How to Prepare and Plan an Upgrade

29 August 2011
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=12300
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 August 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How to Prepare and Plan an Upgrade ).
Contents

Important Information........................................................................................................3
How To Prepare and Plan an Upgrade .............................................................................5
  Objective ..........................................................................................................................5
  Supported Versions ...........................................................................................................5
  Supported Operating Systems .........................................................................................5
  Supported Appliances ......................................................................................................5
Before You Start ..................................................................................................................5
  Assumed Knowledge .......................................................................................................5
  Related Documentation ..................................................................................................5
  Impact on the Environment and Warnings ......................................................................6
Upgrade Preparation and Planning ....................................................................................6
Completing the Procedure ...................................................................................................9
Verifying the Procedure .....................................................................................................9
Index ..................................................................................................................................11
How To Prepare and Plan an Upgrade

Objective

This document describes the non-technical aspects that you must know to upgrade Check Point security environments successfully. Some minor technical aspects are covered as required, but this is not the main focus of this document.

To begin the planning, the licensing and license migration is covered, followed by preparing the backup and fallback strategies as well as choosing the new hardware and target versions. The hardware rollout and testing and well as some pre-upgrade tests are completing this paper.

This document is designed to give you guidelines for a successful upgrade or migration preparation and the listed items here should be resolved before actually starting the upgrade.

All required technical aspects and procedures for the actual upgrades are found in the official upgrade guides located in the UserCenter (http://usercenter.checkpoint.com) and are not covered here.

Supported Versions

This guide is independent of product versions as only non-technical aspects are covered and the procedure is suitable for all versions.

Supported Operating Systems

Although independent of versions, this document focuses on SecurePlatform (SPLAT). Windows and IPSO aspects are also covered but might require minor adjustments in the actual processes.

Supported Appliances

This document supports all Check Point appliances and all open servers.

Before You Start

Assumed Knowledge

The reader must be familiar with Check Point terminology and working procedures such as license generation.

Useful documentation for technical aspects includes the version specific releases notes and upgrade guides.

Related Documentation

Almost all related available documentation that covers the technical aspects of an upgrade can be found in the UserCenter. Check the upgrade guides related to the target version, for example:

Impact on the Environment and Warnings

All information in this document relates to preparation and planning aspects, so there is no impact on the environment.

Upgrade Preparation and Planning

This section describes the non-technical preparations required for an upgrade. All these steps can be done days or even weeks before the actual upgrade is performed.

**Licensing**

1. Backup all old-existing licenses, either directly from the UserCenter or export the license files from SmartUpdate. This might be required in the event of a fallback situation.
2. Check that the licenses have available license moves.
   a) From the UserCenter, identify the relevant product.
   b) From the **Actions** column, select View Product Details.
   c) In the Product Information window, select the **License Information** tab.
   d) Make sure that the value for **Available for IP Move** is **Yes**. If it is not, create a Check Point account services Support Request in the UserCenter to get the new license as required for the upgrade. Note that this procedure can take few days.
3. If you are upgrading from pre-NGX versions, upgrade the licenses if required. You can find the procedures and tools in sk38021 (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30821&js_peid=P-114a7bc3b09-10006&partition=General&product=Security).
4. If you are using Blade licenses on the target version, convert your licenses to Blade licenses first. Details about the process can be found in sk11054 (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk11054&js_peid=P-114a7bc3b09-10006&partition=General&product=Security).
   Make sure that you still have all the required features licensed when using blade licenses. If you are not sure, please contact your reseller or local Check Point representative for assistance.
5. If the IP of the SmartCenter/Security Management server or the license technology changes (blades), generate new licenses and download license files from the UserCenter.
   Make sure to save the license files locally as you may not be able to access the UserCenter during the upgrade and this procedure takes some time to complete.
Contracts
1. Make sure to download the latest contract file from the UserCenter as this is required for IPS updates etc. Contracts are explained in sk33089 (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk33089&js_peid=P-114a7bc3b09-10006&partition=General&product=FDE).
2. Keep your contracts file up-to-date. If you add products to the UserCenter get and install a new contracts file.

Backing Up an Existing Environment
1. Do a full backup or take snapshots of all machines (at least SmartCenter/Security Management server or Provider-1). The procedure is explained in sk54100 (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk54100&js_peid=P-114a7bc3b09-10006&partition=Advanced&product=Security).
2. Move the backup files to a DVD or to a separate machine. The backup files must not reside on the machines being upgraded as the disk drives might be reformatted during the upgrade process. This is necessary in case of a fallback situation and if old configuration files are needed (CRLs, certificates, SIC, etc.).
3. Pre-shared secrets in VPN communities are not visible in SmartDashboard starting from version NGX R65. So if you are upgrading to this version or later, you have to document the VPN pre-shared secrets since they will no longer be visible.

Choosing the Target Version
1. Read the release notes of the current and target version. The target version is the version that you want to upgrade to. Do this to make sure the current version can be upgraded to the target version. The release notes can be found in the SupportCenter, search for Release Notes <version>.
2. Check if the target version can still manage your existing Security Gateways and Edge devices. If not, upgrade them before you continue with the version upgrade.
3. Check the release notes to make sure that the target version will be able to run on your existing hardware, etc.

Hardware Upgrade
1. Before you use new hardware, check the Hardware Compatibility List (http://www.checkpoint.com/services/techsupport/hcl/index.html) and make sure your new hardware is supported and will run on the target version. A hardware testing CD is available to check the functionality (http://www.checkpoint.com/services/techsupport/hcl/testing_tool.html).
2. Decide whether to use open servers or Check Point appliances and compare the pros and cons before ordering new hardware.

Additional Procedures
1. Check which plug-ins are installed on the existing SmartCenter/Security Management server and make sure to install the same plug-ins when installing the new target version. To verify the plug-ins, run fwm ver.
2. Optional - This step is optional and can be skipped, but it is highly recommended and reduces administrative overhead. Create a simple object group for all management objects (SmartCenters or CMAs) and add the management objects to this group. Also create a group for all Security Gateways and Cluster objects and add them to this group. Then if you use any of these management or gateway objects directly in the rule base, replace them all with the respective groups instead. This makes it easier to use HA for management or add new gateways without changing the rule base, since only the groups have to be modified.
3. This step is only required if the IP addresses of the new management servers will change. In this case, enable access to all firewall gateways and clusters via explicit rules in the rule bases from the new IP addresses as all implied rules will not work until the first policy push if the IP addresses have changed. If you already have setup explicit access rules and if you performed step 2 above, just add the new management IP addresses to the management rules and push the policy, otherwise add new access rules.

Additional Considerations for VSX and Provider-1
1. This step only applies to VSX. If the IP addresses of the CMAs or SmartCenter/Security Management servers change, add the new addresses to the VS 0 rule base to allow access from the new IP addresses. Also make sure there is a route in VS0 to the new IPs (best is a host or network route, the default route might not be enough) as otherwise the backroute will not work and the antispooing feature will drop the connections from the new IPs.
2. This step applies to VSX and Provider-1. If the name of the main or the target CMA changes, upgrades or migrations are only supported when done by Check Point Professional Services as several changes with DBEDIT need to be performed on the database. Contact Check Point Professional Services to receive a quote.

**Fallback**

1. Make sure you have a valid fallback scenario in case issues arise. Since a fallback is highly dependent on the environment, it is out of the scope of this document.
2. After creating a fallback scenario, if possible, do a lab test of the fallback (restoring the backup etc) to verify that the fallback will work in case it will be required to perform it. This type of test will give confidence to your administrators, decrease the fallback stress factors and might even shorten the required time for a fallback.

**Additional Steps Required When Upgrading to New Hardware**

1. Check the interfaces and their numbering after installing SPLAT to make sure the interface order is correct. This can be done using `ethtool -p <interface name>`, see sk34779.
2. Make sure the machine is mounted in the datacenter racks and fully cabled. Make sure the interface order is correct and the cables are connected to the correct switches.
3. Keep all switch ports (except the management interface in case the management IP changes during the upgrade) down to avoid duplicate IPs.

**Additional Upgrade Tests**

1. Run the pre-upgrade-verifier on all primary CMAs or the primary SmartCenter/Security Management server and correct all errors and warnings if needed. Always use the verifier of the target version. It can be found in the UserCenter by searching for `pre_upgrade_verifier` in the Support tab and then opening the Downloads tab.
2. Run the verifier again with the `-I` option to verify the integrity of the inspect (*.def) files and document any warnings. Make sure the reported changes are implemented manually in the target version if using `cma_migrate` or manual upgrade methods.
3. This step is optional but it can find database inconsistencies in the object database by using `confwiz`. Export all objects using `confwiz`, but first read the confwiz release notes and be familiar with the confwiz limitations. If the import is successful, import the data on a newly installed SmartCenter/Security Management server of the target version and check for import errors. Solve these errors before doing the upgrade.
4. Test the upgrade in a lab on a staging server. It is recommended to have at least one test gateway in the lab as well. Then compile and push the policy to the lab gateway to make sure the policy compiles without errors and the push is successful. This step cannot always be performed, but it is highly recommended in complex environments.

**Completing the Procedure**

- After you complete the steps in Upgrade Preparation and Planning (on page 6), do the procedures in the Check Point upgrade guides to perform the actual upgrades.
- Upgrade the Security Management server first before upgrading any of the Security Gateways.

**Verifying the Procedure**

- The upgrade is complete only when the policy has been pushed to all Security Gateways and clusters connected to the upgraded SmartCenter/Security Management server.
- Run tests for all critical applications after the upgrade and check the log files for errors or problems.
- For critical environments, consider having Check Point Professional Services on-site for assistance in the event of unexpected issues. Professional Services can be requested via email ps@checkpoint.com.
Index

A
Assumed Knowledge • 5

B
Before You Start • 5

C
Completing the Procedure • 9

H
How To Prepare and Plan an Upgrade • 5

I
Impact on the Environment and Warnings • 6
Important Information • 3

O
Objective • 5

R
Related Documentation • 5

S
Supported Appliances • 5
Supported Operating Systems • 5
Supported Versions • 5

U
Upgrade Preparation and Planning • 6

V
Verifying the Procedure • 9