VSX Migration With Provider-1
White Paper

Arik Goldstein
Software Developer

20 May 2012
Table of Contents
1 Introduction .................................................................................................................................................. 3
  1.1 Terms and Definitions .......................................................................................................................... 3
  1.2 References ............................................................................................................................................ 3
2 Migration Process – General Description ................................................................................................. 4
3 Migration Process – Detailed Description .................................................................................................. 5
  3.1 Create the Destination CMAs .............................................................................................................. 5
  3.2 Extend the VSX security policy to accept traffic from the destination CMAs ..................................... 5
  3.3 Enable the migration of the CMA containing VSX objects ................................................................... 6
  3.4 Migrate the CMAs ............................................................................................................................... 6
  3.5 Update the Destination CMAs databases ............................................................................................. 7
  3.6 Install policy from the Main CMA and from each one of the Target CMAs ....................................... 8
4 Limitations and Recommendations ........................................................................................................... 9
  4.1 Incomplete Migration ......................................................................................................................... 9
  4.2 Customer Names .............................................................................................................................. 9
5 Appendix .................................................................................................................................................. 10
  5.1 Migration process according to specific scenarios ............................................................................... 10
  5.2 Migration of SmartCenter (containing VSX objects) into CMA .......................................................... 10
1 Introduction

In many cases, Provider-1 is used as a management platform for VPN-1 VSX. Migration of Provider-1 environments, containing VSX components, has not been supported in recent releases.

This document describes officially-supported manual procedures to be followed in order to perform such a management migration.

The target audience for this document includes:

- Professional Services consultants who would like to perform the migration of VSX managements.
- Security administrators who manage Provider-1 Environments and are responsible for performing management migrations.

1.1 Terms and Definitions

The following terms will be used in this document:

- **Source CMA:** Customer Management Add-on configuration containing the original definitions of VPN-1 VSX objects. This is the configuration that needs to be migrated to another Provider-1 environment.
- **Destination CMA:** The new CMA which the Source CMA is migrated to.
- **Source MDS:** The Provider-1 Multi-Domain Server (MDS) containing the Source CMA.
- **Destination MDS:** The Provider-1 Multi-Domain Server (MDS) containing the Destination CMA.
- **Virtual Object:** Virtual System (Cluster and Cluster Members), Virtual Router or Virtual Switch.
- **Main CMA:** The CMA which contains the VSX Cluster object.
- **Target CMA:** CMA which contains virtual objects, related to the VSX object from the Main CMA.
- **VSX Environment:** The VSX object and all of its related virtual objects.
- **Provider-1 Environment:** The environment comprised of one or more MDS servers, participating in Provider-1 High-Availability.

1.2 References

The information in this document supplements the basic Provider-1 and VPN-1 VSX product documentation.

The following documents contain the relevant product information:

- Provider-1™/SiteManager-1™ Administration Guide
- VPN-1 Power VSX Administration Guide

The processes described in this document are supported for the following Provider-1 and VPN-1 VSX releases:
• Provider-1 NGX R61 and above
• VPN-1 VSX NGX

2 Migration Process – General Description

The process should be performed as follows:

1. Create the Destination CMAs.
2. Extend the Main CMA security policy (1).
3. Enable the migration of CMAs, containing VSX objects.
4. Migrate all of the Source CMAs to the Destination CMAs.
5. Update the Destination CMAs databases (2).
6. Install policy for the Main CMA, and for each one of the Target CMAs.

In the next section you can find more detailed information about each step in the process.

(1) Necessary only for CMAs whose CMA name, Customer name or IP is being changed during the migration. (For example, the Target CMA and the Source CMA have a different Customer Name, CMA name, or IP).

(2) Necessary only if any CMA's Provider-1 "customer" name has been changed during the migration. (For example, the Source CMA's "customer" name is different from the Destination CMA’s "customer" name).
3 Migration Process – Detailed Description

3.1 Create the Destination CMAs
This step is required as a preparation for the management configuration migration. For detailed documentation of the migration process in Provider-1, please refer to:

- Provider-1™/SiteManager-1™ Administration Guide
- Upgrade Guide

Proceed as follows:

1. For each Source CMA being migrated, create a Destination CMA in the Destination MDS.
2. As in regular migration, the new CMA should not be started until the migration is completed.
   **Note:** The entire VSX Environment must be migrated into the same Provider-1 Environment. Create Destination CMA for each Source CMA belonging to the VSX Environment.

3.2 Extend the VSX security policy to accept traffic from the destination CMAs
Modification of the VSX security policy is required to allow the management traffic from the destination CMA to be accepted, after the migration is completed.

As mentioned above, this action should be performed only for CMAs whose CMA Name, Customer Name or IP Address is being changed during the migration process. Otherwise, this action is not essential (although it can be performed).

1. Extend the Source Main CMA security policy as follows:
   a. For each Destination CMA, create a network object with the Destination CMA’s IP address.
   b. Add a rule to the policy that allows the VSX [cluster] to receive data from each one of the objects that you created in the previous step.
2. Install the extended policy on the VSX [cluster].
3.3  Enable the migration of the CMA containing VSX objects

This step enables the migration of CMA containing VSX objects. This step differs depending on the version of the MDS.

3.3.1  MDS versions until R70 inclusive:

The function `CheckIfVsxObjects`, which checks the existence of VSX objects in the CMA, is found in the following script files:

- `$MDSDIR/scripts/merge_one_customer`
- `$MDSDIR/system/pre_upgrade/PU09000/execute`

These files should be replaced by new files. In order to receive the alternative script files please contact Check Point Support.

To open a service request, go to [http://www.checkpoint.com/services/enterprise/securetrak.html](http://www.checkpoint.com/services/enterprise/securetrak.html), or contact Worldwide Technical Assistance Centers at:

Americas: 972-444-6600 or International: +972-3-6115100

3.3.2  MDS versions higher than R70:

Create a file named `AllowVsxMigration` in the root directory of your MDS machine as follows:

```
touch /AllowVsxMigration
```

3.4  Migrate the CMAs

This step enables the actual migration of each Source CMA to the corresponding Destination CMA. Successful completion of all the previous steps allows migration of the Source CMAs according to the regular migration process, detailed in the Provider-1™/SiteManager-1™ Administration Guide and in the Upgrade Guide.

1. Migrate each Source CMA to the corresponding Destination CMA that you created in step 3.1.

2. Start the Destination CMAs.
3.5 Update the Destination CMAs databases
The next steps are only necessary in the following cases:

- At least one Target CMA’s IP address has been changed during the migration.
- The Main CMA’s "customer" name has been changed during the migration.
- At least one Target CMA’s "customer" name has been changed during the migration.

3.5.1 At least one Target CMA’s IP address has been changed
Each virtual object, related to the VSX [cluster] has a record in the table vs_slot_objects. This table is found in the Main CMA’s database. One of the object’s attributes is masters_addresses, which contains the IP address of the Target CMA.

Every virtual object, defined in a CMA whose IP address has been changed during the migration, should be modified. The masters_addresses attribute of the object should be updated, so that the old IP address will be replaced by the new one. First the old IP should be removed, and then the new one will be added.

The modification should be done as follows:

1. Enter the Main CMA’s environment using mdsenv (type: mdsenv <CMA Name>).
2. Start the dbedit utility by typing dbedit.
3. For each virtual object, whose Target CMA’s IP has been changed, proceed as follows:
   a. rmelement vs_slot_objects <object_name> masters_addresses <old_target_cma_IP>
      (<object_name> is the name of the virtual object.
      <old_target_cma_IP> is the Target CMA’s old IP address).
   b. addelement vs_slot_objects <object_name> masters_addresses <new_target_cma_IP>
      (<object_name> is the name of the virtual object.
      <new_target_cma_IP> is the Target CMA’s new IP address.)
   c. update_all
4. Exit from dbedit utility by typing quit.

3.5.2 The Main CMA "customer" name has been changed
Virtual objects related to the VSX [cluster] are found in the network_objects table in the Target CMA’s database. One of the object’s attributes contains the "customer" name of the Main CMA that should be updated.

In this case, this attribute’s value must be changed for each virtual object. The following steps describe the modifications that should be performed using the command-line management configuration database editing utility (dbedit):

1. For each Target CMA, in the root shell on the MDS machine, proceed as follows:
   a. Enter the Target CMA’s environment using mdsenv (type: mdsenv <CMA Name>).
   b. Start the dbedit utility by typing dbedit.
c. For each virtual object found in this CMA, proceed as follows:
   i. modify network_objects <object_name> main_customer
      <main_customer_name>
      (<object_name> is the name of the virtual object.
      <main_customer_name> is the Main CMA’s new customer name.)
   ii. update_all
   iii. quit

3.5.3 At least one Target CMA "customer" name has been changed
Each virtual object, related to the VSX [cluster] has a record in the table vs_slot_objects. This
table is found in the Main CMA’s database. One of the object’s attributes is target_customer
that contains the "customer" name of the Target CMA.

In this case, this attribute’s value must be changed for each virtual object of the corresponding
Target CMA.
   1. Enter the Main CMA’s environment using mdsenv (type: mdsenv <CMA Name>).
   2. Start the dbedit utility by typing dbedit
   3. For each virtual object, whose "customer" name has been changed, proceed as follows:
      a. modify vs_slot_objects <object_name> target_customer
         <target_customer_name>
         (<object_name> is the name of the virtual object.
         <target_customer_name> is the Target CMA’s new customer name.)
      b. quit

3.6 Install policy from the Main CMA and from each one of the Target CMAs
In order to complete the process, performing policy installation from each Destination CMA is
essential. This operation makes the Destination CMA master of all the virtual objects that it
contains.
   1. Install Policy from the Main CMA.
   2. For each Target CMA, install Policy from the Target CMA on the VSs.
4 Limitations and Recommendations

4.1 Incomplete Migration
The process described previously supports migration of complete VSX environments. When deciding to move the management of a certain VSX environment from one Provider-1 environment to another, all of the CMAs managing virtual components of the VSX environment have to be migrated.

4.2 Customer Names
As described previously, changing "customer" names of the Main CMA, or of any of the Target CMAs, require manual adjustments to the configuration database.

It is recommended to avoid such changes as much as possible.
5 Appendix

5.1 Migration process according to specific scenarios

This appendix instructs you which steps must be performed in your specific scenario. For each CMA check the relevant row. (There might be more than one row. If so, perform the steps from all relevant rows)

<table>
<thead>
<tr>
<th>Requirement/ Step</th>
<th>3.1</th>
<th>3.2</th>
<th>3.3</th>
<th>3.4</th>
<th>3.5.1</th>
<th>3.5.2</th>
<th>3.5.3</th>
<th>3.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMA Name, Customer Name And IP Address are not being changed during the migration.</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMA Name is being changed during the migration</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>IP Address is being changed during the migration</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Customer Name of Main CMA is being changed during the migration</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Name of Non Main CMA is being changed during the migration</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>

* The base steps which must be performed for each migrated CMA are: 3.1, 3.3, 3.4, 3.6.
* If the CMA Name is being changed during the migration, step 3.2 should be performed, as well.
* If the CMA’s IP address is being changed during the migration, steps 3.2 and 3.5.1 should be performed, as well.
* If the Customer Name of the Main CMA is being changed, steps 3.2 and 3.5.2 should be performed, as well.
* If the Customer Name of a CMA (which is not main) is being changed, steps 3.2 and 3.5.3 should be performed, as well.

5.2 Migration of SmartCenter (containing VSX objects) into CMA

This section handles the migration of an existing SmartCenter Server into a Provider-1 CMA. The procedure, described in this section, is based on the detailed procedure in section 3 of this document. In addition, the procedure of a SmartCenter migration into a Provider-1 CMA is detailed in the Provider-1™/SiteManager-1™ Administration Guide and in the Upgrade Guide. This section focuses on the actions to perform when the migrated SmartCenter Server includes VSX objects.

Despite the similarity to the procedure of migrating source CMA (containing VSX objects) into target CMA, certain important actions are necessary to perform the procedure successfully. The actions are:
1. The Source SmartCenter includes both the VSX object and its virtual objects. Therefore the SmartCenter should be considered as a Main CMA.

2. The Customer Name attribute is not part of the source SmartCenter, and this attribute is being added during the migration. Accordingly, each operation which should be made when changing Customer Name attribute (i.e. database updates), should be made as part of this procedure.

3. In the operations described in section 3, the migrated SmartCenter Server plays the role of the Source CMA.

The procedure of migrating a SmartCenter Server into a Provider-1 CMA includes the following steps:

1. Create Destination CMA for the migrated SmartCenter (as detailed in section 3.1 of this document).

2. Extend the VSX security policy to accept traffic from the destination CMA (as detailed in section 3.2 of this document).

   Note: This action is essential when migrating a SmartCenter into a CMA.

3. Enable the migration of a CMA containing VSX objects (as detailed in Section 3.4 of this document). This operation will also enable migration of a SmartCenter containing VSX objects.

4. Migrate the SmartCenter into the Destination CMA (as detailed in Section 3.4 of this document).

5. Update the destination CMA database (as detailed in Section 3.5 of this document).

   Note: This action is essential when migrating a SmartCenter into a CMA.

6. Install policy from the destination CMA (as detailed in Section 3.6 of this document).