システムのバックアップ

バックアップの概要

定期的にバックアップを行うことを推奨します。 ディザスタ リカバリ システム（DRS）を使用して、クラスタ内のすべてのサーバのデータを完全にバックアップできます。 自動バックアップをセットアップすることも、任意の時点でバックアップを起動することもできます。

ディザスタ リカバリ システムで実行するバックアップは、クラスタ レベルであり、Cisco Unified Communications Manager クラスタ内のすべてのサーバのバックアップを 1 箇所に集め、バックアップ データを物理的なストレージ デバイスにアーカイブします。 バックアップ ファイルが暗号化され、システム ソフトウェアによってだけ開くことができます。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定（バックアップ デバイス設定およびスケジュール設定）を復元します。 DRS は drfDevice.xml ファイルと drfSchedule.xml ファイルをバックアップおよび復元します。 これらのファイルとともにサーバを復元するときは、DRS バックアップ デバイスおよびスケジュールを再設定する必要がありません。

システムデータを復元するときには、クラスタ内のどのノードを復元するかを選択できます。

ディザスタ リカバリ システムには、次の機能があります。

- バックアップおよび復元タスクを実行するためのユーザ インターフェイス。
- バックアップ機能を実行するための分散システム アーキテクチャ。
- スケジュール バックアップまたは手動（ユーザが起動する）バックアップ。
- リモート SFTP サーバへのバックアップのアーカイブ。

この表では、ディザスタリカバリシステムがバックアップおよび復元できる機能とコンポーネントを示します。 選択した各機能について、すべてのコンポーネントが自動的にバックアップされます。

表 *1 : Cisco Unified CM* の機能とコンポーネント

機能	コンポーネント
CCM - Unified Communications Manager	Unified Communications Manager データベース
	Platform
	Serviceability
	保留音（MOH）
	Cisco Emergency Responder
	一括管理ツール（BAT）
	優先順位
	電話デバイスファイル（TFTP）
	syslogagt（SNMP syslog エージェント）
	cdpagent（SNMP cdp エージェント）
	tct（トレース収集ツール）
	コール詳細レコード（CDR）
	CDR レポートと分析（CAR）

表 *2 : IM and Presence* の機能とコンポーネント

機能	コンポーネント
IM and Presence Service	IM and Presence データベース
	syslogagt（SNMP syslog エージェント）
	cdpagent（SNMP cdp エージェント）
	Platform
	Reporter（Serviceability Reporter）
	CUP SIP Proxy
	XCP
	CLM
	一括管理ツール（BAT）
	優先順位
	tct（トレース収集ツール）

バックアップの前提条件

- バージョンの要件を満たしていることを確認してください。
  - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケーションを実行している必要があります。
  - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
  - バックアップ ファイルに保存されているソフトウェア バージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

バージョンの文字列全体が一致している必要があります。 たとえば、IM and Presence データベース パブリッシャ ノードがバージョン 11.5.1.10000-1 の場合、すべての IM and Presence サブスクライバ ノードは 11.5.1.10000-1 であり、バックアップ ファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。 現在のバージョンと一致しないバックアップ ファイルからシステムを復元しようすると、復元は失敗します。 バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されているバージョンと一致するよう、ソフトウェア バージョンをアップグレードしたら常にシステムをバックアップするようにしてください。

- DRS 暗号化は、クラスタ セキュリティ パスワードに依存することに留意してください。バックアップの実行中に、DRS は暗号化のためにランダム パスワードを生成し、そのランダム パスワードをクラスタ セキュリティ パスワードを使用して暗号化します。バックアップを実行した後、復元を行うまでの間にクラスタ セキュリティ パスワードが変更された場合、そのバックアップ ファイルを使用してシステムを復元するには、バックアップを実行した時点でのパスワードを把握していなければなりません。あるいは、セキュリティ パスワードを変更/リセットした直後にバックアップを作成するようにしてください。
- リモート デバイスをバックアップする必要がある場合は、必ず SFTP サーバを設定する必要があります。利用可能な SFTP サーバの詳細については、次の項を参照してください。リモート バックアップ用 SFTP サーバ （11 ページ）

バックアップ タスク フロー

次のタスクを実行して、バックアップを設定して実行します。バックアップの実行中は OS 管理タスクを実行しないでください。これは、ディザスタ リカバリ システムがプラットフォーム API をロックすることにより、すべての OS 管理要求をブロックするためです。ただし、CLI ベースのアップグレード コマンドしかプラットフォーム API ロッキング パッケージを使用しないため、ディザスタ リカバリ システムはほとんどの CLI コマンドを妨害しません。

手順

	コマンドまたはアクション	目的
ステップ 1	バックアップ デバイスの設定 （5 ページ）	データをバックアップするデバイスを指定します。
ステップ 2	バックアップ ファイルのサイズの予測 （6 ページ）	SFTP デバイス上で作成されるバックアップ ファイルのサイズを見積もります。
ステップ 3	次のいずれかのオプションを選択します。 • スケジュール バックアップの設定 （7 ページ） • 手動バックアップの開始 （8 ページ）	スケジュールに従ってデータをバックアップするためのバックアップ スケジュールを作成します。 手動バックアップを実行します（任意）。
ステップ 4	現在のバックアップ ステータスの表示 （9 ページ）	これはオプションです。バックアップのステータスをチェックします。バックアップの実行中、現在のバックアップ ジョブのステータスを確認できます。
ステップ 5	バックアップ履歴の表示 （10 ページ）	これはオプションです。バックアップ履歴の表示

バックアップ デバイスの設定

最大10個のバックアップデバイスを設定できます。 バックアップ ファイルを保存する場所を設定するには、次の手順を実行します。

始める前に

- バックアップ ファイルを保存するために SFTP サーバにディレクトリ パスへの書き込みアクセス権があることを確認します。
- DRS マスターエージェントがバックアップデバイスの設定を検証するときに、ユーザ名、パスワード、サーバ名とディレクトリ パスが有効であることを確認します。

（注） バックアップはネットワーク トラフィックが少なくなる時間帯にスケジューリングしてください。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）] > [バックアップ デバイス（Backup Device）]** の順に選択します。

ステップ 2 [バックアップ デバイス リスト（Backup Device List）]ウィンドウで、次のいずれかを実行します。

- 新しいデバイスを設定するには、[新規追加（Add New）]をクリックします。
- 既存のバックアップ デバイスを編集するには、検索条件を入力し、[検索（Find）]、次に[選択項目の編集（Edit Selected）]をクリックします。
- バックアップ デバイスを削除するには、[バックアップ デバイス（Backup Device）]リストでバックアップ デバイスを選択してから [選択項目の削除（Delete Selected）]をクリックします。

バックアップ スケジュールにバックアップ デバイスとして設定されているバックアップ デバイスは削除できません。

ステップ 3 [バックアップデバイス名（Backup device name）]フィールドにバックアップ名を入力します。

バックアップ デバイス名には、英数字、スペース（）、ダッシュ（-）、およびアンダースコア（_）だけを使用します。 それ以外の文字は使用しないでください。

ステップ 4 [接続先の選択（Select Destination）]領域の [ネットワーク ディレクトリ（Network Directory）]で、次を実行します。

- [ホスト名/IP アドレス（Host name/IP Address）]フィールドに、ネットワーク サーバのホスト名または IP アドレスを入力します。
- [パス名（Path name）]フィールドに、バックアップ ファイルを格納するディレクトリ パスを入力します。

- [ユーザ名（User name）]フィールドに、有効なユーザ名を入力します。
- [パスワード（Password）]フィールドに、有効なパスワードを入力します。
- [ネットワーク ディレクトリに保存するバックアップ数（Number of backups to store on Network Directory）]ドロップダウン リストから、バックアップの必要数を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

バックアップ ファイルのサイズの予測 （6 ページ）

バックアップ ファイルのサイズの予測

1 つまたは複数の選択した機能のバックアップ履歴が存在する場合に限り、Cisco Unified Communications Manager は、バックアップ tar のサイズを予測します。

計算されたサイズは正確な値ではなく、バックアップ tar の予測サイズです。 サイズは前のバックアップの実際のバックアップ サイズに基づいて計算され、設定が前回のバックアップ以降変更された場合は異なることがあります。

この手順は、前回のバックアップが存在する場合にのみ使用でき、初めてシステムをバックアップする場合は使用できません。

SFTP デバイスに保存されているバックアップ tar のサイズを予測するには、次の手順に従ってください。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]**>**[手動バックアップ（Manual Backup）]** の順に選択します。

ステップ 2 [機能の選択（Select Features）]領域でバックアップする機能を選択します。

ステップ 3 選択した機能のバックアップの予測サイズを表示するには、[サイズの予測（Estimate Size）]を選択します。

次のタスク

システムをバックアップするには、次のいずれかの手順を実行します。

- スケジュール バックアップの設定 （7 ページ）
- 手動バックアップの開始 （8 ページ）

スケジュール バックアップの設定

最大 10 個のバックアップ スケジュールを作成できます。 各バックアップ スケジュールには、自動バックアップのスケジュール、バックアップする機能セット、保存場所など、独自のプロパティがあります。

バックアップ .tar ファイルはランダムに生成されるパスワードで暗号化されるということに注意してください。 このパスワードは、クラスタ セキュリティ パスワードで暗号化され、バックアップ .tar ファイルとともに保存されます。 このセキュリティ パスワードは忘れないように記憶しておくか、またはセキュリティパスワードを変更またはリセットしたらすぐにバックアップを作成する必要があります。

注意 コール処理が中断してサービスに影響が及ばないように、バックアップはオフピーク時間中にスケジュールしてください。

始める前に

バックアップ デバイスの設定 （5 ページ）

手順

ステップ 1 ディザスタ リカバリ システムで、[バックアップ スケジューラ（Backup Scheduler）] を選択します。

ステップ 2 [スケジュール リスト（Schedule List）]ウィンドウで、新規スケジュールを追加するか、または既存のスケジュールを編集します。

- 新規スケジュールを作成するには、[Add New]をクリックします。
- 既存のスケジュールを設定するには、[スケジュール リスト（Schedule List）] 列でその名前をクリックします。

ステップ 3 [スケジューラ（scheduler）]ウィンドウで、[スケジュール名（Schedule Name）]フィールドにスケジュール名を入力します。

（注） デフォルトのスケジュールの名前は変更できません。

ステップ 4 [バックアップ デバイスの選択（Select Backup Device）]領域でバックアップ デバイスを選択します。

ステップ 5 [機能の選択（Select Features）]領域でバックアップする機能を選択します。 少なくとも 1 つの機能を選択する必要があります。

ステップ 6 [バックアップの開始時刻（Start Backup at）]領域でバックアップを開始する日付と時刻を選択します。

ステップ 7 [頻度（Frequency）]領域でバックアップを行う頻度を選択します。 頻度は、[一度（Once）]、[日次（Daily）]、[週次（Weekly）]、[月次（Monthly）] に設定できます。 [週次（Weekly）]を選択した場合は、バックアップを行う週の曜日も選択できます。

ヒント バックアップ頻度を火曜日から土曜日までの[週次（Weekly）]に設定するには、[デフォルトの設定（Set Default）]をクリックします。

ステップ 8 これらの設定を更新するには、[保存（Save）]をクリックします。

ステップ 9 次のいずれかのオプションを選択します。

- 選択したスケジュールをイネーブルにするには、[選択されたスケジュールの有効化（Enable Selected Schedules）]をクリックします。
- 選択したスケジュールをディセーブルにするには、[選択されたスケジュールの無効化（Disable Selected Schedules）]をクリックします。
- 選択したスケジュールを削除するには、[選択項目の削除（Delete Selected）]をクリックします。

ステップ 10 スケジュールを有効にするには、[スケジュールの有効化（Enable Schedule）]をクリックします。

設定した時刻になると自動的に次のバックアップが実行されます。

（注） クラスタ内のすべてのサーバが、同じバージョンの Cisco Unified Communications Manager または Cisco IM and Presence サービスを実行し、ネットワークから到達可能であることを確認します。スケジュールされたバックアップの時刻にサーバーに到達できないと、そのサーバーはバックアップされません。

次のタスク

次の手順を実行します。

- バックアップ ファイルのサイズの予測 （6 ページ）
- （任意） 現在のバックアップ ステータスの表示 （9 ページ）

手動バックアップの開始

始める前に

- バックアップ ファイルの格納場所としてネットワーク デバイスを使用していることを確認します。Unified Communications Manager の仮想化展開では、テープ ドライブによるバックアップ ファイルの保存はサポートされません。
- Cisco Unified Communications Manager または IM and Presence Service のインストールされているバージョンが、すべてのクラスタ ノードで同じであることを確認します。
- バックアップ プロセスは、リモート サーバに利用可能な容量がないためや、ネットワーク接続が中断されたために失敗することがあります。バックアップが失敗する原因となった問題に対処した後、新規のバックアップを開始する必要があります。

- ネットワークの中断がないことを確認してください。
- バックアップ デバイスの設定 （5 ページ）
- バックアップ ファイルのサイズの予測 （6 ページ）
- クラスタ セキュリティ パスワードのレコードがあることを確認します。 このバックアップの完了後に、クラスタ セキュリティ パスワードを変更した場合は、パスワードを認識している必要があります。パスワードを認識していないと、バックアップ ファイルを使用してシステムを復元できなくなります。

（注） バックアップが実行されている間は、Disaster Recovery System がプラットフォーム API をロックしてすべての要求をブロックするため、Cisco Unified OS の管理または Cisco Unified IM and Presence OS の管理でタスクを実行することはできません。 ただし、CLI ベースのアップグレード コマンドしかプラットフォーム API ロッキング パッケージを使用しないため、ディザスタ リカバリ システムはほとんどの CLI コマンドを妨害しません。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]>[手動バックアップ（Manual Backup）]** の順に選択します。

ステップ 2 [手動バックアップ（Manual Backup）] ウィンドウで、[バックアップ デバイス名（Backup Device Name）] 領域を選択します。

ステップ 3 [機能の選択（Select Features）] 領域から機能を選択します。

ステップ 4 [バックアップの開始（Start Backup）] をクリックします。

次のタスク

（任意） 現在のバックアップ ステータスの表示 （9 ページ）

現在のバックアップ ステータスの表示

現在のバックアップ ジョブのステータスを確認するには、次の手順を実行します。

注意 リモート サーバへのバックアップが 20 時間以内に完了しないとバックアップ セッションがタイムアウトするため、新規バックアップを開始する必要があります。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]**>**[現在のステータス（Current Status）]** の順に選択します。

ステップ 2 バックアップ ログ ファイルを表示するには、ログファイル名リンクをクリックします。

ステップ 3 現在のバックアップをキャンセルするには、[バックアップのキャンセル（Cancel Backup）]をクリックします。

（注） 現在のコンポーネントがバックアップ操作を完了した後、バックアップがキャンセルされます。

次のタスク

バックアップ履歴の表示 （10 ページ）

バックアップ履歴の表示

バックアップ履歴を参照するには、次の手順を実行します。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]** > **[履歴（History）]** の順に選択します。

ステップ 2 [バックアップ履歴（Backup History）]ウィンドウで、ファイル名、バックアップ デバイス、完了日、結果、バージョン、バックアップされている機能、失敗した機能など、実行したバックアップを表示できます。

（注） [バックアップ履歴（Backup History）]ウィンドウには、最新の 20 個のバックアップ ジョブだけが表示されます。

バックアップの連携動作と制限事項

• バックアップの制約事項 （11 ページ）

バックアップの制約事項

バックアップには、次の制約事項が適用されます。

表 *3:* バックアップの制約事項

制約事項	説明
クラスタ セキュリティ パスワード	クラスタセキュリティパスワードを変更したら、必ずバックアップを実行することを推奨します。 バックアップ暗号化では、バックアップ ファイルのデータを暗号化する際にクラスタセキュリティパスワードを使用します。バックアップファイルの作成後にクラスタセキュリティパスワードを編集すると、古いパスワードを忘れてしまった場合に、そのバックアップ ファイルを使用してデータを復元できなくなります。
証明書の管理	ディザスタリカバリシステム（DRS）は、マスターエージェントとローカルエージェントとの間で SSL ベースの通信を使用して、Unified Communications Manager クラスタノード間のデータの認証および暗号化を行います。 DRS は、リリース 14、14SU1、14SU3 以降のバージョンの公開キー/秘密キーの暗号化に、tomcat RSA 証明書を使用します。証明書管理ページから Tomcat 信頼ストア（hostname.pem）ファイルを削除すると、DRS が想定どおりに機能しなくなることに注意してください。 Tomcat-trust ファイルを手動で削除するときは、tomcat RSA 証明書を Tomcat-trust に必ずアップロードしてください。 （注） リリース 14SU2 について、DRS は Tomcat-ECDSA 証明書を使用して、公開キー/秘密キーの暗号化を行います。 証明書管理ページから Tomcat 信頼ストア（hostname.pem）ファイルを削除すると、DRS が想定どおりに機能しなくなることに注意してください。 Tomcat-trust ファイルを手動で削除するときは、Tomcat-ECDSA 証明書を Tomcat-trust に必ずアップロードしてください。 詳細については、「「証明書管理」」の項を参照してください Cisco Unified Communications Manager セキュリティガイド。

リモート バックアップ用 SFTP サーバ

データをネットワーク上のリモート デバイスにバックアップするには、SFTP サーバーを用意して必要な設定を行う必要があります。 内部テストでは、シスコが提供し、Cisco TAC がサ

ポートしている Cisco Prime Collaboration Deployment（PCD）上の SFTP サーバーを使用します。 SFTP サーバオプションの概要については、次の表を参照してください。

以下の表示に記載されている情報を参考に、システムで使用する SFTP サーバ ソリューションを決定してください。

表 *4 : SFTP* サーバ情報

SFTP サーバ	情報
Cisco Prime Collaboration Deployment の SFTP サーバ	このサーバーはシスコが提供およびテストした唯一の SFTP サーバーであり、Cisco TAC が完全にサポートします。 バージョンの互換性は、使用している Unified Communications Manager および Cisco Prime Collaboration Deployment のバージョンに依存します。 バージョン（SFTP）または Unified Communications Manager をアップグレードする前に、『Cisco Prime Collaboration Deployment Administration Guide』を参照して、互換性のあるバージョンであることを確認してください。
テクノロジー パートナーの SFTP サーバ	これらのサーバーはサードパーティが提供およびテストしたものです。 バージョンの互換性は、サード パーティによるテストに依存します。 テクノロジー パートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジー パートナーのページで、互換性のあるバージョンを確認してください。 https://marketplace.cisco.com
他のサードパーティの SFTP サーバ	これらのサーバーはサードパーティが提供するものであり、Cisco TAC はこれらのサーバーを正式にサポートしていません。 バージョンの互換性は、SFTP バージョンと Unified Communications Manager バージョンの互換性を確立するためのベストエフォートに基づきます。 （注） これらの製品はシスコによってテストされていないため、機能を保証することはできません。 Cisco TAC はこれらの製品をサポートしていません。 完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジーパートナーの SFTP サーバーを利用してください。

暗号サポート

Unified Communications Manager 11.5 の場合、Unified Communications Manager は SFTP 接続用に次の CBC および CRT 暗号を通知します。

- aes128-cbc
- 3des-cbc

- aes128-ctr
- aes192-ctr
- aes256-ctr

（注） バックアップ SFTP サーバー Unified Communications Manager と通信するためにこれらの暗号のいずれかをサポートしていることを確認してください。

Unified Communications Manager 12.0 以降のリリースでは、CBC 暗号はサポートされていません。 Unified Communications Manager は、次の CTR 暗号だけをサポートおよび通知します。

- aes256-ctr
- aes128-ctr
- aes192-ctr

（注） バックアップ SFTP サーバーが Unified Communications Manager と通信するためにこれらの CTR 暗号のいずれかをサポートしていることを確認してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。