CommandCenter Secure Gateway (CC-SG) リリース6.2 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) のリリース6.2.0 に関する重要な情報が記載されております。リリース6.2では、前のリリース6.1の機能を網羅し、各種機能の追加と修正およびアップデートを行いました。
リース6.2 のファームウェアならびにこのリリースノートで言及されるすべてのドキュメントおよびファイルはhttp://www.raritan.com/jp/support/commandcenter-secure-gateway/で入手できます。

最新の製品ドキュメント

本リリースにより、以下のCC-SG 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、ユーザガイド、オンラインヘルプ
- CC-SG 6.2 アップグレードガイド (ファームウェアアップグレードに関する詳細説明)
- CC-SG 仮想アプライアンス（ライセンスサーバーでない）向けクイックセットアップガイド
- CC-SG WS-API プログラミングガイド

リリース6.2の新機能およびアップデート

CC-SG リリース6.2に導入されている機能強化およびアップデートは以下の通りです。

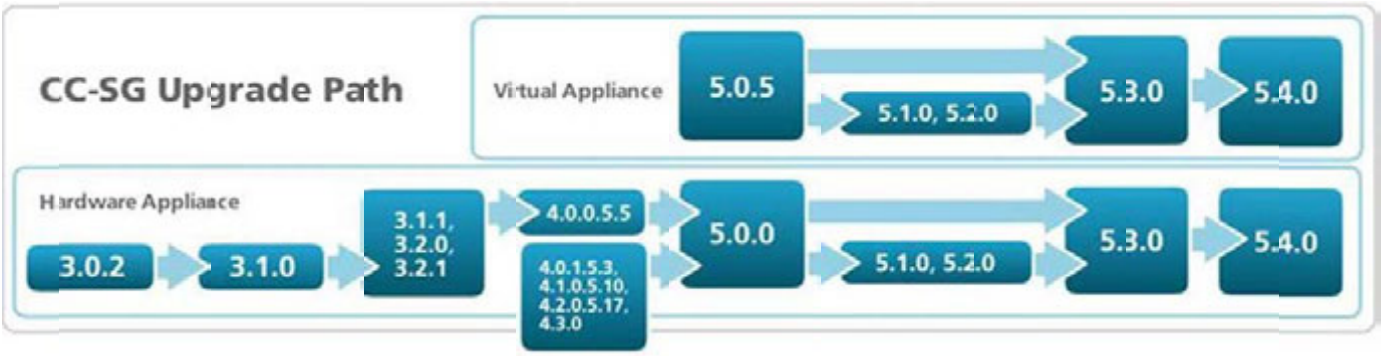
1. TCP/IPおよびSNMPでCC-SGに接続されたラリタンのインテリジェントラックPDU PX2およびPX3によるリモート電源制御をサポートします。
2. 新しいDominion SX IIおよびDominion KX IIIのJava非依存のHTMLクライアントをサポートします（ダイレクトモード）。
3. 新しいDominionシリアルアクセスモジュール(DSAM)に接続されているシリアルデバイスに、ユーザーがアクセスすることが可能です。
4. サードパーティ製サービスプロセッサがアップデートされています - DRAC 7、8 (KVM とPower)および、新iDRAC 6バージョン2.8
5. 新Web UI ViewerでVMwareバージョン6.0をサポートします。VMware vAppをサポートします。
6. デフォルトでSSLv3を無効にして、より安全なTLSプロトコルを使用します。
7. Dominion SX IIに対して参照のみの権限をサポートします。
8. CC-SG SSHクライアントが機能強化されアップデートされています。
9. 新しいバージョンのCC-SG V1ハードウェアアプライアンスをサポートします。
10. ラリタン/ルグランブランディング。
11. CC-SGへの二要素認証のため、RSA SecurIDの最新バージョンを使ったテストおよび認証を行っています。
12. CC-SG APIのユーザーに対して、5つ以上のWS-APIサービスをサポートします。
13. セキュリティのアップデート。Javaおよびブラウザの新バージョンをサポートします。

バージョン6.2へのアップグレードパス

6.0または6.1をご使用の場合は、6.2に直接アップグレードできます。他のリリースでのアップグレードパスは、CC-SGのタイプ（仮想アプライアンスまたはハードウェア）およびライセンスのタイプによって、以下のように異なります。

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バージョンはすべてCC-SG 6.0に直接アップグレードしてから、CC-SG 6.2にアップグレードする必要があります。
   - 3.xおよび4.xバージョンは、下図に示すように先にバージョン5.0にアップグレードした後、CC-SG6.0にアップグレードしてからCC-SG 6.2にアップグレードする必要があります。
2. 仮想アプライアンス - ライセンスサーバーなし（バージョン5.3および5.4)
   - バージョン5.3または5.4からCC-SG 6.0に直接バージョンアップしてから、バージョン6.2にアップグレードします。
3. 仮想アプライアンス – ライセンスサーバーあり(バージョン5.0.5、5.1、5.2、5.3、 5.4)
   1) バージョン5.0.5、5.1、5.2は、バージョン5.3に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（1つまたは複数）取得して、当該ライセンスサーバーから移行する必要があります。ラリタンのテクニカルサポートまでご連絡いただき、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を使って新しいライセンス（1つまたは複数）をアップロードしてください。再ライセンス認証を行ったあと、CC-SG6.0へのアップグレードが可能となります。
   3) 上記手順が完了後、バージョン5.3または5.4からCC-SG 6.0に直接アップグレードしてから、バージョン 6.2にアップグレードすることができます。

上記の特定のバージョンのアップグレードが必要な場合は、下図を参照してください。
(図はバージョン5.4 まで)



アップグレードに関する追加情報:

CC-SG 仮想アプライアンスは、お使いの仮想マシンにセカンドハードディスクを増設してから6.0以降にアップグレードする必要があります。

CC-SG V1 またはCC-SG E1 は6.2 へのアップグレードが可能ですが、それ以前のCC-G1 ユニットではできません。アップグレード手順の前後に、お使いのCC-SG のバックアップをとってください。お使いの他のラリタン製品のアップグレードが必要な場合もあります。

サポート対象デバイスの一覧は、CC-SG 互換性マトリックスを参照してください。管理対象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。アップグレードの手順に関する詳しい説明は、CC-SG 6.2 アップグレードガイドを参照してください。ご不明な点がある場合は、ラリタンのテクニカルサポートまでお問い合わせください。

特記事項及び制限事項

1. 新しいJava非依存のHTML KVMおよびシリアルクライアントは、現時点ではプロキシモードをサポートしていません。ダイレクトモードで動作します。
2. KVM /シリアルクライアント内の電源制御メニューを使用するには、ラリタンPX PDUをDominionアプライアンスに接続する必要があります。
3. ブラウザでJavaを無効にしてHKCを自動的に起動するには、Javaコントロールパネルのセキュリティタブで、[ブラウザでJavaコンテンツを有効にする]オプションの選択を解除します。
4. 新VMware Web Viewerを使用するには、証明書をインストールする必要があります。プロンプトに従って、再接続します。
5. 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はできません。今後のアップデートで修正します。
6. IPv6: 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。
   - Administration Clientは、Firefox 6、7、8、9、10、11、12を使用している場合はIPv6ネットワークで起動することはできません。ユーザー証明書のインストールなどにより回避することができます。詳細は管理者ガイドを参照してください。
   - IPv6ネットワークでVNCを使用する場合は、Real VNCサーバ設定で[Prefer On](オンを選択)を選択してください。
   - IPv6で使用できない特長や機能については、管理者ガイドを参照してください。
7. Windows 7用のVNCおよびRDPインタフェースを追加する場合は、ICMPv4とICMPv6がWindows 7のファイアウォールで許可されていることを確認してください。
8. CC-SG経由でiLO3 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アプレットに署名がないために発生します。
9. サポート対象外のJavaバージョンには、1.7.0_11および1.7 update 9-bo5が含まれます。組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の変更に合わせてアップデートされていないものがあるため、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 Exception Site List（例外サイトリスト）をお使いください。

10. Java 1.7.0.7_71ではIPv6経由でCC-SGにログインできません。前のバージョンはJava 8と同様に機能します。
11. [Bookmark Node]（ノードをブックマークに設定）機能は、Internet Explorerバージョン 8(IE8)を使用する場合はサポートされません。
12. RSAリモートコンソールは、JRE 1.6.0_10以上を使用する場合はCC-SGから起動することはできません。IBMからこれを回避する方法が提供されています。以下のURLからご確認ください。
http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5080396
13. AES 256暗号化を有効にする場合は、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またはデバイスに管轄ファイルをインストールしてください。
14. CC-SGでは、無料試用版のライセンスを使用するESXi仮想ノードの管理またはアクセスはできません。
15. VMwareをクライアントとして使用する場合、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では機能しません。
16. DRAC5ターゲットにアクセスする場合の同時SSHセッションの最大数は4です。
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対応してしない場合、電源制御のためにグレースフルシャットダウン操作を実行すると、「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、認証パスワードとプライバシーパスワードは異なるものでなければなりません。CC-SGはトラップを送信しますが、ブラウザはこれを無視します。
19. CC-SGのHTMLベースのAccess Clientでは、Chromeバージョン45以降およびEdgeブラウザから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。インバンドインターフェースを使用する予定の場合、少なくとも他のブラウザをご使用になることをお勧めします。インバンドインターフェースでこれらのブラウザを使用する必要がある場合は、JavaベースのCC-SG Admin Clientを使用して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。