Check Point NG FP3 Backup Strategy

White Paper

November 2002

Presented by: Oral Mohan

Assumptions

1. The backup files will be restored to an identical machine as the original.
2. Same Check Point version is on the original and restored machines.
3. The backup information presented here is for Check Point-specific backup only. A full backup on any of the Firewall systems will not require these procedures.

Critical Files

The following files are required in order to completely restore a Check Point Management Server (now called Smart Center or Smart Center Pro).

1. $CPDIR/conf/* (including subdirectories)
2. $CPDIR/database/*.C
3. $FWDIR/conf/* (including subdirectories)
4. $FWDIR/log/*
5. Registry SIC keys (see below)

<u>UNIX Registry information</u>

NG FP1 and FP2: Registry is located in $CPDIR/../registry/*
NG FP3: Registry is located in $CPDIR/registry/*

<u>Windows Registry information</u>

The SIC information is located under "HKEY_LOCAL_MACHINE\Software\CheckPoint\SIC". The key can be exported using the "regedit" utility.

Note: In NG FP3 there is an entry "CertPath" containing the path information. If Check Point is installed on a different directory in the restored machine, this entry must be updated accordingly.

Restoration Procedure – Management Server

1. Install Management Server on a new machine. Take intensive care to install exactly the same products, versions, hot fixes etc.
   Reboot the new machine.
2. Stop new Management Server (cpstop).
3. Remove the following files from the new machine:
   a. $CPDIR/database/* (with subdirectories)
   b. $FWDIR/database/* (with subdirectories)
4. Copy the following files from backup files to the new machine:
   a. $CPDIR/conf /* (with subdirectories)
   b. $CPDIR/database/*.C
   c. $FWDIR/conf /* (with subdirectories)
   d. $FWDIR/log/*
5. Remove the following files from the new machine:
   a. $FWDIR/conf /CPMILinksMgr.db, $FWDIR/conf /CPMILinksMgr.db.private (if they exist).

   This will allow them to be recreated automatically when the application starts.
6. Copy the SIC key from the registry backup to the registry of the new machine. Follow procedure outlined in the previous section above.
7. Put an appropriate license on the new machine. Either use a 15 day built-in evaluation license, or get a new license.
   If the original object will be eventually deleted from the database, then new œntral licenses are needed based on the new machine replacing the old central licenses.
8. Start the new Management Server (cpstart).
9. Run ***SmartDashboard*** (***Policy Editor***).
   If a new primary management object was created, it should be configured according to the new machine (IP, topology, products, VPN certificates, etc); otherwise the same primary object exists, edit it to match its new configuration.
   Replace all uses of the original object with the newly created new object. You can find all uses with the "*Where Used…*" utility (right-click on the object to choose the command).
10. If a new primary object was created then both objects now have the same SIC name. **This must be corrected**:
    a. Close ***SmartDashboard*** (***Policy Editor***).
    b. Use Check Point Database Tool or 'dbedit' to clear the SIC name from the old object. The attribute is called 'sic_name'; The object is in the 'network_objects' table. After the update it should look like this ":sic_name ()".
11. If you would like to delete the original management object (assuming there is a new object for the new), do step 12, else jump to step 13.
    Important note: If the original management object has certificates on it, then deleting the object will result in the deletion of these certificates. **Certificates from the Internal CA will also be revoked**. If you intend to eventually use the original management server again, and therefore need to use these certificates again, you can refrain from deleting the original object. In other cases it is recommended to delete the old object.
12. Deleting the original primary management object:
    Stop the new Management Servers (cpstop).
    Make the following change in $FWDIR/conf/objects_5_0.C:

   a. Find the original management’s object.
   b. Change the attribute ‘Deleteable’ to ‘true’ (under ‘AdminInfo’).
   c. Save the changes.

   Start the Management Server and the ***SmartDashboard*** (***Policy Editor***).and delete the original management’s object.

13. Adjusting the FQDN configured in the ICA (Internal Certificate Authority):

    This FQDN is used to create the CRL distribution point URL that is written on the ICA certificates. In most cases (exceptions will follow) you need to change the FQDN definition in the ICA to the new’s machine FQDN.

    Use Check Point Configuration Tool (cpconfig) → Certificate Authority to change the FQDN to its new value.

    Exceptions:

    If the gateways managed by this Management Server are involved in VPN with external entities, and the authentication of these VPN connections is based on ICA certificates, then the external gateways will use the distribution point on these certificates to access the relevant CRL. In order for this to succeed after the migration there are 2 alternatives:

    a. Change the FQDN in the ICA to the new machine’s FQDN, and **reassign new certificates to all gateways and users**.
    b. Update the DNS so that the original FQDN will now be resolved to the new machine. After doing this, the original machine’s FQDN should be changed to avoid ambiguity.

14. Adjust Masters and Log Servers for each module before installing policy on it. The adjustments should be based on the configuration - Centrally Managed or Locally Managed. Without changing this, fetch policy and logs will work with the original machine.
15. Check that the new Management Server functions properly:
    a. Use ***SmartDashboard*** (***Policy Editor***) to check communication with modules through “Test SIC status”.
    b. Install policy on a module.
    c. Use ***SmartView Status*** (***System Status***) to check statuses.
    d. Use ***SmartView Tracker*** (***Log Manager***) to check logs.
    e. Fetch policy from one of the modules you installed policy on.

At this point the new Management Server holds the same configuration as the original Management Server and is ready for work.

You can work on it, make database changes and install policies on the modules.

Restoration Procedure – Modules

1. Install Module software on the new machine. This machine must have the same versions specified on the Management Server for the module. If this is an upgraded version, please ensure that the Management Server supports this module version, and modify the Module object to reflect the version.

   Equally important is the configuration of interfaces, ARP tables and routes on the new management server. These must be identical to the original.

2. If the registry information (as outlined above) was backed up, the keys can be copied to the new module, so that there is no need to re-establish SIC. If this is not the case, please go to step 3 or else proceed to step 4.
3. Re-establish SIC with the Management Server using “cpconfig” on the Module and the Secure Communications utility within the Module object on the Management Server.
4. Push a policy from the Management Server to the Module. Verify that policy installation was successful.
5. The new module should be fully functional now. Verify Firewall Gateway, site-to-site VPN and Client-to-Site VPN operations.

Backup Frequency

Management Server

There should be a weekly full system backup of the Management Server, with daily incrementals. Check Point-specific backups should also be conducted, at a frequency of once a month, and at every Policy Change. Please note that a CPSTOP is required for every Check Point-specific backup.

Modules

Full system backups of the modules should be done once a month. Check Point-specific backups should take place at the same frequency as the Management Server’s Check Point-specific backup. A CPSTOP is not required for the registry backup of the Module.