HyTrust DataControl and HyTrust KeyControl Version 4.0 Release Notes

Version 4.0
First Published: June 2017
Revised: April 2018

This release note describes features, known bugs and system requirements for the HyTrust DataControl and HyTrust KeyControl 4.0 release.

HTKC - HyTrust KeyControl
HTDC - HyTrust DataControl
DCPA - DataControl Policy Agent
RDE - Root/Boot Drive Encryption

Specifications

Please refer to the product administration guide for details of supported platforms, recommended configurations, changes and updates for this release. You can view the latest documentation here:

http://www.hytrust.com/datacontrol/admin_guide

Upgrading to 4.0

HTKC: Upgrade to 4.0 is allowed from 3.4 only.
DCPA: Upgrade to 4.0 is allowed from 3.2.1 and higher

Important: Make sure you reboot the KeyControl node *before* you upgrade it in order to free up any unused log space before the upgrade. Otherwise the upgrade may fail due to a lack of space.

Fixed External Issues

- VMWare ESX servers always provide the VM UUID in SMBios version 2.4 format, even though in VMware hardware version 12 and onwards, the UUID has been upgraded to SMBIOS version 2.7. This causes HTCC to not recognise the VM in Boundary Control setup. HTDC 4.0 works around this limitation. For earlier HTDC versions, set the "acpi.smbiosVersion2.7 = FALSE" configuration parameter in the "vmx" file or through the vSphere client UI.
- On Windows, encryption of multiple partitions on the same disk must be done serially.

- Clarifications added to the Admin Guide for uninstalling the HyTrust Bootloader, the HyTrust KeyControl upgrade path, and XFS filesystem support in linux DCPA.
- On Ubuntu, if root drive encryption was configured with IP settings that differed from the regular network settings (for example, if a static IP was configured for use by HTPA bootloader script on a VM that uses DHCP), previous versions of HTKC sometimes overwrote the changes with the regular network settings. This behavior has been fixed in HTDC 4.0.
- On Windows DCPA, running hcld manually from command prompt no longer causes encrypted devices to detach.
- Windows DCPA no longer assumes that the metadata partition follows the data partition when a disk is being extended. Starting in 4.0, HTDC takes care to not destroy any other partitions that may be in use.
- By default, client certificates will be automatically renewed approximately 10 days before their expiration date. Auto renewal can be disabled by setting Certificate Auto Renewal Period to 0 in the CVM properties in the HTKC webGUI.
- HTKC webGUI now enforces maximum values for name lengths and expiration values.
- The HTKC file system driver has been enhanced to ignore partially allocated sectors when deciding if a sector is eligible for inflation suppression. This prevents a rare case when the audit log could be corrupted during backup/restore or master key recovery events.
- Windows DCPA has been redesigned to improve I/O performance while the drive is being encrypted in the background (rekey).
- Linux RDE no longer overrides a VM's original network configuration. All original network settings are retained during the encryption process.
- To receive email notifications, the cluster must be configured for email notification with the email address and the name or IP address of the mail server. Degraded email is sent out immediately and the audit is posted after the cluster enters healthy state.
- Transfer speed for log bundles copied over SCP can now be increased. HyTrust Support can disable TCP segmentation offload on the HTKC which speeds up the transfer.
- hcl status no longer reports encrypted drives as attached if the disk is removed from the system.
- HTKC webGUI now accurately displays the correct cluster state.
- It is now possible to remove an HTKC node via the webGUI, even if that node has failed to join the cluster.
- Two encrypted partitions are now supported for each virtual disk on Windows DCPA. HyTrust metadata is automatically added into a stand-alone partition on MBR disks. Boot disks will also support one additional data partition. For more details, please see the Admin Guide.

Known Issues

DCPA Issues

- Downgrading the DCPA is not supported on Windows or Linux.
- PA certificate bundle format has changed. If you have upgraded the KC to 3.3 or later and your policy agent is pre-3.3, use "hcl updatecert -a" to update certificate. Do NOT download a renewal certificate and attempt "`hcl updatecert`".

- Root drive encryption is not supported for LVM thin provisioned volumes, mdadm RAID volumes, or UEFI boot volumes.
- hcs3 parallel downloads and uploads do not scale beyond 100 simultaneous processes.
- hcs3 cannot handle files greater than 5GB in size.
- hcs3 only supports creating buckets in the default S3 region "US Standard".
- Windows DCPA RDE will make thin provisioned disks thick. Linux DCPA will make thin provisioned disks thick unless the `-s` flag is used during encryption.
- Encryption of Windows boot and Linux root/system drives from the HTKC WebGUI using the Encrypt Disk action is not supported.
- AWS S3 buckets do not support AES-XTS. Create a keyid using a different cipher for use with S3.
- hicli requires Python 2.6 or higher.

Windows DCPA Issues

- A registry entry `PendingFileRename` is created on hcld startup with location for the file `hcs\hcld.boot`. SEP might refuse to install if this registry key is present. See https://support.symantec.com/en_US/article.TECH98292.html for details. If `hcs\hcld.boot` is the only entry present in `PendingFileRename` (see key value example below), it is advised that the user backup following entry, restart SEP installation, and once the installation completes, restore the backup before any system restart.

  Key:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRename
  ```

  Value:

  ```
  ??\C:\Program Files\hcs\hcld.boot
  ```

- If HTKC is unreachable when you extending the boot volume using the MoveHTBootloader.ps1 script, the new size of the disk may not be accurately displayed in the HTKC webGUI. The volume size can be updated on the webGUI manually using the command "hcl extend C:"
- Early Attach requires the Gateway to be configured if the first network interface has a Static IP address. NIC teaming is not supported.
- Windows DCPA occasionally generates spurious popups from the Windows Plug and Play facility. These popups might suggest that a device needs to be formatted or scanned. If these devices are owned by Windows DCPA, the popups should be ignored or canceled. Do NOT proceed with whatever action the popup suggests.
- Upgrading Windows from 2008r2 to 2012 is not supported if the boot drive encrypted. You must first decrypt the boot drive and then upgrade the OS. After the OS upgrade to 2012 has completed, you can re-encrypt the boot drive.
- Windows DCPA does not support the paging file on encrypted data drives.
- Windows DCPA requires the boot partition to be on C: if it is to be encrypted. Also, encryption of a non-C: device that contains the DCPA agent binary is not supported.
- Upgrading Windows DCPA with encrypted boot drive requires the DCPA agent to be version 2.7.1 or later. Agent versions prior to this should be upgraded incrementally until DCPA agent is at version 2.7.1.

- A Windows DCPA upgraded from 2.6 or earlier does not support the disk rekey feature. Instead, you must manually decrypt and then re-encrypt the disk.
- Azure replaces the Network Interface and assigns a new MAC address on VM Instance restart. Early Attach will not be able to setup access to encrypted data disks in the first boot. Workaround: Reboot the guest OS.
- A system should not be rebooted or shutdown while a data disk being decrypted. If the system is rebooted while a data disk is being decrypted, the data disk might become inaccessible due to NTFS corruption.
- Recovery from interrupted root decryption is not supported. Please back up the C drive before starting decryption in case the virtual machine is interrupted.
- If the Windows DCPA GUI is running during DCPA upgrade, the upgrade will fail. Exit the GUI and retry the upgrade.
- If the system is rebooted while a drive is being encrypted in the background, the drive becomes inaccessible if HTKC is not accessible. Workaround: Reboot the system again after HTKC becomes available.
- If a folder mount contains a comma (","), the Windows HyTrust GUI is not able to perform operations on it. Workaround: Use the hcl cli on the command prompt to perform operations on the affected partitions.
- Windows HyTrust GUI is not able to communicate with HTKC cluster if TLSv1.0 is turned off. The hcl command line will work fine with the latest and most secure version of TLS. If the Windows HyTrust GUI is a requirement, turn on TLSv1.0 support for the HTKC cluster.
- If there is unallocated space between two partitions, extending a partition will leave 10MB of unallocated space after the partition being extended.
- If a system is rebooted while the grace period is expired, reauthorization is required, or the certificate is expired, HTKC does not attach the encrypted data disks. If the Active Directory Database (AD DB) is located on one of the encrypted data disks, the system will not boot.

  Workaround for AD DB issue: Boot the system into Directory Services Restore Mode (DSRM). Take the appropriate corrective action, ensure the data disks are correctly attached, and reboot the system.

  Workaround for all other cases: Take the appropriate corrective action, then either reboot the system or restart any services that failed because disks were not available and restart 'LanManServer' service for File Sharing.
- Performing a reauth or updating the certificate in the Bootloader results in failure to attach encrypted data disks. If the Active Directory Database (AD DB) is located on an encrypted data disk the system will not boot.

  Workaround for the AD DB issue: Boot the system into Directory Services Restore Mode (DSRM) and verify the encrypted data disks are attached. Then reboot the system.

  Workaround for all other cases: Either reboot the system or restart any services that failed because disks were not available and restart 'LanManServer' service for File Sharing.
- If a rekey is aborted, the device is no longer usable. The device must be removed from DCPA control and the partition must be reformatted before attempting to use it again with DCPA.
- Encrypted data drives will become inaccessible if HyTrust DataControl Service 'HCLD' is stopped.
- HTKC webGUI may report devices as Active/Detached even though the encrypted devices are accessible on the client.

- If you see the error message: "HyTrust Bootloader is configured to use network interface which is different from the one used to connnect to Key Control server. Please reconfigure HyTrust bootloader network configuration to use the correct network interface. If you do not wish to update the network configuration (not recommended), please use option 'N'."

  1. Ensure network setting is correct using `htblconf.exe` or powershell script `SetupHTBootloaderNetwork.ps1`.
  2. If you do not wish to update the network configuration or you determine that networking is configured correctly for the bootloader, use the -N option (as suggested), to force encryption in such cases.

  For example: `hcl encrypt -N C:`

- HTKC webGUI may report Active/Encrypt or Active/Rekey or Active/Decrypt even though the encryption/decryption/rekey operation has completed on the Windows client. To update the WebGUI disk status, run the "hcl rekey check" command on the Windows client.
- When importing disks to a Windows VM, Windows may assign a conflicting drive letter to the newly imported partitions. Using the windows Disk Manager, reassign the drive letters as appropriate before using hcl import to incorporate the new drive.
- Migrating an encrypted disk from one VM to another VM may cause incorrect/invalid drive letter assignments. To correct the drive letter assignments:
  1. Remove current drive letter assignments for all the encrypted data disks.
  2. Assign drive letters to the encrypted data disks that were already present on the VM. Each drive letter assignment must be same as what it was before.
  3. Assign any available drive letter to the migrated encrypted data disk.

Linux DCPA Issues

- The following error might be seen on the console: "blk_update_request: I/O error, dev fd0, sector 0". This is generated by Linux command (usually blkid) while scanning block devices, when it comes across floppy disk device. This is not an error condition and can be safely ignored.
- Encryption of multiple swap devices is not supported.
- Encryption of a swap device must be done in conjunction with the root device, using "htroot encrypt". You cannot encrypt the swap device after you have encrypted the root device.
- Root device encryption is not supported with UEFI boot.
- RDE is not supported on CentOS 6.5 AMI in Amazon Web Services.
- Linux RDE in an Azure instance requires the Cloud VM Set/VM property "Reauthenticate on Change of H/W Signature" to be OFF when the instance reboots. Azure replaces the Network Interface and assigns a new MAC address when an Instance is restarted.
- HyTrust File and Folder encryption does not work on NFS mounts on RedHAT 6.x and CentOS 6.x Linux distributions. Also note that eCryptFS driver is not available from the YUM repositories on RedHat 7.x / CentOS 7.x and the support has to be built from the Linux kernel sources.
- Linux DCPA RDE encryption only supports root and swap partitions/volumes called "`/`" and "`swap`". For example, you cannot use partitions such as `/var`, `/home`, `/usr`, or `/opt`.

- Linux DCPA on AWS RHEL 7.1 will show the BIOS boot device as an available device. This device should not be encrypted.
- Linux DCPA in Amazon and Azure requires manual swap of boot and root disks for root encryption prior to reboot. See documentation.
- Linux DCPA RDE on Amazon Linux PV cannot install the "dropbear" package. This package has to be installed manually or you must select "No" for Debug Console support when installing the DCPA.

HTDC Issues

- Fixed an issue where filesystem space was not being freed for certain logs. A reboot of the KeyControl node will free the space. Before upgrading the KeyControl node a reboot is recommended or the space will not be freed.
- It is not currently possible to provide a custom CA to verify the identity of HTKC.
- After MasterKey Recovery, all other nodes that were in the cluster will show in the recovered node as "unreachable". These should be removed in the WebGUI to avoid any confusion.
- If the audit log contains corrupted entries it will not display properly in the HTKC webGUI. If this issue arises, contact HyTrust support.
- A deployed OVA template on ESX may show an erroneous warning when older VMXNET and VMXNET2 network adapters are used. This warning can be ignored.
- HTKC cluster timeout can be lengthened to help with scalability. Doing so causes delays when cluster is degraded equal to 2X the timeout value. These delays will end a few minutes after the cluster enters the degraded state.
- A node joining an HTKC cluster will cause an alert "Could not restore cluster to normal operating mode after adding new node". This alert can be ignored.
- HTKC webGUI only supports Internet Explorer version 11. For details, see the Admin Guide.
- Node joins must be done serially, a single node at a time. Multiple authentication requests to the same node causes mistaken identity of the requesting node.
- Reverting a KeyControl node is not supported if the node to be reverted is part of a cluster. Perform revert after removing other nodes from the cluster.
- If the HTKC webGUI user is using Firefox and a Mac specific Scolling feature, the Scrolling feature should be set to Always. If Scrolling is set to show "When Scrolling", the user must wait for couple of seconds for the scroll to disappear before they click on the Expand icon (>) in order to avoid click issues.
- HyTrust KeyControl time zone is set to UTC (Coordinated universal time), whereas the webGUI translates the time to the browser's local time zone. While changing key or device expiration date or certificate expiration date from browser, the operation might fail with error -- "Expiration date must be in future". This happens when the admin is setting the expiration date to next day local time but the UTC date has already passed. For example, if the browser timezone is "Pacific daylight time" or PDT it is 7 hours behind UTC during day light savings. After 5 PM every day the UTC would have moved to next day, so setting the expiration date to next day would fail.
- After renaming a Cloud VM Set, the user needs to refresh the VMs tab to see updated data.
- An HTKC that doesn't meet minimum System Resource Recommendations in the Admin Guide may not fully install.

- MasterKey Recovery on a node that is part of a cluster will cause a corrupted entry in the Audit Log, making the log display improperly from the webGUI. Fixing this issue requires help from HyTrust support. Reminder: MKR is not needed if ANY node of a cluster is not in MKR; rather, the nodes showing MKR can just be reinstalled and rejoined to the cluster.
- An HTKC node that has been removed from a cluster because it has hit MasterKey Recovery cannot be added back to the cluster. Workaround: Reinstall HTKC on the node before rejoining the cluster.
- When an HTKC is removed from a cluster, it should be powered off to ensure clients will failover to remaining cluster nodes.
- HTKC restore via the System Console Menu option currently does not work. Workaround: Restore the system using the HTKC webGUI.
- An HTKC node that fails to properly join a cluster may be listed as "unreachable". Manually remove the "unreachable" node using the HTKC webGUI (Cluster->Servers) and retry authentication process.
- Using IE11 to run the HTKC webGUI requires a minimum of 100MB free space to run properly.
- Using ssh to connect to sysmenus console in Azure and AWS requires TERM type of vt100. Using other TERM types may result in improper display of console output.
- If the HTKC webGUI tab in the browser is closed without logging out of the session, the user might be able to access webGUI from another tab without additional login even after Session Timeout. Workaround: Either keep the webGUI tab in the browser open or log out of HTKC before closing the browser tab.
- Reversion of an HTKC node results in loss of ALL changes since the upgrade.