Release Notes

CommandCenter Secure Gateway (CC-SG) Release 10.0 リリースノート

はじめに

このリリースノートは、CommandCenter Secure Gateway (CC-SG) の 10.0 に関する重要な情報が記載されています。
Release 10.0 の内容：Release 9.0 の全ての機能に加え、新機能の追加と修正を含みます。
Release 10.0 は、CC-SG の保守契約を締結している（期限切れを除く）お客様が利用できます。

http://www.raritan.com/jp/support/product/commandcenter-secure-gateway

Release 10.0 の新機能およびアップデート

Release 10.0 に含まれる機能強化およびアップデートは以下のとおりです。

1. Amazon AWS および Microsoft Azure 環境のサポート
2. ビデオポートグループのサポート
3. 仮想環境の CC-SG によるクラスタリング機能の追加
4. CC-SG によるユーザーステーションの管理機能を追加
5. Node Lockout on Disconnect（切断時の一時的ロックアウト）機能の追加
6. Web services API の拡張（Web services API のサポートは米国／台湾となります）
7. VMware 7 環境をサポート
8. ILO 5 をサポート

重要なおしらせ

・Release 10.0 は、古いシングルポートモデルである DKX-101、DKX2-101 をサポートしません。
・ユーザーステーションと連携するためには、ユーザーステーションのファームウェアバージョンを 4.5.0 へアップグレードする必要があります。
・ユーザーステーションの新しいファームウェア 4.5 は、2022 年 4 月に提供予定です。
・Dominion KX II モデル（DKX2-xxx）は、CC-SG 8.0 以降、サポート対象外となりました。
・AWS と Azure 向け CC-SG は、専用のファイルと手順をサポートサイトから入手する必要があります。

製品ドキュメントの更新

本リリースにより、以下のドキュメントが更新されました。（英語版のみ）
・CC-SG 管理者ガイド、ユーザーガイド、オンラインヘルプ
・CC-SG 仮想アプライアンスおよびクラウド環境（AWS & Azure）用クイックセットアップガイド
・CC-SG Web Services API（WS-API）プログラミングガイド

10.0 へのアップグレードパス ※2023 年 4 月誤植修正

CC-SG 10.0 へアップグレードするためには、ご利用環境が 9.0/9.5 である必要があります。

7.0/8.0 の場合: 最初に 9.0 へアップグレードしてから、10.0 へアップグレードします。

6.x の場合：最初に 7.0、次に 9.0 へアップグレードしてから、10.0 へアップグレードします。

※重要事項 5.x もしくは 6.x からアップグレードした仮想アプライアンスを 10.0 へアップグレードする場合、アップグレードを開始する前に元の古いディスクイメージ（disk 1）を必ず **remove しなければいけません**。これを行わなかった場合、アップグレードプロセスが中断します。

その他のアップグレードにつきましては、CC-SG のタイプ（「ハードウェアアプライアンス」と「仮想アプライアンス」のいずれか）、ライセンスによって異なります。

1. ハードウェアアプライアンス（CC-SG V1 および E1）

・CC-SG 5.x をご利用の場合、はじめに 6.0 へアップグレードしてから、7.0 へアップグレードする必要があります。

・CC-SG 3.x および 4.x をご利用の場合、5.0 → 6.0 → 7.0 といったアップグレード手順となります。

・以下のハードウェアアプライアンスは、7.0 へアップグレードすることはできません。

CC-SG-V1-A, CC-SG-V1-1（2009 年以前のモデル）, CC-SG-E-0

2. 仮想アプライアンス －ライセンスサーバー無し（5.3／5.4）

・CC-SG 5.3／5.4 をご利用の場合、6.0 → 7.0 といったアップグレード手順となります。

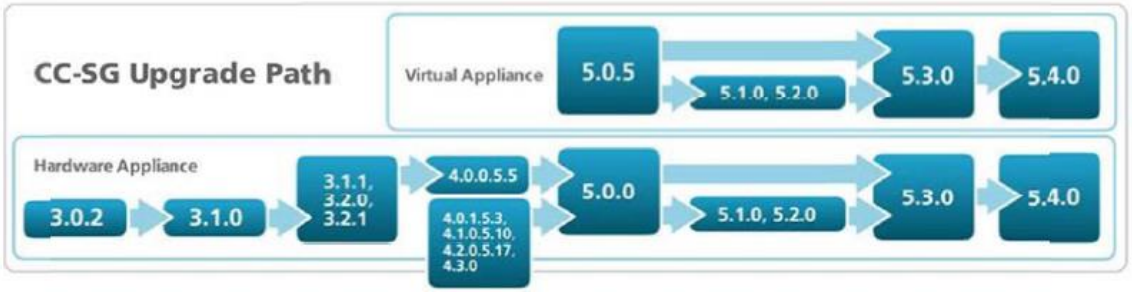
3. 仮想アプライアンス －ライセンスサーバーあり（5.0.5／5.1／5.2／5.3／5.4）

1）5.0.5／5.1／5.2 をご利用の場合、5.3 へアップグレードする必要があります。

2）CC-SG 6.0 は、Flexera lmadmin や lmgrd ライセンスサーバーをサポートしていないため、新しいライセンスファイルを必要分取得し、当該ライセンスサーバーから移行する必要があります。ラリタンのサポート窓口へご連絡いただき、新たなライセンスファイルを取得してから、CC-SG ライセンスマネージャーにて新しいライセンスを必要分アップロードしてください。ライセンス認証を再び行った後、CC-SG 6.0 へアップグレードが可能となります。

3）上記手順完了後、6.0 から 7.0 へのアップグレードが行えます。

※任意の古い CC-SG へアップグレードが必要な場合は、以下のアップグレードパスをご参照ください。



アップグレードに関する追加情報

仮想アプライアンス：
・4GB メモリが必要です。
・7.0 へアップグレードする前に仮想マシンに 40GB の HDD を追加する必要があります。
・10.0 へアップグレードする前に、仮想マシンのハードディスイメージは 1 つだけにしてください。
※6.x から 7.0 へアップグレードした場合、6.x のイメージを含む古いハードディスクが削除されるまで、10.0 へのアップグレードは中断されます。

ハードウェアアプライアンス：
・CC-SG V1 もしくは E1 は 7.0 へのアップグレードが可能ですが、CC-G1 以前のモデルはアップグレードできません。また、以下の旧製品は、アップグレード対象外です。

- CC-SG-V1-A
- CC-SG-V1-1（2009 年以前のモデル）
- CC-SG-E-0

その他：
・アップグレードを実施する際には、アップグレード前と後でそれぞれバックアップを実施してください。加えて、段階アップグレードの場合は、その都度実施するようにしてください。
・ご利用の構成によっては、CC-SG 以外のラリタン製品のアップグレードが必要になる事があります。CC-SG 10.0 のサポート対象デバイスの一覧は、「互換性マトリックス」（Compatibility Matrix）を参照してください。管理対象となるラリタン製品のアップグレードについては、CC-SG 管理者ガイド（Administrators Guide）を参照してください。
・アップグレード手順の詳細については、CC-SG 10.0 管理者ガイドを参照してください。
・ご不明点は、ラリタンのサポート窓口までお問い合わせください。

特記事項および制限事項

1. プロキシモードの HSC と HKC は、2401/tcp を使用します。これは他の KVM クライアントとは異なりますので、プロキシモードのドキュメントを参照してください。

2. SSLv3.0 は、セキュリティの問題により初期状態では無効となっています。古い機器との接続のために、有効にすることは可能です。

3. TLS1.0 は、以下のラリタン製品で利用されています。

    KSX2 v2.7, LX v2.7, KX2-101v2 v3.7

4. KVM およびシリアルクライアントの電源制御を行なう場合は、ラリタン製 PX シリーズの PDU を D2CIM-PWR を介して Dominion 製品に接続する必要があります。

5. ブラウザで Java を無効にして HKC を自動的に起動するためには、Windows の「コントロール パネル」に用意された「Java」から「Java コントロール・パネル」を起動して、「セキュリティ」タブの「ブラウザおよび Web Start アプリケーションで Java コンテンツを有効にする」のチェックボックスを解除します。

6. VMware の Web Viewer を使用するためには、証明書をインストール必要があります。

7. Microsoft RDP クライアントは、CC-SG ブックマーク経由で起動することができません。今後のアップデートで対応見込みです。

8. IPv6 の利用：CC-SG を IPv4／IPv6 デュアルスタックモードで使用する場合は、以下の点にご注意ください。

・Admin Client は、IPv6 環境で Firefox 6 ～12 を使用することができません。回避策として、ユーザー証明書のインストールが挙げられます。詳細は管理者ガイドをご参照ください。

・IPv6 環境で VNC を使用する場合、Real VNC サーバーの設定において「Prefer On」を選択してください。

・IPv6 環境における制限事項は、管理者ガイドを参照ください。

9. Windows 7 用の VNC および RDP のインターフェースを追加する場合、ICMPv4 と ICMPv6 を Windows Firewall で許可してください。

10. CC-SG 経由で iLO3 の KVM アプリケーションを起動すると、「セキュリティ保護されていないコンテンツをロードしますか」という警告が表示され、これを承認する必要があります。これは、HP 社のアップレットに署名が無いため発生します。

11. Java のバージョン v6 と v7 はサポート対象外です。組み込み型サービスプロセッサのバージョンによっては、最新の Java へのアップデート対応がされていないものもあるため、その場合は Java セキュリティレベルを「低」に設定するか、Java コントロール・パネルのセキュリティタブにある「例外サイト・リスト」を使用してください。

12. RSA リモートコンソールは、JRE1.6.0_10 以降を使用する場合、CC-SG から起動することができません。IBM から回避策が掲示されていますので、ご参照ください。

http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5080396

13. AES-256bit 暗号化を有効にする場合、CC-SG からのロックアウトを回避するため、必ずクライアント PC またはデバイスに JCE Unlimited Strength Jurisdiction Policy ファイルをインストールしてください。

14. CC-SG は無料試用版ライセンスで動作する ESXi 上の仮想ノードに対する管理と接続はできません。

15. VMware クライアントを利用する場合、シングルマウスモードは、Windows または Linux のターゲットサーバーでは機能しません。

16. DRAC5 をターゲットとしてアクセスする場合、SSH 同時接続数は 4 つに制限されます。

17. お使いの DRAC のバージョンがグレースフルシャットダウンに未対応の場合、電源制御のためにグレースフルシャットダウンの操作を実行すると、「graceful shutdown not supported」（グレースフルシャットダウンはサポートされていません）というメッセージが表示されます。

18. SNMPv3 オプションおよび MGSOFT MIB Browser を使用する場合、「Authentication Passphrase」（認証パスワード）と「Privacy Passphrase」（個別パスワード）は異なるものでなければなりません。このように設定されていない場合、CC-SG が SNMP トラップを送信しても、ブラウザの情報は反映されません。

19. CC-SG の HTML ベースの Access Client（HKC）では、Chrome バージョン 45 以降および Edge ブラウザから Java アプレットベースのインバンドインターフェースを起動することはできません。Java アップレットベースのインバンドインターフェースを使用する場合、他のブラウザ（Internet Explorer 等の対応ブラウザ）をご使用することをお勧めします。また、利用時は、Java ベースの CC-SG Admin Client で、インバンドインターフェースにアクセスしてください。ただし、iLO、DRAC、RSA は起動しません。