maintain the software. The complete installation and initial configuration can be done in less than 15 minutes.

The Cleondris DMT software for Windows comes as an MSI based installer with Windows Installer intdgration. The size of the software is about 50 MB. The DMT software can be installed and configured within minutes.

The Cleondris DMT software for Linux comes as a tar.gz archive, which includes an automated setup script. The DMT software can be installed and configured within minutes.

Please note that SnapGuard is internally based on the well-established Cleondris Data Manager software (backup & restore for NetApp Data ONTAP, available as a virtual appliance since 2010) and the dynamically launched, external FPolicy engines (FPE) rely on the well-established Cleondris Data Manager Tools software (DMT, available since 2014).

# 4 Hardware Requirements

Depending on how the software components are installed, there are slight differences in the hardware / base OS requirements:

| Software | Hardware Requirements |
|---|---|
| **SnapGuard**<br>Cleondris<br>Virtual Appliance | • Min. 1 virtual 64-bit CPU<br>• Min. 4 GB memory, 8 GB preferred<br>• 16 GB disk space (single VMDK)<br>• Min. 1 virtual network interface (min. 1 GigE) |
| **SnapGuard**<br>RHEL 7/8 64-bit<br>CentOS 7/8 64-bit | • Min. 1 virtual or physical 64-bit CPU<br>• Min. 4 GB memory, 8 GB preferred<br>• 16 GB disk space<br>• Min. 1 network interface (min. 1 GigE)<br>• PostgreSQL 9.6+ installed |
| **Cleondris DMT**<br>Windows Server 2008 | • Min. 1 virtual or physical 64-bit CPU<br>• Min. 1,5 GB available memory for the DMT software<br>• Min. 1 GB disk space for the DMT software<br>• Min. 1 network interface (min. 1 GigE) |
| **Cleondris DMT**<br>RHEL 7/8 64-bit<br>CentOS 7/8 64-bit | • Min. 1 virtual or physical 64-bit CPU<br>• Min. 1,5 GB available memory for the DMT software<br>• Min. 1 GB disk space for the DMT software<br>• Min. 1 network interface (min. 1 GigE) |

# 5 Networking Requirements

There are different message flows in the system:

- Administrators need to be able to manage SnapGuard Tier-1 installations
- SnapGuard Tier-1 need to communicate with ONTAP cluster management interfaces
- SnapGuard Tier-1 needs to communicate with Syslog, SNMP or E-Mail servers
- SnapGuard Tier-1 needs to communicate with Tier-2 DMT instances (running the FPolicy modules)
- ONTAP cluster nodes and 7-mode controllers need to report FPolicy events to FPolicy Engines running either on SnapGuard or on dedicated, external servers (DMT)
- FPolicy Engines running on either SnapGuard or DMT need to communicate with AD servers (SID resolution) and optionally with Clustered Data ONTAP SVM data interfaces (in case the file verification feature is used)

Please refer to the following communication matrix:

| Source | Target | Protocol | Use |
|---|---|---|---|
| Administrator | SnapGuard | HTTPS over TCP Port 443 | Webinterface |
| SnapGuard | ONTAP<br>Cluster Management | HTTPS over TCP Port 443 | Management<br>via NetApp ZAPI protocol |
| SnapGuard | SNMP/Syslog/E-Mail Servers | TCP Ports 161, 514, 25/465 | Event Notification |
| SnapGuard | AD (Active Directory) Servers | MSRPC/SMB2 via TCP port 445 | SID/username lookups (if built-in FPE is used) |
| SnapGuard | ONTAP SVM Data Interface | SMB2 via TCP port 445 | Optional, if built-in FPE shall use file verification |
| SnapGuard | DMT | HTTPS over TCP Port 7683 | Management/Deployment<br>via Cleondris proprietary protocol |
| DMT | AD (Active Directory) Servers | MSRPC/SMB2 via TCP port 445 | SID/username lookups |
| DMT | ONTAP SVM Data Interface | SMB2 via TCP port 445 | Optional, if built-in FPE shall use file verification |
| **Clustered Data ONTAP** | | | |
| cDot<br>ONTAP<br>SVM Data-LIF | FPolicy Engine running on DMT or SnapGuard | XML via TCP port 10000-10099 | FPolicy Events<br>via NetApp proprietary protocol |
| **7-Mode Data ONTAP** | | | |
| 7-Mode<br>vFiler Interface | FPolicy Engine running on DMT | SMB1 or SMB2 via TCP port 445 | FPolicy Events<br>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<br>via NetApp proprietary protocol over CIFS/DECRPC |

# 6 Sample Deployment Procedure

The instructions in this section guide you to setup a basic SnapGuard installation.

## 6.1 Installing the Cleondris Appliance

There is dedicated documentation available for installing a Cleondris appliance. The most important steps for a virtualized installation on VMware vSphere are reproduced here:

- Download the latest Cleondris Appliance OVA file from the Cleondris website.
- Deploy the OVA using the VMware vSphere client.
- Attach the VM to a network which allows communication as described in this document.
- Start the VM and use the console configurator to…
  - Configure networking (IP address, gateway, DNS and NTP)
  - Configure a user/password for the web GUI
- Restart the appliance to activate the new network settings.
- Check that the web gui is accessible and that you can login.

## 6.2 Installing the latest SnapGuard update

Once the Cleondris appliance has been installed, all configuration and updates of Cleondris software take place over the web interface.

- Download the latest unified CDM/SGEE update file (.zip) from the Cleondris website
- Deploy the update using the appliance web gui. The appliance will be automatically rebooted.
- Login again and enter your license key to activate SnapGuard features of the appliance.

## 6.3 Basic SnapGuard Configuration

### 6.3.1 NetApp Data ONTAP Filers/Clusters

The most important step when configuring SnapGuard is the registration of NetApp ONTAP systems. As long as no filer/cluster has been added, SnapGuard  shows a wizard after the login. You can either use the wizard or skip it and configure NetApp ONTAP systems in the “Setup → NetApp” menu.

- For NetApp 7-mode systems (“filers”) you need to enter the hostname of “vfiler0” and the credentials of a “root” user.
- For NetApp clustered Data ONTAP (“clusters”) you need to enter the hostname of the cluster management SVM and the credentials of a cluster administrator.

NDMP credentials are optional (and can be added at any time), however, they are beneficial in case you want to…

- Use the differential restore capability with improved performance
- Use the volume analyzer with improved performance
- If you have a CDM license, you can use more features like NDMP copy and NDMP based volume indexing

### 6.3.2 Adding DMT hosts (Optional)

The Data Manager Tools can be run on other hosts to implement Tier-2 of the SnapGuard architecture. There is a separately available, dedicated documentation on how to install DMT. Such a configured host can be added in SnapGuard using the "Setup → Hosts" menu. Please ensure that you enable the "Use DMT as FPE" checkbox.

Note: if you want to implement a NetApp Data ONTAP 7-mode FPolicy firewall, you cannot use the FPE integrated into SnapGuard running on the Cleondris appliance. You need to use an FPE running on DMT on Microsoft Windows.

### 6.3.3 Adding an Event Receiver (Optional)

Events generated by SnapGuard can be sent automatically to SYSLOG, SNMP and E-Mail targets. To setup such a target, proceed as follows:

- Go to the "Setup → Events" menu
- Either keep the default and activate all events, or selectively select only the events in the CDM-08XXX category (if you are only interested in FPolicy related events).
- Add a SNMP or SYSLOG server or an E-Mail target using the "New Server" button in the top right corner. The "filter" setting can be used to reduce the event types (please specify a comma separated list of event numbers) that are sent to a given server – this can be used, if you have multiple receivers where you want send different subsets of events to.

Note: for a basic testing setup, you can skip this step and watch the generated firewall audit events via the web gui in the respective firewall log.

### 6.3.4 Defining a basic Firewall Ruleset

A SnapGuard firewall is based on the concept of rulesets. A ruleset defines triggers and corresponding actions. To protect the data on a NetApp volume, a ruleset must be assigned. There is exactly one ruleset per protected NetApp volume, but a ruleset can be assigned to many different volumes.

These are the steps involved in defining a basic protection ruleset that protects a filer from malware using one of the patterns in the common **fsrm.experiant.ca** pattern set:

- Open the "Firewall" section in the left pane
- In the "Rulesets"box, click the "New Ruleset" button

- Enter a name for the ruleset, e.g., "Malware Prevention"
- Click the "Add Rule" button
- Select the "create" and "rename" events for both "File Operations" and "Directory Operations".
- Press the "Edit" button in the "Filename include patterns" box
- Use the malware pattern list from **https://fsrm.experiant.ca/api/v1/combined** (open the website with a web browser, select the complete blob with CTRL-A and CTRL-C, then paste the blob with CTRL-V into the SnapGuard pattern editor.
- Click "OK" to accept the "filename include patterns" for this rule. There should now be more than 1000 malware patterns configured in this rule.
- Select "Block User" in the "Action" section
- Select the "Info" Audit-Level in the "Action" section
- Click "Accept" to add this rule to the ruleset.
- Click "Save" to permanently add the just created ruleset.

### 6.3.5 Starting a Firewall for a SVM

SnapGuard uses a dedicated firewall for each protected SVM (on Data ONTAP clusters) or vFiler (on 7-mode filers). For each firewall, you need to choose on which FPE it shall run. You have the option between the SnapGuard integrated FPE and external FPEs running on DMT agents. In case you want to run a 7-mode firewall, you must choose an external FPE running on a Microsoft Windows server.

These are the steps involved in protecting one or more NetApp volumes in a given SVM/vfiler:

- Choose a SVM that can be used for testing
- Open the "Firewall" section in the left pane
- In the "Firewalls"box, click the "New Firewall" button
- Select the cluster/filer and the SVM/vfiler that needs to be protected.
- In the "FPolicy Engine" dropdown, select the FPE that shall run the firewall. Note: to disable a firewall, simply open the firewall settings again and choose "None" in this dropdown.
- In case this is a 7-mode firewall, enter the credentials of a CIFS user that has "backup" privileges on the filer. For clustered Data ONTAP these input fields are not shown.
- For each volume to be protected, use a firewall ruleset using the dropdown on the right.
- Click "Save" to store the configuration and activate the firewall.

## 6.4 Testing the Setup

In case the configuration passes all checks, the state of the firewall shall change to "screen" within a few seconds and the screening throughput indicator should show any screening requests (create/rename requests in the example ruleset) that you have triggered via a CIFS connection to one of the protected volumes.

To test the audit/blocking features, simply create a file using a forbidden pattern in the filename (e.g., create a file with the name “ATLAS_FILES.txt”).

- The CIFS request must be blocked immediately (an error is shown in the Windows Explorer used to provoke the block operation)
- The client will be put on the blocklist for 20 seconds (see example ruleset), no file or directories can be created or renamed by this client during this timeframe. Note: the blocking is extended to the cumulative set of triggering file operations defined in all rules of the used ruleset.
- The blocked client is listed in the “Block List” tab of the respective firewall (while it is being blocked).
- An audit event is logged in the “Audit Events” tab of the respective firewall. In case an external event receiver has been defined during setup, a SNMP/SYSLOG event is generated as well.

Cleondris GmbH
Buchkauserstrasse 17
CH-8142 Uitikon