バックアップ/復元操作

バックアップ データのタイプ

Cisco ISE では、プライマリ PAN とモニタリング ノードからデータをバックアップすることができます。バックアップは CLI またはユーザ インターフェイスから実行できます。

Cisco ISE では次のタイプのデータのバックアップが可能です。

- 設定データ：アプリケーション固有および Cisco ADE オペレーティング システム両方の設定データが含まれます。バックアップは、GUI または CLI を使用してプライマリ PAN を介して実行できます。
- 運用データ：モニタリングおよびトラブルシューティング データが含まれます。バックアップは、プライマリ PAN GUI を介して、またはモニタリング ノードの場合は CLI を使用して実行できます。

Cisco ISE が VMware で実行されている場合、ISE データをバックアップするのに、VMware スナップショットはサポートされていません。

（注） Cisco ISE は、ISE データのバックアップ用の VMware スナップショットをサポートしていません。これは、VMware スナップショットが特定の時点で VM のステータスを保存するためです。マルチノード Cisco ISE 環境では、すべてのノードのデータは、現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。シスコは、データのバックアップおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。

VMware スナップショットまたはサードパーティのバックアップを使用して ISE データをバックアップすると、Cisco ISE サービスが停止します。バックアップが VMware または CommVault SAN レベルのバックアップのようなサードパーティによって開始された場合、ファイル システムを休止してクラッシュ整合を維持するため、ISE のフリーズを引き起こします。ISE のサービスを再開するには再起動が必要です。

例：VM スナップショット、CommVault SAN レベルのバックアップなど。

復元操作は、以前のバージョンの Cisco ISE のバックアップ ファイルを使用して実行でき、以降のバージョンで復元できます。たとえば、Cisco ISE リリース 1.3 または 1.4 からの ISE ノードのバックアップがある場合、そのバックアップを Cisco ISE リリース 2.1 で復元できます。

Cisco ISE リリース 2.4 は、リリース 2.0 以降から取得したバックアップからの復元をサポートしています。

バックアップ/復元リポジトリ

Cisco ISE では管理者ポータルを使用してリポジトリを作成および削除することができます。次のタイプのリポジトリを作成できます。

- ディスク（DISK）
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

（注） リポジトリは、各デバイスに対してローカルです。

どのタイプの展開（小規模、中規模、大規模）であっても、最低でも 100 GB のリポジトリ サイズを用意することを推奨します。

次の表に、Cisco ISE 操作と外部リポジトリ タイプのサポート情報を示します。

表 *1*:外部リポジトリのサポート マトリックス

リポジトリ タイプ（Repository Type）	バックアップの設定	復元の設定	のアップグレード	操作バックアップ	復元操作	サポート バンドル	ユーザ インターフェイスからの検証	ユーザ インターフェイスからのレポートのエクスポート	ユーザ インターフェイスからのポリシーのエクスポート
FTP	√	√	√	√	√	√	√	√	√
SFTP	√	√	√	√	√	√	√	√	√
TFTP	√	√	√	√	√	√	X	√	√
HTTP	X	X	√	X	X	X	X	X	X
HTTPS	X	*X*	√	X	X	X	X	X	X
NFS	√	√	√	√	√	√	√	√	√

関連トピック

リポジトリの作成 （3 ページ）
オンデマンドおよびスケジュール バックアップ （5 ページ）

リポジトリの作成

リポジトリを作成するには、CLI と GUI を使用できます。次の理由により、GUI を使用することを推奨します。

- CLI で作成されたリポジトリはローカルに保存され、他の展開ノードに複製されません。これらのリポジトリは、GUI のリポジトリ ページに表示されません。
- プライマリ PAN で作成されたリポジトリは、他の展開ノードに複製されます。

キーはプライマリ PAN でのみ GUI で生成されます。このためアップグレード時に、新しいプライマリ管理ノードの GUI でキーを再生成して、SFTP サーバにエクスポートする必要があります。展開からノードを除去する場合、非管理ノードの GUI でキーを生成し、SFTP サーバにエクスポートする必要があります。

RSA 公開キー認証を使用する Cisco ISE の SFTP リポジトリを設定できます。データベースとログを暗号化するために管理者が作成したパスワードを使用する代わりに、セキュア キーを使用する RSA 公開キー認証を選択できます。RSA 公開キーを使用して作成された SFTP リポジ

トリの場合、GUI から作成されたリポジトリは CLI では複製されず、CLI から作成されたリポジトリは GUI では複製されません。CLI と GUI で同じリポジトリを設定するには、CLI と GUI の両方で RSA 公開キーを生成し、この両方のキーを SFTP サーバにエクスポートします。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- RSA 公開キー認証を使用する SFTP リポジトリを作成する場合は、次を実行してください。
  - SFTP リポジトリの RSA 公開キー認証を有効にします。
  - **crypto host_key add** コマンドを使用して Cisco ISE CLI から SFTP サーバのホスト キーを入力します。ホスト キー文字列は、リポジトリの設定ページで、[パス（Path）] フィールドに入力したホスト名と一致する必要があります。
  - GUI でキーペアを生成し、ローカル システムに公開キーをエクスポートします。Cisco ISE CLI から **crypto key generate rsa passphrase***test123* コマンドを使用してキー ペアを生成し（この場合パスフレーズは 5 文字以上でなければなりません）、キーを任意のリポジトリ（ローカル ディスクまたは設定されているその他のリポジトリ）にエクスポートします。
  - エクスポートした RSA 公開キーを PKI 対応の SFTP サーバにコピーし、「authorized_keys」ファイルに追加します。

ステップ 1 [管理（Administration）]>[システム（System）]>[メンテナンス（Maintenance）]>[リポジトリ（Repository）] を選択します。

ステップ 2 [追加（Add）] をクリックして、新しいリポジトリを追加します。

ステップ 3 新しいリポジトリのセットアップの必要に応じて値を入力します。フィールドの説明については、リポジトリの設定を参照してください。

ステップ 4 [送信（Submit）] をクリックしてリポジトリを作成します。

ステップ 5 左側の [操作（Operations）] ナビゲーション ペインで [リポジトリ（Repository）] をクリックするか、このページ上部の [リポジトリ リスト（Repository List）] リンクをクリックして、リポジトリのリスト ページに移動して、リポジトリが正常に作成されていることを確認します。

次のタスク

- 作成したリポジトリが有効であることを確認します。これは、リポジトリのリストページから行います。リポジトリを選択し、[確認（Validate）] をクリックします。また、Cisco ISE コマンドライン インターフェイスから次のコマンドを実行することもできます。

  show repository *repository_name*

  ここで、*repository_name* は作成したリポジトリの名前です。

（注） リポジトリの作成時に指定したパスが存在しない場合、「%無効なディレクトリです（%Invalid Directory）」というエラーが表示されます。

- オンデマンド バックアップを実行するかバックアップのスケジュールを設定します。

関連トピック

オンデマンド バックアップの実行 （6 ページ）
バックアップのスケジュール （9 ページ）

SFTP リポジトリでの RSA 公開キー認証の有効化

SFTP サーバでは、各ノードに 2 つの RSA 公開キー（CLI 用と GUI 用にそれぞれ 1 つずつ）が必要です。SFTP リポジトリの RSA 公開キー認証を有効にするには、以下のステップに従います。

ステップ 1 */Etc/ssh/sshd_config.file* を編集する権限を持つアカウントで SFTP サーバにログインします。

（注） *sshd_config* ファイルのロケーションは、インストールされているオペレーティング システムによって異なる可能性があります。

ステップ 2 **vi etc/ssh/sshd_config** コマンドを入力します。

Sshd_config ファイルの内容がリストされます。

ステップ 3 RSA 公開キー認証を有効にするには、以下の行の「#」記号を削除します。

- RSAAuthentication yes
- PubkeyAuthentication yes

（注） Public Auth Key が no の場合は yes に変更してください。

- AuthorizedKeysFile ~/.ssh/authorized_keys

オンデマンドおよびスケジュール バックアップ

Cisco ISE では、プライマリ PAN およびプライマリ モニタリング ノードのオンデマンド バックアップができます。バックアップ データがすぐに必要な場合にオンデマンド バックアップを実行します。

Cisco ISE では、1 回、毎日、毎週、または毎月実行するようにシステム レベルのバックアップをスケジュールできます。バックアップ操作は長時間かかる場合がありますが、スケジュー

ルできるため中断が発生することはありません。Cisco ISE 管理者ポータルからバックアップをスケジュールできます。

（注） Cisco ISE リリース 1.2 にアップグレードする場合は、バックアップ ジョブのスケジュール設定を再作成する必要があります。

関連トピック

バックアップのスケジュール （9 ページ）
オンデマンド バックアップの実行 （6 ページ）
CLI を使用したバックアップ （11 ページ）
バックアップ履歴 （11 ページ）
バックアップの失敗 （11 ページ）
Cisco ISE 復元操作 （12 ページ）
メンテナンスの設定

オンデマンド バックアップの実行

オンデマンドバックアップを実行して、即座に設定データまたはモニタリング（運用）データをバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。

重要 バックアップと復元を行う場合、復元によって、ターゲット システムの信頼できる証明書のリストがソース システムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  長所：ソース システムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲット システムによって発行された新しい証明書は、同じキーによって署名されます。

  短所：復元機能を使用する前にターゲット システムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  長所：このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソース システムによって発行された証明書は引き続き信頼されます。

  短所：復元機能を使用する前にターゲット システムによって発行された証明書は信頼されないため、再発行する必要があります。

始める前に

- この作業を実行する前に、Cisco ISE のバックアップ データのタイプの基本を理解している必要があります。
- バックアップ ファイルを格納するリポジトリを作成したことを確認します。
- ローカル リポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- バックアップを取得する前に、すべての証明書関連の変更を実行します。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

（注） バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。バックアップを復元するには、リポジトリを選択し、[復元（Restore）] をクリックします。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 バックアップのタイプ [設定（Configuration）] または [動作中（Operational）] を選択します。

ステップ 3 [すぐにバックアップ（Backup Now）] をクリックします。

ステップ 4 バックアップを実行するために必要な値を入力します。

ステップ 5 [OK][バックアップ（Backup）]をクリックします。

ステップ 6 バックアップが正常に完了したことを確認します。

Cisco ISE はタイムスタンプを持つバックアップ ファイル名を付け、指定されたリポジトリにファイルを保存します。タイムスタンプに加えて、Cisco ISE は設定バックアップには CFG タグ、操作バックアップには OPS タグを追加します。バックアップ ファイルが指定リポジトリにあることを確認します。

分散展開では、バックアップの実行中にノードのロールを変更したり、ノードの設定を行ったりすることはできません。バックアップの実行中にノードのロールを変更すると、すべてのプロセスがシャットダウンし、データに不一致が生じる場合があります。ノードのロールを変更する際は、バックアップが完了するまで待機してください。

バックアップの実行中はノードを昇格しないでください。これによりすべてのプロセスがシャットダウンし、バックアップを同時に実行中の場合はデータに不一致が生じる場合があります。ノードを変更する際は、バックアップが完了するまで待ってください。

（注） バックアップが実行されているときに、高いCPU使用率が観察されたり、[負荷平均が高い（High Load Average）] アラームが表示されたりする可能性があります。バックアップが完了すると、CPU 使用率は通常に戻ります。

関連トピック

バックアップ データのタイプ （1 ページ）
リポジトリの作成 （3 ページ）
バックアップ/復元リポジトリ （2 ページ）
バックアップのスケジュール （9 ページ）
CLI を使用したバックアップ （11 ページ）
バックアップ履歴 （11 ページ）
バックアップの失敗 （11 ページ）

Cisco ISE 復元操作 （12 ページ）
認証および許可ポリシー設定のエクスポート （20 ページ）

バックアップのスケジュール

オンデマンドバックアップを実行して、即座に設定データまたはモニタリング（運用）データをバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。

重要 バックアップと復元を行う場合、復元によって、ターゲットシステムの信頼できる証明書のリストがソースシステムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  長所：ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲットシステムによって発行された新しい証明書は、同じキーによって署名されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  長所：このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソースシステムによって発行された証明書は引き続き信頼されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

始める前に

- この作業を実行する前に、Cisco ISE のバックアップ データのタイプの基本を理解している必要があります。
- リポジトリを設定していることを確認します。

- ローカル リポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- Cisco ISE 1.1 以前のリリースから Cisco ISE 1.2 にアップグレードする場合、バックアップのスケジュールを再設定する必要があります。『*Cisco Identity Services Engine Upgrade Guide, Release 1.2*』の「Known Upgrade Issues」の項を参照してください。

（注） バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 [作成（Create）][スケジュール（Schedule）]をクリックして、設定または操作バックアップをスケジュールします。

ステップ 3 必要に応じてバックアップをスケジュールするための値を入力します。

ステップ 4 [保存（Save）] をクリックして、バックアップをスケジュールします。

ステップ 5 次のいずれかの操作を実行します。

- [リポジトリの選択（Select Repository）] ドロップダウンリストから、必要なリポジトリを選択します。
- [リポジトリの追加（Add Repository）] リンクをクリックして新しいリポジトリを追加します。

ステップ 6 [更新（Refresh）] リンクをクリックして、スケジュール バックアップのリストを表示します。

作成できる設定または操作バックアップのスケジュールは 1 回に 1 つだけです。スケジュール バックアップは有効化または無効化できますが、削除はできません。

関連トピック

バックアップ データのタイプ （1 ページ）
オンデマンドおよびスケジュール バックアップ （5 ページ）
オンデマンド バックアップの実行 （6 ページ）
CLI を使用したバックアップ （11 ページ）
バックアップ履歴 （11 ページ）
バックアップの失敗 （11 ページ）
バックアップ/復元リポジトリ （2 ページ）

CLI を使用したバックアップ

CLI と GUI の両方からバックアップをスケジュールできますが、GUI から実行することを推奨します。ただし、セカンダリ モニタリング ノードの操作バックアップは、CLI からのみ実行できます。

バックアップ履歴

バックアップ履歴は、スケジュールまたはオンデマンドバックアップに関する基本情報です。バックアップ履歴には、バックアップ名、バックアップ ファイルのサイズ、バックアップが保存されているリポジトリ、バックアップが取られたタイム スタンプを表示します。この情報は、操作監査レポートまたは、履歴テーブルの [バックアップ/復元（Backup and Restore）] ページから入手できます。

バックアップが失敗すると、Cisco ISE がアラームをトリガーします。バックアップ履歴ページに失敗の原因が表示されます。障害の原因は操作監査レポートにも記載されます。障害の原因が欠落しているか明確でない場合は、Cisco ISE CLI から **backup-logs** コマンドを実行し、ADE.log でより詳細な情報を確認できます。

バックアップ操作の実行中は、**show backup status** CLI コマンドを使用して、バックアップ操作の進行状況を確認することができます。

バックアップ履歴は、Cisco ADE オペレーティング システムの設定データとともに保存されています。つまり、アプリケーションのアップグレード後もそこに残っており、PAN のイメージを再作成した場合にのみ削除されます。

バックアップの失敗

バックアップが失敗した場合は、次を確認してください。

- NTP 同期またはサービス障害の問題があるかどうかを確認します。Cisco ISE の NTP サービスが動作していない場合、Cisco ISE では、[NTPサービスの障害（NTP Service Failure）] のアラームが発生します。Cisco ISE が、設定されているすべての NTP サーバと同期できない場合、Cisco ISE では、[NTP同期に失敗（NTP Sync Failure）] のアラームが発生します。NTP サービスがダウンしている場合、または同期の問題がある場合は、Cisco ISE のバックアップが失敗する可能性があります。バックアップ操作を再試行する前に、[アラーム（Alarm）] ダッシュレットを確認し、NTP 同期またはサービスの問題を修正してください。
- 他のバックアップが同時に実行されていないことを確認します。
- 設定したリポジトリの使用可能なディスク領域を確認します。
  - （操作）バックアップのモニタリングは、モニタリング データがモニタリング データベースに割り当てられたサイズの 75% を超えると失敗します。たとえばモニタリング ノードに 600 GB 割り当てられており、モニタリング データがストレージの 450 GB を超える領域を消費すると、モニタリングのバックアップは失敗します。

- データベースのディスク使用量が 90% を超える場合、消去が発生してデータベースを割り当てられたサイズの 75% 以下のサイズにします。

- 消去が進行中かどうかを確認します。消去の進行中はバックアップ/復元操作は動作しません。
- リポジトリが正しく設定されていることを確認します。

Cisco ISE 復元操作

プライマリまたはスタンドアロン 管理ノードで設定データを復元できます。プライマリ PAN にデータを復元したら、手動でセカンダリ ノードをプライマリ PAN と同期する必要があります。

運用データを復元するプロセスは、展開のタイプによって異なります。

（注） Cisco ISE の新しいバックアップ/復元ユーザ インターフェイスでは、バックアップ ファイル名にメタデータが使用されます。したがって、バックアップが完了後に、バックアップ ファイル名を手動で変更しないでください。バックアップ ファイルの名前を手動で変更すると、Cisco ISE バックアップ/復元ユーザ インターフェイスがそのバックアップ ファイルを認識できなくなります。バックアップ ファイル名を変更しなければならない場合は、バックアップの復元に Cisco ISE CLI を使用する必要があります。

関連トピック

CLI からの設定またはモニタリング（操作）バックアップの復元 （14 ページ）
GUI からの設定バックアップの復元 （16 ページ）
モニタリング データベースの復元 （17 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （20 ページ）

データの復元に関するガイドライン

次は、Cisco ISE バックアップ データを復元する場合に従うべきガイドラインです。

- Cisco ISE では、ある ISE ノード（A）からバックアップを取得して、別の ISE ノード（B）に復元することができます。両方のノードは同じホスト名（IP アドレスは異なる）です。ただし、ノード B 上のバックアップを復元した後は、証明書とポータル グループ タグの問題が生じる可能性があるため、ノード B のホスト名を変更することはできません。
- あるタイムゾーン内のプライマリ PAN からバックアップを取得して、別のタイムゾーン内の別の Cisco ISE ノードに復元する場合、復元プロセスが失敗することがあります。この問題は、バックアップ ファイルのタイムスタンプが、バックアップが復元される Cisco ISE ノードのシステム時刻より新しい場合に発生します。同じバックアップを、取得後 1

日経過してから復元すると、バックアップ ファイルのタイムスタンプが過去のものになり、復元プロセスは成功します。

- バックアップを取得したホスト名と別のホスト名を持つプライマリ PAN にバックアップを復元すると、プライマリ PAN はスタンドアロン ノードになります。展開が切断し、セカンダリ ノードは機能しなくなります。スタンドアロン ノードをプライマリ ノードにし、セカンダリ ノードの設定をリセットしてプライマリ ノードに再登録する必要があります。Cisco ISE ノードの設定をリセットするには、Cisco ISE CLI から次のコマンドを入力してください。
  - **application reset-config ise**
- システムのタイムゾーンは、最初の Cisco ISE インストールおよびセットアップ後に変更しないことを推奨します。
- 展開の 1 つ以上のノードの証明書設定を変更した場合は、データを復元するための別のバックアップをスタンドアロン Cisco ISE ノードまたはプライマリ PAN から取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。
- プライマリ PAN 上で設定バックアップを復元した後に、以前にエクスポートした Cisco ISE CA 証明書およびキーをインポートできます。

（注） Cisco ISE CA 証明書およびキーをエクスポートしなかった場合は、プライマリ PAN 上で設定バックアップを復元した後に、プライマリ PAN およびポリシー サービス ノード（PSN）でルート CA および下位 CA を生成します。

- 適切な FQDN（プラチナ データベースの FQDN）を使用せずにプラチナ データベースを復元する場合は、CA 証明書を再生成する必要があります。（[管理（Administration）]>[証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）] > [ISEルートCA証明書チェーンの置き換え（Replace ISE Root CA certificate chain）] を選択します）。ただし、適切な FQDN でプラチナ データベースを復元する場合は、CA 証明書が自動的に再生成されます。
- Cisco ISE がバックアップ ファイルを格納するデータ リポジトリが必要です。オンデマンドまたはスケジュール設定されたバックアップを実行する前に、リポジトリを作成する必要があります。
- スタンドアロン管理ノードに障害が発生した場合、設定バックアップを実行して復元する必要があります。プライマリ PAN で障害が発生した場合、分散セットアップを使用してセカンダリ管理ノードをプライマリに昇格できます。その後、新しいプライマリ PAN にデータを復元できます。

（注） Cisco ISE では、**backup-logs** CLI コマンドも使用できます。このコマンドを使用して、ログやコンフィギュレーションファイルの収集を行い、これらをトラブルシューティングに利用できます。

CLI からの設定またはモニタリング（操作）バックアップの復元

Cisco ISE CLI から設定データを復元するには、EXEC モードで **restore** コマンドを使用します。設定または操作バックアップからデータを復元するには、次のコマンドを使用します。

restore *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

構文の説明

restore	設定または操作バックアップからデータを復元するには、このコマンドを入力します。
filename	リポジトリに存在するバックアップ ファイルのファイル名。最大 120 文字の英数字をサポートします。 （注） ファイル名の後に、tar.gpg という拡張子を付ける必要があります（myfile.tar.gpg など）。
repository	バックアップを含むリポジトリを指定します。
repository-name	バックアップを復元するリポジトリの名前。
encryption-key	（オプション）バックアップを復元するユーザ定義の暗号キーを指定します。
hash	バックアップを復元するためのハッシュされた暗号キー。使用する暗号化された（ハッシュ化された）暗号化キーを指定します。40 文字までで指定します。
plain	バックアップを復元するためのプレーン テキストの暗号キー。使用する暗号化されたプレーンテキストの暗号化キーを指定します。15 文字までで指定します。
encryption-key name	暗号キーを入力します。

include-adeos	（オプション、設定バックアップのみに該当）設定バックアップから ADE-OS 設定を復元する場合に、このコマンドオペレータ パラメータを入力します。設定バックアップを復元する場合にこのパラメータを含めないと、Cisco ISE は Cisco ISE アプリケーション設定データのみを復元します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

使用上のガイドライン

Cisco ISE で restore コマンドを使用すると、Cisco ISE サーバが自動的に再起動します。

データの復元処理で、暗号キーはオプションです。暗号キーを指定しなかった以前のバックアップの復元をサポートするために、暗号キーなしで **restore** コマンドを使用できます。

例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

関連コマンド

	Description
backup	バックアップ（Cisco ISE と Cisco ADE OS）を実行して、そのバックアップをリポジトリに保存します。
backup-logs	システム ログをバックアップします。
repository	バックアップ設定のリポジトリ サブモードを入力します。
show repository	特定のリポジトリにある使用可能なバックアップ ファイルを表示します。
show backup history	システムのバックアップ履歴を表示します。
show backup status	バックアップ操作のステータスを表示します。
show restore status	復元操作のステータスを表示します。

いずれかのセカンダリ ノードでアプリケーション復元後の同期ステータスおよび複製ステータスが [非同期（Out of Sync）] になっている場合、該当セカンダリ ノードの証明書をプライマリ PAN に再インポートして、手動同期を実行する必要があります。

関連トピック

GUI からの設定バックアップの復元 （16 ページ）
復元履歴 （19 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （20 ページ）

GUI からの設定バックアップの復元

管理者ポータルで設定バックアップを復元できます。GUI には現在のリリースから取得されたバックアップのみが表示されます。このリリースより前のバックアップを復元するには、CLI から restore コマンドを使用します。

始める前に

プライマリ PAN の自動フェールオーバー設定が展開でイネーブルになっている場合はオフにします。設定バックアップを復元すると、アプリケーション サーバ プロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ PAN の自動フェールオーバーが開始される場合があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 バックアップの名前を設定バックアップのリストから選択し、[復元（Restore）] をクリックします。

ステップ 3 バックアップ時に使用した暗号キーを入力します。

ステップ 4 [復元（Restore）] をクリックします。

次のタスク

Cisco ISE CA サービスを使用する場合は、次のことを実行する必要があります。

1. Cisco ISE CA ルート チェーン全体を再生成します。
2. Cisco ISE CA 証明書およびキーのバックアップをプライマリ PAN から取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN が外部 PKI のルート CA または下位 CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

関連トピック

CLI からの設定またはモニタリング（操作）バックアップの復元 （14 ページ）

モニタリング データベースの復元

モニタリングデータベースを復元するプロセスは、展開のタイプによって異なります。次の項では、スタンドアロンおよび分散展開でモニタリングデータベースを復元する方法について説明します。

Cisco ISE の以前のリリースからのオンデマンド モニタリング データベースのバックアップを復元するには、CLI を使用する必要があります。Cisco ISE リリース間でのスケジュール バックアップの復元はサポートされていません。

（注） データが取得されたノードとは別のノードにデータを復元しようとする場合、新しいノードを指すロギング ターゲット設定を設定する必要があります。これにより、モニタリング syslog が正しいノードに送信されるようになります。

関連トピック

スタンドアロン環境でのモニタリング（運用）バックアップの復元 （17 ページ）
管理およびモニタリングペルソナによるモニタリング バックアップの復元 （18 ページ）
モニタリング ペルソナによるモニタリング バックアップの復元 （19 ページ）

スタンドアロン環境でのモニタリング（運用）バックアップの復元

GUI には現在のリリースから取得されたバックアップのみが表示されます。前のリリースから取得されたバックアップを復元するには、CLI から restore コマンドを使用します。

始める前に

- 古いモニタリング データを消去します。

- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 バックアップの名前を操作バックアップのリストから選択し、[復元（Restore）] をクリックします。

ステップ 3 バックアップ時に使用した暗号キーを入力します。

ステップ 4 [復元（Restore）] をクリックします。

関連トピック

バックアップのスケジュール （9 ページ）
オンデマンド バックアップの実行 （6 ページ）
CLI からの設定またはモニタリング（操作）バックアップの復元 （14 ページ）
管理およびモニタリングペルソナによるモニタリング バックアップの復元 （18 ページ）
モニタリング ペルソナによるモニタリング バックアップの復元 （19 ページ）

管理およびモニタリングペルソナによるモニタリング バックアップの復元

管理およびモニタリング ペルソナを使用して、分散環境でのモニタリング バックアップを復元することができます。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 プライマリとセカンダリ PAN を使用している場合は、PAN と同期します。

PAN と同期する場合、アクティブなプライマリに昇格するように PAN を選択する必要があります。

ステップ 2 モニタリング ノードを登録解除する前に、モニタリング ペルソナを展開内の別のノードに割り当てます。

展開ごとに、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 3 バックアップされるモニタリング ノードを登録解除します。

ステップ 4 新しく登録解除されたノードにモニタリング バックアップを復元します。

ステップ 5 現在の管理ノードにより新たに復元されたノードを登録します。

ステップ 6 新たに復元されて登録されたノードをアクティブなモニタリング ノードに昇格します。

関連トピック

バックアップのスケジュール （9 ページ）
オンデマンド バックアップの実行 （6 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （20 ページ）

スタンドアロン環境でのモニタリング（運用）バックアップの復元 （17 ページ）
モニタリング ペルソナによるモニタリング バックアップの復元 （19 ページ）

モニタリング ペルソナによるモニタリング バックアップの復元

分散環境のモニタリングバックアップは、モニタリングペルソナによってのみ復元できます。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 復元されるノードを登録解除する準備を行います。そのためには、モニタリング ペルソナを展開内の別のノードに割り当てます。

展開内に、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 2 復元されるノードを登録解除します。

（注） 登録解除が完了するのを待機してから、復元に進みます。復元を続行する前に、ノードがスタンドアロン状態になっている必要があります。

ステップ 3 新しく登録解除されたノードにモニタリング バックアップを復元します。

ステップ 4 現在の管理ノードにより新たに復元されたノードを登録します。

ステップ 5 新たに復元されて登録されたノードを PAN に昇格します。

関連トピック

スタンドアロン環境でのモニタリング（運用）バックアップの復元 （17 ページ）
管理およびモニタリングペルソナによるモニタリング バックアップの復元 （18 ページ）

復元履歴

操作監査レポートからは、すべての復元操作、ログイベント、ステータスに関する情報を取得することができます。

（注） ただし操作監査レポートには、前回の復元操作に対応する開始時間に関する情報はありません。

トラブルシューティング情報を入手するには、Cisco ISE CLI から **backup-logs** コマンドを実行して、ADE.log ファイルを調べる必要があります。

復元操作の進行中は、すべての Cisco ISE サービスは停止します。**show restore status** CLI コマンドを使用して、復元操作の進行状況を確認できます。

認証および許可ポリシー設定のエクスポート

認証および許可ポリシー設定を XML ファイルの形式でエクスポートし、これをオフラインで読み取って設定エラーを特定し、トラブルシューティングのために使用できます。この XML ファイルには認証および許可ポリシー ルール、単純および複合ポリシー条件、dACL、および許可プロファイルが含まれます。XML ファイルを電子メールで送信するか、ローカル システムに保存することを選択できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup & Restore）]** を選択します。

ステップ 2 [ポリシーのエクスポート（Policy Export）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [エクスポート（Export）] をクリックします。

XML ファイルの内容を表示するには、ワードパッドなどのテキスト エディタを使用します。

分散環境でのプライマリノードとセカンダリノードの同期

分散環境では、PAN のバックアップ ファイルの復元後に、プライマリおよびセカンダリ ノードの Cisco ISE データベースが自動的に同期されないことがあります。この場合には、PAN からセカンダリ ISE ノードへの完全複製を手動で強制実行できます。強制同期は、PANからセカンダリ ノードにのみ可能です。同期操作中は、設定を変更することはできません。Cisco ISE では、同期が完全に完了した後にのみ、他の Cisco ISE 管理者ポータル ページに移動して設定変更を行うことができます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択します。

ステップ 2 非同期レプリケーション ステータスのセカンダリ ISE ノードの横にあるチェックボックスをオンにします。

ステップ 3 [同期を更新（Syncup）] をクリックし、ノードが PAN と同期されるまで待ちます。Cisco ISE 管理者ポータルへのアクセスは、このプロセスが完了するのを待たなければなりません。

スタンドアロンおよび分散展開での失われたノードの復元

この項では、スタンドアロンおよび分散展開での失われたノードの復元に使用できるトラブルシューティング情報を提供します。次の使用例の一部では、失われたデータの復旧にバックアップと復元機能を使用し、その他の使用例では、複製機能を使用しています。

分散展開での既存IPアドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。復元後に、既存 IP アドレスとホストネームを使用します。

たとえば、2 つのノード、N1（プライマリ ポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリ ポリシー管理ノードすなわちセカンダリ PAN）があります。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。

前提

展開内のすべての Cisco ISE ノードが破壊されました同じホスト名と IP アドレスを使用して、新しいハードウェアのイメージが作成されました。

解決手順（Resolution Steps）

1. N1 および N2 ノードの両方を置き換える必要があります。N1 および N2 ノードはスタンドアロン構成になりました。
2. N1 と N2 のノードの UDI を使用してライセンスを取得し、N1 ノードにインストールします。
3. 置き換えた N1 ノードでバックアップを復元する必要があります。復元スクリプトは N2 にデータを同期しようとしますが、N2 はスタンドアロン ノードであるため同期は失敗します。N1 のデータは時刻 T1 にリセットされます。
4. N1 の管理者ポータルにログインして、N2 ノードを削除して再登録する必要があります。これで、N1 および N2 ノードのデータが時刻 T1 にリセットされます。

関連トピック

CLI からの設定またはモニタリング（操作）バックアップの復元 （14 ページ）

分散展開の新IPアドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。新しいハードウェアのイメージが新しい場所で再作成され、新しい IP アドレスとホスト名が必要です。

たとえば、2 つの ISE ノード N1（プライマリ ポリシー管理ノード（プライマリ PAN））と N2（セカンダリ ポリシー サービス ノード）があります。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。Cisco ISE ノードが新しいロケーションで置き換えられ、新しいホスト名は N1A（プライマリ PAN）および N2A（セカンダリ ポリシー サービス ノード）です。N1A および N2A はこの時点ではスタンドアロン ノードです。

前提条件

展開内のすべての Cisco ISE ノードが破壊されました新しいハードウェアのイメージが、異なるホスト名と IP アドレスを使用して異なる場所で作成されました。

解決手順（Resolution Steps）

1. N1 のバックアップを入手し、これを N1A 上で復元します。復元スクリプトは、ホスト名とドメイン名の変更を認識し、現在のホスト名に基づいて展開設定内のホスト名とドメイン名を更新します。
2. 新しい自己署名証明書を生成する必要があります。
3. N1A で Cisco ISE 管理者ポータルにログインし、**[管理（Administration）] > [システム（System）] > [展開（Deployment）]** を選択して、次の操作を行う必要があります。

   古い N2 ノードを削除します。

   新しい N2A ノードをセカンダリ ノードとして登録します。N1A ノードのデータが N2A ノードに複製されます。

関連トピック

CLI からの設定またはモニタリング（操作）バックアップの復元 （14 ページ）

スタンドアロン展開の既存IPアドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノードN1があったとします。N1データベースのバックアップは、時刻 T1 に取得されました。物理的な障害により N1 ノードがダウンし、イメージの再作

成または新しいハードウェアが必要です。N1 ノードを、同じ IP アドレスとホスト名を使用して回復させる必要があります。

前提条件

この展開はスタンドアロン展開であり、新規またはイメージを再作成したハードウェアは、同じ IP アドレスとホスト名を持ちます。

解決手順（Resolution Steps）

イメージの再作成後、または同一 IP アドレスとホスト名で新しい Cisco ISE ノードを導入した後に N1 ノードが起動したら、古い N1 ノードから取得したバックアップを復元する必要があります。ロールを変更する必要はありません。

関連トピック

CLI からの設定またはモニタリング（操作）バックアップの復元 （14 ページ）

スタンドアロン展開の新 IP アドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノード N1 があったとします。時刻 T1 に取得された N1 データベースのバックアップが利用可能です。物理的な障害により N1 ノードがダウンし、異なる IP アドレスとホスト名を使用した新しいハードウェアに別のロケーションで置き換えられます。

前提条件

これはスタンドアロン展開であり、置き換えられたハードウェアは、異なる IP アドレスとホスト名を持ちます。

解決手順（Resolution Steps）

1. 新しいハードウェアで N1 ノードを置き換えます。このノードはスタンドアロン状態となり、ホスト名は N1B です。
2. バックアップを N1B ノード上で復元できます。ロールを変更する必要はありません。

関連トピック

CLI からの設定またはモニタリング（操作）バックアップの復元 （14 ページ）

設定のロール バック

問題

意図せずに設定を変更してしまい、後でそれが正しくないことがわかる場合があります。たとえば、いくつかの NAD を削除したり、一部の RADIUS 属性を誤って修正したりして、数時間

後にこの問題に気付く場合があります。この場合、変更を行う前に取得したバックアップを復元することにより、元の設定に戻すことができます。

考えられる原因

N1（プライマリ ポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリ ポリシー管理ノードすなわちセカンダリ PAN）の 2 つのノードがあり、N1 ノードのバックアップを使用できます。N1 上で誤った変更をいくつか行い、変更を元に戻す必要があります。

ソリューション

誤った設定変更を行う前に取得したN1 ノードのバックアップを入手します。N1 ノード上でこのバックアップを復元します。復元スクリプトにより、N1 のデータで N2 が同期されます。

関連トピック

CLI からの設定またはモニタリング（操作）バックアップの復元 （14 ページ）

分散展開での障害発生時のプライマリ ノードの復元

シナリオ

マルチノード展開内で、PAN に障害が発生しました。

たとえば、2 つの Cisco ISE ノード、N1（PAN）と N2（セカンダリ管理ノード）があります。ハードウェアの問題で N1 に障害が発生します。

前提条件

分散展開内のプライマリ ノードのみに障害が発生します。

解決手順（Resolution Steps）

1. N2 管理者ポータルにログインします。**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択して、N2 をプライマリ ノードとして設定します。

   N1 ノードが新しいハードウェアで置き換えられ、イメージが再作成され、スタンドアロン状態となります。

2. N2 管理者ポータルで、セカンダリ ノードとして新しい N1 ノードを登録します。

   これで、N2 ノードがプライマリ ノードになり、N1 ノードがセカンダリ ノードになります。

N1 ノードを再びプライマリ ノードにするには、N1 の管理者ポータルにログインして、このノードをプライマリ ノードに設定します。N2 は、自動的にセカンダリ サーバとなります。データが失われることはありません。

分散展開での障害発生時のセカンダリ ノードの復元

シナリオ

マルチノード展開で、1台のセカンダリ ノードに障害が発生しました。復元の必要はありません。

たとえば、N1（プライマリ PAN）、N2（セカンダリ PAN）、N3（セカンダリ ポリシー サービス ノード）、N4（セカンダリ ポリシーサービス ノード）の複数のノードが存在します。セカンダリ ノードの 1 つである N3 に障害が発生しました。

解決手順（Resolution Steps）

1. 新しいN3A ノードのイメージを再作成して、デフォルトのスタンドアロン状態にします。
2. N1 の管理者ポータルにログインし、N3 ノードを削除します。
3. N3A ノードを登録します。

   N1 から N3A へ、データが複製されます。復元の必要はありません。