How to Perform VSX Migration for Multi-Domain Management

4 August 2014
VSX Migration for Multi-Domain Management

Objective

This document explains the steps needed to perform a migration of Domains and the associated Domain Management Servers containing VSX objects to a new Multi-Domain Server (MDS).

Details

Supported Versions

- Multi-Domain Management R71 - R77
- VSX R65, R67.x, R75.40VS, R76 and R77

Supported OS

- SecurePlatform
- GAia
- Windows (Multi-Domain and SmartDashboard GUI)

Supported Appliances

- Smart-1
- Open Servers

Reference Materials

- VSX_migration_to_Provider-1_white_paper
- Multi-Domain Security Management Administration Guide

Procedure Outline

1. Create the Destination Domain Management Servers.
2. Extend the Main Domain Management Server security policy.
3. Enable the migration of Domain Management Servers containing VSX objects.
4. Migrate all of the Source Domain Management Servers to the Destination MDS.
5. Update the Destination Domain Management Server databases.
6. Install policy for the Main Domain Management Server and for each of the Target Domain Management Servers.

Before You Start

Related Documentation and Assumed Knowledge

- R71 – R77 Multi-Domain Management
- VSX on R65, R67, R67.10, R75.40VS, R76 and R77

Warnings and Environmental Impact

- Make an mds_backup of the source MDS prior to any changes.
- Migrate all Domains and Domain Management Servers when moving Domain Management Servers containing VSX objects to a new MDS.
- Ensure that all licenses and contracts are in place for the new MDS and its contents. This includes, but is not limited to, the Multi-Domain Server, Domain Management Server(s) and firewalls.
- This procedure was written with the assumption that no Global Policies or objects are in use.
- This procedure should not have a negative impact on the environment.

Creating the new Domains and Management Servers

To extend the policy of the VSX gateway/cluster:
1. Log in to the Multi-Domain GUI.
2. Right-click on Multi-Domain Security Management.
Use the Wizard to create and configure the new domain. Click **Next** after completing the steps in each Dialog box.

1. Click **Customized Domain Creation** and select the desired checkboxes.
2. Enter the Domain name.

![Add Domain window]

- **Domain Name**: Chassis_Management
- **QoS Support**: Enable QoS

[Next button visible]
3. Complete the Domain properties. **Note: The Name, Contact Person and email can be provided as needed.**

4. Assign the Global Policy configuration.
5. Assign Administrators to the Domain.

![Assign Administrators to Domain dialog box]

6. Assign GUI clients to the Domain.

![Assign GUI Clients to Domain dialog box]
8. Select the number of Domain Management Servers you want to define.

10. Click **Finish** to add the new Domain.

Note: When this step is completed, do not start the new Domain Management Server.
The General - Domain Contents pane should look similar to this:

These steps must be completed for all of the original CMAs/Domain Management Servers that contain VSX objects on the VSX gateways/cluster(s).

Extending the security policy on the VSX gateway/cluster

To extend the policy of the VSX gateway/cluster:

1. Log in to the MDG and access the Source Domain Management Server with SmartDashboard.
2. Create a new network object representing the network/subnet of the new Domain Management Server(s). An address range can be used instead of a whole network.
3. Create a new rule at the top of the rule base allowing all communications from the new Domain Management Server to the VSX gateway(s)/cluster(s).
4. Push this newly edited policy to the gateway(s)/cluster(s).
5. Confirm communication between the new MDS/Domain Management Server and the VSX gateway(s)/cluster(s).
6. Click Save and exit SmartDashboard.

Policy before being extended:
Policy after being extended:

To export the CMA/Multi-Domain Management Servers:

1. Create 2 new directories in /var/tmp on the MDS:
   - Tools
   - Exports

2. Place the Migration tools into the /var/tmp/tools directory

3. Run `tar -zxvf Check_Point_migration_tools_<destination version>_<for current OS>.tgz` in the /var/tmp/tools directory.

```
[Expert@mds01]# pwd
/var/tmp/tools

[Expert@mds01]# ls -la

total 17512
drwxrwxr-x 2 root  root  4096 Nov 23 21:18 ...
-rw-rw-r-- 1 root  root 17898731 Nov 23 21:14 Check_Point_migration_tools_R75.40.linux32.tgz
```

4. `mdserv <Domain Management Server Name | IP>`

5. `mcd`

6. `cd /var/tmp/tools`

7. Make sure that all GUI Clients connected to the source Domain Management Server have been closed and/or the Domain Management Server is stopped. This can be done through the MDG or by running `mdstop_customer <ip address of Domain Management Server | Domain Management Server name>`.

8. `/migrate export /var/tmp/exports/<filename without extension>`
   - This results in a file named `<file name you chose>.tgz` being created in the /var/tmp/exports directory.
   - Verify the file was created by running `ls -la /var/tmp/exports`.
9. Download the exported configuration from the MDS file system.

Repeat steps 4-8 in order to export all of the Domain Management Servers associated with the VSX gateway/cluster being managed on the new MDS.

**These steps are run on the destination MDS:**

10. Log in to the CLI of the MDS.
11. Make a directory on the destination MDS file system in /var/tmp called **Imports**.
12. cd /var/tmp/import
13. Upload the exported configurations, placing them into the /var/tmp/imports directory.
14. Run touch /AllowVsxMigration through the MDS CLI.

```
[Expert@mds2]#
[Expert@mds2]# touch /AllowVsxMigration
[Expert@mds2]# ls -la /var/tmp/imports
-rw-rw---- 1 admin root 0 Nov 23 23:23 AllowVsxMigration
```

15. Log in to the MDG.
16. Right click the newly created **Domain Management Server** and select **Import Domain Management server**.
17. Provide the full path to the exported CMA configuration i.e. `/var/tmp/import/<file name>.tgz`
18. Click **OK**. After some time, a dialog box opens regarding the migration process.

19. If there are no errors preventing the import, click **Continue**.
20. When asked whether or not to start the domain management server, select **Yes**.

![Image](https://via.placeholder.com/150)

21. Run watch mdsstat through the MDS CLI and continue monitoring the process of the CMA coming up through the MDG.

**Note:** Step 14 must be completed every time a new CMA/Multi-Domain Management Server is imported.

Once completed, the General Domain Contents window will look similar to this:

<table>
<thead>
<tr>
<th>General - Domain Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Contents</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>Multi-Domain Security Management</td>
</tr>
<tr>
<td>Physical_Domain</td>
</tr>
<tr>
<td>prodvxs</td>
</tr>
<tr>
<td>vsx1</td>
</tr>
<tr>
<td>vsx2</td>
</tr>
<tr>
<td>vsswitch_01</td>
</tr>
<tr>
<td>vsx1_vswitch_01</td>
</tr>
<tr>
<td>vsx2_vswitch_01</td>
</tr>
<tr>
<td>Virtual_01</td>
</tr>
<tr>
<td>Virtual_01_Management</td>
</tr>
<tr>
<td>vix1</td>
</tr>
</tbody>
</table>

**Things to consider about this process:**

- Depending on the number of objects in the Domain Management Server's database and the resources available on the MDS, this process can take quite a long time.
- Distance (i.e. the number of hops) between the GUI Client and the MDS is also factor.
- Eliminating as many hops as possible will help prevent timeouts, which can result in a failed import of the Domain Management Server.
- If the Domain/Customer, CMA/Domain Management Server or IP address of the CMA/Domain Management server is changed, database edits are required.

**To edit the database:**

You must be logged in to dbedit in the Domain Management Server's environment to edit the virtual system(s). These commands are used in order to update the database for each CMA/Domain Management Server that was migrated:
• Removing masters information
  rmelement vs_slot_objects <virtual object name> masters_addresses <Original Customer/Domain Name>

• Adding masters information
  addelement vs_slot_objects <object_name> masters_addresses <New Domain Management Server IP>

• Changing the Main Domain name
  modify network_objects <virtual object name> main_customer <New Main Domain Management Server Name>

• Saving database changes
  update_all

• Exiting the dbedit utility
  quit

[Expert@nds2]# mdserv 192.168.10.81
[Expert@nds2]# mod
changing to /opt/CFmds-R75.40/customers/Chassis_Management_Server/CFsuite-R75.40/fw1/
[Expert@nds2]# dbedit
Enter Server name (ENTER for 'localhost'): 192.168.10.81

Enter Administrator Name: admin
Enter Administrator Password:

Please enter a command, -h for help or -q to quit:
dbedit> Commands:
crtobj <object_type> <object_name>
modify <table_name> <object_name> <field_name> <value>
rename <table_name> <object_name> <newObject_name>
update <table_name> <object_name>
update_all
delete <table_name> <object_name>
print <table_name> <object_name>
printxml <table_name> <object_name>
addelement <table_name> <object_name> <field_name> <value>
renbyindex <table_name> <object_name> <field_name> <index_number>
add owned remove_name <table_name> <object_name> <field_name> <value>
is_deleted allowed <table_name> <object_name>
quit [--update_all|--noupdate]

dbedit>
Main Domain Management Server database edits

The image shows:

- Removing and changing masters information for a Virtual Switch
- Modification of the Main Domain information for a Virtual Switch

```
[Expert@mds2]$
[Expert@mds2]$
[Expert@mds2]# mdserv 192.168.10.81
[Expert@mds2]# pwd
/opt/CFmds-R75.40/customers/Chassis_Management_Server/CPsuite-R75.40/fw1
[Expert@mds2]# dedit
Enter Server name (ENTER for 'localhost'): 192.168.10.81

Enter Administrator Name: admin
Enter Administrator Password:

Please enter a command, -h for help or -q to quit:
```
```
dedit> Commands:

create <object_type> <object_name>
modify <table_name> <object_name> <field_name> <value>
rename <table_name> <object_name> <new_object_name>
update <table_name> <object_name>
update_all
delete <table_name> <object_name>
print <table_name> <object_name>
printxml <table_name> <object_name>
addelement <table_name> <object_name> <field_name> <value>
rmelement <table_name> <object_name> <field_name> <value>
rmbyindex <table_name> <object_name> <field_name> <index_number>
add_owned_remove <table_name> <object_name> <field_name> <value>
is_delete_allowed <table_name> <object_name>
quit [-update_all|-noupdate]
```
```
dedit> rmelement vs_slot_objects vsswitch_01 masters_addresses 192.168.10.61
dedit> addelement vs_slot_objects vsswitch_01 masters_addresses 192.168.10.81
dedit> modify network_objects vsswitch_01 main_customer Chassis_Management
```
```
This image capture shows:

- Modification of the Main Domain information for a Virtual Firewall

```bash
[Expert@mds2]$
[Expert@mds2]# mdserver 192.168.10.82
[Expert@mds2]# pwd
/opt/CPmds-R75.40/customers/Chassis_Management_Server/CPsuite-R75.40/ful
[Expert@mds2]# dedit
Enter Server name (ENTER for 'localhost'): 192.168.10.82

Enter Administrator Name: admin
Enter Administrator Password:

Please enter a command, -h for help or -q to quit:
```

`dedit> Commands:

create <object_type> <object_name>
modify <table_name> <object_name> <field_name> <value>
rename <table_name> <object_name> <new_object_name>
update <table_name> <object_name>
update_all
delete <table_name> <object_name>
print <table_name> <object_name>
printxml <table_name> <object_name>
addelement <table_name> <object_name> <field_name> <value>
rmdelement <table_name> <object_name> <field_name> <value>
rmbyindex <table_name> <object_name> <field_name> <index_number>
add_owned_remove_name <table_name> <object_name> <field_name> <value>
is_delete_allowed <table_name> <object_name>
quit [-update_all|-noupdate]
```

`dedit> modify network_objects virt_01 main_customer Chassis_Management
```

`dedit> update_all
network_objects::virt_01 Updated Successfully
```

### Completing the Procedure

1. Make sure all licensing is in place for the Domain Management Server and the VSX gateway(s)/Cluster(s).
2. Log in to the Main Domain Management Server.
3. Open the gateway/cluster objects and click **OK**. This will provision the Gateway/Cluster.
4. Push policy to the gateway/cluster.
5. Log in to the Domain Management Server containing each of the Virtual Firewalls.
6. Open The Virtual Firewall objects and click **OK**. This will provision the firewall.
7. Push policy to the Virtual Firewalls.
Formulating the Procedure

1. Open SmartView Tracker to verify logs are being sent properly.
2. Use SmartView Monitor to view the gateway(s)/cluster(s) status, licensing permitting.
3. Log in to the VSX gateway(s) and run commands such as vsx stat to verify the functionality.
4. Test traffic resources access for the various virtual systems on the gateway/cluster.
5. You can also verify the migration process was successful by provisioning and pushing policy.