



STORMSHIELD



GUIDE

STORMSHIELD VISIBILITY CENTER

ADMINISTRATION GUIDE

Version 1.3

Date: February 15, 2018

Reference: `svc-en-svc_administration_guide-v1.3`



Table of contents

1. Getting started	4
1.1 Requirements	4
1.2 Help with hardware capacity	4
2. Deploying the SVC server in the virtual environment	5
2.1 Deploying the .OVA file in the VMWare environment	5
2.2 Deploying .VHD files in the Microsoft Hyper-V environment	5
3. Configuring SVC after installation	6
3.1 Defining passwords	6
3.2 Opening SVC Configurator	6
3.3 Modifying passwords	7
3.4 Modifying the keyboard configuration	7
3.5 Modifying the duration of log retention	7
3.6 Modifying the duration of archived log retention	7
3.7 Modifying network configuration	8
3.8 Modifying enabled protocols	8
3.9 Forwarding logs to an external syslog server	8
3.9.1 Configuring the transfer of logs to a syslog server	8
3.9.2 Viewing log forwarding parameters	8
3.9.3 Disabling the transfer of logs to a syslog server	9
3.10 Configuring the number of source syslog connections	9
3.11 Enabling the SNMP service	9
3.12 Synchronizing SVC with an NTP server	10
3.12.1 Synchronizing SVC with Stormshield NTP servers	10
3.12.2 Synchronizing SVC with your own NTP servers	10
3.12.3 Stopping NTP synchronization	10
3.13 Logging on to the SVC web interface	11
4. Configuring log sending to SVC	12
4.1 Using TCPTLS in SVC	12
4.1.1 Enabling TCP TLS	12
4.1.2 Retrieving files generated by the SVC PKI	12
4.2 Configuring SNS to send logs to SVC	13
4.2.1 Configuring SNS in versions lower than V3	13
4.2.2 Configuring SNS from V3 upwards	14
4.3 Configuring SES to send logs to SVC	18
4.3.1 Configuring syslog in SES	18
4.3.2 Converting log formats	18
4.3.3 Selecting the type of logs to be sent to SVC	19
4.4 Configuring SDS Enterprise to send logs to SVC	20
4.4.1 Prior conditions	20
4.4.2 Preparing logs to be used by SVC	20
4.4.3 Using TCP	21
4.4.4 Using TCP TLS	22
4.5 Configuring SDMC to send logs to SVC	23
4.5.1 Using TCP	23
4.5.2 Using TCP TLS	23
4.6 Configuring SVC to collect Panda Adaptive Defense logs	25
4.6.1 Connecting SVC to Panda's cloud server	25



- 4.6.2 Connecting SVC to an sFTP server 26
- 5. Monitoring Stormshield solutions with SVC 28
 - 5.1 Logging on to the SVC web interface 28
 - 5.2 Kibana documentation 28
 - 5.3 Dashboard Presentation 28
 - 5.3.1 SNS views 28
 - 5.3.2 SES views 29
 - 5.3.3 SDMC views 29
 - 5.3.4 SDS Enterprise views 29
 - 5.3.5 Panda Views 29
 - 5.3.6 MLCS views 29
 - 5.3.7 SVC views 29
 - 5.4 Navigating the SVC web interface 29
 - 5.4.1 Viewing information about a Stormshield product range 29
 - 5.4.2 Defining periods 30
 - 5.4.3 Filtering displayed data 31
 - 5.4.4 Going directly to a dashboard or a view 32
 - 5.5 Customizing dashboards 32
 - 5.5.1 Recommendations 32
 - 5.5.2 Use case: modifying a dashboard by adding a customized view to it 32
- 6. Managing and maintaining the server 37
 - 6.1 Backing up the virtual machine 37
 - 6.2 Displaying the version of SVC server components 37
 - 6.3 Updating the geolocation database 37
 - 6.4 Extending the size of the partition allocated to SVC 37
 - 6.4.1 Modifying the hypervisor's disk parameters 38
 - 6.4.2 Extending the size of the partition 38
 - 6.5 Dedicating a partition to data analysis 41
 - 6.5.1 Recommendations 41
 - 6.5.2 Adding a disk to the hypervisor 41
 - 6.5.3 Configuring SVC 43
 - 6.6 Resetting the "root" administrator password 43
 - 6.6.1 Changing the server startup mode 43
 - 6.6.2 Changing the password 44
 - 6.7 Troubleshooting 44
 - 6.8 Updating the SVC server 45
 - 6.8.1 Requirements 45
 - 6.8.2 Exporting new dashboards 45
 - 6.8.3 Performing the SVC upgrade. 46
 - 6.8.4 Importing dashboards 46
 - 6.8.5 Troubleshooting 46

In the documentation, Stormshield Visibility Center is referred to in its short form: SVC. Panda Adaptive Defense and Panda Adaptive Defense 360 are referred to as Panda.



1. Getting started

Stormshield Visibility Center is Stormshield's monitoring solution.

Based on logs generated by our various products, it provides intuitive and customizable views, giving you a quick summary of your information system's security status.

The SVC server is a virtual machine provided in the form of an .OVA or .VHD archive file.

In your [MyStormshield](#) personal area, under the Downloads section, you will find the installation file for the SVC server *Stormshield-Visibility-Center-x.x.x.ova* or *Stormshield-Visibility-Center-x.x.x.vhd*.

1.1 Requirements

In order to ensure the optimal use of SVC, check that you have met the system requirements below.

- SVC requires a hypervisor with at least the following characteristics:
 - CPU: 2VCPU,
 - Memory: 8 GB,
 - Processor: 64 bits,
 - Disk space required on the virtual environment: 200 GB.
- Do ensure that all appliances in the SVC environment have been set to the valid date and time.

1.2 Help with hardware capacity

The table below indicates the required hardware configuration according to the amount of logs that SVC receives:

Load (million logs/month)	X < 99	99 <= X < 150	150 <= X < 210	210 <= X < 240
CPU	2	4	4	6
RAM	8	16	24	24
Disk usage	50 GB	75 GB	105 GB	120 GB
Read-only access	120 MB/s	150 MB/s	150 MB/s	180 MB/s

Test conditions are as follows:

- Configuration of the SSD/RAID hard disk:
 - Read throughput: 2.0 GB/s,
 - Write throughput: 1.3 GB/s,
- No data ingestion during query testing,
- Retention in the database: 30 days,
- One query at a time over a 30-day stretch,
- Resources are dedicated to the SVC virtual machine.

Adjustments may need to be made to these configurations depending on the deployment environment.



2. Deploying the SVC server in the virtual environment

The SVC server is compatible with VMWare and Microsoft Hyper-V virtual environments.

2.1 Deploying the .OVA file in the VMWare environment

The *Stormshield-Visibility-Center-x.x.x.ovf* file from the SVC server can be deployed in one of the following virtual environments:

- VMware ESXi versions 5.5 and 6,
- VMware Workstation version 12.

Deploying the .OVA file on VMware ESX

1. Open the VMware vSphere client on your administration workstation.
2. In the **File** menu, select **Deploy an OVF template**.
3. In the VMware deployment wizard, complete the steps for deploying the .OVA file.

Deploying the .OVA file on VMware Workstation

- Double-click on the .OVA file or open the .OVA file from the **File>Open** menu in VMware Workstation.

2.2 Deploying .VHD files in the Microsoft Hyper-V environment

.VHD files can be deployed in the following virtual environments:

- Microsoft Hyper-V for Windows Server 2008 R2,
- Microsoft Hyper-V for Windows Server 2012 R2.

The *Stormshield-Visibility-Center-x.x.x-hyperv.tar.gz* archive contains two .vhd files:

- svc-system.vhd,
- product-data.vhd.

1. In the Hyper-V Manager tool, select a hypervisor.
2. Create a new virtual machine and follow the steps shown in the wizard.
 - Only for Hyper-V 2012 R2, select **Generation 1** to generate the virtual machine.
 - In the **Assign Memory** menu, allocate 8192 MB of memory.
 - In the **Connect Virtual Hard Disk** menu, select **Use an existing virtual hard disk** and select the *svc-system.vhd* file.
3. Finish the creation of the new virtual machine.
4. Edit the parameters of this machine and select the **SCSI Controller** menu.
5. Click **Add**.
6. In the **Virtual hard disk** section, select the file *product-data.vhd*.
7. Confirm.



3. Configuring SVC after installation

SVC is installed with the following default settings:

- **Keyboard configuration:** English,
- **Log retention:** 92 days,
- **Archived log retention:** 92 days,
- **Network configuration:** DHCP,
- **Log sending protocols:** rfc-3164-udp protocol enabled,
- **SNMP service:** disabled.

These settings may be modified via SVC Configurator.

3.1 Defining passwords

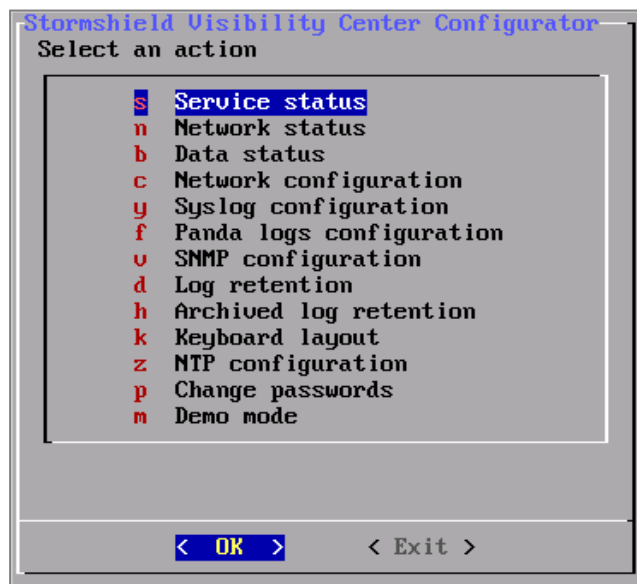
When the virtual machine starts up, enter the desired password and confirm it. This password will apply to the following users:

- The `root` user of the SVC virtual machine,
- The `log` user for access to the web interface.

You can change this password later and/or assign two separate passwords to both users. For more information, please refer to the section [Modifying passwords](#).

3.2 Opening SVC Configurator

1. At the `svc login` command prompt, log on with the root account, then run the command `svc-configurator`. SVC Configurator will then open.



2. Using the up or down buttons, scroll until you reach the desired menu, or type the letter next to the menu and press Enter.



3.3 Modifying passwords

The very first time you started up the SVC server, you had to define a shared password for the `root` and `log` users. You can change this password and/or assign two separate passwords to both users via Configurator.

1. In SVC Configurator, select the **Change Passwords** menu.
2. In the Change Passwords window, choose either one of these menus:
 - **'root' account Unix password** to change the password of the `root` user on the SVC virtual machine.
 - **'log' account Kibana password** to change the password of the `log` user accessing the web interface.
3. In the **Enter the new password** field, enter your new password and confirm.
4. In the **Enter the new password (verify)** field, type the password again and confirm.

3.4 Modifying the keyboard configuration

By default, the keyboard configuration is in English. However, this configuration may be modified when necessary.

1. In SVC Configurator, select the **Keyboard layout** menu.
2. Enter the configuration of the keyboard you wish to use:
 - *fr*: French,
 - *it*: Italian,
 - *us*: English,
 - *ch*: French (Switzerland),
 - *de*: German,
 - *es*: Spanish,
 - *pl*: Polish.
3. Press Enter.

3.5 Modifying the duration of log retention

By default, logs are kept in the database for three months before being deleted. However, this duration may be modified.

1. In SVC Configurator, select the **Log retention** menu.
2. Define the desired retention duration and confirm.

3.6 Modifying the duration of archived log retention

Logs that SVC collects are automatically archived in the `/var/archive/product_name` folder. For example, `/var/archive/sds` contains logs from SDS Enterprise.

Each folder contains one file per product and per day.

By default, archives are kept for three months before being deleted. However, this duration may be modified.



1. In SVC Configurator, select the **Archived log retention** menu.
2. Define the desired retention duration and confirm.

3.7 Modifying network configuration

1. In SVC Configurator, select the **Network configuration** menu.
2. Select the desired network configuration, either *DHCP* or *Static IP*.
3. For a static IP address, enter its parameters, then confirm.

3.8 Modifying enabled protocols

UDP is enabled by default. However, this configuration can be modified whenever necessary [e.g., to enable TCP and/or TCP TLS].

1. In SVC Configurator, select the **Syslog configuration** menu.
2. Select **Syslog sources** and confirm.
3. Select the desired protocol then press the spacebar to enable or disable it. An asterisk [*] will appear on the same row as the protocol when it is enabled.
4. Select **OK**.

3.9 Forwarding logs to an external syslog server

While SVC processes logs, you can enable their transfer to one or several external syslog servers.

3.9.1 Configuring the transfer of logs to a syslog server

1. In SVC Configurator, select the **Syslog configuration** menu.
2. Select **Syslog destination**.
3. Select **Configure / Disable log forwarding**.
4. Press the spacebar to enable the log transfer. An asterisk will appear on the line **[*] Enable Log forwarding**.
5. Select **OK**.
6. Select the desired destination protocol then press the spacebar. An asterisk [*] will appear on the same row as the protocol.
7. Select **OK**.
8. Enter the IP address of the destination syslog server.
9. Enter the port number of the destination syslog server.

Log forwarding is now enabled.

3.9.2 Viewing log forwarding parameters

1. In SVC Configurator, select the **Syslog configuration** menu.
2. Select **Syslog destination**.
3. Select **View current log forwarding parameters**. The **Log forwarding parameters** window then appears, showing the following information:



- Protocol: Protocol used for forwarding logs,
- IP address: IP address of the external syslog server.
- Port: Port number of the external syslog server.

3.9.3 Disabling the transfer of logs to a syslog server

1. In SVC Configurator, select the **Syslog configuration** menu.
 2. Select **Syslog destination**.
 3. Select **Configure / Disable log forwarding** and confirm.
 4. Press the spacebar to disable the log transfer. The asterisk will disappear from the line [] **Enable Log forwarding**.
 5. Select **OK**.
- Log forwarding is now disabled.

3.10 Configuring the number of source syslog connections

SVC accepts by default a maximum of 10 simultaneous source syslog connections. Whenever necessary, for example, if you wish to analyze logs for an environment of more than 10 SNS firewalls, you can increase this value.

1. In SVC Configurator, select the **Syslog configuration** menu.
2. Select **Syslog parameters**.
The window to configure the number of syslog connections appears. **Actual** represents the current value.
3. Enter the desired number of connections in the field, or use the Up and Down arrows on your keyboard to change the value. The maximum number of connections possible has been set at 500.
4. Select **OK**.
The **actual** value now displays the new value.

3.11 Enabling the SNMP service

Support for SNMP v2 can be enabled to allow access to the SVC server in read-only mode.

1. In SVC Configurator, select the **SNMP configuration** menu.
2. Select **Enable SNMP support** then press the spacebar. An asterisk [*] will appear on the row.
3. Select **OK**.

The SNMP service is now enabled.

The table below sets out a non-exhaustive list of supported MIBs:

Category	RFC	MIB	Details
system	RFC 1213	.1.3.6.1.2.1.1	Information regarding the system, its location, the services it provides, duration of its usage, and contact details of the person in charge.
ifaces	RFC 1213, RFC 2863	.1.3.6.1.2.1.2, .1.3.6.1.2.1.31	Information on the network interfaces. The OID.
ips	RFC 1213	.1.3.6.1.2.1.4	Information regarding IP transfers, including counters that track exchanges of IP packets.



tcp	RFC 1213	.1.3.6.1.2.1.6	Information regarding TCP transfers, including imposed limits, and the status of connections.
udp	RFC 1213	.1.3.6.1.2.1.7	Information regarding UDP transfers, including counters that track exchanges of UDP datagrams.
snmp	RFC 1213	.1.3.6.1.2.1.11	Information and statistics on SNMP traffic.
mem	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.4	Objects that enable monitoring of memory use.
disk	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.9	Disk monitoring information.
load	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.10	Average load information.
cpu	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11	CPU information.
sysstats	UCD-SNMP-MIB	.1.3.6.1.4.1.2021.11	Statistics that describe the various parts of the system (memory, CPU use, peripheral devices in block-by-block mode).
perf	RFC 1514	.1.3.6.1.2.1.25.4, .1.3.6.1.2.1.25.5	Performance indicators of the various software modules that are either active or have been loaded in the physical or virtual memory before being run (including the operating system, drivers and host's applications).

3.12 Synchronizing SVC with an NTP server

SVC can be synchronized with two types of NTP servers:

- Stormshield *ntp1.stormshieldcs.eu* and *ntp2.stormshieldcs.eu* servers. An Internet connection is required for this synchronization.
- Your own NTP servers.

3.12.1 Synchronizing SVC with Stormshield NTP servers

1. In SVC Configurator, select the **NTP configuration** menu.
2. In the NTP server configuration window, select **Enable Stormshield NTP servers**. The names of Stormshield NTP servers will appear at the top of the window.

3.12.2 Synchronizing SVC with your own NTP servers

1. In SVC Configurator, select the **NTP configuration** menu.
2. In the NTP server configuration window, select the **Enable custom NTP server** menu.
3. Enter the IP address or FQDN name of your NTP servers. Separate each server name with a space.
4. Select **OK**.
The names of your NTP servers will appear at the top of the window.

3.12.3 Stopping NTP synchronization

1. In SVC Configurator, select the **NTP configuration** menu.
2. In the NTP server configuration window, select the **Disable NTP** menu.



3.13 Logging on to the SVC web interface

1. In SVC Configurator, select the **Network status** menu. The **Address** field indicates the IP address of your SVC server.
2. Using your web browser, log on to this IP address in HTTPS (*https://svc_ip_address*).

i NOTE

Look up this web site to check which browser versions SVC supports:
https://www.elastic.co/fr/support/matrix#matrix_browsers.

3. In the connection window, enter the following information:
 - User: `log`
 - **Password** : by default it is the same password as the `root` user of the SVC server, except if you have modified it afterwards via the Configurator. For more information, please refer to the section [Modifying passwords](#).

The SVC web interface will appear.



4. Configuring log sending to SVC

You will need to configure the Stormshield products in your environment so that they send their logs to SVC.

i NOTE

For certain visualizations, specific features need to be enabled on appliances (e.g.: proxy, antivirus or Breach Fighter).

Three types of protocols may be used for sending logs:

- **RFC 5424 TCP** on port 601
This protocol enables the exchange of data without encryption but with data acknowledgment.
- **RFC 5424 TCP TLS** on port 6514
This protocol enables the encrypted exchange of data, with identification and data acknowledgment. Certificates must be deployed on each client (SNS, SDS Enterprise, SES and SDMC).
- **RFC 3164 UDP** on port 514
This protocol enables the exchange of data without encryption or data acknowledgment. It is enabled by default once SVC is installed.

4.1 Using TCP TLS in SVC

In order to use TCP TLS, you will need to retrieve the certificate files generated by the SVC server's PKI (Public Key Infrastructure).

The first time it is started up, the SVC PKI will generate:

- A self-signed certificate authority (CA),
- A server certificate, used by the SVC syslog-ng service,
- A client certificate and its private key, available for Stormshield applications.

4.1.1 Enabling TCP TLS

1. Open SVC Configurator. For more information, please refer to the section [Opening SVC Configurator](#).
2. Select the **Syslog configuration** menu, then **Syslog sources** and confirm.
3. Select *rfc-5424-tcp-tls* and press the spacebar. An asterisk [*] will appear on the same row as the protocol.
4. Select **OK**.

With this configuration, it will be guaranteed that Stormshield applications contact the relevant SVC server.

4.1.2 Retrieving files generated by the SVC PKI

1. In the SVC web interface, in the menu of a dashboard on the left (*Dashboard* tab), click on **Download SVC server public certificate and client certificate**.
2. Save the file named *svc_self_signed_certificate.zip*. This archive includes the following files:



- *ca.cert.pem*: Certificate authority generated by SVC,
- *server.pub.cert.pem*: Server certificate needed for identifying the SVC server,
- *client.syslog-ng.cert.pem*: Client certificate needed for identifying the syslog-ng client for SVC,
- *client.syslog-ng.key.pem*: Private key of the client certificate,
- *client.sns.cert.pem*: Client certificate as well as its private key needed for identifying the TLS syslog client for SNS.

4.2 Configuring SNS to send logs to SVC

You will need to configure each SNS firewall so that it sends its logs to SVC.

4.2.1 Configuring SNS in versions lower than V3

SNS v2.x only supports UDP for the purpose of sending logs. For further information on the various protocols, please refer to the section [Configuring log sending to SVC](#).

1. On the SVC server, enable UDP. For more information, please refer to the section [Modifying enabled protocols](#).
2. In the firewall's administration interface, select **Configuration>Notifications>Logs-syslog**. The **Logs-Syslog** panel will appear.
3. In the *Syslog* tab, select the option **Enable sending logs by Syslog**.

Status	Family
<input checked="" type="radio"/> Enabled	Administration (serverd)
<input checked="" type="radio"/> Enabled	Authentication
<input checked="" type="radio"/> Enabled	Network connections
<input checked="" type="radio"/> Enabled	System events
<input checked="" type="radio"/> Enabled	Alarms
<input checked="" type="radio"/> Enabled	HTTP proxy
<input checked="" type="radio"/> Enabled	Application connections (plugin)
<input checked="" type="radio"/> Enabled	SMTP proxy
<input checked="" type="radio"/> Enabled	Filter policy
<input checked="" type="radio"/> Enabled	IPSec VPN
<input checked="" type="radio"/> Enabled	SSL VPN
<input checked="" type="radio"/> Enabled	POP3 proxy
<input checked="" type="radio"/> Enabled	Statistics
<input checked="" type="radio"/> Enabled	Vulnerability Manager
<input checked="" type="radio"/> Enabled	FTP proxy
<input checked="" type="radio"/> Enabled	SSL proxy
<input type="radio"/> Disabled	Sandboxing



4. In the **Destination server** field, select the host object that represents your SVC server. If the object does not yet exist, you can create it by clicking on the + icon.
 5. In the **Port** field, select *syslog*.
 6. Select the log families to be sent to SVC by double-clicking in the **Status** column.
- Your SNS firewall will now send its logs to SVC.

4.2.2 Configuring SNS from V3 upwards

From SNS v3 upwards, the use of TCP or TCP/TLS is preferable as these protocols are more reliable.

Using TCP

1. On the SVC server, enable TCP. For more information, please refer to the section [Modifying enabled protocols](#).
2. In the firewall's administration interface, select **Configuration > Notifications > Logs-syslog**. The **Logs-Syslog** panel will appear.
3. In the *Syslog* tab, select the syslog profile that you wish to assign to SVC, for example Syslog Profile 1.

The screenshot shows the 'LOGS - SYSLOG - IPFIX' configuration page. The 'SYSLOG PROFILES' table lists four profiles: VLA 1 (Disabled), SVC (Enabled), Syslog Profile 2 (Disabled), and Syslog Profile 3 (Disabled). The 'SVC' profile is selected. The 'Details' section shows the following configuration:

- Name: SVC
- Comments: Stormshield Visibility Center
- Syslog server: virtual-SVC
- Protocol: TCP
- Port: syslog-conn
- Certificate authority: (empty)
- Server certificate: (empty)
- Client certificate: (empty)
- Format: RFC5424

The 'Advanced properties' section shows:

- Backup server: (empty)
- Backup port: syslog-conn
- Category (facility): none

The 'LOGS ENABLED' section shows a table with columns 'Status' and 'Name'. The 'Allow all' radio button is selected. The table lists the following log families, all of which are enabled:

Status	Name
Enabled	Alarms
Enabled	Network connections
Enabled	Filter policy
Enabled	HTTP proxy
Enabled	SMTP proxy
Enabled	FTP proxy

4. In the **Details** section, fill in the following fields:
 - **Name:** Enter the name of your new syslog profile. For example, *SVC*.
 - **Syslog server:** Select the host object that represents your SVC server. If the object does not yet exist, you can create it by clicking on the + icon.
 - **Protocol:** Select *TCP*,
 - **Port:** Select *syslog-conn*,
 - **Format:** Select *RFC5424*.



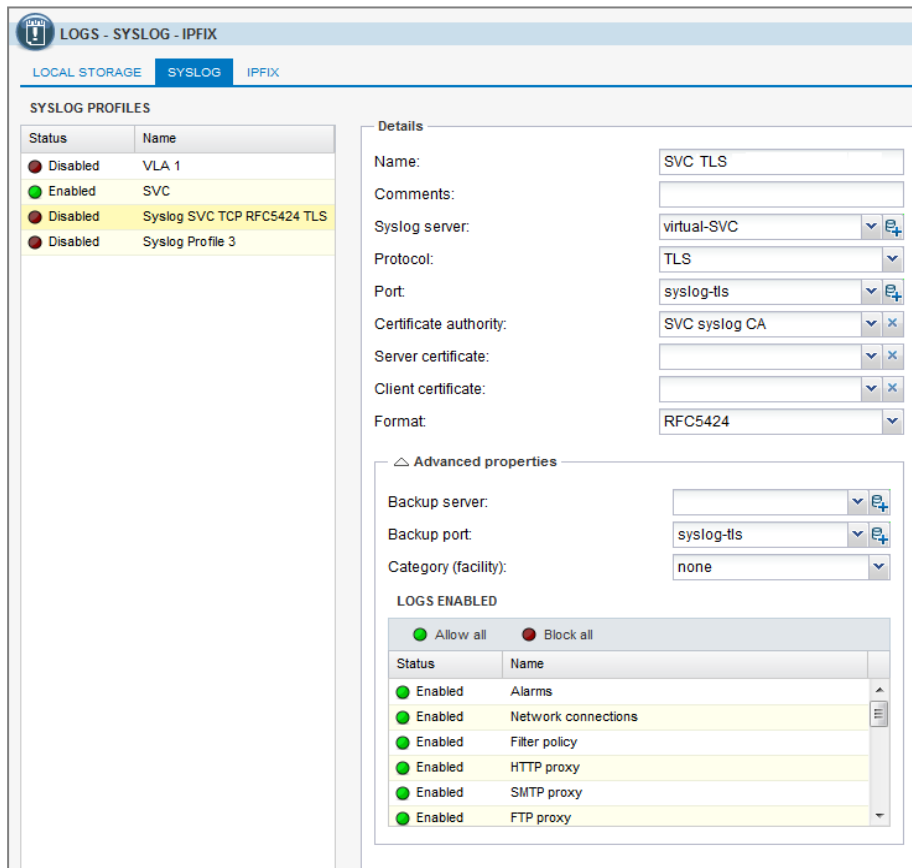
5. In the **Advanced properties** section, if necessary, filter the log families to be sent to SVC by double-clicking in the **Status** column.
6. Click **Apply**.

Using TCP TLS by importing certificates generated by the SVC server's PKI

1. On the SVC server, enable TCP TLS. For more information, please refer to the section [Modifying enabled protocols](#).
2. In the firewall's administration interface, select **Configuration>Objects>Certificates and PKI**. The **Certificates and PKI** panel will appear.
3. Select **Add > Import** and import the following files:
 - *ca.cert.pem*: Certificate authority generated by SVC,
 - *server.pub.cert.pem*: Server certificate needed for identifying the SVC server,
 - *client.sns.cert.pem*: Client certificate as well as its private key needed for identifying the TLS syslog client for SNS.

For further information, refer to the Stormshield firewall *User and configuration manual*. Once they have been imported, the certificates will appear in the list.

4. Select **Configuration>Notifications>Logs-syslog-IPFIX**. The **Logs - Syslog - IPFIX** panel will appear.
5. In the *Syslog* tab, select the syslog profile that you wish to assign to SVC, for example Syslog Profile 1.





6. In the **Details** section, fill in the following fields:
 - **Name:** Enter the name of your new syslog profile. For example, *SVC TLS*,
 - **Syslog server:** Select the host object that represents your server. If the object does not yet exist, you can create it by clicking on the + icon,
 - **Protocol:** Select *TLS*,
 - **Certificate authority:** Select the SVC certificate authority,
 - **Server certificate:** Select the SVC server certificate,
 - **Client certificate:** Select the SVC client certificate,
 - **Format:** Select *RFC5424*,
 - **Port:** Select *syslog-tls*.
7. In the **Advanced properties** section, if necessary, filter the log families to be sent to SVC by double-clicking in the **Status** column.
8. Click **Apply**.

Your SNS firewall will now send its logs to SVC.

Using TCP TLS via the SNS firewall's PKI

You can ensure the security of communications between SNS and SVC by generating certificates extracted from a certificate authority belonging to SNS that is under your control. To manage an SNS PKI, refer to the SNS firewall *User and configuration manual*.

1. Create an SNS PKI containing the following items:
 - A certificate authority,
 - A server certificate for SVC,
 - A client certificate for syslog clients, including the one for SNS.
2. Once all the certificates have been created, export them.
3. Configure the syslog in TLS. For more information, refer to steps 3 to 7 of the procedure in [Using TCP TLS by importing certificates generated by the SVC server's PKI](#)
4. Copy the certificates generated by SNS on the SVC server.

IMPORTANT

Certificate files must be correctly named on SVC:

- *server.cert.pem*: for the SVC certificate,
- *server.key.pem*: for the SVC certificate key,
- *ca.cert.pem*: for the certificate authority.



5. On the SVC virtual machine, run the following commands in order to deploy the certificates:

- To extract the private key of the authority's certificate in order to produce a public certificate:

```
openssl x509 -outform pem -in syslog-ng.pem -out ca.cert.pem
```

- To extract the private key of the SVC certificate in order to produce a public certificate:

```
openssl x509 -outform pem -in svccert.com.pem -out server.cert.pem
```

- To extract the private key of the SVC certificate:

```
openssl pkey -in svccert.com.pem -out server.key.pem
```

- To copy the certificate authority into the `/data/syslog-ng/ca/certs` folder and modify its access privileges:

```
cp ca.cert.pem /data/syslog-ng/ca/certs/
```

```
sudo chmod 444 "/data/syslog-ng/ca/certs/ca.cert.pem"
```

- To create a hashed symbolic link to the certificate authority in the `/data/syslog-ng/ca/certs` folder:

```
sudo ln -s ca.cert.pem $(openssl x509 -noout -hash -in ca.cert.pem).0
```

- To copy the client certificate into the `/data/syslog-ng/ca/certs` folder and modify its access privileges:

```
cp server.cert.pem /data/syslog-ng/ca/certs/
```

```
sudo chmod 400 "/data/syslog-ng/ca/certs/server.cert.pem"
```

- To copy the private key of the client certificate into the `/data/syslog-ng/ca/private/` folder and modify its access privileges:

```
cp server.key.pem /data/syslog-ng/ca/private/
```

```
sudo chmod 400 "/data/syslog-ng/ca/private/server.key.pem"
```

- To restart the syslog-ng server on SVC:

```
sudo service syslog restart
```

SVC will now collect SNS logs securely.



4.3 Configuring SES to send logs to SVC

SES logs are sent via UDP. They are configured in three steps. First of all, you will need to configure syslog in SES, then convert the log format before selecting the type of logs to send to SVC.

4.3.1 Configuring syslog in SES

You will need to configure the SES server so that it sends its logs to a syslog server via UDP.

1. In the SES administration console, select **Environment Manager > Policies**, then the **Server Configuration** folder.

Server Roles	
Stormshield Endpoint Security server	Enabled
Antivirus server	Enabled

Agent connections management	
Number of simultaneous connections	20
Maximum number of handled clients	1000
Token refresh time (sec.)	300
Reconnection time (sec.)	300
Logs upload period (sec.)	1800
Minimum agent version allowed	Not limited
Maximum agent version allowed	Not limited

Log Monitoring Configuration	
SQL server instance	192.168.56.105\SES
Database password	*****
Reporting language	English

Syslog Configuration	
Address/Hostname	192.168.56.105
Port	1468
Protocol	Tcp
Facility	0 ~ kernel messages
Severity	0 ~ Emergency

SMTP Configuration	
--------------------	--

2. In the **Syslog configuration** section, fill in the following fields:
 - **Address/Hostname:** Enter the IP address of the SVC server. In order to obtain the IP address, refer to the section [Configuring SVC after installation](#).
 - **Port:** Enter the port number used for syslog.
 - **Protocol:** Enter *UDP*,
 - **Facility/Severity:** Enter the syslog level you wish to position on sent logs.
3. Click **Apply changes to the environment**.

4.3.2 Converting log formats

In order for SVC to use SES logs correctly, you need to convert their format. A conversion modifies the log format in the database.

The procedure varies according to SES version.

Converting logs from SES version 7.2.18 and upwards

1. In the SES administration console, click on the **Tools** menu at the top of the screen, then on **Open DBInstaller** to open the console's maintenance wizard.



2. Select **Configuration database maintenance**.

Stormshield Endpoint Security

Stormshield Endpoint Security

Introduction
Super Admin
Tasks
Validation
Maintenance

Configuration database maintenance wizard

Please specify the operation type and provide necessary information if needed.

Operation type: Backup
 Restore
 Update
 Configure logs for SVC

Backup file path: ...

< Back Next > Cancel

3. Select the option **Configure logs for SVC**.
4. Click on **Next**, then on **Finish**.
The format of the logs has now been converted in the SES database.

Converting logs for SES in versions lower than 7.2.18

1. Log on to the SVC web interface. For more information, refer to the section [Configuring SVC after installation](#).
2. In the menu on the left, click on **Download SQL configuration script for SES** in order to retrieve the SQL script *ses_dbscript.sql*.
3. Use a tool such as Microsoft SQL Server Management Studio to run this script in the SQL instance in which the SES configuration database has been installed.

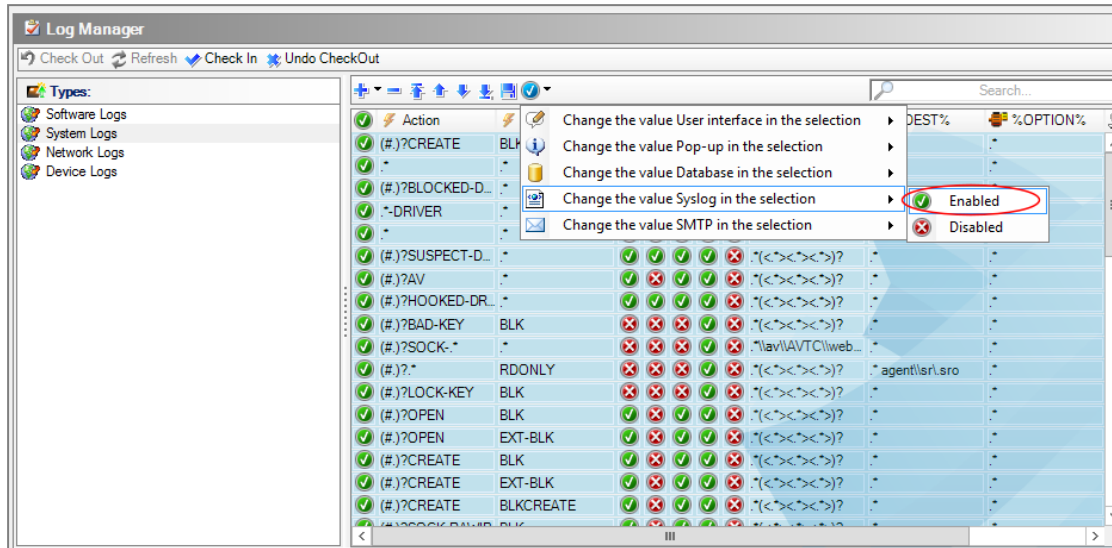
4.3.3 Selecting the type of logs to be sent to SVC

You need to select the type of logs that SES sends to SVC.

1. In the SES administration console, select **Environment Manager > Log Manager**.
2. In the **Log Manager** panel, click **Edit**.
3. In the **Types** area, select the type of logs, then select those that you wish to send to SVC. For example, if you wish to send all system logs, select **System Logs**, then all the rows that appear in the panel on the right.



- Click on the blue check icon, then select **Change the value Syslog in the select > Enabled**.



- Repeat the operation for the other types of logs to be sent, then click on **OK** to confirm changes.

4.4 Configuring SDS Enterprise to send logs to SVC

Workstations must be configured in order for SDS Enterprise to send its logs to SVC. You can either use TCP or TCP TLS. For further information on the various protocols, please refer to the section [Configuring log sending to SVC](#).

4.4.1 Prior conditions

- Event logging must be enabled centrally on workstations in the organization via the Group Policy Object (GPO) manager. For more information, refer to the *Event logging* section in the *Stormshield Data Security Enterprise administration guide*.
- An intermediate Microsoft log collection server can also be used for event logging, and will be the only workstation sending logs to the SVC server. To simplify deployment, Stormshield recommends this configuration. For more information, refer to the *Viewing logs on another remote server* section in the *Stormshield Data Security Enterprise administration guide*.
- If you are not enabling a Microsoft log collection server, do not enable **Name of server on which the events must be sent**. Otherwise, Windows will send logs to another server and subsequently delete them from the workstations.
- The desired protocol (i.e., TCP or TCP TLS) must be enabled on the SVC server. For more information, please refer to the section [Modifying enabled protocols](#).

4.4.2 Preparing logs to be used by SVC

Regardless of the protocol used for sending logs (TCP or TCP TLS), you must first convert logs in Windows format to syslog format using the NXLOG utility (freeware).

SVC is compatible with NXLOG version 2.9.1716.

- Download the NXLOG msi:
<http://nxlog.org/products/nxlog-community-edition/download>.



2. If you have configured a Microsoft log collection server, deploy the msi only on this server.
- or -
If you have not configured a Microsoft log collection server, deploy the msi on all SDS Enterprise workstations.
3. Check that the Windows *nxlog* service has been configured in automatic startup mode.
4. Log on to the SVC web interface. For more information, refer to the section [Configuring SVC after installation](#).
5. In the menu on the left, click on Download nxlog configuration template for SDS in order to retrieve the `sds_enterprise_nxlog.conf` configuration template.
6. Rename the `sds_enterprise_nxlog.conf` file as `nxlog.conf`.

4.4.3 Using TCP

1. Customize the `nxlog.conf` file by uncommenting and entering the following blocks according to your environment:

- For a 32-bit Windows environment, uncomment the line `define ROOT C:\Program Files\nxlog` and comment the line `define ROOT C:\Program Files (x86)\nxlog`.

```
# Uncomment the next line in case of 32Bits Windows
# define ROOT C:\Program Files\nxlog
# Uncomment the next line in case of 64Bits Windows
define ROOT C:\Program Files (x86)\nxlog
```

- Uncomment all the lines found between the markers `<output SVC_TCP>` and `</Output>` except for the line `## Replace XXX.XXX.XXX.XXX with your SVC ip`.
- In the `Host` field, replace `XXX.XXX.XXX.XXX` with the IP address of your SVC server. In order to find out the IP address, refer to the section [Configuring SVC after installation](#).

```
## IETF-style syslog RFC5424
<output SVC_TCP>
  Module om_tcp
  ## Replace XXX.XXX.XXX.XXX with your SVC ip
  Host XXX.XXX.XXX.XXX
  Port 601
  Exec to_syslog_ietf();
  OutputType Syslog_TLS
</Output>
```

- Uncomment the line `<code>Path SDS_events=> SVC_TCP</code>` in order to use TCP.

```
<Route 1>
# Uncomment ONLY ONE of those next routes
# Path SDS_events=> SVC_UDP
Path SDS_events=> SVC_TCP
# Path SDS_events=> SVC_TLS
</Route>
```

2. On the Microsoft log collection server, or on each SDS Enterprise workstation if you do not have such a server, copy the file `nxlog.conf` into the following folder:
 - **64-bit Windows:** `C:\Program Files (x86)\nxlog\conf\`,
 - **32-bit Windows:** `C:\Program Files\nxlog`.



4.4.4 Using TCP TLS

1. Customize the *nxlog.conf* file by uncommenting and entering the following blocks according to your environment:

- For a 32-bit Windows environment, uncomment the line `define ROOT C:\Program Files\nxlog` and comment the line `define ROOT C:\Program Files (x86)\nxlog`.

```
# Uncomment the next line in case of 32Bits Windows
# define ROOT C:\Program Files\nxlog
# Uncomment the next line in case of 64Bits Windows
define ROOT C:\Program Files (x86)\nxlog
```

- Uncomment all the lines found between the markers `<output SVC_TLS>` and `</Output>` except for the line `## Replace XXX.XXX.XXX.XXX with your SVC ip`.
- In the `Host` field, replace `XXX.XXX.XXX.XXX` with the IP address of your SVC server. In order to find out the IP address, refer to the section [Configuring SVC after installation](#).

```
## IETF-style syslog RFC5424/RFC5425
<Output SVC_TLS>
  Module          om_ssl
  ## Replace XXX.XXX.XXX.XXX with your SVC ip
  Host            XXX.XXX.XXX.XXX
  Port            6514
  Exec            to_syslog_ietf();
  OutputType      Syslog_TLS
  CertFile        %ROOT%/cert/client.syslog-ng.cert.pem
  CertKeyFile     %ROOT%/cert/client.syslog-ng.key.pem
  CAFile          %ROOT%/cert/ca.cert.pem
  AllowUntrusted  FALSE
</Output>
```

- Uncomment the line `Path SDS_events=> SVC_TLS` in order to use TCP/TLS.

```
<Route 1>
#   Uncomment ONLY ONE of those next routes
#   Path SDS_events=> SVC_UDP
#   Path SDS_events=> SVC_TCP
  Path SDS_events=> SVC_TLS
</Route>
```

2. On the Microsoft log collection server, or on each SDS Enterprise workstation if you do not have such a server, copy the file *nxlog.conf* into the following folder:
 - **64-bit Windows:** `C:\Program Files (x86)\nxlog\conf\`,
 - **32-bit Windows:** `C:\Program Files\nxlog\`.
3. Retrieve the certificate files generated by SVC the first time it was started up. For more information, please refer to the section [Retrieving files generated by the SVC PKI](#).
4. Copy the files *client.syslog-ng.cert.pem*, *client.syslog-ng.key.pem*, and *ca.cert.pem* to the root of the NXLOG installation in the *nxlog\cert* folder. Create the folder beforehand if it does not already exist.
5. Start the Windows *nxlog* service.



4.5 Configuring SDMC to send logs to SVC

SDMC must be configured in order for it to send its logs to SVC using TCP or TCP TLS. For further information on the various protocols, please refer to the section [Configuring log sending to SVC](#).

4.5.1 Using TCP

1. Enable TCP in SVC. For more information, please refer to the section [Modifying enabled protocols](#).
2. From the SDMC server, log on to the SVC web interface. For more information, refer to the section [Configuring SVC after installation](#).
3. In the menu on the left, click on **Download syslog configuration template for SDMC** in order to retrieve the *sdmc_syslog_config.zip* archive.
4. Unzip the archive that contains these two files:
 - *syslog-stormshield-TCP.conf*,
 - *syslog-stormshield-tcp-tls.conf*.
5. Copy the *syslog-stormshield-TCP.conf* file into the */etc/syslog-ng/conf.d* folder. Create this folder beforehand if it does not already exist. The contents of the file are as follows:

```
source s_sdmc
    unix-dgram("/dev/log" flags(no-parse) );

};

# Remplacer les xx.xx.xx.xx par l'adresse IP de votre SVC
destination d_svc_syslog_rfc5424_TCP {
    syslog("xx.xx.xx.xx" port(601) transport("TCP"));
};

filter s_sdmc_filter {match("sdmc*" value("MESSAGE")); };

log {
    source(s_sdmc);
    destination(d_svc_syslog_rfc5424_TCP);

    filter(s_sdmc_filter);
};
```

6. In the file, replace *xx. xx. xx. xx* with the IP address of your SVC server. In order to find out the IP address, refer to the section [Configuring SVC after installation](#).
7. At the end of the */etc/syslog-ng/syslog-ng.conf* configuration file, add the following line to include the Stormshield TCP configuration file:

```
@include "/etc/syslog-ng/conf.d/*.conf"
```

8. Restart *syslog-ng* using the following command:

```
/etc/init.d/syslog.syslog-ng restart
```

4.5.2 Using TCP TLS

1. Enable TCP TLS in SVC. For more information, please refer to the section [Modifying enabled protocols](#).



2. Retrieve the certificate files generated by SVC the first time it was started up. For more information, please refer to the section [Retrieving files generated by the SVC PKI](#).
3. Copy the zipped file retrieved from the `/tmp` folder on the SDMC server.
4. On the SDMC server's virtual machine, run the following commands in order to deploy the certificates:

- To unzip the archive:

```
cd /tmp/  
unzip svc_self_signed_certificates.zip
```

- To create the tree needed for certificates:

```
mkdir -p /opt/syslog-ng/etc/syslog-ng/key.d/ /opt/syslog-ng/etc/syslog-ng/cert.d/ /opt/syslog-ng/etc/syslog-ng/ca.d/
```

- To copy the certificate authority and modify its access privileges:

```
cp certificates/ca.cert.pem /opt/syslog-ng/etc/syslog-ng/ca.d/  
chmod 444 "/opt/syslog-ng/etc/syslog-ng/ca.d/ca.cert.pem"
```

- To create the hashed symbolic link to the certificate authority:

```
cd /opt/syslog-ng/etc/syslog-ng/ca.d/  
ln -s ca.cert.pem $(openssl x509 -noout -hash -in ca.cert.pem).0  
cd /tmp/
```

- To copy the client certificate into the folder and modify its access privileges:

```
cp certificates/client.syslog-ng.cert.pem /opt/syslog-ng/etc/syslog-ng/cert.d/  
chmod 444 "/opt/syslog-ng/etc/syslog-ng/cert.d/client.syslog-ng.cert.pem"
```

- To copy the private key of the client certificate and modify its access privileges:

```
scp certificates/client.syslog-ng.key.pem /opt/syslog-ng/etc/syslog-ng/key.d/  
chmod 400 "/opt/syslog-ng/etc/syslog-ng/key.d/client.syslog-ng.key.pem"
```

5. In the menu on the left in the SVC web interface, click on **Download syslog configuration template for SDMC** in order to retrieve the `sdmc_syslog_config.zip` archive.
6. Unzip the archive that contains these two files:
 - `syslog-stormshield-TCP.conf`,
 - `syslog-stormshield-tcp-tls.conf`.
7. Copy the `syslog-stormshield-tcp-tls.conf` file into the `/etc/syslog-ng/conf.d` folder. Create this folder beforehand if it does not already exist. The contents of the file are as follows:

```
source s_sdmc {  
    unix-dgram("/dev/log" flags(no-parse) );  
};  
  
# Remplacer xx.xx.xx.xx par l'adresse IP du serveur SVC.  
destination d_svc_syslog_rfc5424_tcp_tls {  
    syslog("xx.xx.xx.xx"  
        port(6514)  
        transport("tls")  
        tls(  
            key_file("/opt/syslog-ng/etc/syslog-ng/key.d/client.syslog-ng.key.pem")  
            cert_file("/opt/syslog-ng/etc/syslog-ng/cert.d/client.syslog-ng.cert.pem")  
        )  
    }  
};
```




```
        ca_dir("/opt/syslog-ng/etc/syslog-ng/ca.d/ca.cert.pem")
        peer-verify(required-untrusted)
    )
};

filter s_sdmc_filter {match("sdmc*" value("MESSAGE")); };

log {
    source(s_sdmc);
    destination(d_svc_syslog_rfc5424_tcp_tls);
    filter(s_sdmc_filter);
};
```

8. In the file, replace `xx.xx.xx.xx` with the IP address of your SVC server. In order to find out the IP address, refer to the section [Configuring SVC after installation](#).
9. At the end of the `/etc/syslog-ng/syslog-ng.conf` configuration file, add the following line to include the Stormshield TCP/TLS configuration file:

```
@include "/etc/syslog-ng/conf.d/*.conf"
```

10. Restart `syslog-ng` using the following command:

```
/etc/init.d/syslog.syslog-ng restart
```

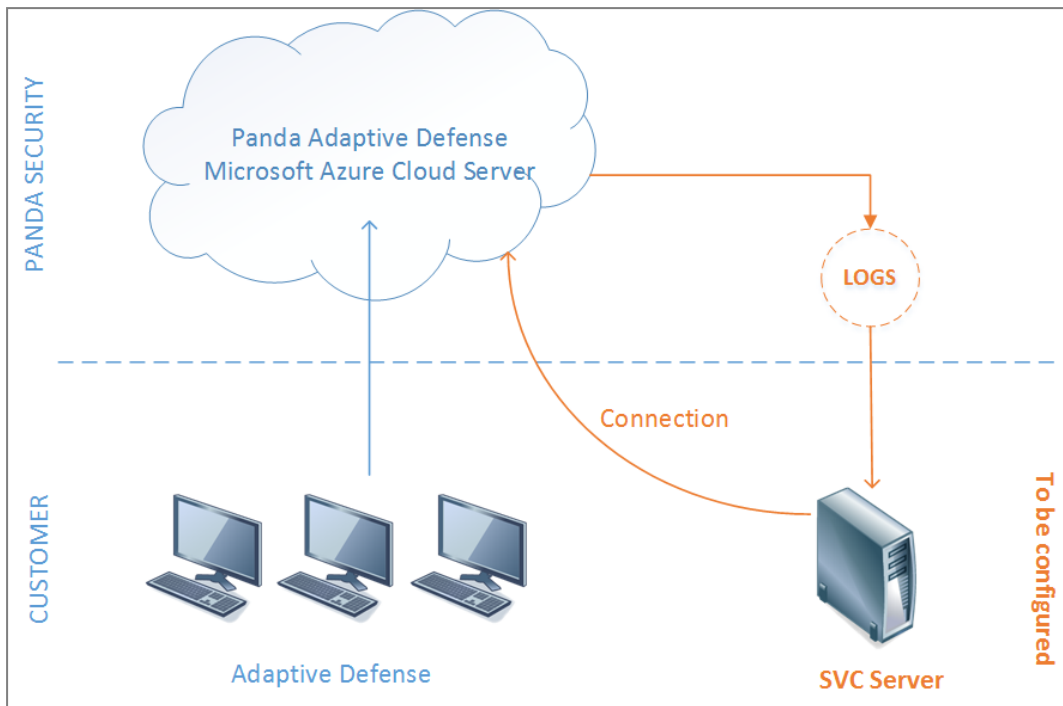
4.6 Configuring SVC to collect Panda Adaptive Defense logs

SVC can collect logs from Panda Adaptive Defense and Panda Adaptive Defense 360 products. Stormshield recommends connecting SVC directly to the Panda cloud server. If you have previously installed Panda SIEMFeeder, configure a connection to an sFTP server. For more information, please refer to the section [Connecting SVC to an sFTP server](#).

You must have a Panda SIEMFeeder license to be able to collect Panda logs via SVC.

4.6.1 Connecting SVC to Panda's cloud server

Panda's logs are processed in Panda's cloud, then collected by SVC.



To collect Panda logs directly on the Panda cloud server, you need to:

- In SVC, [configure the connection to Panda cloud](#),
- In SVC, [enable Panda log collection](#),
- Leave https port 443 open on your firewall.

Configure the connection to Panda cloud

1. Open SVC Configurator. For more information, refer to [Opening SVC Configurator](#).
2. Select the **Panda server configuration** menu, then **Configure Panda cloud logs synchronization** and confirm.
3. Enter your Panda client number and confirm.
4. Enter the email address of your Panda account as well as the corresponding password and confirm.
5. In the window that opens, check the Panda cloud configuration.

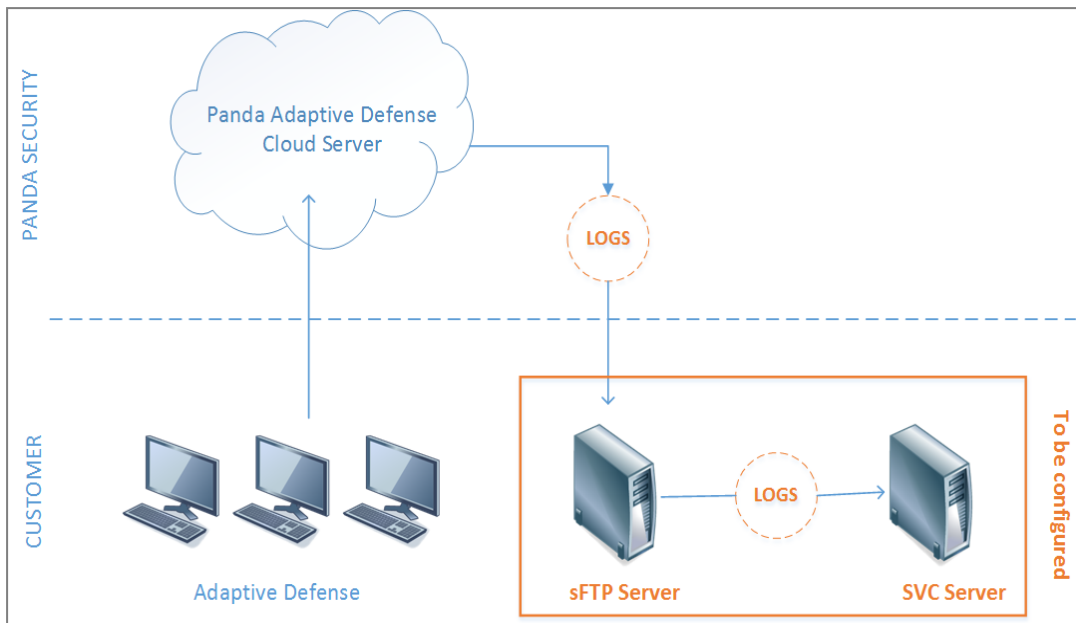
Enable Panda log collection

1. Open SVC Configurator. For more information, refer to [Opening SVC Configurator](#).
2. Select the **Panda server configuration** menu, then **Enable/Disable Panda logs collection** and confirm.
3. Select **Enable Panda cloud logs synchronization**, press the spacebar, and confirm.
The connection to Panda is now enabled for collecting logs.

4.6.2 Connecting SVC to an sFTP server

If you have previously installed Panda SIEMFeeder, configure a connection to an sFTP server to collect Panda's logs.

These logs are processed in Panda's cloud, then sent to an sFTP server where they are then collected by SVC.



To collect Panda logs via an sFTP server, you need to:

- Install an sFTP server,
- Send the login credentials for logging on to this server to Panda Security, as well as the path of the folder to which Panda logs will be sent,
- In SVC, [configure the connection to this sFTP server](#),
- In SVC, [enable Panda log collection](#).

This section only describes how to configure and enable the connection in SVC.

Configuring the connection to the Panda sFTP server

1. Open SVC Configurator. For more information, refer to [Opening SVC Configurator](#).
2. Select the **Panda server configuration** menu, then **Configure FTP logs synchronization** and confirm.
3. Enter the IP address or DNS name of the sFTP server used for collecting Panda Adaptive Server logs.
4. Enter the name of a user allowed to log on to this sFTP server and confirm.
5. Enter this user's password and confirm.
6. Enter the path of the folder on the sFTP server in which logs will be collected, and confirm.
7. In the window that opens, check the FTP configuration.

Enable Panda log collection

1. Open SVC Configurator. For more information, refer to [Opening SVC Configurator](#).
2. Select the **Panda server configuration** menu, then **Enable/Disable Panda logs collection** and confirm.
3. Select **Enable FTP logs synchronization**, press the spacebar, and confirm.
The connection to Panda is now enabled for collecting logs.



5. Monitoring Stormshield solutions with SVC

Stormshield solutions can be monitored on a Kibana-based web interface. This interface enables the generation of customizable dashboards, graphs and statistics based on logs sent by the various Stormshield solutions.

5.1 Logging on to the SVC web interface

1. In SVC Configurator, select the **Network status** menu. The **Address** field indicates the IP address of your SVC server.
2. Using your web browser, log on to this IP address in HTTPS (https://svc_ip_address).

i NOTE

Look up this web site to check which browser versions SVC supports:
https://www.elastic.co/fr/support/matrix#matrix_browsers.

3. In the connection window, enter the following information:
 - **User**: `log`
 - **Password** : by default it is the same password as the `root` user of the SVC server, except if you have modified it afterwards via the Configurator. For more information, please refer to the section [Modifying passwords](#).

The SVC web interface will appear.

5.2 Kibana documentation

This guide describes some of the main principles regarding the navigation and customization of SVC dashboards, but you will find the full procedures in Kibana's documentation.

1. In the SVC web interface, in the menu on the left, select **Management** in order to find out the version of Kibana that SVC uses.
2. On Kibana's website, look up the Kibana User Guide:
<https://www.elastic.co/guide/en/kibana/current/index.html>

5.3 Dashboard Presentation

The main dashboard presents an overview of your entire infrastructure's security. You can also display views corresponding to the different product ranges.

5.3.1 SNS views

SNS views provide you with full visibility over your UTM environment. Specifically, they inform you about your security status (identification of vulnerabilities, reporting of IPS alarms), your users' web activity (most frequently visited websites, most frequently used applications), or how your networks are running (bandwidth use, protocol-based load balancing).

All SNS logs that SVC collects are described in the technical note *Description of audit logs* available on [MyStormshield](#).



5.3.2 SES views

SES views inform you about the security of your workstations, in particular, by allowing you to identify blocked programs or affected users, or even geolocate the source of attacks.

5.3.3 SDMC views

With the help of such views, you can easily monitor how your encryption product is being used in the cloud and for mobile devices, identify the most active users, the most frequently shared documents, the most frequently used shared areas, etc.

5.3.4 SDS Enterprise views

Thanks to SDS views, you can track the use of your encryption solution: for example, identifying the users or hosts that have been accessing confidential documents, etc. All events may also be inspected (connections, encryption operations, errors, etc).

5.3.5 Panda Views

Panda views give you details about the security status of the workstations that Panda Adaptive Defense manages, in particular by allowing you to identify undesirable programs that have been blocked, the distribution of installed Microsoft programs, as well as the deployment status of Panda agents.

5.3.6 MLCS views

The MLCS view gives you an overview of your infrastructure's security, based on the combined analysis of logs from our various products: SES, SDS and SNS. Thanks to this view, it is possible, for example, to determine which sensitive machines (i.e., those that have encrypted documents) are under greatest threat.

5.3.7 SVC views

This view provides a comprehensive status of how your SVC solution is running.

It shows indicators on log collection and on the use of hardware resources (CPU, memory, disk space).

5.4 Navigating the SVC web interface

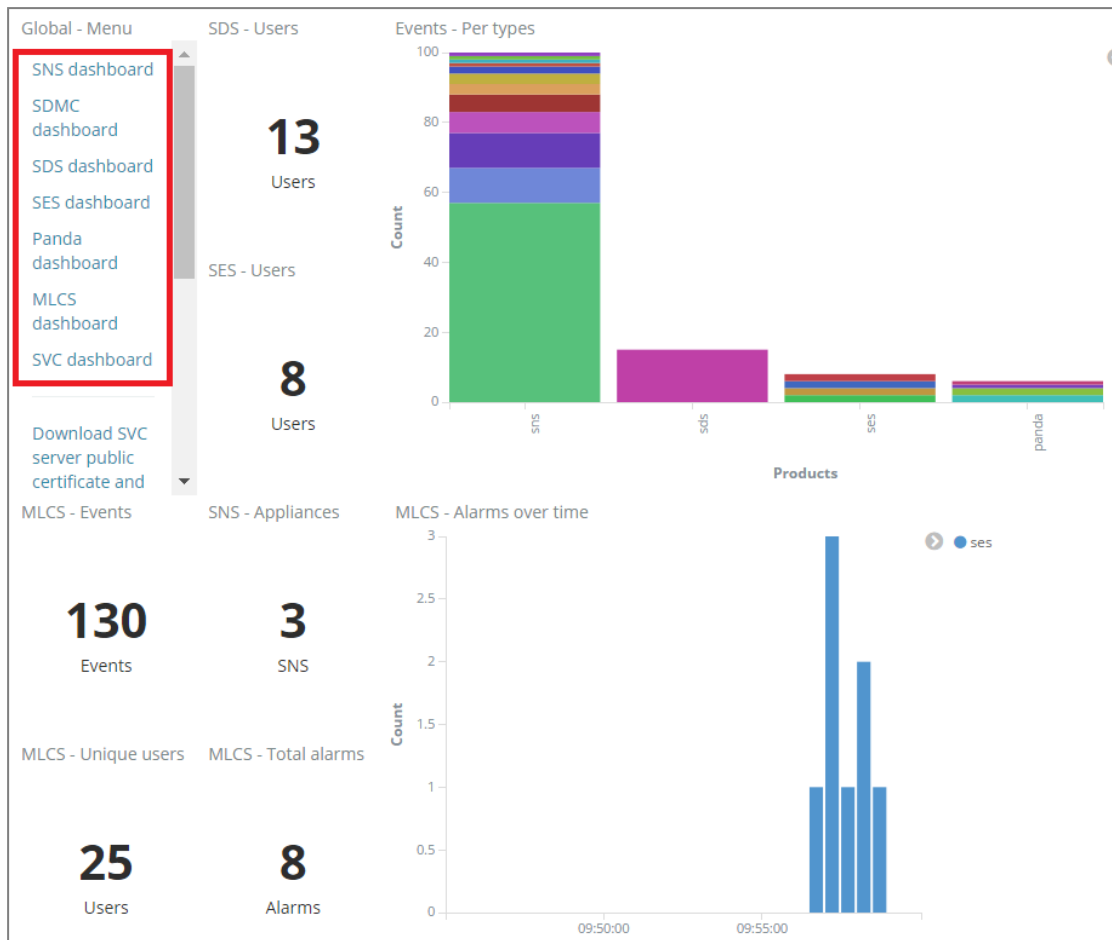
Navigating through the web interface allows you to display views by product range and modify the periods viewed.

Regardless of where you are in the interface, you can return to the main dashboard at any time

by clicking on .

5.4.1 Viewing information about a Stormshield product range


1. In the menu on the left, click on the menu corresponding to the product range, for example **SNS Dashboard**. The main dashboard will appear.



2. In the menu on the left, click on the various views offered for the range, e.g. **Data Volume View**.

5.4.2 Defining periods

By default, dashboards and views display a limited period that you can modify.

1. At the top right side of the web interface, click on the  icon. The selection of periods then appears.



- Click on a pre-defined period.
- or -
To express a relative period, click on **Relative** in the menu to the left, then manually enter the desired period and click on **Go**.

- or -
To express an absolute period, click on **Absolute** in the menu to the left, select your start and end dates in the calendars and click on **Go**.
The dashboard will take into account your new period.


TIP

You can also modify the period from a graph by selecting the desired period with the mouse.

5.4.3 Filtering displayed data

The data in the dashboard can be filtered in order to show only logs that belong to a certain category. For example, filter by firewall to see only information generated by a given firewall.

- In the **SNS - Events - Per appliance** view in the main **SNS** dashboard, click on one of the firewalls.
The name of the filter will appear at the top left corner against a gray background. The dashboard will refresh to show only relevant information about this firewall.

- To delete the filter and show all information again, scroll the mouse over the filter name and click on the  icon.



5.4.4 Going directly to a dashboard or a view

1. In the menu at the top right, click on **Open**. The list of dashboards and views will appear in alphabetical order.
2. If necessary, enter part of the name of your view in the Dashboards Filter field to show only relevant names.
3. Click on the name of the desired dashboard or view. It will then appear.

**TIP**

This procedure also allows you to go back to the dashboards if you end up on an empty page.

5.5 Customizing dashboards

A dashboard (or view) is made up of several visualizations that each display a different type of information.

SVC comes with a wide array of predefined dashboards for all Stormshield product ranges. Nonetheless, you can modify existing dashboards or create new customized dashboards.

This guide provides a use case on how to modify a dashboard. However, it does not offer detailed procedures on creating dashboards, searched and visualizations. You will find all the necessary information in the Kibana documentation. For more information, refer to the section [Kibana documentation](#).

5.5.1 Recommendations

Upgrading SVC does not automatically allow the migration of modified dashboards. You are therefore advised to:

- refrain from modifying existing dashboards and views,
- create new dashboards instead. For simplicity, duplicate an existing dashboard that you can then use as a baseline,
- name your new dashboards by adding a *CUSTOM* prefix (for example, *CUSTOM SNS View*). This will allow you to identify them easily in order to export them and import them later into a new version of SVC.

5.5.2 Use case: modifying a dashboard by adding a customized view to it

We wish to modify the **SNS > Applications View** as follows:

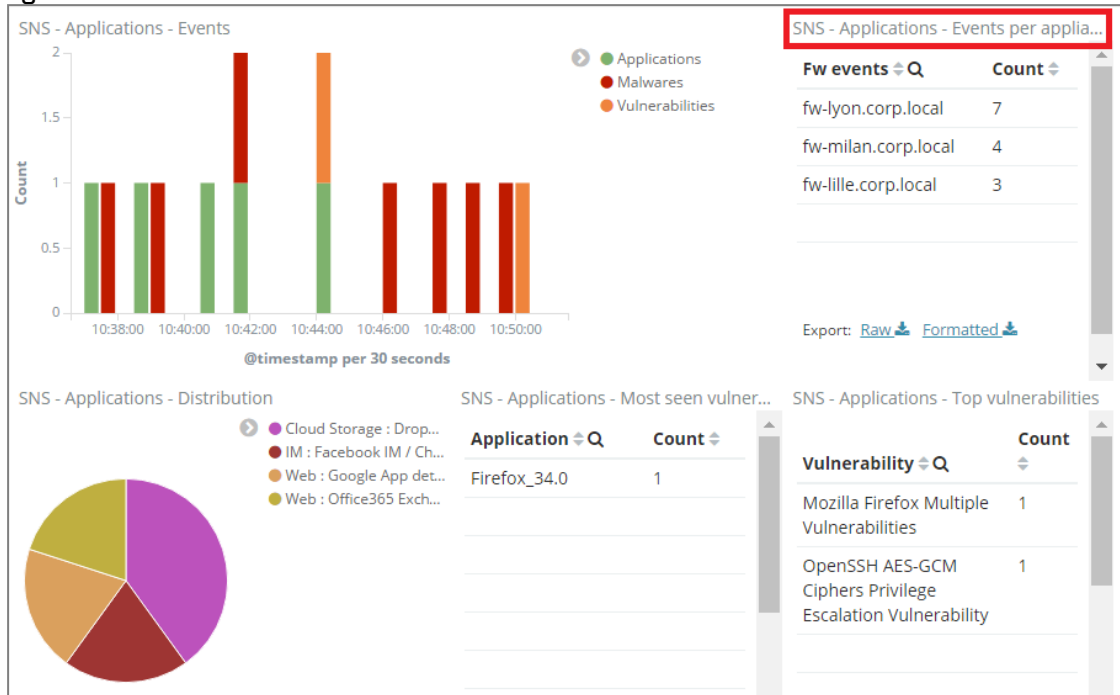
- By deleting the view of events by firewall (SNS-Applications-Events per appliance),
- By creating and adding a new visualization : the list of the top 10 users that generate the most logs.

This new view will then allow filtering logs by user.

1. In the menu on the left, click on **SNS Dashboard** then **Applications View**. The **SNS - Applications - View** dashboard will then appear.



2. Delete the **SNS-Applications-Events per appliance** view by clicking on the cross in the top right corner.



3. Create a new view by clicking on **Visualize**. The **Create a new visualization** page appears.

Stormshield 1.2.0-DEV-24 develop
Visibility Center

Visualize / Step / 1

Create New Visualization

- Area chart**
Great for stacked timelines in which the total of all series is more important than comparing any two or more series. Less useful for assessing the relative change of unrelated data points as changes in a series lower down the stack will have a difficult to gauge effect on the series above it.
- Data table**
The data table provides a detailed breakdown, in tabular format, of the results of a composed aggregation. Tip, a data table is available from many other charts by clicking the grey bar at the bottom of the chart.
- Heatmap chart**
A heat map is a graphical representation of data where the individual values contained in a matrix are represented as colors.

4. Create a list of users by selecting a **Data Table** view.
5. In the **From a New Search** panel, **Select index**, select **stormshield-sns*** as the aim is to use logs from the SNS product range.
The **Count** field in the right panel will show the total amount of logs for the SNS range: 9298 logs for this demo version.



- In the **Buckets** zone in the left panel, click on **Split Rows**, then fill in the fields as follows in order to filter logs by user:

buckets

Split Rows ⊞

Aggregation

Terms ▼

Field

user ▼


Order By

metric: Count ▼

Order Size

Descending ▼ 10

Custom Label

- **Aggregation:** select Terms
 - **Field:** select string>user
 - **Order By:** select metric: Count,
 - **Order:** select Descending
 - **Size:** enter 10
- Click on . The list of the top 10 users generating the most logs appears in the panel on the right.
 - In the menu at the top right, click on **Save** to save the visualization.
 - In the **Save Visualization** field, enter a name that complies with the recommendations, i.e., with a *CUSTOM* prefix (for example *CUSTOM Top 10 Users*). For more information, see the section [Customizing dashboards](#).
 - Click on **Save**.
 - Go back to the **SNS - Applications - View** dashboard and click on **Add** in the menu at the top right.
 - In the **Visualization Filter** field, enter part of or the whole name of the "CUSTOM Top 10 Users" visualization that you have just created, and select it in the list. The visualization will appear in the dashboard.



13. Position it and adjust its size to your preferences.

The screenshot displays a dashboard with several monitoring components:

- SNS - Applications - Events:** A bar chart showing event counts over time. The x-axis is labeled '@timestamp per 30 seconds' with ticks at 15:25:00, 15:27:00, 15:29:00, 15:31:00, 15:33:00, 15:35:00, and 15:37:00. The y-axis is labeled 'Count' and ranges from 0 to 1. The legend includes Applications (green), Malwares (red), and Vulnerabilities (orange).
- SNS - Applications - Distribution:** A pie chart showing the distribution of applications. The legend includes Cloud Storage : Apple... (purple), IM : Facebook IM / Ch... (red), and Web : Office365 Exch... (orange).
- SNS - Applications - Top vulnerabilities:** A table listing vulnerabilities and their counts.

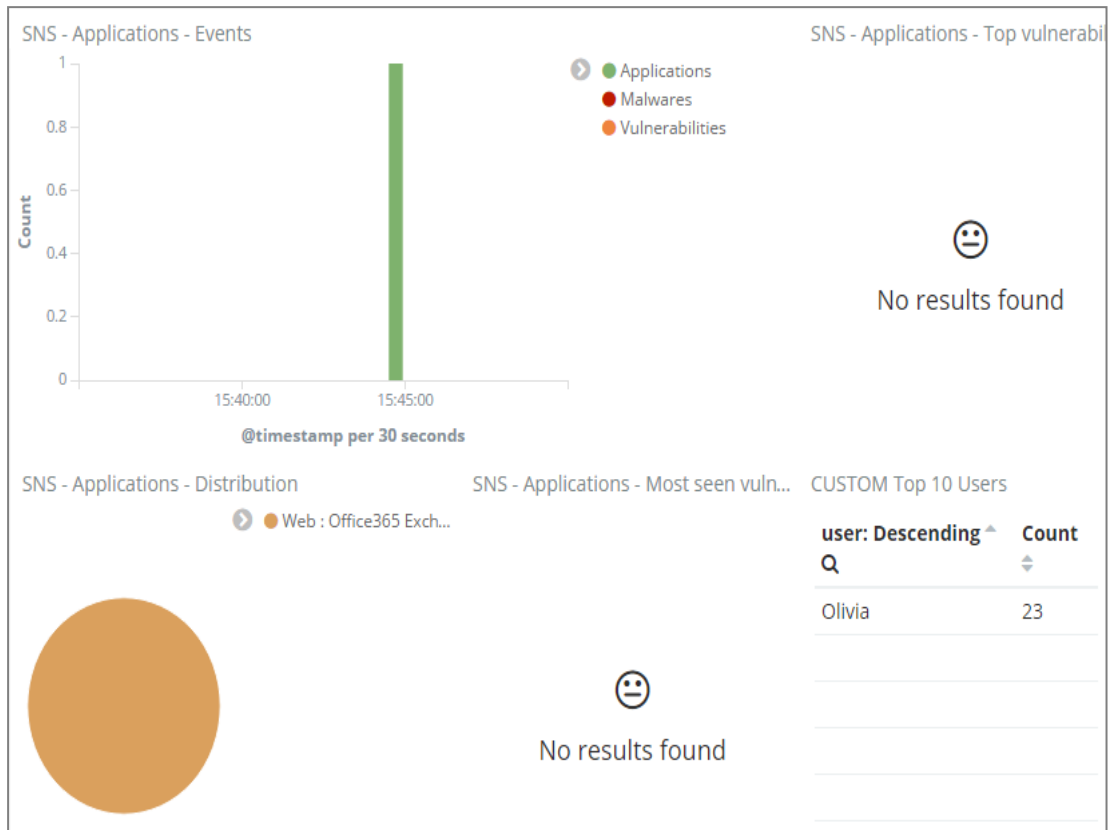
Vulnerability	Count
OpenSSH AES-GCM Ciphers Privilege Escalation Vulnerability	2
Google Chrome Flash Player Multiple Vulnerabilities	1
Oracle Java Multiple Vulnerabilities	1
PHP XML Parsing Buffer	1
- SNS - Applications - Most seen vulnera...:** A table listing applications and their counts.

Application	Count
Google_Chrome_39.0.2171.71	1
JRE_1.7.0_51	1
- CUSTOM Top 10 Users:** A table listing the top 10 users and their counts, highlighted with a red border.

user: Descending	Count
Emily	21
Harry	20
Isla	19
Charlie	18
George	18
James	17
Poppy	17
Isabella	16
Thomas	16
Jessica	15



- Click on a user, Olivia for example, in order to filter the dashboard data by this user. Only logs generated by this user will be shown.



- To remove a filter on the user, scroll the mouse over the **user: "Olivia"** filter icon, and click on

The page will refresh and the dashboard will show data for all users again.

- In the menu at the top right, click on **Save** to save the modified dashboard. Select a name that complies with the recommendations, i.e., with a *CUSTOM* prefix (for example *CUSTOM SNS View*). For more information, see the section [Recommendations](#).



6. Managing and maintaining the server

6.1 Backing up the virtual machine

Back up the SVC server virtual machine on a regular basis to be able to restore it if a problem occurs.

6.2 Displaying the version of SVC server components

- At the `svc login` command prompt, log on with the `root` account, then run the following command:

```
svc-version-cmp
```

The list of components displays with the component versions.

6.3 Updating the geolocation database

SVC uses the MaxMind database to geolocate the IP addresses of computers mentioned in logs. MaxMind regularly provides updates for this database, which you can import into SVC whenever you wish.

1. On the Maxmind website, download the GeoLite2 City database in MaxMind DB format (`.mmdb` extension). The freeware version is available at <https://dev.maxmind.com/geoip/geoip2/geolite2>, but you can also purchase a full version with more comprehensive features.
2. On the SVC server, browse until you reach the folder `/data/logstash/vendor/bundle/jruby/1.9/gems/logstash-filter-geoip-4.0.4-java/vendor`.

```
[root@svc] > cd /data/logstash/vendor/bundle/jruby/1.9/gems/logstash-filter-geoip-4.0.4-java/vendor
```

3. Delete the `GeoLite2-City.mmdb` file found in this folder.

```
[root@svc] > rm GeoLite2-City.mmdb
```

4. In this same folder, copy the GeoLite2 City database file that you had downloaded at the beginning of this procedure.
5. Restart the SVC Logstash component.

```
[root@svc] > service logstash restart
```

The geolocation database is now up to date.

6.4 Extending the size of the partition allocated to SVC

The disk partition allocated to SVC is 200 GB by default. The partition contains the configuration files of various components as well as SVC archives and data.

The size of this partition can be increased when needed.

The SVC virtual machine needs to be restarted for this procedure; log collection will therefore be disrupted while it restarts.



6.4.1 Modifying the hypervisor's disk parameters

In the event you need to increase the amount of disk space allocated to the virtual machine of the SVC server, simply shut down the virtual machine and modify the disk parameters of the hypervisor that hosts it.

For more information on how to modify disk parameters, refer to your hypervisor's documentation.

6.4.2 Extending the size of the partition

After having modified your hypervisor's disk settings, you need to increase the size of the partition in order to use the space that has become available.

Run the following commands on the SVC server.

1. Using the `fdisk` command, determine the partition for which you wish to extend the size. In the example below, you are increasing the size of the partition `/dev/hdb1` to 400 GB. This procedure also applies to `/dev/hdx` and `/dev/sdx`.

```
[root@svc] > fdisk -l
...
...
Disk /dev/hdb: 200 GiB, 214748364800 bytes, 419430400 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0b297230

Device      Boot Start      End          Sectors      Size Id Type
/dev/hdb1  2048        419430399  419428352    200G 83 Linux
```

2. Check that the allocated disk space is indeed available on the disk (`/dev/hdx` or `/dev/sdx`) and on the partition (`/dev/hdx1` or `/dev/sdx1`).

```
[root@svc] > fdisk -s /dev/hdb
419430400
[root@svc] > fdisk -s /dev/hdb1
209714176
```

You will see that the partition is 200 GB whereas the disk space is 400 GB.

3. Shut down all processes using the partition. The `fuser` command lists all processes that access the partition.

```
[root@svc] > fuser -vm /dev/hdb1
/dev/hdb1:  USER      PID ACCESS COMMAND
           root      kernel mount /data
           elasticsearch  705 f..ce. java
           kibana      736 ...e. node
           logstash    822 f..e. java
           root        857 ...e. metricbeat-god
           root        859 ...e. metricbeat
```

You will then see that the services `elasticsearch`, `kibana`, `logstash` and `metricbeat` use the partition `/dev/hdb1`, so you need to shut them down. First stop the `monit` service, then all the other services.

```
[root@svc] > service monit stop
[root@svc] > service metricbeat stop
...
...
```



4. Check that no more services access the partition.

```
[root@svc] > fuser -vm /dev/hdb1
          USER      PID ACCESS COMMAND
/dev/hdb1: root      kernel mount /data
```

5. Unmount the partition using the umount command.

```
[root@svc] > umount -l /dev/hdb1
```

6. Check that the partition is no longer available using the df command.

```
[root@svc] > df
Filesystem      1K-blocks      Used    Available Use%    Mounted on
/dev/root        1693072      232428    1352604   15%    /
devtmpfs         1020916         0      1020916   0%    /dev
tmpfs            1022196       232      1021964   1%    /run
tmpfs            1022196         0      1022196   0%    /tmp
none             206292664    1959060    193831512 2%    /var
```

7. Display information about the disk using the fdisk p command.

```
[root@svc] - > fdisk /dev/hdb

Welcome to fdisk (util-linux 2.26.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): p
Disk /dev/hdb: 400 GiB, 429496729600 bytes, 838860800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0b297230

Device      Boot Start          End      Sectors  Size Id Type
/dev/hdb1    2048 419430399 419428352  200G 83 Linux
```

You will see that the disk space is 400 GB whereas the partition is 200 GB.

8. Delete the partition `/dev/hdx` or `/dev/sdx` using the fdisk d command. No data will be lost.

```
[root@svc] > fdisk /dev/hdb
Command (m for help): d
Selected partition 1
Partition 1 has been deleted.
```



9. Create a new partition using the fdisk n command. Use default parameters.

```
Command (m for help): n
Partition type
p   primary (0 primary, 0 extended, 4 free)
e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-838860799, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-838860799, default
838860799):

Created a new partition 1 of type 'Linux' and of size 400 GiB.

Command (m for help): p
Disk /dev/hdb: 400 GiB, 429496729600 bytes, 838860800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0b297230

Device      Boot Start          End      Sectors  Size Id Type
/dev/hdb1                2048 838860799 838858752  400G 83 Linux
```

You will see that the disk space is 400 GB and the partition is now 400 GB.

10. Confirm changes using the fdisk w command.

```
Command (m for help): w

The partition table has been altered.

Calling ioctl() to re-read partition table.

Re-reading the partition table failed.: Device or resource busy
The kernel still uses the old table. The new table will be used at the next
reboot or after you run partprobe(8) or kpartx(8).
```

11. Reboot the SVC server's virtual machine in order to apply the changes.

```
[root@svc] > reboot
```

When the server is restarting, log collection will be temporarily suspended and certain logs will not appear in the dashboards.

12. Configure the partition so that it occupies all the space allocated to it using the resize2fs command.

```
[root@svc] - {~} > resize2fs /dev/hdb1
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/hdb1 is mounted on /data; on-line resizing required
old_desc_blocks = 13, new_desc_blocks = 25
The filesystem on /dev/hdb1 is now 104857344 blocks long.

[root@svc] - {~} > df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       1.7G  227M  1.3G  15% /
devtmpfs        997M     0  997M   0% /dev
tmpfs           999M  240K  999M   1% /run
tmpfs           999M  172K  999M   1% /tmp
/dev/hdb1       394G  1.9G  374G   1% /data
none            394G  1.9G  374G   1% /var
```

The partition now takes up 400 GB.



6.5 Dedicating a partition to data analysis

In order to improve SVC's performance, you can dedicate a partition to the Elasticsearch database, which takes charge of analyzing data. This partition must run on a fast hard disk (e.g., SSD). If your SVC configuration already includes fast hard disks, this procedure will not change anything.

To begin with, you need to add a disk to your hypervisor, then configure SVC by running a script.

6.5.1 Recommendations

- This procedure can be applied from version 1.2 of SVC upwards.
- Do not use the commands *svc-replay* or *svc-forensic* when carrying out this procedure.
- As Elasticsearch will not take into account logs collected during this procedure, they cannot be viewed in the SVC web interface as a result. However, you can still access them in the folder */var/archives*.
- To optimize performance, the hard disk created must not be located on a network file server, such as NFS for example.

6.5.2 Adding a disk to the hypervisor

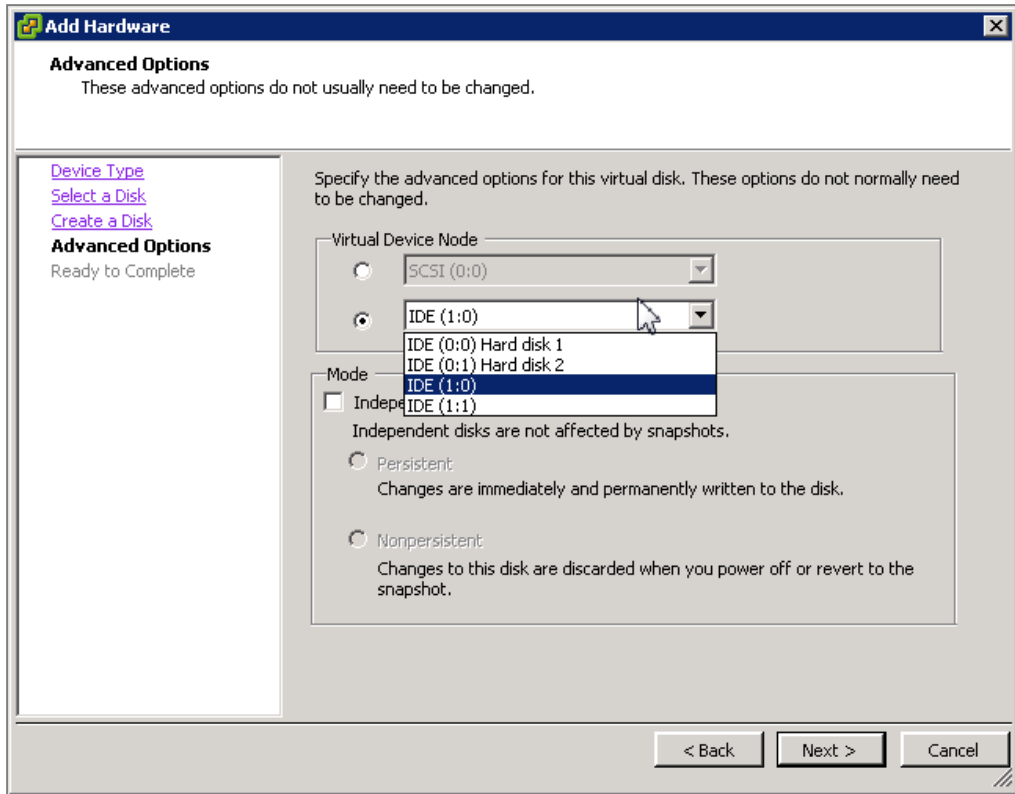
The configuration of the SVC virtual machine's hypervisor must be modified by adding a disk to the IDE or SCSI controllers. If adding an IDE disk, you must first power down the virtual machine.

ESX

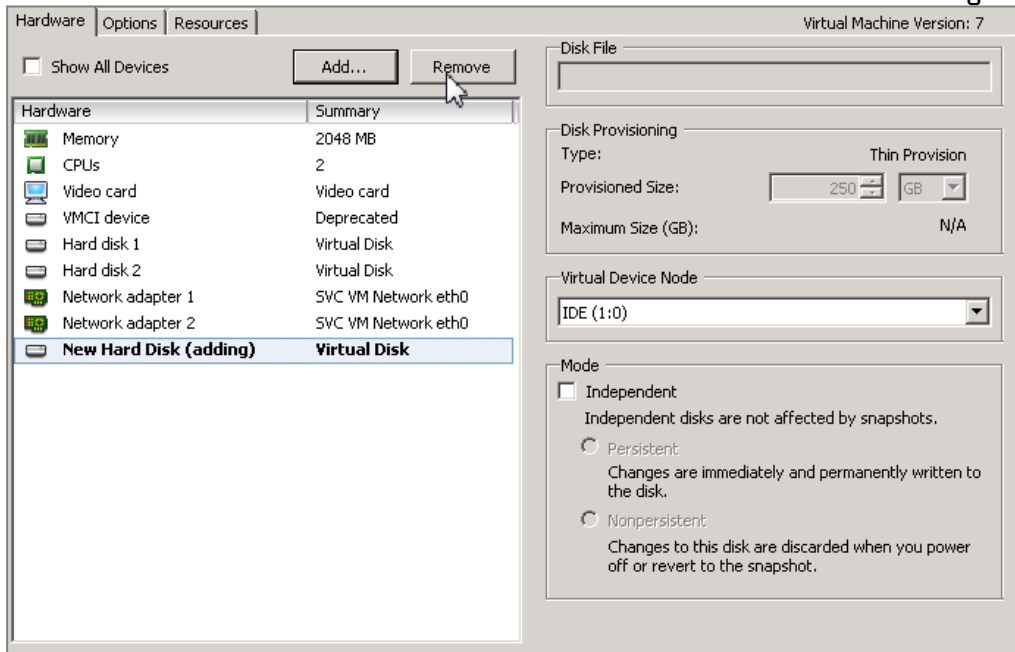
1. In the hypervisor console, edit the properties of the virtual machine.
2. In the **Hardware** tab, click on **Add**.
The Add Hardware wizard then appears.
3. In the **Device type** section, select **Hard disk**.
4. In the **Select a disk** section, select **Create a virtual disk**.
5. In the **Create a disk** section, select the size of the disk that will contain Elasticsearch data (> 100 GB). Select an SSD that will serve as a data bank.



6. In **Advanced options**, select **IDE** in **Virtual device node**. Ensure that you select an available location.



7. Click on **OK** to confirm the addition of the new hard disk. You will obtain the following result.



Hyper-V

1. In the hypervisor console, edit the parameters of the virtual machine.
2. Add a disk to the IDE or SCSI controller. Opt for SCSI controllers where possible as IDE disks are not compatible with disks exceeding 127 GB.



3. Configure this new disk with a set size and create a blank virtual disk with the desired size. The minimum size for Hyper-V 2008 is 100 GB. There is no minimum size for Hyper-V 2012.
4. Once you have completed the configuration, click on **Apply**.
Ensure that the number found on the **Location** list has not already been used by another disk belonging to the same disk controller.

6.5.3 Configuring SVC

1. On MyStormshield, select **Downloads > Stormshield Visibility Center > Tools** and click on **Elasticsearch partition creator** in order to download the script `svc-create-elastic-partition.sh`. This script makes it possible to automatically create and set up the partition dedicated to Elasticsearch.
2. Copy the script to the SVC server.
3. Run the command `lsblk` to obtain the name of the virtual disk that you have just added. If the disk is linked to an IDE controller, its name in the device folder will look like `/dev/hdX` where X= c, d, e, etc. If the disk is linked to an SCSI controller, the name will look like `/dev/sdX` where X= c, d, e, etc. In the example below, a 250 GB IDE disk is used.

```
[root@svc] - {~} > lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
hda         3:0    0   4G  0 disk
├─hda1      3:1    0 38.8M 0 part
├─hda2      3:2    0    2G  0 part /
└─hda3      3:3    0    2G  0 part
hdb         3:64   0 200G  0 disk
└─hdb1      3:65   0 200G  0 part /data
hdc         22:0    0 250G  0 disk
```

4. Run the script by specifying the path of the device using the option `-n`.
In the example below, the script has been copied to the SVC server at the location `/home/root` and the command was run for a virtual hard disk added to an IDE controller in ESX.

```
[root@svc] > sh /home/root/svc-create-elastic-partition.sh -n /dev/hdc
```

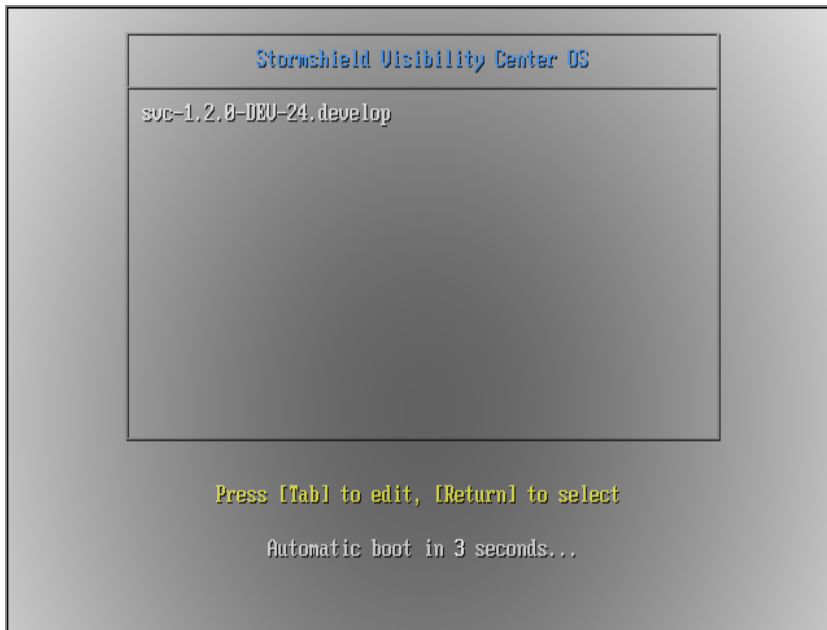
5. Confirm by typing *yes*, then *Enter* to continue creating the dedicated partition. This operation may take a while as it will move all Elasticsearch data.
6. Run the command `df -h` to check that the partition has been properly mounted.
It may take several minutes before the Elasticsearch database becomes fully operational, and you can use your web interface again and analyze data.

6.6 Resetting the "root" administrator password

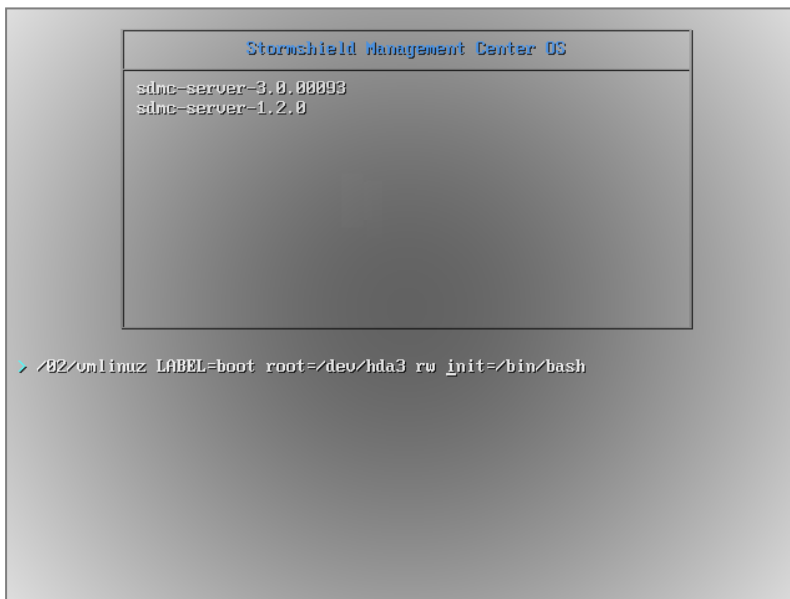
⚠ WARNING
QWERTY keyboard layout is required to perform these actions.

6.6.1 Changing the server startup mode

1. From the virtual environment, restart the SVC server.
2. When the server restarts and the screen to select the server version displays, press the **TAB** key to enter the start-up screen **Edition** mode.



3. The command line to edit server startup displays. At the end of the line add: `rw init=/bin/bash`.



4. Press **Enter** to validate and start the server.

6.6.2 Changing the password

1. The server starts. Enter the command `passwd`.
2. Enter and confirm the new password (QWERTY keyboard layout).
3. Enter the command `shutdown -nr now` to restart the server.

6.7 Troubleshooting

If you encounter issues while monitoring Stormshield applications in SVC, the window below will appear, allowing you to determine the plugin causing such issues.



Status: Red		SVC
Heap Total (MB) 71.84	Heap Used (MB) 58.98	Load 0.11, 0.11, 0.14
Response Time Avg (ms) 5.92	Response Time Max (ms) 41.00	Requests Per Second 2.10
Status Breakdown		
ID	Status	
ui settings	▲ Elasticsearch plugin is red	
plugin:kibana@5.2.0	✓ Ready	
plugin:elasticsearch@5.2.0	▲ Unable to connect to Elasticsearch at http://localhost:9200.	
plugin:console@5.2.0	✓ Ready	
plugin:timelion@5.2.0	✓ Ready	

6.8 Updating the SVC server

To upgrade SVC to a higher version, you will need to:

1. Export dashboards and visualizations if you have customized them. There is the likelihood of them being overwritten during the upgrade. See [Exporting new dashboards](#).
2. Perform the SVC upgrade. See [Performing the SVC upgrade](#).
3. Import customized dashboards and visualizations if you have exported them earlier. See [Importing dashboards](#).

If you do not have customized dashboards or visualizations, perform only the upgrade without imports or exports.

6.8.1 Requirements

- Ensure that the SVC virtual machine has at least 5% disk space available.
- Before performing the upgrade, you must disable the network cards in order to stop collecting logs. Enable them again after the upgrade, once the SVC server has restarted.

6.8.2 Exporting new dashboards

If you have followed the [Recommendations](#), names of new dashboards should contain the *CUSTOM* prefix.

1. Log on to the SVC console and run the following commands in order to export dashboards:

```
[root@svc] > elasticdump \
  --input=http://localhost:9200/.kibana \
  --output=$ \
  --type=data \
  --searchBody="{\"filter\": {\"bool\": { \"filter\": [{ \"terms\": {
  \"_type\": [\"search\", \"dashboard\", \"visualization\"] }}, {
  \"prefix\": {\"_id\": \"CUSTOM\"} }]} }" \
  > custom_objects.json
```

The file *custom_objects.json* is created in the local folder.



2. Copy the file `custom_objects.json` in a location other than the SVC server. It contains information that you will need in order to re-import customized dashboards and can be overwritten during the upgrade.

6.8.3 Performing the SVC upgrade.

1. From your **MyStormshield** personal area, download the update archive on your workstation.
2. Copy the archive `Stormshield-Visibility-Center-update-x.x.x.upd` to the SVC server.
 - On a Linux machine, create the copy using the SSH protocol with the "root" account

```
$> scp Stormshield-Visibility-Center-update-1.2.0.upd root@<virtual_machine_ip>:/tmp
```
 - On a Windows machine, create the copy using a WinSCP tool.
3. On the SVC server, enter the command `svc-update -u Stormshield-Visibility-Center-update-x.x.x.upd`. Replace `x.x.x` by the product version.

```
[root@svc] > svc-update -u /tmp/Stormshield-Visibility-Center-update-1.2.0.upd
Information:
=====
- Update archive      : /tmp/Stormshield-Visibility-Center-update-1.2.0.upd
- Extract directory  : /tmp/tmp/update
...
SUCCESS: update installed successfully. Please reboot.
```

4. Once the upgrade is complete, restart the SVC server. How long the upgrade takes depends on the volume of the database to be migrated.

When the server is restarting, log collection will be temporarily suspended and certain logs will not appear in the dashboards.

i NOTE

After the upgrade, demo mode will be disabled.

6.8.4 Importing dashboards

After the upgrade, if customized dashboards have been lost, you will need to re-import them.

1. Copy the export file `custom_objects.json` to the SVC server.
2. Log on to the SVC console and go to the folder in which the export file is located.
3. Run the following commands:

```
[root@svc] > elasticdump \
--input=custom_objects.json \
--output=http://localhost:9200/.kibana \
--type=data
```

6.8.5 Troubleshooting

Refer to this section in order to resolve frequently encountered issues while upgrading SVC.

Upgrade archive cannot be copied via WinSCP

- **Situation:** When you copy the upgrade archive to the SVC server, WinSCP generates an error message indicating a communication issue (Host is not communicating for more than 15 seconds. Still waiting...).
- **Cause:** The default WinSCP shell is not suitable for SVC.



- *Solution:* In WinSCP advanced options, select `/bin/bash` in the **Shell** field of the **Environment** > **SCP/Shell** menu.

Some visualizations no longer work after an upgrade

- *Situation:* Certain visualizations no longer appear in the dashboards and show a message resembling the following:
`Could not locate that index-pattern-field (id: client8)`
- *Cause:* The data model changed during the upgrade and certain fields are no longer available.
- *Solution:* Manually correct the affected dashboards in the SVC web interface.



STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2018. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.