CommandCenter Secure Gateway (CC-SG) Release 6.1

Release Notes

はじめに

このリリースノートは、CommandCenter Secure Gateway (CC-SG) のリリース 6.1.0 に関する重要な情報が記載されております。

リリース 6.1 では、前のリリース 6.0.0.5.4 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。

リリース 6.1 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。

最新の製品マニュアル

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 Administrators Guide、User Guide & Online Help
- CC-SG 6.1 Upgrade Guide (ファームウェアアップグレードに関する詳細説明)
- Quick Setup Guide for CC-SG Virtual Appliance - No License Server
- CC-SG WS-API Programming Guide

新機能およびアップデート (リリース6.1)

CC-SG リリース 6.1 に導入されている機能およびアップデートは以下の通りです

1. **Dominion SX II 対応。** 新しい次世代の Dominion SX II コンソールサーバーに対応しています。
2. **Dominion KX III リリース 3.2。** もうすぐ発表予定の Dominion KX III リリース 3.2 に対応しています。
3. **CC-SG Hyper-V 仮想アプライアンス。** CC-SG が Microsoft Hyper-V 仮想アプライアンスとして使用できるようになりました。
4. **CC-SG XenServer 仮想アプライアンス。** CC-SG が XenServer 仮想アプライアンスとして使用できるようになりました。
5. **新しい 64 ノード仮想アプライアンス。** 64 ノードの CC-SG 仮想アプライアンスをご購入いただけます。この仮想アプライアンスにより、低コストで CommandCenter 管理を導入できます。ラリタン部品番号：CCSG64-VA。
6. **セキュリティの大幅なアップデート。** セキュリティの重要なアップデートと強化が行われました。下記を参照してください。
7. **VMware バージョン 5.5 対応。** VMware のバージョン 5.5 に対応しています。
8. **KVM で [view only] (参照のみ) を許可。** リリース 3.1 以降の Dominion KX III スイッチでは参照のみも可能です。他のスイッチについては、今後のファームウェアのアップデートが必要となります。
9. **Dominion KX KVM クライアントのサポート。** Dominion KVM クライアントでは、(1) Java ベースではない Active KVM Client (AKC) および (2) Java ベースの Virtual KVM Client (VKC) について、次のような強化が行われました。
    a. CC-SG で、[Auto-Detect] (自動検出) オプションの選択時に Windows プラットフォームで AKC を起動できるようになりました。
    b. AKC および VKC 内からリモートでの電源管理が可能になりました。
    c. Chrome ブラウザでの VKC および AKC KVM-over-IP セッションに対応しています。
    d. KX2-101-V2 リリース 3.6 以降では AKC に対応しています。
    e. Chrome ブラウザ (45 以降) から CC-SG Admin Client を起動できます。

10. **CSV でデバイスを削除。** CSV ファイルを使用してデバイスを削除できるようになりました。
11. **最新バージョンの Java 8 対応。** サポート対象バージョンは、互換性マトリックス (Compatibility Matrix) を参照してください。CC-SG は、今後のバージョンの Java にも対応していく予定です。Java 開発者が新しいバージョンの Java に互換性のない変更を行った場合、ソフトウェアのアップデートが必要となる場合があります。問題がある場合は、ラリタンまでご連絡ください。
12. **その他のさまざまな修正。**

セキュリティアップデート (リリース 6.1)

このリリースでは、セキュリティ面で、以下のような多くのアップグレードと強化が行われました。

1. TLS 対応、およびオプションで SSLv3 を無効化 (POODLE 問題)
2. CC-SG での SHA-2 証明書の使用と生成
3. SHA-2 証明書での新バージョンのコード署名
4. TCP/IP ポート 4446 および 4457 のブロック
5. OpenSSH バージョンのアップグレードによる脆弱性への対処
6. OpenSSL バージョンのアップグレードによる FREAK などの脆弱性への対処
7. OpenSSL パッチによる TLS 時の MitM (Man-in-the-Middle：中間者) の脆弱性の修正
8. 証明書生成について、キーサイズを 4096 ビットに拡大
9. Nessus セキュリティスキャンの実行
10. CCSG Web ユーザーインターフェースでのクロススクリプティングの脆弱性に対処
11. BASH のセキュリティ脆弱性に対処
12. CCS Injection (OpenSSL) および GNUtils の脆弱性に対処

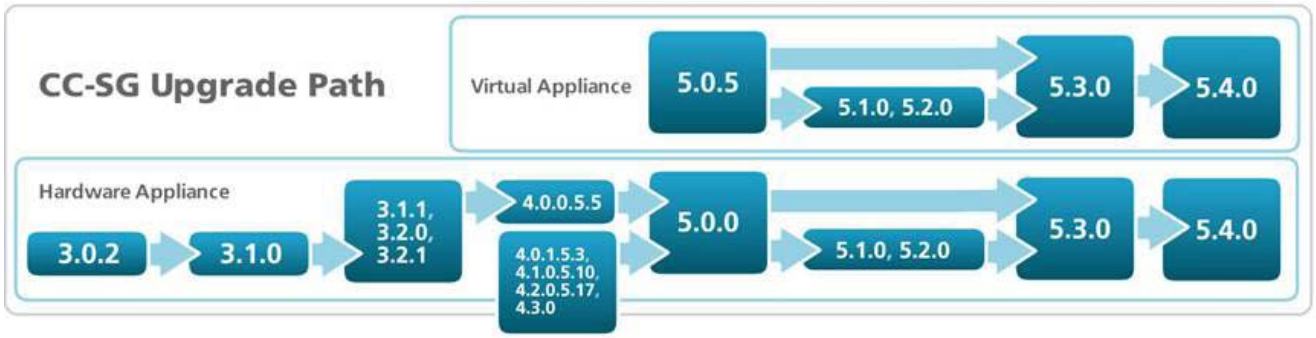
バージョン 6.1 へのアップグレードパス

6.0.0.5.x をご使用の場合は、6.1 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)**
   - 5.x CC-SG バージョンはすべて、CC-SG 6.0.x に直接アップグレードしてから CC-SG 6.1 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-SG 6.0.x にアップグレードしてから CC-SG 6.1 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)**
   - 5.3 または 5.4 から CC-SG 6.0.x に直接アップグレードしてから、バージョン 6.1 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 6.0.5 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-SG 6.0.5.x 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 からバージョン CC-SG 6.0.5.x に直接アップグレードしてから

6.1.0 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 6.0.5.x 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 6.1 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 6.1 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、ラリタンまでお問い合わせください。

特記事項および制限事項

1. 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。
2. 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。
   - Administrators Client は、Firefox6、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 サーバー設定で [Prefer On] (オンを選択) を選択してください。
   - IPv6 の Static Route (静的ルート) を追加する場合は、以下にご注意ください。
     1. CC-SG を再起動すると、値は保持されません。
     2. IP フェイルオーバが発生すると、値は保持されません。
   - 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。
3. 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。
4. CC 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。
5. 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、最近の 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。

6. Java 1.7.0.7_71 では IPv6 経由で CC-SG にログインできません。前のバージョンも Java 8 と同様に機能しました。
7. [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。
8. 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 URL からご確認ください。
   http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&Indocid=MIGR-5080396
9. 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。
10. 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。
11. 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ーでは機能しません。
12. 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。
13. 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。
14. 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。
15. 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。