CommandCenter Secure Gateway Release 5.3.0

Release Notes

Introduction

These release notes contain important information regarding a new release of CommandCenter Secure Gateway. Please read the entire document and the related documentation available for this release.

Release 5.3.0 includes several new features and maintenance enhancements.

Release 5.3.0 firmware and all documents & files mentioned in these release notes are available at **http://www.raritan.com/support/commandcenter-secure-gateway/**.

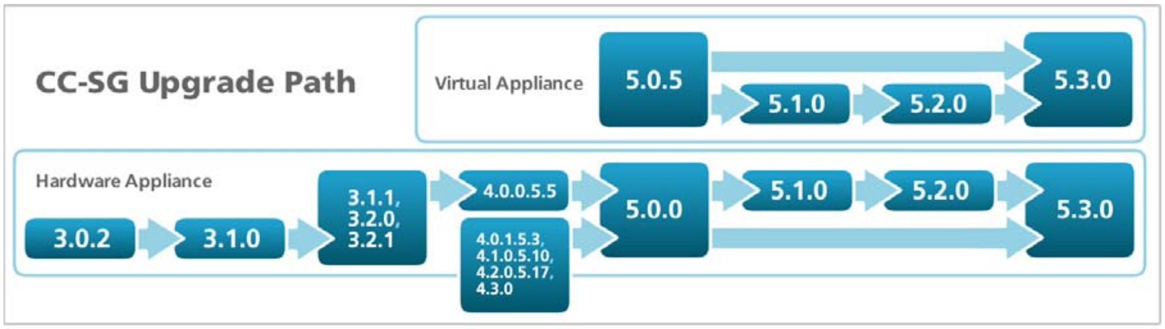
Updated Product Documentation

This following CC-SG documents have been updated for this release:

- CC-SG Administrators Guide
- CC-SG User Guide
- CC-SG Virtual Appliance and lmadmin License Server Management Quick Setup Guide
- CC-SG Virtual Appliance and lmgrd License Server Management Quick Setup Guide
- CC-SG Virtual Appliance No License Server Quick Setup Guide

Upgrade Path

To upgrade your CC-SG to this release you must be running firmware version 5.0.0 or higher (hardware appliance) or 5.0.5 (virtual appliance), as depicted in the diagram below.   You can upgrade CC-SG V1 or CC-SG E1 but not CC-G1 units to 5.3.0.



Please back up your CC-SG before and after any upgrade step. For detailed step by step instructions on upgrading, refer to the Readme file available with this CC-SG release. You may also need to upgrade your other Raritan devices. For a complete list of supported devices, refer to the CC-SG Compatibility Matrix.   For instructions on upgrading managed Raritan devices, refer to the CC-SG Administrators Guide.

New Features and Updates in This Release

This new release of CC-SG includes the enhancements listed below. Please see the updated Administrators Guide and User Guide for details on using each new feature.

1. **IPv6 Support**

   CC-SG now supports IPv4/IPv6 dual stack networks. CC-SG administrators may choose between “IPv4/IPv6” or “IPv4 Only” operations. IPv6 support is being phased in over a few releases. As a result, some CC-SG features and functions are not supported in this release over an IPv6 network. IPv4-only features include:

   a. Communication between clustered and neighborhood units
   b. Power IQ API
   c. Mobile client access
   d. KX II-101 and KSX II access
   e. SX and serial interfaces
   f. IPMI, including PX1 access
   g. iLO, DRAC4 & DRAC5
   h. Java based RDP
   i. CC-SG Access via SSH

   Notable features that are supported in IPv6 networks include KX II access, VMware access, SSH to Admin Console, Telnet, Web Browser Access, VNC, Microsoft RDP and iDRAC6. Additional feature support when using IPv6 will be available in the next release.

2. **SNMPv3 Support**

   CC-SG’s SNMP functions now include SNMPv3.

3. **Direct port Access (DPA) to Dominion SX Ports via SSH**

   CC-SG now enables direct access to SX ports originated in an SSH session. Please see the Administrators Guide for details, including the specific syntax to be used when accessing the SX port through CC-SG.

4. **Licensing Update – License Server No Longer Required for Virtual Appliance**

   Use of the Flexera license server is no longer required for deployment of the CC-SG Virtual Appliance. New Virtual CC-SG customers are to deploy without the Flexera license server.

   If desired, **existing** CC-SG virtual appliance users that upgrade to 5.3 may continue to use the license server with no licensing changes. *If you would like to remove the license server from your virtual CC-SG solution*, please contact Raritan Tech Support and request to have your license files reset in the licensing portal (base license and add-on licenses) so you can generate new files. A non-license server configuration utilizes a different license file. As a result, generating and installing new license files (along with installation of release 5.3) is required in order to remove the license server from your solution.

   Please see the new ***CC-SG Virtual Appliance No License Server Quick Setup Guide*** for step-by-step details.

5. **Single Sign-on for Active Directory users**

   CC-SG can be configured to accept Windows log-in credentials, enabling access to CC-SG without needing to enter the credentials again in CC-SG. The use of Kerberos authentication protocols and Internet Explorer is required.

6. **KX II Dual Monitor Support**

   When connecting to Dominion KX II to access KVM targets, CC-SG users may leverage the Dual Monitor features. Dual Monitor is configured in KX II.

7. **VMware VSphere 5.0 Support**

   CC-SG now supports accessing virtual servers running in a VSphere 5.0 environment. CC-SG may also be deployed as a virtual appliance running in VSphere 5.0.

8. **VMware Fault Tolerance Support**

   For virtual appliance redundancy, VMware's Fault Tolerance feature has been tested and verified to be usable with CC-SG. Fault Tolerance is a VMware feature that provides continuous availability; much like clustering. Administrators can now choose between High Availability and Fault Tolerance for failover/redundancy of virtual CC-SG appliances.

9. **Create and use certificates using SAN (subject alternative names)**

   Please refer to the Administrators Guide for details.

10. **Automatic Deletion of Backup Files**

    The backup task can now be configured to automatically delete older system backup files after a configurable number of files have been saved. When a new file is created, the oldest one is deleted.

Special Notes and Limitations

1. IPv6 - Please note the following when utilizing CC-SG in IPv4/IPv6 Dual Stack Mode:
   - The Administrators Client cannot be launched in an IPv6 network when using Firefox 6, 7, 8, 9, 10, 11, 12. This is a certificate bug caused by Firefox. A workaround is available that includes installation of a user certificate. Details are provided in the Administrators Guide. Please contact Raritan Tech Support for assistance.
   - If using VNC in an IPv6 network, please select "Prefer On" in the Real VNC server settings.
   - If adding static routes for IPv6, please note:
     1. Upon reboot of CC-SG, the values are not retained
     2. In the event of IP failover, the values are not retained.
   - A list of features and functions that cannot be used with IPv6 is provided in the Administrators Guide.
2. When adding VNC and RDP interfaces for Windows 7, please make sure that ICMPv4 and ICMPv6 are allowed by your Windows 7 firewall.
3. When launching the iLO3 KVM app via CC, a warning 'do you wish to load unsecure content' will be presented to the user that needs to be accepted. This is because the HP applet is not signed.
4. Supported JRE versions for this release include 1.6.0_10 thru 1.6.0_31.
5. The "Bookmark Node" feature is not supported when using Internet Explorer version 8 (IE8).
6. RSA Remote Console cannot be launched from CC-SG when using JRE 1.6.0_10 and higher. IBM has provided a workaround here: **http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5080396**.
7. If enabling AES 256, to avoid lockout from CC-SG ensure that the jurisdiction files are installed on the client PC or device.
8. VMware Viewer and Firefox version 3.6.x are not compatible.
9. CC-SG cannot manage or access ESXi virtual nodes that use a free trial license.
10. Single mouse mode does not function on Windows or Linux servers as targets when using VMware as a client.
11. When accessing DRAC5 targets, there is a limit of 4 concurrent SSH sessions.
12. If your version of DRAC does not support graceful shutdown, a "graceful shutdown not supported" message is received when executing a graceful shutdown operation for power control.