ESET Tech Center

Migrate from ERA Proxy (Virtual appliance) to Apache HTTP Proxy in ESMC 7

Anish | ESET Nederland - 2018-08-20 - Comments (0) - 7.x

Issue

You have an ERA 6.x environment running with ERA Proxy (on a Virtual Appliance) component and you want upgrade to ESET Security Management Center (ESMC) 7, which does not support ERA Proxy. You can replace your appliance with a new one and enable Apache HTTP Proxy to substitute the role of ERA Proxy in the infrastructure. The transition must follow strict rules described in this article.

Are you using ERA Proxy on a Windows host?

Details

Solution

Connection limitations

The ERA 6.x Proxy component is discontinued in ESMC 7. Be careful about the connection compatibility:

- ERA 6.x Agents can connect to ESMC 7 Server.
- ESET Management (EM) Agent (version 7) cannot connect to ESMC Server via ERA Proxy.
- EM Agent (version 7) cannot connect to ERA 6.x Server.
- Do not upgrade ERA 6.x Agents before a proper proxy solution is set up.
- It is not possible to run the Agent deployment task on clients which ESMC server can reach only via Apache HTTP Proxy.

I. Prepare your ERA 6.x environment

1. Back up your ERA Server (backup database, CA and certificates).
2. Upgrade your ERA Server to ESMC 7 via **Remote Administrator Components Upgrade Task**. (Server, Agent and Web Console are upgraded).
3. Wait approximately 24 hours to make sure that the upgraded environment runs smoothly.

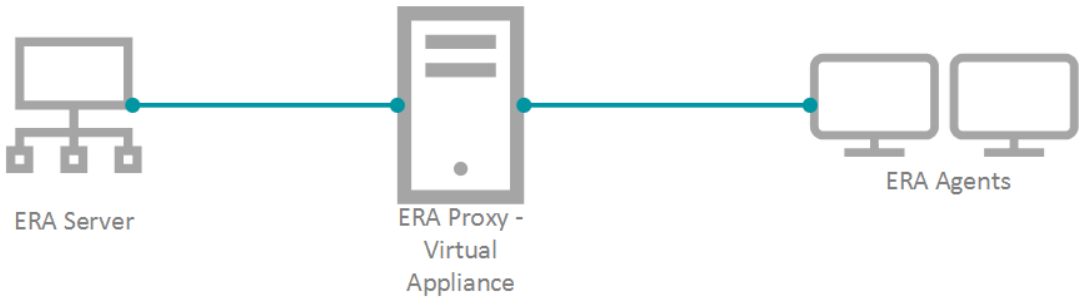

Figure 1-1

II. Deploy the new Virtual Appliance and connect it to your ESMC Server

NOTE:

To keep your proxy safe and well configured, you have to replace your old ERA Proxy - Virtual Appliance with the new one. However, ESMC 7 does not provide a standalone proxy configuration, like ERA 6.x did. We recommend you to deploy a new ESMC Server - Virtual Appliance. The new Server is not used as a administration server, but just a proxy. The correctly configured Apache HTTP Proxy is included in the ESMC 7 VA.

1. Download ESET Security Management Center 7 Virtual Appliance from the ESET download page.

2. Deploy the ESMC 7 VA on your hypervisor.

3. Configure the new Appliance as ESMC Server.
   - Keep the password you set-up here safe. You will need it later.
   - **Enable HTTP Forward Proxy** during the configuration.

4. When the Appliance is deployed and configured, you have to reinstall EM Agent on this Appliance to connect to you main ESMC Server. Open the virtual machine with your ESMC VA **> Enter Management mode >** enter your password **> Login > Exit to terminal.**

5. The Agent installer is located: `/root/eset_installers/Agent-Linux-x86_64.sh`
   Reinstall the Agent to connect to your main ESMC Server. We recomment to use the server-assisted installation. E.g.:

   ```
   /root/eset_installers/Agent-Linux-x86_64.sh \
   --skip-license \
   --hostname=10.1.179.36 \
   --port=2222 \
   --webconsole-user=Administrator \
   --webconsole-password=aB45$45c \
   --webconsole-port=2223
   ```

   Replace the *hostname* and *password* values with actual values from your main ESMC Server. Read more Agent installation.

Figure 2-1

1. Optional: You can stop certain services on the new Appliance to save resources.
   Run following commands in the Terminal:

   ```
   service eraserver stop
   service mysql stop
   service tomcat stop
   ```

   if you are using System V init, use following commands:

   ```
   systemctl stop eraserver
   systemctl stop mysql
   systemctl stop tomcat
   ```

   To prevent ESMC and MySQL services to start after reboot, disable them:

   ```
   systemctl disable eraserver
   systemctl disable mysql
   systemctl disable tomcat
   ```
2. Modify the Apache HTTP Proxy configuration file */etc/httpd/conf.d/proxy.conf*. You can use **nano** editor in the Terminal or access the file using the Webmin. For nano use command:

   ```
   nano /etc/httpd/conf.d/proxy.conf
   ```
   1. If you have changed the default port (2222) for the Agent, find the line `AllowCONNECT 443 2222` and change `2222` to the number of your port.

   2. Add the hostname or IP address of your ESMC Server to the configuration file. The hostname you add must be exactly the same as Agents use to connect the ESMC Server. You can add IP address, hostname or both.
      See the example code below. Add the whole segment of the code to your configuration file.
      Substitute `hostname.example` for your hostname, and `10.1.1.123` for your IP address.

```
#Allow connection to my ESMC Server machine

<ProxyMatch ^(hostname.example|10.1.1.123)$>

Allow from all

</ProxyMatch>
```

If you want to use only the hostname (or IP), use the following syntax and substitute `hostname.example` for your hostname (or IP):

```
#Allow connection to my ESMC Server machine

<ProxyMatch ^hostname.example$>

Allow from all

</ProxyMatch>
```

3. Close the file (Ctrl + x) and save the changes.
4. Restart the **Apache HTTP Proxy** service.

   ```
   systemctl restart httpd
   ```

3. Check on your main ESMC Web Console, if the new Agent is connecting. You can use it for the future maintenance of the proxy machine.

III. Assign a transition policy to a test client

1. Create a new policy on your ESMC Server. In the ESMC Web Console click **Policies** > **Create New**.
2. In the **Basic** section, type a **Name** for the policy.
3. In the **Settings** section select **ESET Management Agent**.
4. Navigate to **Connection** > **Server connects to** > **Edit server list**.
5. Click **Add** and enter the address (the address must match what Agent use in the configuration) of your ESMC Server in the **Host** field. Click **OK**.
6. Change the operator from **Replace** to **Append**.

Figure 3-1

1. Click **Save**.
2. Navigate to **Advanced Settings** > **HTTP Proxy** and set **Proxy Configuration** to **Different Proxy Per Service**.
3. Click **Replication** > **Edit** and enable the **Use proxy server** option.
4. Type the IP address of the proxy machine to the **Host** field.
5. Leave the default value *3128* for the **Port**.
6. Click **Save** and **Finish** to save the policy. Do not assign it to any computer yet.

Important!

It is necessary to have both IP addresses in one list applied on the client. If the Agent does not have this information in the policy, it is unable to connect to the Proxy and the ESMC Server after the upgrade. Such an Agent must be fixed manually by running a repair installation and using the correct ESMC Server address.

If HTTP Proxy setting is not applied in the policy, the Agent is not be able to connect the ESMC Server.

1. Choose one computer which is connected via ERA Proxy and assign the new policy to that test client.

2. Wait a few minutes until the policy is applied and check if the computer is still connecting the ESMC Server.

IV. Upgrade ERA Agents on client computers

1. Run the **Security management Center Components Upgrade Task** to upgrade the selected test client computer.

2. After the client is upgraded to version 7, check if it is still connecting to the ESMC Server. If the computer is successfully connecting after the upgrade, continue to upgrade other computers.

Important!

If you have a more extensive network, begin the upgrade at departments with IT experienced users or those who are physically closer to computers to make the troubleshooting easier.

1. Apply the policy (from the part III.) to the other computers connected via the ERA Proxy.

Figure 4-1

1. Wait a few minutes until the policy is applied and check if clients are still connecting to the ESMC Server.

2. Run the **Security management Center Components Upgrade Task** on these clients.

3. If all clients are connecting to the ESMC Server after the upgrade is finished, you can proceed with next steps.

V. Remove ERA Proxy address from the list of servers

1. Modify the policy (from the part III.): navigate to **Policies >** click the gear icon next to the policy you want to modify and click **Edit**.

2. In the **Settings > Connection** change the operator from **Append** to **Replace.**

Figure 5-1

1. Click **Save**.

2. Click **Finish** to save and apply the policy.

3. You can remove the ERA Proxy Virtual Appliance (remove the virtual machine from hypervisor).

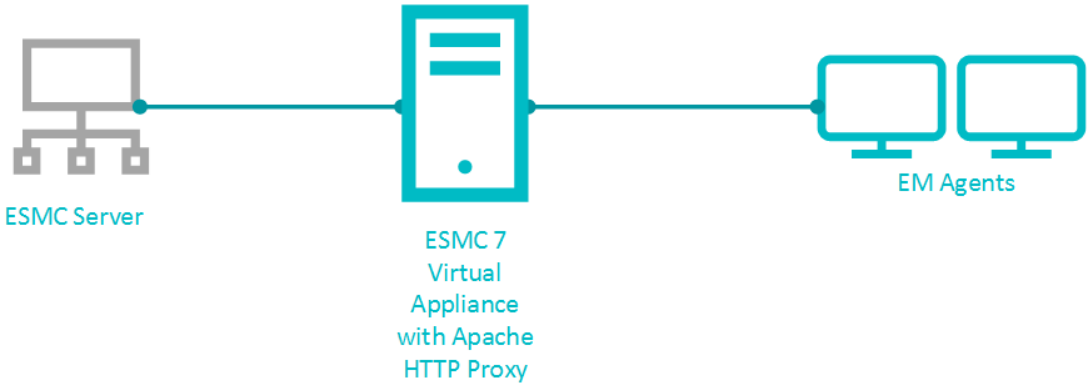
ESMC Server
ESMC 7
Virtual
Appliance
with Apache
HTTP Proxy
EM Agents

Figure 5-2