



Agilent OpenLab Server および OpenLab ECM XT 管理者ガイド

注意

文書情報

文書番号 D0013947ja Rev. C.00
2024 年 2 月

著作権

© Agilent Technologies, Inc. 2024

本マニュアルの内容は米国著作権法および国際著作権法によって保護されており、Agilent Technologies, Inc. の書面による事前の許可なく、本書の一部または全部を複製することはいかなる形態や方法（電子媒体への保存やデータの抽出または他国語への翻訳など）によっても禁止されています。

Agilent Technologies, Inc.
5301 Stevens Creek Blvd.
Santa Clara, CA 95051

ソフトウェアリビジョン

このガイドは改訂版が発行されるまで Agilent OpenLab Server および OpenLab ECM XT のリビジョン 2.7 に対応します。

保証

このマニュアルの内容は「現状有姿」提供されるものであり、将来の改訂版で予告なく変更されることがあります。Agilent は、法律上許容される最大限の範囲で、このマニュアルおよびこのマニュアルに含まれるいかなる情報に関しても、明示黙示を問わず、商品性の保証や特定目的適合性の保証を含むいかなる保証も行いません。Agilent は、このマニュアルまたはこのマニュアルに記載されている情報の提供、使用または実行に関連して生じた過誤、付随的損害あるいは間接的損害に対する責任を一切負いません。Agilent とお客様の間に書面による別の契約があり、このマニュアルの内容に対する保証条項がここに記載されている条件と矛盾する場合は、別に合意された契約の保証条項が適用されます。

技術ライセンス

本書で扱っているハードウェアおよびソフトウェアは、ライセンスに基づき提供されており、それらのライセンス条項に従う場合のみ使用または複製することができます。

権利の制限

米国政府の制限付き権利について：連邦政府に付与されるソフトウェアおよび技術データに係る権利は、エンドユーザーのお客様に通例提供されている権利に限定されています。Agilent は、ソフトウェアおよび技術データに係る通例の本商用ライセンスを、FAR 12.211（Technical Data）および FAR 12.212（Computer Software）、並びに、国防総省に対しては、DFARS 252.227-7015（Technical Data -Commercial Items）および DFARS 227.7202-3（Rights in Commercial Computer Software or Computer Software Documentation）の規定に従い提供します。

安全にご使用いただくために

注意

注意は、取り扱い上、危険があることを示します。正しく実行しなかったり、指示を遵守しないと、製品の破損や重要なデータの損失に至るおそれのある操作手順や行為に対する注意を促すマークです。指示された条件を十分に理解し、条件が満たされるまで、**注意**を無視して先に進んではなりません。

警告

警告は、取り扱い上、危険があることを示します。正しく実行しなかったり、指示を遵守しないと、人身への傷害または死亡に至るおそれのある操作手順や行為に対する注意を促すマークです。指示された条件を十分に理解し、条件が満たされるまで、**警告**を無視して先に進んではなりません。

目次

1	概要	8
	OpenLab Server/ECM XT Server	
	システムアーキテクチャ	9
	21 CFR Part 11 サポート	10
2	コントロールパネルとセキュリティ	11
	ライセンス管理	12
	FlexNet Publisher Suite	12
	診断	14
	管理レポート	15
	セキュリティ	16
	システムアクティビティログ	16
	認証プロバイダー	16
	ユーザー、グループ、ロール	17
	セキュリティポリシー	21
	ホストサーバーの変更後に	
	Content Management の再認証	22
3	システムの保護	23
	概要	24
	OpenLab Server/ECM XT サーバーの保護手順	26
	証明書の作成	26
	キーストアの作成	27
	証明書署名要求 (CSR) の作成	27
	証明書の要求	28
	キーストアへ証明書のインストール	28
	OpenLab Server/ECM XT リバースプロキシの設定	29
	民間の証明書を使用するポート 52088 の設定	31
	AlfrescoTomcat Shared Services 接続の再設定	32
	オプション：Content Management または DNS エイリアスへのアクセス再設定	32
	OpenLab Server/ECM XT の HTTPS への	

目次

強制トラフィック 34

CSRF (Cross-Site Request Forgery) フィルターの
設定 35

OpenLab Control Panel から再起動して
ライセンス認証 36

**インデックスサーバーコンフィグレーション - 4 サーバースステムの
み 37**

TLS/SSL の無効化 38

4 メンテナンス 39

定期的なサーバーメンテナンス 40

データベース統計の更新 40

PostgreSQL データベースのメンテナンス手順 40

SQL Server のメンテナンス手順 42

OpenLab Server/ECM XT Server でのリソース使用量のモニタ 44

その他の最適な方法 45

Windows ドメイン 46

サーバー用のドメイン、ユーザー名、
またはパスワードの更新 46

ユーザーの読み取り権限の有効化 46

サーバー設定 47

FTP サーバースプロトコル 48

OpenLab Server/ECM XT Server を FTP サーバーとして使用 48

FTP プロトコルから OpenLab Server/ECM XT Server に接続 48

OpenLab Server/ECM XT Server を FTP サーバーとして使用しない 49

アーカイブ 50

自動アーカイブ実行スケジュールの変更 50

検疫 52

5 バックアップとリストアの手順 54

バックアップとリストアに関する重要な情報 55

Amazon Web Services S3 をバックアップロケーションとして使用 56

障害復旧プランの作成 57

バックアップおよびリストアユーティリティの使用 59

バックアップユーティリティを使用する OpenLab Server/ECM XT のバックアップ 62

バックアップユーティリティの使用手順 65

バックアップバリデーション 69

PostgreSQL データベースの差分バックアップ 71

差分コンフィグレーションツールを使用する差分バックアップの設定 71

PostgreSQL データベースのカスタムデータディレクトリを設定 73

PostgreSQL データベースのデータリポジトリのカスタムデータディレクトリを設定 74

リストアユーティリティを使用する OpenLab Server/ECM XT のリストア 75

PostgreSQL または Microsoft SQL データベース搭載のシステムのリストア 76

リストア中の再設定 81

バックアップおよびリストアスクリプトの使用 84

システム準備 86

バックアップスクリプトを使用する

OpenLab Server/ECM XT のバックアップ 87

リストアスクリプトを使用する OpenLab Server/ECM XT のリストア 90

バックアップとリストア手順の一時的なデータベースロケーションの変更 94

6 手動バックアップとリストアの手順 95

OpenLab Server/ECM XT Server の手動バックアップ手順 96

手動システムバックアップの実行 97

データリポジトリデータベースの手動バックアップ 103

OpenLab Server/ECM XT Server の手動リストア手順	105
異なるサーバー間の手動バックアップの データ移行	115
7 手動ホットバックアップ手順	118
バックアップのガイドライン	119
概要	120
Solr インデックスのバックアップ	121
定期的なバックアップ	121
データベースの手動バックアップ	125
SQL サーバーデータベースのバックアップ	127
PostgreSQL データベースのバックアップ	129
Oracle データベースのバックアップ	133
データリポジトリのバックアップ	137
コンテンツストアの手動バックアップ	138
OpenLab Server/ECM XT Server および インデックスサーバーコンフィギュレーション 情報の手動バックアップ	139
カスタム証明書のバックアップ	139
バックアップファイルの保存	140
システムの手動リストア	141
Solr インデックスのリストア	142
SQL サーバーデータベースをバックアップからリストア	142
PostgreSQL データベースをバックアップからリストア	146
Oracle データベースをバックアップからリストア	147
データリポジトリのリストア	148
アクティビティログインデックスの再構築	148

8 アップグレードと再設定 150

**オペレーティングシステムを変更した場合の OpenLab Server/ECM XT
Server の
アップグレード 151**

OpenLab Server/ECM XT Server の再設定 151

OpenLab Server/ECM XT の停止 152

インフラストラクチャへの変更 152

OpenLab Server のコンフィグレーションユーティリティの実行 **159**

OpenLab Server/ECM XT の起動 163

追加のコンテンツまたはアーカイブストア設定 164

9 付録 165

営業およびサポートのお問い合わせ先 166

アジレントコミュニティ（英語サイト） 166

OpenLab Server/ECM XT システムアーキテクチャ 9

21 CFR Part 11 サポート 10

本書は、OpenLab Server/ECM XT のシステム管理者を対象としています。使用するデータベース管理システムに関する管理者としての基本的な知識が必要です。また、Windows のバックアップとリストアに関する知識も必要です。

本書では、長期的に安定して高いパフォーマンスを確保するための、OpenLab Server/ECM XT の管理およびメンテナンス手順について説明します。

また、21 CFR Part 11 のサポートや、コントロールパネルを使用した Shared Services コントロール機能へのアクセス、サーバーの定期的なバックアップ、サーバーのハードウェアの不具合など障害が発生したときのサーバーのリストアのガイドラインも提供しています。

ドキュメントには、概念をわかりやすく説明するために特定のツール名が示されています。同一のタスクを実行できるツールであれば、お好みのツールを使用することもできます。

OpenLab Server/ECM XT Server システムアーキテクチャ

OpenLab Server/ECM XT Server を、Microsoft Windows Server オペレーティングシステムにインストールします。サポートするオペレーティングシステムのリストについては、『*Agilent OpenLab Server および ECM XT のハードウェアおよびソフトウェア要件ガイド*』を参照してください。OpenLab Server/ECM XT Server には、Shared Services (OLSS) および Content Management データベースが含まれており、同じマシンに自動的にインストールされます。

インストール後にサーバーのドメインを変更する場合は、Agilent サポートに直接お問い合わせください。

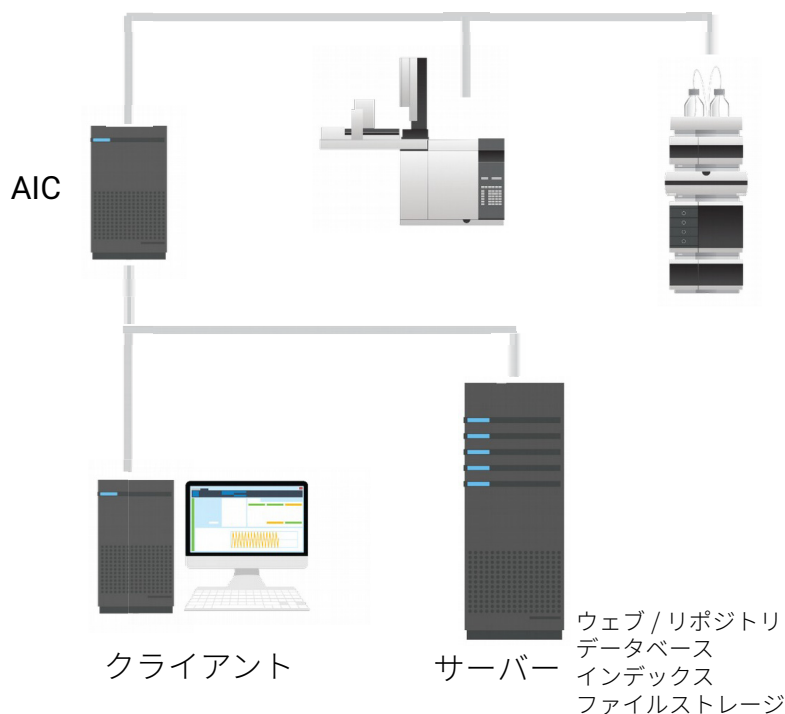


図 1 OpenLab Server/ECM XT Server のオールインワンシステムアーキテクチャ

OpenLab Server/ECM XT Server にアクセスするクライアントマシンは、次のコンポーネントを使用します。

- **Content Management ウェブクライアント** - OpenLab Server/ECM XT は、Web ブラウザを使用してアクセスできるシンクライアント型の Web ベースのユーザーインターフェイスを提供しています。Web インターフェイスからは、Content Management のフォルダーとファイルにアクセスできます。
- **コントロールパネル** - コントロールパネルは、OpenLab Server/ECM XT Server と Shared Services の管理に使用される管理機能へのアクセスを提供するユーザーインターフェイスです。

21 CFR Part 11 サポート

OpenLab Server/ECM XT は、21 CFR Part 11 への準拠をサポートする方法でデータを保存します。アクセスコントロールおよび監査証跡機能のある安全なデータ保存を提供します。データファイルは、データの完全性とトレーサビリティを確保するためにバージョン化されています。また、OpenLab Server/ECM XT では電子署名を利用してデータをサインオフすることが可能です。

2

コントロールパネルとセキュリティ

ライセンス管理 12

診断 14

管理レポート 15

セキュリティ 16

ホストサーバーの変更後に Content Management の再認証 22

コントロールパネルを使用して、セキュリティポリシー、セントラルコンフィグレーションなどの Shared Services コントロール機能にアクセスします。これらの機能を、本章で詳細に説明します。

ライセンス管理

このサービスは、システムに必要なすべてのライセンスの管理を行います。

FlexNet Publisher Suite

OpenLab Server/ECM XT では、Flexera 製の *FlexNet Publisher Suite* と呼ばれるサードパーティツールを使用してライセンスを管理しています。必要なライセンスサーバーコンポーネントは、OpenLab Server/ECM XT Server にデフォルトでインストールされています。

Shared Services のライセンスを管理するには、ライセンスを管理するサーバー上で追加の Windows サービスが必要です。この Windows サービスは、*Agilent OpenLab License Server* です。

ライセンスファイルを追加する前にまずライセンスを購入し、SubscribeNet を利用してライセンスファイルを作成する必要があります。新規ライセンスファイルの作成についての詳細は、『*Agilent OpenLab Server* および *OpenLab ECM XT* インストールガイド』を参照してください。

コントロールパネル内のライセンス管理で以下の機能を利用できます。

- ライセンスファイルをライセンスサーバーに追加できます。
- ライセンスモニタへ移動し、ライセンスサーバーにインストール済みのすべてのライセンスのプロパティを表示することが可能です。
- ライセンスファイルをライセンスサーバーから削除できます。これは、無効なライセンスファイルが追加された場合に便利です。
- ライセンスサーバーを表示または変更することが可能です。
- ライセンスサーバーの MAC アドレスを表示、コピー、または保存することが可能です。
- Agilent Electronic Software and License Delivery の Web ページからライセンスを入手できます。

ライセンスファイルの追加およびライセンスプロパティの表示についての詳細は、コントロールパネルのオンラインヘルプを参照してください。

インストール済みライセンスについては以下のプロパティが表示されます。

- **Feature:** 使用しているライセンスタイプを表示します。
- **Version :** ライセンスにバージョン番号がある場合、バージョン番号を見ることができます。バージョン番号が付いていないライセンスの場合には、バージョンは常に 2.0 として表示されます。
- **In Use (Available):** 現在使用中のライセンスの数（括弧内はライセンスの総数）を示します。OpenLab Server/ECM XT のライセンス手法は、ソフトウェアのインスタンスが実行されているときのみ、ライセンスが使用中になります（12 ページの「[ライセンス管理](#)」を参照）。
- **Expiration:** ライセンスに期間が設定されている場合、有効期限が表示されます。
- **[Alerts]** ペインでは、特定の機能を使用できるライセンス数がゼロになった場合、または使用できないライセンスでソフトウェアインスタンスを起動した場合に、通知が表示されます。

診断

〔診断〕ビューでは、診断の目的でいくつかのレポートおよびツールにアクセスできます。

- Shared Services サーバーへの ping を行います。
- Shared Services サーバーに関する、Operating System（オペレーティングシステム）、Processors（プロセッサ）、Disk Drives（ディスクドライブ）、processes（プロセス）、Network（ネットワーク）、および Connection（接続）についての情報が含まれるレポートを作成します。
- 登録モジュールが作成するログファイル、トレースファイルなどに一元的にアクセスすることができます。

Content Management は、アップロードの失敗をサーバーログに登録します。アップロードの失敗に応じて、デバッグ情報が以下のいずれかに書き込まれます。

- C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\logs\alfresco.log

または

- C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\logs\datastore.log

管理レポート

「管理レポート」ビューでは、システムのコンフィグレーションに関連した種々なレポートを作成し、XML または PDF ファイルにエクスポートすることができます。

- **ロールと権限レポート**

システム上で定義されたすべてのロールについて、各ロールに含まれるすべての権限についての詳細を含めた情報を提供します。

- **ロール割り当てのレポート（ユーザー / グループ）**

このレポートは、システム上の機器およびプロジェクトに対するすべてのユーザーおよびグループアクセス権限についての概要です。機器またはプロジェクトへのアクセスを付与されていないユーザーおよびグループは、このレポートに含まれません。

セキュリティ

システムアクティビティログ

システムアクティビティログでは、すべてのシステムアクティビティに一元的にアクセスできます。ここには、Shared Services に関連するさまざまなイベントの情報が含まれます。特定のタイプ、期間、ユーザー、または特定の説明を含むイベントだけをフィルタリングして表示できます。

以下のイベントタイプが記録されます。

- システム
- ユーザー
- グループ
- セキュリティ
- プリンタ
- ライセンス

イベントに関する詳細情報を見るには、作業ログブックビューア内で対象行を拡大します。

注記

デフォルトでは、アクティビティログが無効になっています。コントロールパネルで有効にするには、**[アクティビティログのプロパティの編集]** 権限が必要です。アクティビティログは一度有効にすると、再度無効にすることができません。

認証プロバイダー

認証プロバイダーは、システムにログインするユーザーを識別証明するために使用されます。

OpenLab Server/ECM XT はインストール中に内部認証の設定が自動的に有効になります。デフォルトのユーザーは **admin**、パスワードは **openlab** です。初めてログインする場合、最初にシステムがユーザーにパスワードの変更を求めます。必要に応じて認証モードを変更することができます。

OpenLab Server/ECM XT は以下の認証プロバイダーをサポートしています。

- **内部**

内部モードでは、ユーザーの資格情報が Shared Services データベースに保存されます。その他のユーザーを設定する前に、Shared Services のための管理者アカウントを作成するよう促されます。システムにユーザーを作成できるのは内部モードのみで、その他のモードでは別のシステムに存在するユーザーへのマッピングのみ行えます。

- **Windows ドメイン**

既存の Windows ユーザーを Shared Services にインポートします。認証はエンタープライズ内の Windows ドメインによって行われます。Shared Services は、マッピングされたユーザーの ID およびパスワードのみを使用します。OpenLab Server/ECM XT のロールおよび権限は、Shared Services で設定します。

ユーザー、グループ、ロール

Shared Services では、特定のロールをユーザーまたはユーザーグループに割り当てることができます。Windows ドメイン内でユーザーを管理する場合、これらの既存のユーザーを Shared Services にマッピングできます。

1 人のユーザーが複数グループのメンバーである場合もあります。各グループに対して特定のロールを割り当てる必要があります。1 人のユーザーにロールを割り当てることもできますが、簡素化のためロールの割り当てはグループレベルでのみ行うことを強く推奨します。

ロールには多くの固有権限が付随しており、それら権限によりユーザーはコントロールパネルおよび Content Management での表示や実行が許可されます。
表 1 にユーザー資格情報を示します。

表 1 ユーザー資格情報

値	説明	必須
名前	システムにログインするユーザー名	はい
説明	ユーザーについての追加情報（部署、機能など）	いいえ
パスワード	ユーザーのパスワード。セキュリティポリシーで定義されている長さ以上のもの。	はい
電子メール	ユーザーの電子メールアドレス	いいえ
フルネーム	ユーザーのフルネーム	いいえ
連絡先情報	一般的な問い合わせ先（電話番号、ポケットベルなど）	いいえ
アカウントを無効にする	チェックボックスを選択するとユーザーを無効にします。無効にされたユーザーはログインできません。ログインを何度も失敗すると、そのユーザーは自動的に無効にされます。ユーザーが無効にされると、チェックボックスの代わりに対応するメッセージが表示されます。一定時間が経過すると（ 【セキュリティポリシー】 設定内の 【アカウントロック時間】 を参照）、再び有効となります。	いいえ
ユーザーはパスワードを変更できない	ユーザーが自分自身のパスワードを変更可能かどうかを示すフラグです。デフォルトではフラグがオフになっています（つまり、ユーザーは自身のパスワードを変更できます）。	いいえ
ユーザーは次回ログイン時にパスワードの変更が必要	有効になっている場合、ユーザーは次のログインの際に自身のパスワードを変更しなければなりません。ユーザーがパスワードを変更すると、このフラグは自動的にオフになります。このフラグは、新規ユーザーの場合はデフォルトでオンになっています。	いいえ
パスワードを無期限にする	設定をオンにすると、ユーザーはパスワードを変更する必要がなくなります。	いいえ
グループメンバーシップ	ユーザーに関連するグループに割り当てます。	いいえ
ロールメンバーシップ	ロールを直接ユーザーに割り当てます。	いいえ

ユーザー

外部認証プロバイダーとして Windows ドメインを利用する場合、ユーザーを作成することはできません。代わりに認証システム内の既存ユーザーをインポートする必要があります。検索機能を利用して、認証システム内の特定ユーザーを見つけることができます。コントロールパネルでこれらの外部ユーザー用のロールを管理できますが、ユーザー名やパスワードといった実際のユーザー資格情報を管理することはできません。外部ユーザーを削除するには、コントロールパネル内でユーザーのマッピングを解除します。当該ユーザーは外部認証システムにそのまま残ります。

グループ

外部認証プロバイダーを利用する場合、外部システムの既存のグループ名をインポートするか、新規内部グループを作成するかのいずれかが可能です。マッピングおよび作成できるグループの数に制限はありません。

外部システムまたはコントロールパネルのグループにユーザーを割り当てることができます。さらに OpenLab CDS にだけ関連するユーザー割り当てが必要な場合は、コントロールパネルでそのグループを作成します。特に必要がない場合は、グループをインポートして必要なロールを割り当てただけで十分です。

グループを削除またはマッピング解除する場合、そのグループのメンバーであるユーザーに対する変更は行われません。

ロールと権限

ロールは、ユーザーまたはユーザーグループにグローバルに権限を割り当てるために使用されます。システムにはインストール時に作成される定義済みのロールがあります（表 2 を参照）。各ロールには、固有の権限が割り当てられています。

権限をロールに割り当てる場合、まず必要なロールタイプを選択してからそのロールタイプに関連する権限を選択します。各ロールは、特定のロールタイプ 1 つに対応する権限のみを有します。例外として、定義済みロールの **[すべて]** だけは、すべてのロールタイプのすべての権限を有します。ユーザーまたはグループがシステム機能を実行するためには、複数のロールが必要な場合があります。

注記

V2.7 以降、Content Management ユーザーは、アクティビティログとそのすべてのエントリを表示するための「アクティビティログの表示」権限が必要になります。前のバージョンからのアップグレードの場合、すべてのユーザーに「アクティビティログのアクセス」ロールが割り当てられるため、ユーザーは機能を失いません。アップグレード後に、ユーザーがアクティビティログにアクセスできないように変更するには、ユーザーからそのロールを削除する必要があります。

表 2 Content Management の定義済みロール

権限	Content Management のロール
プロジェクト：プロジェクトまたはプロジェクトグループの表示 コントロールパネルでプロジェクトを表示。 Content Management コンテンツを表示、レビュー、ダウンロード	- Content Management 閲覧者 - Content Management 投稿者 - Content Management 管理者 - Content Management 承認者 - アーキビスト - システム管理者 - すべて
プロジェクト：プロジェクトコンテンツの編集 ファイルとフォルダーの作成、更新、およびコピー	- Content Management 投稿者 - Content Management 管理者 - Content Management 承認者 - システム管理者 - すべて
プロジェクト：データファイルの電子署名 ファイルに電子署名を適用	- Content Management 承認者 - システム管理者 - すべて
プロジェクト：プロジェクトコンテンツの削除 プロジェクトに関連するコンテンツの削除または移動	- Content Management 管理者 - すべて
プロジェクト：ウェブクライアントからコンテンツにアクセス ウェブクライアントからプロジェクトコンテンツにアクセス	- Content Management 閲覧者 - Content Management 投稿者 - Content Management 管理者 - Content Management 承認者 - すべて
管理：テンプレート管理 フォルダーへの PDF テンプレートの適用	- Content Management PDF テンプレートの管理 - すべて
管理：コンテンツのアーカイブ ファイルとフォルダーのオンラインアーカイブ、デアーカイブ、および自動アーカイブタスクの設定	- アーキビスト - すべて
管理：セキュリティの管理 ユーザー、グループ、ロールの作成。セキュリティロールの割り当て。Content Management 内のファイルおよびフォルダーの移動、プロジェクトに含まれない Content Management 内のファイルおよびフォルダーの削除	- システム管理者 - すべて
管理：アクティビティログの表示 アクティビティログへのアクセス	- アクティビティログのアクセス - システム管理者 - すべて

セキュリティポリシー

認証プロバイダーが **【内部】** の場合、**表 1** で説明するパラメータをコントロールパネルで設定できます。**【Windows ドメイン】** 認証の場合、コントロールパネルでは非アクティブの時間のみを設定でき、その他のパラメータはすべて外部システムによって定義されます。**表 3** にセキュリティポリシーの設定を示します。

表 3 セキュリティポリシーの設定

設定	説明
パスワードの長さ	ユーザーがパスワードを変更する場合、指定された文字数以上の長さのパスワードを入力しなければなりません。デフォルト設定は 5 です。 【内部】 認証プロバイダーのみで利用可能です。
パスワードの有効期間 (日)	デフォルト値は 0 日です。この期間は OpenLab システムの管理者がリセットできます。この期間後にユーザーがログインしようすると、パスワードの変更を促すシステムメッセージが表示されます。有効期間は、最後のパスワード変更時または新規デフォルトパスワードを持つユーザーの作成時から開始します。 【内部】 認証プロバイダーのみで利用可能です。
アカウントロックまでの ログイン試行回数	無効なユーザー情報で所定の回数ログインを試行した場合、そのユーザーを一定期間システムからロックアウトします（以下の 【アカウントロック時間】 を参照してください）。有効なユーザー資格情報を用いてもログインができなくなります。許容するログイン試行回数を定義できます。デフォルト設定は 3 です。 【内部】 認証プロバイダーのみで利用可能です。
アカウントロック時間 (分)	ユーザーがアカウントロックまでのログイン試行回数を超過したときに、再試行可能になるまでに経過しなければならない時間です。デフォルト設定は 5 分です。 【内部】 認証プロバイダーのみで利用可能です。
アプリケーションをロック するまでの時間	コントロールパネルを使用しない状態がこの時間続くと、ユーザーインターフェイスがロックされます。この設定は、ChemStation におけるタイムベースセッションロックの設定にも利用されます。 デフォルト設定は 10 分です。ロックさせない場合は、値を 0 に設定してください。
シングルサインオン	シングルサインオンを有効にすると、コントロールパネルのログイン画面は表示されなくなります。 【Windows ドメイン】 認証プロバイダーのみで利用可能です。OpenLab ECM XT バックエンドではシングルサインオンはサポートされていません。

ホストサーバーの変更後に Content Management の再認証

新しいホストサーバーを指定した後に Content Management を再度認証するには、以下の手順を使います。

- 1 コントロールパネルにログインします。アップグレードの場合、アップグレード前に存在していたユーザーとしてログインしてください。
- 2 **【管理】 > 【システムコンフィグレーション】 > 【システム設定の編集】** をクリックします。
- 3 **【他のストレージタイプを選択する場合は、リストから別のオプションを選択してください】** ドロップダウンリストで、**【Content Management】** を選択し、**【次へ】** をクリックします。
- 4 **【サーバーの変更】** を選択し、使用する Content Management サーバーの URL を入力します。
- 5 **【ライセンス認証】** をクリックします。
- 6 **【資格情報の入力】** ダイアログボックスに、ユーザー名とパスワードを入力し、（必要に応じて）ドメインを選択します。
- 7 **【OK】** をクリックします。
- 8 Content Management が正常に認証されたメッセージが表示されます。**【OK】** をクリックします。

3

システムの保護

概要 24

OpenLab Server/ECM XT サーバーの保護手順 26

インデックスサーバーコンフィグレーション - 4 サーバーシステムのみ 37

TLS/SSL の無効化 38

次の手順を使用して Content Management 用の証明書を作成およびインストールし、OpenLab Server/ECM XT Server をコンフィグレーションします。

概要

このセクションの手順は、オールインワンサーバー、2サーバー、および4サーバーのトポロジーに適用されます。

サーバー、AIC、クライアントといった OpenLab コンポーネント間で、信頼のある安全なネットワーク通信を可能にするには、証明書が必要です。サーバーが有効な証明書を使用して識別証明できる場合、クライアントはサーバーを信頼することができます。OpenLab CDS は、HTTPS 経由のセキュリティで保護されたネットワーク通信に依存しています。インストール時に、OpenLab Server の OpenLab Certificate Service により Agilent OpenLab ルート証明機関が作成され、これにより OpenLab Server/ECM XT、OpenLab CDS AIC、および OpenLab CDS クライアント用の自己署名証明書が発行されます。サーバーに接続されているすべての OpenLab マシンの「ローカルコンピューター」の Windows 証明書ストアに OpenLab Root CA 証明書が自動的にインストールされると、これらの証明書によって、AIC、クライアントとサーバーで信頼された安全な通信が可能になります。OpenLab 内部証明書によって OpenLab エコシステム内の信頼された安全な通信が技術的に可能な場合でも、民間の証明書を使用することにより、セキュリティで保護された通信の信頼レベルをさらに高めることができます。

民間の証明書を使用し OpenLab Server を保護することで、以下の利点があります。

- IT セキュリティポリシーへの準拠。
- OpenLab CDS がインストールされていない PC や、IT 担当者によって設定されたウェブ閲覧機能を持つその他のデバイスのウェブインターフェイス経由で Content Management にアクセスする場合や、Sample Scheduler ウェブインターフェイスを使用する場合に、OpenLab Server/ECM XT サーバーを信頼します。
- クライアントを2台の OpenLab Server 間で切り替える場合に、2台目の OpenLab Server/ECM XT ルート証明書を各クライアントの証明書ストアに手動でインストールする必要がありません。
- VPN のみのネットワークに依存しない OpenLab CDS クラウドインストールの場合に必要です。

注記

民間の証明書を使用しているセキュリティで保護された OpenLab Server/ECM XT システムをアップグレードする場合、Agilent では、アップグレード時に新しい民間のサーバー証明書にすべてのサブジェクト別名（SAN）エントリを維持することをお勧めしています。サーバーへの接続に指定されたサーバーアドレスがインストールされた民間証明書のサブジェクトの別名の一部である場合のみ、既存の AIC またはクライアントからのセキュリティで保護された接続が、確立できることに注意してください。AIC またはクライアントのインプレースアップグレードする前に、OpenLab Server/ECM XT システムへの AIC およびクライアントの接続を調整してください。

注記

民間の証明書を用いた OpenLab Server/ECM XT のインプレースアップグレード後のシステムは、内部証明書を使用している状態になります。アップグレード後に、民間の証明書を再設定してください。

OpenLab Server/ECM XT サーバーの保護手順

このセクションに示される手順に従って、証明書を使用してシステムを保護します。

証明書の作成

証明書を保存する Java キーストアを作成します。

前提条件：Java Development Kit (JDK) 11

Oracle または他のプロバイダーから JDK をダウンロードするか、OpenLab Server/ECM XT に付属（C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\java\bin）の JDK を使用します。

Microsoft 管理コンソール（MMC）に含まれる Windows Server の証明書ストアを keytool の代替として使用できます。これについてはここでは説明しません。

注記

証明書プロバイダーまたは社内のプライベートキーのインフラストラクチャによって発行された証明書は Base64 でエンコードされている必要があります。一般的にこれらの証明書は、ルート証明機関までのすべての中間証明機関の証明書を含めて PKCS #7 バイナリ証明書パッケージ（.p7b）で提供されます。この手順では、.p7b パッケージを使用した必要な証明書の作成について説明していますが、.crt または .cer ファイルタイプの Base64 エンコード証明書を使用しても同じ結果が得られます。後者では、中間ルート証明機関による証明書を手動でインストールすることが必要な場合があります。

証明書の形式の詳細については、次を参照してください。 **証明書の形式**

キーストアは、PKCS #12 バイナリ証明書パッケージとして作成され、証明書署名要求の作成や、証明機関から発行された証明書のインポート、OpenLab CDS のと互換性がある情報のエクスポートを行うために必要となります。

キーストアの作成

- 1 コマンドプロンプトを管理者として実行します。
- 2 トレーサビリティを高めるため、サーバー上に作業ディレクトリを作成します。例では、ディレクトリを c:\https としています。

例：

```
mkdir c:\https
```

- 3 keytool ディレクトリ C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\java\bin へ移動します。

```
cd "C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\java\bin"
```

- 4 以下のパラメータを使用して、PKCS #12 バイナリ証明書パッケージ形式でキーストアを作成します。

```
keytool -genkey -alias <choose an alias> -keysize 2048 -keyalg RSA -keystore <choose a keystore file name> -storetype pkcs12
```

ホスト名 ecmxtserver がドメインの agilent.com に結合された OpenLab Server/ECM XT の例、

```
keytool -genkey -alias ecmxtserver.agilent.com -keysize 2048 -keyalg RSA -keystore c:\https\ssl.keystore -storetype pkcs12
```

このプロセス中にパスワードを求められます。適切なパスワードを入力し、メモに残します。Keytool に名および姓を求められます。これは OpenLab Server/ECM XT サーバーの共通名（CN = Common Name）を指します。ecmxtserver.agilent.com のように、サーバーの完全修飾ドメイン名を入力することをお勧めします。

証明書署名要求（CSR）の作成

HTTPS を有効にするサーバー用の CSR ファイルを作成するには、以下の keytool パラメータを使用します。前に入力したパスワードが求められます。

```
keytool -certreq -alias <Alias chosen in step Create the Keystore> -keysize 2048 -keyalg RSA -keystore <your keystore filename including path> -storetype pkcs12 -ext "san=dns:<Server-Fully-Qualified-Domain-Name>,dns:<Optional DNS Alias FQDN>" -file <Certificate Signing request including path>
```

例：

```
keytool -certreq -alias ecmxtserver.agilent.com -keysize 2048
-keyalg RSA -keystore c:\¥https¥ssl.keystore -storetype pkcs12
-ext "san=dns:ecmxtserver.agilent.com" -file
c:\¥https¥ecmxtserver.agilent.com.csr
```

証明書の要求

.csr ファイルが作成された信頼済み証明書プロバイダーにアクセスし、証明書を要求します。プロバイダーは、組織内の PKI（プライベートキーインフラストラクチャ）や、VeriSign/DigiCert などの民間のベンダーにすることもできます。

信頼のあるプロバイダーにより、ルート CA 証明書（.crt）と併せて PKCS #7 バイナリ証明書パッケージ（.p7b）が提供されます。どちらの証明書も個別のファイルに保存します。

サーバー証明書：

```
c:\¥https¥ecmxtserver.p7b
```

ルート証明機関の証明書：

```
c:\¥https¥RootCA.crt
```

キーストアへ証明書のインストール

- 1 以下の keytool パラメータを使用して、ルート CA 証明書をキーストアへインポートします。

```
keytool -importcert -alias <choose a new alias for the Root CA>
-keystore <your keystore file name> -storetype pkcs12 -file
<root certificate file>
```

例：

```
keytool -importcert -alias agilent.com -keystore
C:\¥https¥ssl.keystore -storetype pkcs12 -file
c:\¥https¥RootCA.crt
```

キーストアのパスワードを入力するよう要求されます。「はい」と入力して、この証明書を信頼することを確認します。

- 2 以下の keytool パラメータを使用して、サーバーの証明書をキーストアへインポートします。

```
keytool -importcert -alias <Alias chosen in step Create the Keystore> -keystore <your keystore file name> -storetype pkcs12 -file <your provided server certificate package>
```

例：

```
keytool -importcert -alias ecmxtserver.agilent.com -keystore C:\¥https¥ssl.keystore -storetype pkcs12 -file c:\¥https¥ecmxtserver.p7b
```

キーストアのパスワードを入力するよう要求されます。「Certificate reply was installed in keystore」というメッセージが表示されます。プライベートキーを含めた PKCS #12 バイナリ証明書パッケージとしての ssl.keystore の作成は完了です。

OpenLab Server/ECM XT リバースプロキシの設定

注記

このステップには OpenSSL v.1.1.1 が必要です、これは以下の手順で説明するインストールフォルダーに提供されています。

前のステップで作成した、PKCS #12 バイナリ証明書パッケージ、ssl.keystore が必要です。

プライベートキーの ssl.keystore のパスワードを準備しておきます。

以下の手順で、インストール済みの OpenSSL を使用して PEM 証明書およびキーファイルをキーストアから抽出します。OpenSSL は OpenLab Server の以下のフォルダーにインストールされています。C:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin\libressl

- 1 openssl ディレクトリへ移動します。

```
cd "c:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin\libressl"
```

- 2 OpenSSL の現在のコマンドセッションを設定します。

```
set OPENSSL_CONF=C:\Program Files (x86)\Agilent Technologies\Certificate Service\Bin\libressl\openssl.cnf
```

- 3 サーバー証明書と、キーストアの各プライベートキーをエクスポートします。要求されたら、ssl.keystore のパスワードを入力します。

以下のコマンドを実行して、プライベートキーをエクスポートします。

```
openssl pkcs12 -in <your keystore filename> -nocerts -out <your privatekey file> -nodes
```

例：

```
openssl pkcs12 -in c:\https\ssl.keystore -nocerts -out c:\https\ecmxtserver.key -nodes
```

「MAC verified OK」という確認メッセージが表示されます。

以下のコマンドを実行して、サーバー証明書をエクスポートします。

```
openssl pkcs12 -in <your keystore file name> -nokeys -out <your server certificate file>
```

例：

```
openssl pkcs12 -in c:\https\ssl.keystore -nokeys -out c:\https\ecmxtserver.crt
```

「MAC verified OK」という確認メッセージが表示されます。

- 4 サーバーコンフィグレーションユーティリティを使用してリバースプロキシサーバーをコンフィグレーションします。

注記

サーバーコンフィグレーションユーティリティを実行する前に、インストール後のコントロールパネルで初期デフォルト OLSS パスワードが変更されていることを確認します。

- a OpenLab Server/ECM XT Server をインストールすると Windows の [スタート] メニューにサーバーコンフィグレーションユーティリティが追加されます。サーバーコンフィグレーションユーティリティで、[証明書のセットアップ] ページへ移動します。
- b **[既存のカスタム証明書を使用]** を選択します。
- c エクスポートしたサーバー証明書ファイルを入力します (ecmxtserver.crt など)。
- d エクスポートしたプライベートキーを入力します (ecmxtserver.key など)。
- e ルート CA 証明書を入力します (RootCa.crt など)。
- f 証明書に記載されたサーバー名 / エイリアスを入力します (ecmxtserver.agilent.com など)。

サーバーコンフィグレーションユーティリティのコンフィグレーションステップが完了すると、リバースプロキシサービスが、入力した値を使用して OpenLab Server/ECM XT の受信トラフィックを保護します。

設定を適用してコンフィグレーションを続行すると、OpenLab Shared Services (OLSS) 管理者の資格情報を入力するよう促されます。

サービスが停止され変更が適用されたら、民間の証明書のコンフィグレーションは完了です。

「証明書のセットアップ」ステップで「Agilent OpenLab の内部証明書を使用」を選択した場合、上記の手順を無効にすることができます。

注記

「Content Management 権限の導入」ステップで入力フィールドが表示されない場合、証明書のサブジェクトの別名セクションから <Server-FQDN> が抜けているか、スペルが間違っている可能性があります。

民間の証明書を使用するポート 52088 の設定

証明書サービスを使用して Windows の証明書ストアに証明書をインポートします。

- 1 コマンドプロンプトを管理者として実行します。
- 2 以下のコマンドを使用して ssl.keystore ファイルのコピーを作成し、ファイル名を ssl.pfx に変更します。
`copy c:\¥https¥ssl.keystore c:\¥https¥ssl.pfx`
- 3 証明書インポートウィザードを起動するには、c:\¥https にある **ssl.pfx** をダブルクリックします。
- 4 PKCS #12 証明書パッケージを証明書ストアの保存場所「ローカルマシン」にインストールし、**「証明書の種類に基づいて、自動的に証明書ストアを選択する」**を選択してインポートを完了します。

「The import was successful」というメッセージが表示されます。

- 5 管理者としてコマンドプロンプトを開き、C:\¥Program Files (x86)\¥Agilent Technologies¥Certificate Service¥bin フォルダへ移動します。以下のコマンドを実行して、証明書をインストールします。

```
cd "C:\¥Program Files (x86)\¥Agilent Technologies¥Certificate Service¥Bin"
```

```
Agilent.OpenLab.CertService.CertServiceCore.exe
useexternalcert -certfilename c:\¥https¥ssl.pfx -certpassword
<Password defined for ssl.keystore>
```

証明書のサービスが再起動され、使用された証明書のサムプリントが表示されます。

上記のステップを無効にして Agilent OpenLab 証明書に戻るには、以下のコマンドを使用します。

```
Agilent.OpenLab.CertService.CertServiceCore.exe useinternalcert
```

AlfrescoTomcat Shared Services 接続の再設定

この手順は、OpenLab Server/ECM XT サーバーで必須です。システムを再起動するまで変更は実装されません（36 ページの「[OpenLab Control Panel から再起動して ライセンス認証](#)」を参照）。

- 1 管理用のメモ帳を使用して、C:\¥Program Files (x86)\¥Agilent Technologies¥OpenLAB Data Store¥tomcat¥shared¥classes¥alfresco-global.properties にある AlfrescoTomcat コンフィグレーションファイルを開きます。

- 2 olss.host プロパティを localhost から以下に変更します。

```
olss.host=<Server-FQDN>
```

例：

```
olss.host=ecmxtserver.agilent.com
```

オプション：Content Management または DNS エイリアスへのアクセス再設定

この手順は、OpenLab Server/ECM XT サーバーでオプションの DNS エイリアスを経由して Content Management にアクセスするために必要です。前提条件：DNS エイリアスがサーバー証明書のサブジェクトの別名に含まれていること。

オプション：Content Management または DNS エイリアスへのアクセス再設定

システムを再起動するまで変更は反映されません（36 ページの「OpenLab Control Panel から再起動して ライセンス認証」を参照）。

- 1 管理用のメモ帳を使用して、C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco\Web-extension\share-config-custom.xml を開きます。
- 2 assertReferer および assertOrigin セクションへの最後のエントリとして、|https://<DNS Alias FQDN>.* を追加します。

```
<config evaluator="string-compare" condition="CSRFPolicy" replace="true">
  <filter>
    <rule>
      <action name="assertReferer">
        <param name="referer">https://localhost/. *|http://localhost/. *|http://<hostname>.*|https://<hostname>.*|https://<DNS Alias FQDN>.*</param>
      </action>
      <action name="assertOrigin">
        <param name="origin">https://localhost|http://localhost|http://<hostname>.*|https://<hostname>.*|https://<DNS Alias FQDN>.*</param>
      </action>
    </rule>
  </filter>
</config>
```

たとえば、サーバー ecmxtserver.agilent.com は DNS エイリアス openlab.agilent.com 経由でアクセスできなければなりません。

```
<config evaluator="string-compare" condition="CSRFPolicy" replace="true">
  <filter>
    <rule>
      <action name="assertReferer">
        <param name="referer">https://localhost/. *|http://localhost/. *|http://ecmxtserver.*|https://ecmxtserver.*|https://openlab.agilent.com.*</param>
      </action>
      <action name="assertOrigin">
        <param name="origin">https://localhost|http://localhost|http://ecmxtserver.*|https://ecmxtserver.*|https://openlab.agilent.com.*</param>
      </action>
    </rule>
  </filter>
</config>
```

OpenLab Server/ECM XT の HTTPS への 強制トラフィック

セキュリティ保護されない HTTP 通信を防ぐため、以下のように Proxy Configuration Service の CONFIG ファイルにエントリを手動で追加します。

- 1 管理用のメモ帳を使用して、以下にある Proxy Configuration Service の CONFIG ファイルを開きます。

```
c:\Program Files (x86)\Agilent Technologies\OpenLab Reverse Proxy
Configuration Service\ConfigurationService\Agilent.OpenLab.ReverseProxy.
ConfigurationService.dll.config
```

ポート 80 の VirtualHost コンフィグレーションに値が 3 つのみ含まれていることを確認します。

```
<VirtualHost>
<add name="ServerName" value="*" />
<add name="PortNumber" value="80" />
<add name="Redirect" value="permanent / https://<Server-FQDN>" />
</VirtualHost>
```

例：

```
<VirtualHost>
<add name="ServerName" value="*" />
<add name="PortNumber" value="80" />
<add name="Redirect" value="permanent /
https://ecmxtserver.agilent.com" />
</VirtualHost>
```

- 2 ファイルを保存します。
- 3 管理用のメモ帳を使用して、以下にある OpenLab Reverse Proxy の CONF ファイルを開きます。

```
C:\Program Files\OpenLab Reverse Proxy\Apache24\conf\httpd.conf
```

<VirtualHost *:80> ブロックで、ポート 80 コンフィグレーションに表示されたエントリのみが含まれていることを確認します。

```
<VirtualHost *:80>Redirect permanent / https://Server-FQDN/
#<partnerconf80>
IncludeOptional "c:\programdata\agilent\openlab reverse
proxy\customconf\http*.conf"
#</partnerconf80>
</VirtualHost>
```

例：

```
<VirtualHost *:80>
Redirect permanent / https://ecmxtserver.agilent.com/
#<partnerconf80>
IncludeOptional "C:¥ProgramData¥Agilent¥OpenLab Reverse
Proxy¥customconf¥http¥*.conf"
#</partnerconf80>
</VirtualHost>
```

4 httpd.conf ファイルを保存します。

この変更で、受信するすべての http トラフィックが強制的に https になります。たとえば、「システムの保護」のステップを完了した後で、リンクに <http://ecmxtserver.agilent.com> と入力すると、自動的に <https://ecmxtserver.agilent.com> へ転送されます。システムを再起動するまで反映されません（36 ページの「[OpenLab Control Panel から再起動して ライセンス認証](#)」を参照）。

CSRF (Cross-Site Request Forgery) フィルターの 設定

この手順は、OpenLab Server/ECM XT サーバーで実行します。これらの変更は、システムを再起動し再度アクティブ化するまで有効になりません（36 ページの「[OpenLab Control Panel から再起動して ライセンス認証](#)」を参照）。

- 1 管理用のメモ帳を使用して、C:¥Program Files (x86)¥Agilent Technologies¥OpenLAB Data Store¥tomcat¥shared¥classes¥alfresco-global.properties にある AlfrescoTomcat コンフィグレーションファイルを開き、以下のプロパティを変更します。

デフォルトでは、**csrf.filter.origin** および **csrf.filter.referer** プロパティには "*" ワイルドカード演算子の値が含まれ、この値はすべてのドメインがデフォルトで許可されることを示すために使用されます。

origin および referer ヘッダーを追加するには、*ワイルドカード演算子を **csrf.filter.referer** および **csrf.filter.origin** プロパティの有効な完全修飾ドメイン名に変更してください。

以下は、ECM XT が完全修飾ホストとポート 443 で動作するコンフィグレーションの例です。

```
csrf.filter.origin=https://<Server-FQDN>/.*  
csrf.filter.referer=https://<Server-FQDN>/.*
```

例：

```
csrf.filter.referer=https://ecmxtserver.agilent.com/.  
csrf.filter.origin=https://ecmxtserver.agilent.com/.*
```

OpenLab Control Panel から再起動して ライセンス認証

- 1 Windows の [スタート] メニューから、[Agilent Technologies] で **【メンテナンスユーティリティ】** を選択し、**【サーバー設定】** タブを選択します。
 - a サーバーを追加します。
 - b サーバーの名前を入力します。
 - c サーバー：<サーバーの完全修飾ドメイン名（FQDN）>
 - d オプションで、サーバーの説明を追加します。
 - e 追加したサーバーをデフォルトに設定します。
- 2 システムを再起動します。
- 3 OpenLab Control Panel を使用して HTTPS 経由で Content Management の通信をアクティブにします。
 - a OpenLab Control Panel を開き、[管理] > **【システムコンフィグレーション】** > **【システム設定の編集】** へ移動します。
 - b **【他のストレージタイプを選択する場合は、リストから別のオプションを選択してください】** ドロップダウンリストで、**【Content Management】** を選択し、**【次へ】** をクリックします。
 - c **【サーバーの変更】** を選択します。
 - d Content Management サーバーの 'https' 付き URL とホストの完全修飾ドメイン名を入力します。
例：https://ecmxtserver.agilent.com
 - e **【ライセンス認証】** をクリックします。

すべての AIC およびクライアントが <Server FQDN> に登録されている必要があります。ホスト名のみでは許可されず、作成した証明書に含まれません。

インデックスサーバーコンフィグレーション - 4 サーバースystemのみ

4 サーバースystemの場合、以下の手順に従ってインデックスサーバーのセキュリティを設定します。

- 1 OpenLab Server/ECM XT サーバーで使用したルート証明機関の証明書をインデックスサーバーにコピーします。
- 2 Agilent OpenLab Shared Services サービスのスタートアップの種類を無効から手動に変更します。
- 3 **Windows の [スタート] メニュー > [Agilent Technologies]** からサーバーコンフィグレーションユーティリティを起動します。（OpenLab インデックスサーバーのインストール後に利用できます。）
- 4 サーバーコンフィグレーションユーティリティで、[証明書のセットアップ] ページへ移動します。
- 5 **[サーバーコンフィグレーション]** 画面で、（プライマリ）Content Management 完全修飾ドメイン名（FQDN）を入力および確認します。
- 6 **[証明書のセットアップ]** 画面で、**[既存のカスタム証明書を使用]** を選択し、ルート証明機関の証明書を参照して RootCa.crt を選択します。
- 7 サーバーコンフィグレーションユーティリティを完了します。
- 8 Agilent OpenLab Shared Services サービスのスタートアップの種類を手動から無効に変更します。
- 9 インデックスサーバーを再起動します。

TLS/SSL の無効化

組織によっては、Windows の古いセキュリティプロトコルを無効にするよう要求されます。TLS 1.0、TLS 1.1、および SSL 3.0 は OpenLab Server/ECM XT では不要なため、無効にすることができます。

セキュリティプロトコルを無効にする場合、システム内のすべてのコンピューター（Content Management、インデックス、ファイルサーバー、DB サーバー、AIC および CDS クライアント）で無効にしてください。

4

メンテナンス

定期的なサーバーメンテナンス 40

Windows ドメイン 46

サーバー設定 47

FTP サーバープロトコル 48

アーカイブ 50

OpenLab Shared Services メンテナンスユーティリティプログラムは、OpenLab ソフトウェアと同時に自動的にインストールされ、管理者がシステムを管理するために使用します。

プログラムを開くには、Windows の **【スタート】 > 【Agilent Technologies】 > 【メンテナンスユーティリティ】** を選択します。

このプログラムにアクセスするには Windows 管理者権限が必要です。

定期的なサーバーメンテナンス

データベース統計の更新

データベースの最適なパフォーマンスを維持するには、OpenLab Server/ECM XT Server データベース統計を定期的に更新してください。データベースエンジンがクエリーを実施する最善の方法を決定する際に、この統計が使用されます。

OpenLab Server/ECM XT Server および OpenLab Shared Services データベースの統計を更新してください。インストール時にカスタムデータベース名を選択した場合、インストールメモから正しい名前を使用してください。

PostgreSQL データベースのメンテナンス手順

PostgreSQL データベースの場合、次の手順を定期的に行う必要があります。頻度は、システムの使用状況により異なります。ガイドラインとして、少なくともフルバックアップを実施するたびにこの手順を実行します。

PostgreSQL データ管理ツールの実行

- 1 [Windows] > [PostgreSQL 14 - OLCM] > [pgAdmin 4] へ移動します。pgAdmin を初めて実行する場合、Master Password を設定し、サーバーグループにサーバーを追加します。[Servers] を右クリックし、[Create] > [Server] を選択してサーバーを作成します。
- 2 [General] タブで、[Name] フィールドに *localhost* と入力します。
- 3 [Connection] タブで、[Host name/address] に *localhost* と入力し、postgres ユーザーのパスワードを入力します。パスワードはインストール時に設定しています。パスワードを保存するには、[Save password?] を選択します。
- 4 [Save] をクリックします。[Servers] グループの下に *localhost* と表示されます。
- 5 *localhost* を展開し、[Databases] を展開します。
- 6 [DataStore] と [OLSharedService] をダブルクリックして両方のデータベースを接続します。

メンテナンスウィザードを使用した統計の更新

- 1 PostgreSQL pgAdmin を起動して、データベース管理者として接続し、統計を更新するデータベースを選択します。デフォルトのデータベース管理者の名前は「postgres」です。デフォルトのパスワードは、OpenLab Server/ECM XT インストール時に **ステップ 1 - ソフトウェアに必要なコンポーネントのインストールおよびアップグレード** で設定したパスワードです。
- 2 データベースを右クリックし、**[Maintenance]** を選択します。以下のフォームが表示されます。

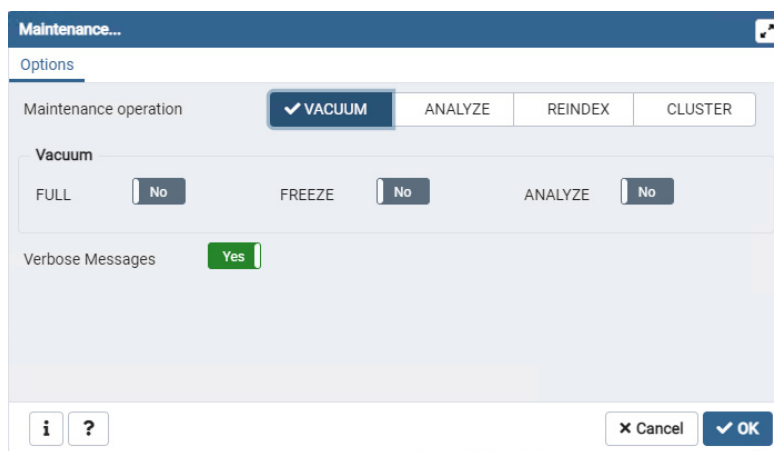


図 2 データベースのメンテナンス

- 3 **[ANALYZE]** を選択し、**[OK]** をクリックしてデータベースを解析します。

PostgreSQL データベースの追加メンテナンス

PostgreSQL では、データベースシステムの円滑な運用を維持するために、追加のメンテナンスコマンドをサポートしています。このようなコマンドとして VACUUM と REINDEX があります。これらのコマンドの詳細については、PostgreSQL のドキュメントを参照してください。

注意

OpenLab PostgreSQL サーバーにはアジレントが提供するサービスパックまたは修正プログラムのみを適用してください。

SQL Server のメンテナンス手順

Windows オペレーティングシステムには、少なくとも 4 GB 確保してください。

Microsoft SQL Server のパフォーマンスチューニング

ドキュメントの数が 1,000 万を超えると、SQL Server にある OpenLab Server/ECM XT は、SQL Server のパラメータスニффینگが ON に設定されることにより、以下の領域で動作が遅くなることがあります。

- 1 Bootstrap time (ブートストラップ時間)
- 2 サーバー再起動後の Web と DA 両方での初期ファイル一覧表示

上記のいずれかが生じた場合、パラメータスニффینگを OFF にしないでください。この設定はサポートされていません。

不適切なカバリングインデックスがパラメータ - スニффینگの根本原因であることがよくあります。SQL Server は少数の値の場合は Key Lookup プランを選択し、多数の値の場合はクラスター化インデックスのシークまたはスキャンを選択することがあります。カバリングインデックスを用いると、オプティマイザーがこれらの選択を行わず、多くの場合により安定した実行プランが得られます。

パフォーマンスを向上させるには、SQL Server Management Tool で以下の 2 つのインデックスを手動で追加します。

- 1 ブートストラップ時間を向上させるには以下のインデックスを作成します。

```
USE [DataStore]
GO

SET ANSI_PADDING ON
GO

/***** Object:  Index [idx_alf_cass_qnln]      Script Date:
12/7/2018 8:00:46 PM *****/

CREATE NONCLUSTERED INDEX [idx_alf_cass_qnln] ON
[dbo].[alf_child_assoc]
(
    [parent_node_id] ASC,
    [qname_ns_id] ASC,
    [qname_localname] ASC,
    [qname_crc] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
SORT_IN_TEMPDB = OFF, DROP_EXISTING = OFF, ONLINE = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
GO
```

- 2 サーバー再起動後の Web および DA での初期ファイル一覧表示時間を向上させるには、以下のインデックスを作成します。

```
USE [DataStore]
GO

/***** Object:  Index [idx_alf_node_tqn_id]      Script Date:
12/10/2018  5:20:05 PM *****/

CREATE NONCLUSTERED INDEX [idx_alf_node_tqn_id] ON
[dbo].[alf_node]
(
    [type_qname_id] ASC
) WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
SORT_IN_TEMPDB = OFF, DROP_EXISTING = OFF, ONLINE = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
GO
```

- 3 以下の推奨事項に基づいてインデックスを再構築します。インデックスの断片化確認を実行：
- 30% 以上の場合は再構築します。
 - 5 ～ 30% の場合は再構成します。詳細については、
<https://docs.microsoft.com/ja-jp/sql/relational-databases/indexes/reorganize-and-rebuild-indexes> を参照してください。

Content Management 用に Microsoft SQL サーバーをカスタマイズする

パフォーマンスが低下しないようにするには、SQL サーバーで以下のようなメンテナンス作業を毎週実行してください。

- 次のコマンドから統計を再計算：EXEC sp_updatestats
- 次のコマンドからバッファを消去：DBCC DROPCLEANBUFFERS
- 次のコマンドからキャッシュを消去：DBCC FREEPROCCACHE

メンテナンスプラン ウィザードを使用した統計の更新

MS SQL Server データベースの場合、SQL Server Management Studio を使用して統計の更新手順を簡単に自動化できます。

- 1 **SQL Server Management Studio** を起動し、データベース管理者として接続します。
- 2 サーバーを展開します。
- 3 管理フォルダーを展開します。
- 4 **【メンテナンスプラン】** を右クリックし、**【メンテナンスプラン ウィザード】** を選択します。ウィザードを使用して、メンテナンス要件に合わせてカスタマイズされたプランを作成します。
 - a アクティビティが少ないと思われる時刻に実行する、**【週単位のスケジュール】** を選択します（たとえば、日曜日、昼 12:00）。
 - b メンテナンスタスクとして **【統計の更新】** を選択します。
 - c タスクの実行対象となるデータベースとして、OpenLab Server/ECM XT Server データベース（DataStore）と Shared Services データベース（OLSharedServices）を選択します。

お使いのサーバーの移動

サーバーをドメインからワークグループに移動する、またはドメインから別のドメインに移動するには、SQL サーバーを（ドメインアカウントではなく）ローカルアカウントに設定する必要があります。サーバーを移動する場合の詳細については Agilent のサポートにお問い合わせください。

OpenLab Server/ECM XT Server でのリソース使用量のモニタ

データファイル、インデックス、データベースはサーバーのハードディスクまたは AWS S3 に保存されます。サーバーのコンフィグレーションによっては、1 つ以上のディスクドライブに保存される場合もあります。

システム管理者は、データが保存されているすべてのディスクのディスク領域の使用率を定期的にモニタする必要があります。ディスクの使用率が 80% に近づいた場合、ディスク領域の拡張を検討してください。CPU、メモリ、ネットワーク使用率をモニタして、サーバーにパフォーマンスのボトルネックがあるかどうかを確認する必要があります。

リソース使用量をモニタする最適な方法

- 1 OpenLab Server/ECM XT Server のディスクの使用率を毎週 1 回以上モニタします。
- 2 オプションとして、ディスクの使用率がスレッシュホルドを超えると電子メール通知を送信し、自動ディスク領域モニタツールを実行する。このようなツールの例として、Monit、Munin、Cacti、Nagios があります。
- 3 メモリ、CPU などのリソース使用量と、ネットワークスループットをモニタする。これには Windows パフォーマンスモニタが利用できます。

その他の最適な方法

- OpenLab Server/ECM XT Server にサードパーティのアップデートとパッチを適用します。

Agilent SubscribeNet には、OpenLab ソフトウェアスイートに使用できる検証済みのサードパーティアップデートおよびパッチの情報が定期的に公開されています。これには、OS セキュリティパッチおよびアップデート、データベースのアップデート、アプリケーションのアップデートが含まれます。

カスタマケアポータル URL は次のとおりです。

<https://agilent.subscribenet.com>

- Agilent ソフトウェアアップデートを適用します。

OpenLab Server/ECM XT Server に Content Management と Shared Services のソフトウェアアップデートを適用します。アップデートの通知を受け取ったら必ず内容を確認し、アップデートが適用可能かどうか、およびその緊急度を判断してください。

Windows ドメイン

サーバー用のドメイン、ユーザー名、 またはパスワードの更新

Windows ドメイン認証を使用して OpenLab ユーザーを識別する場合、資格情報が保存されているサーバーに OpenLab がアクセスできる必要があります。

[Windows ドメイン] を使用して、Windows ドメインサーバーにアクセスするために OpenLab が使用する資格情報を指定または変更します。この機能は、Shared Services メンテナンスユーティリティプログラムを開いたコンピューターに保存された資格情報のみアクセスできます。

Windows ドメインサーバーへのアクセスに使用する Windows アカウントの**ドメイン、ユーザー名、またはパスワード**を指定または変更するには、サーバー上にインストールされている **Shared Services メンテナンスユーティリティ** プログラムを使用します。

ユーザーの読み取り権限の有効化

Windows ドメイン認証を使用する際に、ユーザーが OpenLab のパスワードを変更する必要があるかどうかに関する情報を取得するために、OpenLab Server/ECM XT がユーザー属性を読み取ります。読み取り権限がユーザーに与えられていない場合、OpenLab Server/ECM XT はそのユーザーのパスワードの期限が切れていると見なし、アクセスを拒否します。

ユーザーの読み取り権限を有効にするには、

- 1 ドメインコントローラで、**[Active Directory ユーザーとコンピューター]**を開きます。
- 2 **[表示] > [拡張機能]** の順に選択します。
- 3 **[Users]** を右クリックし、**[プロパティ]** を選択します。
- 4 **[セキュリティ]** タブで、**[Authenticated Users]** を選択します。
- 5 **[読み取り]** 許可を選択して **[OK]** をクリックします。

サーバー設定

クライアント / サーバー構成では、**【サーバー設定】**を使用して、ローカルシステムでのサーバー接続を管理します。表示されるサーバーのリストによって、OpenLab にログインする際にユーザーが接続先として選択できるサーバーが決まります。管理者は、このタブでユーザーがデフォルト以外のサーバーに切り替えることを制限できます。

この機能は、**Shared Services メンテナンスユーティリティ**プログラムを使用しているコンピューターのサーバー接続を管理します。

したがって、クライアントのサーバー接続を変更するには、そのクライアントにインストールされている **Shared Services メンテナンスユーティリティ**プログラムにアクセスします。

FTP サーバープロトコル

OpenLab Server/ECM XT Server は FTP サーバーとして使用可能で、すべての FTP サーバープロトコルからアクセスできます。

注意

FTP はデフォルトでは無効になっています。FTP サービスを有効にした場合、これはデータの保全性に対するリスクとみなされる場合があるため、対象となるシステムは、不要な場合 FTP サービスを無効にするかブロックすることをお勧めします。49ページの「[OpenLab Server/ECM XT Server を FTP サーバーとして使用しない](#)」を参照してください。

OpenLab Server/ECM XT Server を FTP サーバーとして使用

- 1 サーバー上で、**C:¥Program Files (x86)¥Agilent Technologies¥OpenLab Data Store¥tomcat¥shared¥classes** に移動します。
- 2 テキストエディタで、alfresco-global.properties ファイルを開きます。
- 3 **ftp.enabled=false** を **ftp.enabled=true** に変更します。
- 4 ファイルを保存します。
- 5 tomcat サービスを再起動します。

FTP プロトコルから OpenLab Server/ECM XT Server に接続

- 1 FTP クライアントにアクセスします。
- 2 FTP プロトコル内では以下を使用してください。
 - FTP ホスト名として OpenLab Server/ECM XT Server アドレス
 - OpenLab Server/ECM XT Server ポート
 - コントロールパネルのユーザー名とパスワード
- 3 FTP プロトコルに従って接続します。

OpenLab Server/ECM XT Server を FTP サーバーとして使用しない

サーバー上で FTP アクセスをブロックするには、ファイアウォール内の FTP ポートをブロックする必要があります。ワークステーションのインストールで、FTP サービスを無効にする必要があります。

- 1 サーバー上で、**C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\tomcat\shared\classes** に移動します。
- 2 テキストエディタで、alfresco-global.properties ファイルを開きます。
- 3 **ftp.enabled=true** を **ftp.enabled=false** に変更します。
- 4 ファイルを保存します。
- 5 tomcat サービスを再起動します。

アーカイブ

自動アーカイブ実行スケジュールの変更

この手順を使用して、自動アーカイブタスクの実行日時を Content Management プロパティファイルで変更します。自動アーカイブタスクを実行すると、コンテンツフォルダーに割り当てられたユーザー指定のアーカイブルールが実施され、コンテンツがアーカイブ先ロケーションへ移動します。デフォルトでは、自動アーカイブタスクは月に 1 回実行されますが、 Quartz Cron 記法でサポートされるスケジュールを使用できます。

自動アーカイブ実行スケジュールを変更するには、以下が必要です。

- **<INSTALLATION**
PATH>%tomcat%shared%classes%alfresco-global.properties ファイルの読み取り / 書き込み権限を持つオペレーティングシステムユーザー資格情報。デフォルトインストールでは、ファイルは以下のロケーションにあります。
C:%Program Files (x86)%Agilent Technologies%OpenLab Data Store%tomcat%shared%classes%alfresco-global.properties
- alfrescoTomcat サービスを開始および停止する権限。

実行値の変更

- 1 alfrescoTomcat サービスを停止します。
- 2 ファイルを開きます：**<INSTALLATION**
PATH>%tomcat%shared%classes%alfresco-global.properties
- 3 プロパティ：**archive-job.cron** を見つけます。例：

```
### Archive Job Cron Expression
# default runs first sunday at 2:30 AM of every month
archive-job.cron=0 30 2 ? * 1#1 *
```
- 4 要件に合わせて式を変更します。51 ページの「**Cron 記法**」を参照してください。
- 5 ファイルを保存します。
- 6 alfrescoTomcat サービスを再開します。

Cron 記法によって記述される日時にタスクが自動的に実行されます。

Cron 記法

Cron 記法は、スケジュールの個々の詳細を記述する 6 つまたは 7 つのフィールドで構成される文字列です。

白いスペースで区切られたこれらのフィールドには、使用できる任意の値と、各フィールドで使用できるさまざまな文字の組み合わせを含めることができます。

Seconds	Minutes	Hours	Day Of Month	Month	Day Of Week	Year
0	0	0	?	*	*	*

表 4 に、自動アーカイブ用の Cron 記法の例を記載しています。

表 4 Cron 記法の例

説明	Cron 記法
毎日 2:30 a.m. に実行	0 30 2 ? * * *
毎週日曜日 2:00 a.m. に実行	0 0 2 ? * 1 *
1 日 2 回正午と真夜中に実行	0 0 */12 ? * *
毎月 2 日と 17 日の 11:00 p.m. に実行	0 0 23 2,17 * ? *

変数の意味は次のとおりです。

* = すべての値

? = 不特定の値

自動アーカイブタスクを 1 日に複数回実行することはお勧めできません。作業時間外に自動アーカイブタスクを実行するようスケジュールすることをお勧めします。

検疫

アーカイブ中の隔離

アーカイブ / アーカイブ解除プロセスを中断すると、アーカイブ元とアーカイブ先の両方にファイルが存在することがあります。このような状況が発生した場合、アーカイブ / アーカイブ解除を再度実行すると、自動的に以下の措置が講じられます。

- 1 アーカイブ先ロケーションにファイルが存在することが検出されると、ファイルは検疫フォルダーへ移動します。この隔離プロセスはユーザーには表示されません。
元ファイルが常にオリジナルで、「良好な」ファイルバージョンであると見なされます。

- 2 ファイルが隔離されたことを示すログエントリが作成されます。エントリの説明は以下のとおりです。

< 'ファイル' / フォルダー ' > < ファイル / フォルダーのパスと名前 > は < 'アーカイブ' / アーカイブ解除 ' > の実行中に検疫され < 検疫フォルダーロケーション > に隔離されました

< ファイル / フォルダーのパスと名前 > は、Content Management インターフェイスに表示されるファイル名による論理パスで、< 検疫フォルダーロケーション > は、物理ファイルの暗号化された名前（.bin ファイル）を含めた、検疫フォルダーへの物理パスです。

隔離中のファイルに関連付けられた .bin ファイルごとに 1 つのログエントリが作成されます。たとえば、ファイルに 2 つのバージョンがある場合、2 つの .bin ファイルがこのファイルに関連付けられます。ファイルが検疫フォルダーへ移動すると、2 つのログエントリが作成されます。

- 3 隔離後は、重複したファイルが検出されなかったかのようにアーカイブ / アーカイブ解除が続行され、ユーザーには Content Management インターフェイスでの違いは分かりません。

検疫フォルダー

検疫フォルダーは、Content Management 内のフォルダー構造と一致するよう構造化されます。検疫フォルダーに追加されるファイルはソースフォルダーと同じパスになります。同じ名前のファイルが検疫フォルダーにすでに存在する場合、新しいファイルが番号付きのサブフォルダー内に配置されます。このため、ファイルは上書きされず、データが失われることはありません。

検疫フォルダーには「contentstore.quarantined」という名前が付けられ、その保存場所はシステムストレージロケーションの設定場所になります。

- プライマリコンテンツロケーションとプライマリアーカイブロケーションの両方が同じ場所にある場合（オンプレミスまたは AWS S3）、検疫フォルダーはプライマリコンテンツロケーションに作成されます。
- プライマリコンテンツロケーションとプライマリアーカイブロケーションが異なる場所にある場合（オンプレミスと AWS S3 との混合）、両方のロケーションに検疫フォルダーがあります。検疫フォルダーは、重複するファイルが検出されたロケーション（アーカイブ先ロケーション）に作成されます。たとえば、プライマリコンテンツロケーションがオンプレミスで、プライマリアーカイブロケーションが AWS S3 上にあるコンフィギュレーションの場合、
- 正しくアーカイブされなかったファイルがある場合、検疫フォルダーは AWS S3 アーカイブロケーションに存在します。（これは、アーカイブを再度実行したときにアーカイブロケーションで重複するファイルが検出された場合に発生します。）
- 正しくアーカイブ解除されなかったアーカイブファイルがある場合、検疫フォルダーはオンプレミスのコンテンツロケーションに存在します。（これは、アーカイブ解除を再度実行したときにコンテンツロケーションで重複するファイルが検出された場合に発生します。）

5

バックアップとリストアの手順

バックアップとリストアに関する重要な情報 55

障害復旧プランの作成 57

バックアップおよびリストアユーティリティの使用 59

バックアップユーティリティを使用する OpenLab Server/ECM XT の
バックアップ 62

リストアユーティリティを使用する OpenLab Server/ECM XT のリストア 75

バックアップおよびリストアスクリプトの使用 84

バックアップとリストアに関する重要な情報

すべての OpenLab Server/ECM XT Server を必ず定期的にバックアップしてください。定期的なフルバックアップと、フルバックアップの間に実行する差分バックアップは、OpenLab Server/ECM XT Server 管理者が作成します。これらのバックアップは、ハードウェアまたはソフトウェアの不具合が発生したときに OpenLab Server/ECM XT Server をリストアする唯一の方法です。

致命的なシステム障害が発生した場合、バックアップはデータ損失量を軽減します。バックアップを実施することで、バックアップの時点で収容されたデータをリストアすることができるよう保証されます。アップロード待ちでまだコミットされていないデータや、バックアップを実施した後にシステムに追加または更新されたデータは、バックアップをリストアしても復旧できません。

バックアップが正しく実施され、リストアに使用できることを確認するには、必ずリストア手順もテストする必要があります。有効なリストアを実行するには、障害復旧プランの作成が必要です。57 ページの「[障害復旧プランの作成](#)」を参照してください。

注意

リストアされたシステムが、(バックアップが取得された) ソースシステムと同時に動作する場合、リストアされたシステムがソースシステムから分離されたネットワーク上にあることを確認してください。たとえば、運用システムのバックアップからテストシステムを作成した場合、テストシステムは運用システムから分離されたネットワーク上にある必要があります。テストシステムと運用システムが同じネットワーク上にあると、2 台のサーバーがクラスターを作成し互いに作用する場合があります。これはデータの破損や損失につながる可能性があります。

さらに、リストアされたシステムのクラスタリングを以下の手順でオフにすることが重要です。

- 1 リストアされたサーバーで「C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes\alfresco-global.properties」を開きます。
- 2 `alfresco.cluster.enabled` プロパティを検索し、以下のように `false` に設定します。
`alfresco.cluster.enabled=false`
- 3 AlfrescoTomcat サービスを再開します。

OpenLab Server/ECM XT は、ファイルとインデックスをサーバーのファイルシステムに保存します。フォルダーの場所は、製品のインストール時に決定します。フォルダー情報、監査証跡、署名などのその他のデータは、リレーショナルデータベースに保存されます。

フルバックアップは、アップロードしたファイルやそのデータベースも含む OpenLab Server/ECM XT のすべてのデータを取り込みます。差分バックアップは、前回のフルバックアップ以降に発生した変更だけをバックアップします。差分バックアッププロセスは、変更された要素のみバックアップするので、フルバックアップよりも短時間で行えます。

サーバーをアップグレードする場合は、アップグレードする前にマシンで以下の手順を実行してください。アップグレードの前に、すべての作業領域とファイルアップロードキューをクリアしてください。異なるオペレーティングシステムへアップグレードする場合、キューにデータがないようにしてください。すべてのファイルアップロードが完了していることを確認してください。アップグレードの前に、ファイルバッファアアップロードキューをクリアしてください。

バックアップユーティリティは、OpenLab Server/ECM XT Server（オールインワンサーバーまたは 2 サーバー）の即時バックアップや定期的なバックアップの実行に使用できます。

Amazon Web Services S3 をバックアップロケーションとして使用

- S3 バケットがインターネット経由で「公的に」アクセス可能でないことを確認してください。集中管理を使用してアクセスを制限してください。
- 「最低特権アクセス」の原則に従ってください。タスクを実行するために必要な権限のみ付与してください。
- OpenLab バックアップ / リストアツールを使用するシステムのバックアップロケーションとして S3 を使用する場合、バックアップを含むバケットに以下の権限を（上記で定義された権限に加えて）割り当ててください。

```
s3:DeleteObjectVersion
s3:GetObjectVersionTagging
s3:ListBucketVersions
s3:PutObjectVersionTagging
s3:DeleteObjectVersionTagging
```

- サーバー側の暗号化を有効にしてください。
- オブジェクトのバージョン管理を有効にしてください。

障害復旧プランの作成

OpenLab Server/ECM XT がハードウェアやソフトウェアの不具合により操作不能になるという予期せぬ事態に備えて、復旧プランを準備します。このプランには、オペレーティングシステム、OpenLab Server/ECM XT のソフトウェア、データを（必要な場合は物理的に異なるサーバーに）完全にリストアするための情報とプロシージャを含める必要があります。障害復旧プランが機能することを、あらかじめ確認しておいてください。

障害復旧プランの策定には、次の点を考慮に入れてください。

- 必要とするバックアップの頻度を決めてください。たとえば、障害が発生した場合に許容できる最大のサンプル損失数（やり直しが必要なサンプル）は？
特に大規模システムの場合、バックアップの頻度とリストアのコスト / 工数はトレードオフの関係にあります。
- システムトポロジーと可用性要件に対して最適なバックアップおよびリストア方法は？
 - バックアップユーティリティ / リストアユーティリティ（オールインワンおよび 2 サーバートポロジーのみ対応）ユーティリティはフルバックアップまたは差分バックアップ（日ごと）を提供します。
 - バックアップおよびリストアスクリプト
スクリプトは差分バックアップをサポートしていないため、大規模システムには適さない場合があります。
 - 手動の手順（一般に、大規模システムに最適）Agilent のバックアップユーティリティ / リストアユーティリティ以外のバックアップソリューションを構成するための手順です。

OpenLab Server/ECM XT のバックアップおよびリストアは、データベースのコンフィグレーションのタイプが完全に同じ場合のみサポートされます。異なるタイプのアーカイブ済みデータベース（同じデータベースでコンフィグレーションが異なる場合も含む）間でバックアップおよびリストアを実行しようとすると、コントロールパネルはエラーを表示します。“障害復旧プラン”には次の情報を含める必要があります。

- サーバーハードウェア情報：CPU、メモリ、ハードディスクのコンフィグレーション情報
- サーバー ID：名前、IP、ドメイン、URL など
 - サーバー管理者情報：サーバーにログインするためのユーザー名とパスワードデータベースに対するユーザー名とパスワード（必要であれば）
- サーバーソフトウェア情報：OS バージョン、パッチレベル
- OpenLab Server/ECM XT インストールパラメータ：

- インストールフォルダー
- インストールログファイル
- OpenLab Server/ECM XT のデータベースタイプ
- OpenLab Server/ECM XT のコンテンツおよびアーカイブフォルダー
- OpenLab Server/ECM XT のインデックスフォルダー
- OpenLab Server/ECM XT Content Management データベース名
- Shared Services の言語
- Shared Services データベース名
- インストールライセンス
- 登録済みアプリケーション
- サードパーティソフトウェア情報：アプリケーションとリビジョン、インストールパス
- トポロジーのプロシージャ 59 ページの「**バックアップおよびリストアユーティリティの使用**」または第 6 章「**手動バックアップとリストアの手順**」を参照してください。
- バックアップメディアのロケーションと機構の詳細
- リモートデータベースサーバーが正しく構成されている。『OpenLab Server/ECM XT インストールガイド』の「リモートデータベースサーバーのコンフィグレーション」を参照してください。

バックアップおよびリストアユーティリティの使用

バックアップおよびリストアユーティリティは、OpenLab Server/ECM XT システムを容易にバックアップとリストアするツールです。

オールインワンおよび 2 台のサーバーを使用するトポロジの場合、以降のセクションで説明するバックアップとリストアの自動ツールを使用できます。4 台のサーバーのバックアップおよびリストアは、バックアップとリストアのスクリプト（84 ページの「[バックアップおよびリストアスクリプトの使用](#)」を参照、または手動で実行）、または手動による方法を使用してください。スケーラブルトポロジの場合は、[第 6 章](#)「手動バックアップとリストアの手順」で説明する手動バックアップとリストアの手順を使用してください。以下の表に、バックアップおよびリストアユーティリティでサポートされる OpenLab Server/ECM XT のトポロジを記載しています。

注意

バックアップ中にウィルス対策スキャンが行われると、バックアップが正常に完了できない場合があります。定期的 / スケジュール済みスキャンとリアルタイム保護の両方でバックアップロケーションが除外されていることを確認してください。リアルタイム保護からバックアップロケーションを除外できない場合やリアルタイム保護をオフにできない場合、最終的なバックアップタスクが正常に完了しない可能性があります。

このような失敗を回避するため、Delay および Retry 設定があります。デフォルトでは、10 秒の間隔で 3 回試行するよう設定されています。この設定は、%ProgramData%\Agilent\Installation フォルダにある configuration.xml ファイルの [Backup] > [BackupFinalizationSettings] セクションで変更できます。このファイルを更新するには、システム管理者の権限が必要です。Delay は 0 より大きい値、Retry は 1 より大きい値に設定できます。Delay と Retry は、「即時バックアップ」時の [処理中] ページのステップ開始前と、「定期的なバックアップ」からのバックアップの開始時に適用されます。

バックアップ中にウィルス対策が実行される場合、バックアップが正常に完了したことを次の手順で確認できます。

バックアップが完了したら、バックアップロケーションにある「Current」（または「Current」と「Incremental」）のサブフォルダを確認します。

バックアップ時間に対応するログファイルに、「The backup has completed」と最後に記載されたエントリが含まれているか確認します。バックアップログは「C:\ProgramData\Agilent\LogFiles\Backup」フォルダに保存されます。

表 5 バックアップおよびリストアユーティリティでサポートされるトポロジー

トポロジー	バックアップ ユーティリティ	リストアユーティリティ	注記
オールインワン	+	+	スクリプトおよび手動でも実行可能。スクリプトは差分バックアップをサポートしていません。
2 サーバー	+	+	スクリプトおよび手動でも実行可能。スクリプトは差分バックアップをサポートしていません。 Oracle データベースのバックアップとリストアは手動で実行

表 5 バックアップおよびリストアユーティリティでサポートされるトポロジー（続き）

トポロジー	バックアップユーティリティ	リストアユーティリティ	注記
4 サーバー	スクリプト対応、手動はオプション	スクリプト対応、手動はオプション	スクリプトは差分バックアップをサポートしていません。 Oracle データベースのバックアップとリストアは手動で実行
スケーラブルシステム	手動のみ	手動のみ	Oracle データベースのバックアップとリストアは手動で実行

バックアップユーティリティを使用する OpenLab Server/ECM XT のバックアップ

バックアップユーティリティを使用して、サポートされるトポロジーの即時バックアップまたは定期的なバックアップを実行します。バックアップユーティリティは、フルバックアップと差分バックアップをサポートしています。バックアップユーティリティでサポートするトポロジーのリストについては、59 ページの「[バックアップおよびリストアユーティリティの使用](#)」を参照してください。

バックアップは、以下を含むすべての OpenLab データを取り込みます。

- コンフィグレーションファイル
- Shared Services、Content Management、およびデータリポジトリのデータベース
- Solr インデックス
- ローカルコンテンツおよびアーカイブのストレージロケーション
- Alfresco キャッシュ
- 証明書サーバー

注記

バックアップユーティリティは、OpenLab データのみをバックアップします。Master や MSDB などのコアデータベース要素のバックアップは、一般的なデータベースメンテナンスの一環として、お客様の責任において実施してください。

注記

バックアップユーティリティは、AWS S3 ストレージロケーションのデータをバックアップしません。

注記

リモートデータベースサーバー（PostgreSQL または MSSQL）搭載の非ドメイン（ワークグループ）環境の場合、データベースサーバーで LocalAccountTokenFilterPolicy が有効になっていることを確認してください。レジストリ DWORD 値「HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System¥LocalAccountTokenFilterPolicy」を作成するか、1 に更新してください。

注記

バックアップユーティリティは Oracle データベースをサポートしていません。Oracle データベースの場合、データベースのバックアップはスキップされるため、手動でバックアップする必要があります。Oracle データベースのバックアップ方法は、Oracle のドキュメントを参照してください。Oracle データベースのバックアップは、システムの他のバックアップの前に実行してください。

注記

バックアップユーティリティは、セキュリティで保護された接続用のカスタム証明書をバックアップしません。カスタム証明書を使用した場合、手動でバックアップし、リストアプロセスでできるようにセキュリティで保護された場所に保存してください。

カスタム証明書は、C:\Program Files\OpenLab Reverse Proxy\Apache24\conf\ssl\custom\ にあります。

注記

システムが特定（システム外）のユーザーアカウントで構成されている場合、そのユーザーに「バッチジョブとしてログオン」、「サービスとしてログオン」権限を割り当て、ECM XT Server およびデータベースサーバーの管理者でなければなりません。

注意

Agilent OpenLab バックアップユーティリティを使用して定期的なバックアップをする場合、SQL Server Management Studio、SQL スクリプトまたはツールを使用して OpenLab Content Management データベースをバックアップしないでください。差分バックアップが実行されなくなります。

必要な領域

バックアップ処理に必要な空き領域は、サーバーコンフィグレーション、バックアップロケーション、データベースのバックアップサイズなど、さまざまな要因によって異なります。最もリソースの消費量が多いケースでは、バックアップのロケーションの空き領域が、すべてのオンプレミスファイルストレージとデータベースサイズの合計の少なくとも 2 倍あることを確認してください。以前成功したバックアップが、何らかの理由で途中で終了したバックアップに上書きされるのを避けるために必要です。

バックアップおよびリストアユーティリティでは、AWS S3 バックアップロケーションとのバックアップ/リストア中に一時的なバックアップロケーションとして特定のデータベースフォルダーを使用します。

- PostgreSQL データベース用のデータディレクトリ。73 ページの「[PostgreSQL データベースのカスタムデータ ディレクトリの設定](#)」および 74 ページの「[PostgreSQL データベースのデータリポジトリのカスタムデータディレクトリを設定](#)」を参照してください。
- MS SQL データベース用のデフォルトバックアップロケーション。MS SQL ガイドに従ってデフォルトバックアップロケーションを設定してください。新しいロケーションにアクセス資格情報および MSSQLSERVER (NT Service¥MSSQLSERVER) の権限があることを確認してください。

指定したロケーションは、データベースのバックアップを一時的に保存するのに十分なスペースがあることを確認してください。

差分バックアップのデータベースの設定

差分バックアップを実行する場合、最初に OpenLabCDS および PostgreSQL データベースのデータリポジトリを設定する必要があります。71 ページの「[PostgreSQL データベースの差分バックアップ](#)」を参照してください。

トラブルシューティング

バックアップユーティリティのログは、%ProgramData%\Agilent\LogFiles¥Backup フォルダーに保存されます。バックアップ中にすべてのステップが確認され、失敗したステップで手順が停止します。失敗したステップのリンクから、現在のバックアップログファイルを開き、失敗の原因を特定します。バックアップが失敗した場合、バックアップロケーションの Temp フォルダーにバックアップの一部が保存されます。

バックアップユーティリティの使用手順

バックアップユーティリティを使用したバックアップ

ステップ	オプション	注記
1 [スタート] > [Agilent Technologies] > [バックアップユーティリティ] からバックアップユーティリティを開始します。ユーザーアカウント制御アクセスのリクエストが表示された場合、[はい] をクリックします。[次へ] をクリックします。	[ステータス] ページに、前回完了したバックアップの日付と時刻が表示されます。 リンクをクリックするとバックアップロケーションが表示されます。	- バックアップユーティリティを実行するにはシステム管理者権限が必要です。 - 定期的なバックアップがスケジュールされている場合、現在のバックアップステータスと次回バックアップの開始日時が表示されます。 - バックアップが現在実行中の場合、ステータスに [実行中] と表示されます。定期的なバックアップが失敗した場合、ステータスに [失敗] と表示されます。 [前回完了したバックアップ] に最後に成功したバックアップ（「定期的なバックアップ」または「即時バックアップ」タイプ）が取得された日時とそのロケーションが表示されます。バックアップロケーション（オンプロミスまたはAWS S3）がリンクされています。一度バックアップに成功するとこの情報が含まれます。 - タイムゾーンが変更された場合はシステムを再起動してください。再起動しないと、[ステータス] ページの日時が一致しないことがあります。
2 [バックアップオプション] ページで、バックアップオプションを選択します。	定期的なバックアップ	- 自動バックアップの手段としてこのオプションを使用します。 - バックアップタイプおよびスケジュール設定を指定します。スケジュールの時間には 24 時間形式を使用します。 - 自動バックアップをスケジュールすることをお勧めします。メンテナンス中に自動バックアップを無効にするには、[定期的なバックアップを有効にする] チェックボックスをオフにします。メンテナンスが完了したら、忘れずに定期的なバックアップを再度有効にしてください。

バックアップユーティリティを使用したバックアップ（続き）

ステップ	オプション	注記
	- 即時バックアップ - ホットバックアップ - コールドバックアップ	- ホットバックアップまたはコールドバックアップがすぐに開始されます。 - 定期的なバックアップへの影響はありません。 - バックアップ設定の正確性チェックや1回のバックアップで必要なディスク領域と所用時間を確認するのに役立ちます。さらに、このオプションはリストア手順全体のテストの一部にすることができます。
3 [設定] ページで、バックアップの設定をします。	- 定期的なバックアップの場合、バックアップを有効にしてスケジュールの設定をします。 - バックアップ中にシステムを利用するかどうかが選択します。 - はい：ホットバックアップ - いいえ：コールドバックアップ - 差分バックアップを有効にする場合は選択します。差分バックアップの時間と曜日を入力します。	- 定期的なバックアップを有効にすることを強くお勧めします。【定期的なバックアップを有効にする】チェックボックスをオフにすると、スケジュールされたバックアップは実行されません。 - フルバックアップと差分バックアップを同じ曜日にスケジュールすると、フルバックアップが実行されます。 - 差分バックアップを行う前に1度フルバックアップを実行する必要があります。 - 定期的なフルバックアップが失敗した場合、次にスケジュールされたフルバックアップが成功するまでは、差分バックアップは失敗します。差分バックアップが失敗しないようにするには、定期的なバックアップで指定されたロケーションに即時バックアップを実行します。
	- 即時バックアップの場合、バックアップ中にシステムを利用するかどうかが選択します。 - はい：ホットバックアップ - いいえ：コールドバックアップ	- ホットバックアップ：バックアップ中もシステムは稼働したままとなります。 - コールドバックアップ：OpenLab server/ECM XT のすべての操作を停止する必要があります。バックアップユーティリティがサービスを停止します。

5 バックアップとリストアの手順

バックアップユーティリティの使用手順

バックアップユーティリティを使用したバックアップ（続き）

ステップ	オプション	注記
4 バックアップロケーションの指定		バックアップは、フォルダーの設定ができません。 現在の Windows ユーザーの許可は必要ありません。バックアップはシステムユーザーが実行し、成功したバックアップを保存できます。定期的にスケジュールされたバックアップは実行されますが、現在の Windows ユーザーは適切な権限がなければ結果を表示できません。
	ファイルシステム	- オンプロミスバックアップの場合のロケーションは、ローカルまたは Windows 共有となります。ネットワークドライブはサポートされていません。 - ネットワーク共有を使用する場合、指定されたユーザーアカウントでサーバーを構成してください。サーバーの [サーバーコンフィグレーションユーティリティ] > [アクセス資格情報] からこの設定を構成します。ユーザーはバッチジョブとしてログオン権限を持ち、管理者でなければなりません。 - システムアカウントのサーバーコンフィグレーションは、ローカルフォルダーのみサポートしています。
	- AWS S3（Amazon AWS S3 ロケーション） - S3 バケットのリージョン、バケット名、およびアクセスキーを提供	- AWS S3 バケット設定のオブジェクトのバージョン管理を有効にします。 - AWS S3 設定が有効であることを確認します。サービスが到達不能か設定が無効の場合は AWS S3 にメッセージが表示されます。
5 通知を設定します。即時バックアップを選択した場合、これはスキップされます。	- バックアップ通知の有効 - 差出人アドレス - 送信先アドレス	- コントロールパネルで設定された差出人アドレスを使用します。電子メールアドレスの設定方法については、コントロールパネルのオンラインヘルプを参照してください。 - 複数の送信先アドレスは、カンマで区切ります。 - 各アドレスは長い形式（名前と電子メール）または短い形式（電子メールのみ）で表記できます。

バックアップユーティリティを使用したバックアップ（続き）

ステップ	オプション	注記
	件名にテキスト入力	電子メール通知の件名の接頭語を指定します。
	テストメッセージの送信	[テストメールの送信] を使用して、通知の設定が正しいことを確認します。
6	バックアップをレビューおよび開始します。バックアップを開始するには、[適用] をクリックします。	[処理中] ページで進行状況を確認できます。
7	バックアップが完了したら、[完了] をクリックします。	

注記

Sample Scheduler を使用する場合、コールドバックアップの後に Sample Scheduler サービスを再起動する必要があります。

バックアップユーティリティを実行すると、指定したロケーションにバックアップフォルダーが作成されます。

> ドキュメント > Backup > Current ▼ 🔄 Currentの1			
名前	更新日時	種類	サイズ
 CertificateService	2021/05/13 11:18	ファイル フォルダー	
 DR	2021/05/13 11:18	ファイル フォルダー	
 DSArchiveDir	2021/05/13 11:18	ファイル フォルダー	
 DSCContentDir	2021/05/13 11:18	ファイル フォルダー	
 DSIndexDir	2021/05/13 11:17	ファイル フォルダー	
 Installation	2021/05/13 11:17	ファイル フォルダー	
 PostgreSQLDataDir	2021/05/13 11:18	ファイル フォルダー	
 Verification	2021/05/13 11:18	ファイル フォルダー	
 backup.xml	2021/05/13 11:18	XML ドキュメント	1 KB

バックアップが失敗した場合、バックアップロケーションの Temp フォルダーにバックアップの一部が保存されます。

注記

ウィルス対策スキャンが行われると最終ステップで Temp フォルダー名を Current に変更できない場合があります。この場合は、バックアップが「失敗」しても、backup.xml ファイルの作成は成功しています。これが失敗の原因となっている場合、Temp フォルダー名を手動で Current に変更できます（フルバックアップを実行した場合）。差分バックアップを実行した場合、Temp フォルダー名を Incremental に変更します。

バックアップバリデーション

バックアップバリデーションでは、バックアップの完了後にバックアップされたデータを検証します。

バックアップ後に 2 種類のレポートが作成されます。どちらのレポートも Verification サブフォルダーに保存されます。

- VerificationReport.xml - このファイルには、ファイルやそれらのハッシュ、データベースのエンティティなど、バックアップされたエンティティに関する情報を含めた、バックアップの技術情報が含まれます。リストアのために、このレポートを使用してファイルとデータベースのエンティティを比較します。
- VerificationReport.html - バックアップに関する情報、バリデーションされたファイルの数、不合格に関するファイル情報、データベースエンティティのバリデーション結果が、人が読み取れるビューで表示されます。

バリデーションでは、メインエンティティ（アップロードされたファイル、データベースエンティティ）が適切にバックアップされていることを確認します。バリデーションするファイルの数は、バックアップコンフィグレーション後にコンフィグレーションファイルで指定します（デフォルトでは 10% または 10000）。Oracle データベースのバックアップはデータベースユーティリティではサポートされていないため、データベースエンティティのバリデーションはスキップされます。

バックアップ手順の後に、オンプレミスロケーションに保存されたファイルがバリデーションされ、レポートに含まれます。AWS S3 ストレージロケーションのファイルは AWS 手順を使用してバックアップされ、バリデーションに含まれないためバリデーションされません。オンプレミスと AWS S3 の混合ファイルストレージの場合もファイルのバリデーションは実行されず、Content Management 内の総ファイル数のみ表示および比較されます。

リストアの場合、バックアップレポートに含まれているすべてのエンティティがバリデーションされます。

バックアップ開始時間後に変更されたエンティティ（またはそのバージョン）はレポートに含まれず、リストア実施中にバリデーションされません。

ファイルのバリデーション

ファイルのバリデーションには、以下のロジックが使用されます。

- バックアップユーティリティは、最初にバックアップされたすべてのファイルをカウントし、バリデーション用に全ファイルの最小 10% から上限までのファイルをランダムに取り出します。バリデーションに使用されるファイルのパーセントは常に切り上げられます。たとえば、3 ファイルの 10% は 0.3 であるため、この値は 1 に切り上げられます。Content Management 内のファイルが少ない場合でも、このツールが 1 つ以上のファイルをバリデーションします。
- 次に、各ファイルのランダムなバージョンをユーティリティが取り出します。たとえば、Content Management 内の 1 つのファイルに 3 種類のリビジョンがある場合（1.0、2.0、3.0）、ユーティリティはランダムにリビジョンを選択し取り出します。
- バリデーションでは、削除されたファイルを除外します。
- バリデーションは、バックアップされたファイルのチェックサムおよびサイズと、Content Management のファイル情報を比較します。チェックサムが等しい場合、バリデーションは合格です。そうでない場合、バリデーションは不合格です。

バリデーションするファイル数は、%ProgramData%\Agilent\Installation フォルダにある configuration.xml ファイルの [Backup] セクションの以下のプロパティで変更できます。このファイルを変更するには、システム管理者である必要があります。

- PercentFilesVerification - バリデーションするファイルの割合（デフォルトは 10%）、1 - 100 の範囲。
- TotalFilesVerificationLimit - バリデーションするファイル数の上限（デフォルトは 10,000）、値は 0 より大きくなければなりません。負の値や小数は設定できません。

新しい値は、「即時バックアップ」時の [処理中] ページのステップ開始前と、「定期的なバックアップ」からのバックアップの開始時に適用されます。

データベースのバリデーション

以下のデータベースエンティティの数の確認もバリデーションに含まれます。

- メソッド
- 一意のサンプル名
- Shared Services アクティビティログ
- Content Management アクティビティログ

PostgreSQL データベースの差分バックアップ

累積的な差分バックアップは、最後のフルバックアップ以降に変更されたデータファイルやオブジェクトを保存するプロセスです。すべてのデータではなく変更されたデータのみ更新するデータバックアップの方法です。これらの手順は、PostgreSQL (olcm-postgresql-x64-14) システムの場合は PostgreSQL データベースサーバー側で、PostgreSQL のデーターポジトリの場合はローカルで実行します。

PostgreSQL は、差分バックアップを実行するツールは備えておらず、差分バックアップ戦略を備えています。この戦略は、ファイルシステムレベルのバックアップと WAL ファイルのバックアップを組み合わせることができます。

断続的アーカイブ（多くのデータベースベンダーで「オンラインバックアップ」とも呼ばれます）を使用して正常に復旧させるには、少なくともバックアップの開始時間まで遡る連続した一連のアーカイブされた WAL ファイルが必要です。この方法を使用するには、最初のベースバックアップを行う前に、WAL ファイルのアーカイブ手順を設定してテストしてください。

差分コンフィグレーションツールを使用する差分バックアップの設定

差分コンフィグレーションツールは、差分バックアップサポートを自動的に設定します。OpenLab Server/ECM XT で使用するすべての PostgreSQL インスタンスを一度に設定できます。差分コンフィグレーションツールによって以下のアクションが実行されます。

- Content Management PostgreSQL（インストールされている場合）と PostgreSQL のデーターポジトリの差分バックアップサポートの設定の更新。
- 更新後に必要な PostgreSQL サービスの再起動。
- バックアップユーティリティによる差分バックアップサポートの BackupUtility.config ファイルの更新。

ツールは、デフォルトで C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Incremental Config Tool\PgIncrementalConfigTool.exe にあります。

PgIncrementalConfigTool はコマンドラインから実行できます。管理者として PgIncrementalConfigTool を実行し、82 ページの「**アクセス資格情報の再設定**」に従ってアクセス資格情報を設定します。

パラメータ：

- -on - 必須。差分バックアップを有効にし、デフォルトパスを設定します。
- -off - 必須。差分バックアップを無効にします。
- -olcmWalDir <path> - オプション。OLCM PostgreSQL の特定のパスを設定します。パラメータが「on」の場合のみ。
- -drWalDir <path> - オプション。PostgreSQL のデータリポジトリの特定パスを設定します。これは、パラメータが「on」の場合のみです。

例：

PgIncrementalConfigTool.exe -on

差分バックアップを有効にし、デフォルトパスを設定します。

PgIncrementalConfigTool.exe -off

差分バックアップを無効にします。

PgIncrementalConfigTool.exe -on -olcmWalDir D:¥wal¥olcm -drWalDir "D:¥wal¥dr files"

差分バックアップを有効にし、特定のパスを設定します。

Tool output

ツールは、トポロジに応じて PostgreSQL データベースを設定し、PostgreSQL サービスを再起動して、「Configuration completed successfully」というメッセージを表示します。

エラーが発生した場合、「PgIncrementalConfigTool has failed. The log files: <log file path>」と表示されます。

PostgreSQL データベースのカスタムデータ ディレクトリの設定

- 1 現在の PostgreSQL サービス設定を取得します。
 - a コマンドラインを実行し、PostgreSQL データベースがインストールされたマシンで、`sc qc olcm-postgresql-x64-14` というコマンドを実行します。
 - b `-D` オプションの後に現在のデータの保存場所が表示されます。
- 2 PostgreSQL サービス `olcm-postgresql-x64-14` を停止します。
- 3 現在のデータの保存場所にあるコンテンツを新しい保存場所へ移動します。
- 4 現在の設定に基づいて PostgreSQL サービス設定を変更します。データの新しい保存場所を設定します。例：`sc config olcm-postgresql-x64-14 binPath="¥C:¥Program Files (x86)¥PostgreSQL-14-OLCM¥bin¥pg_ctl.exe¥" runservice -N ¥"olcm-postgresql-x64-14¥" -D ¥"E¥NewDataLocation¥" -w`
- 5 PostgreSQL サービスのレジストリ値を更新します。新しいデータ保存場所を以下に設定します。
 - HKEY_LOCAL_MACHINE¥SOFTWARE¥PostgreSQL¥Installations¥olcm-postgresql-x64-14¥DataDirectory
 - HKEY_LOCAL_MACHINE¥SOFTWARE¥PostgreSQL¥Services¥olcm-postgresql-x64-14¥DataDirectory
- 6 PostgreSQL サービス `olcm-postgresql-x64-14` を起動します。
- 7 コンピュータを再起動します。

PostgreSQL データベースのデータリポジトリのカスタムデータディレクトリを設定

- 1 現在の PostgreSQL サービス設定を取得します。
 - a コマンドラインを実行し、以下のコマンドを実行します。
`sc qc postgresql-x64-14-dr`
 - b -D オプションの後に現在のデータの保存場所が表示されます。
- 2 PostgreSQL サービスを停止します。 PostgreSQL 14.1.1 (x64)
- 3 現在のデータの保存場所にあるコンテンツを新しい保存場所へ移動します。
- 4 現在の設定に基づいて PostgreSQL サービス設定を変更します。データの新しい保存場所を設定します。例：`sc config postgresql-x64-14-dr binPath="¥C:¥Program Files¥PostgreSQL¥14¥bin¥pg_ctl.exe¥" runservice -N ¥"postgresql-x64-14-dr¥" -D ¥"E:¥NewDataLocation¥" -w"`
- 5 PostgreSQL サービスのレジストリ値を更新します。新しいデータ保存場所を以下に設定します。
`HKEY_LOCAL_MACHINE¥SOFTWARE¥PostgreSQL¥E998E784-031A-4F94-9A3A-AB474D21C135¥Installations¥postgresql-x64-14¥DataDirectory`
`HKEY_LOCAL_MACHINE¥SOFTWARE¥PostgreSQL¥E998E784-031A-4F94-9A3A-AB474D21C135¥Services¥postgresql-x64-14¥DataDirectory`
- 6 PostgreSQL サービスを起動します。 PostgreSQL 14.1.1 (x64)
- 7 コンピュータを再起動します。

リストアユーティリティを使用する OpenLab Server/ECM XT のリストア

ハードウェアやソフトウェアの不具合により OpenLab Server/ECM XT Server が操作不能になった場合、次の手順を実行して既存のバックアップファイルからシステムをリストアします。

サーバーをアップグレードする場合、アップグレードする前に以下の手順を実行してください。

リストア手順は、成功したバックアップで取り込まれたコミット済みデータのみリストアします。アップロード待ちでまだコミットされていないデータや、バックアップを実施した後に追加または更新されたデータは、バックアップをリストアしても復旧されません。

注意

リストアシステムの OpenLab Server/ECM XT の 更新プログラムは、バックアップが作成されたシステムと同じになるようにしてください。

注意

リストアされたシステムが、（バックアップが取得された）ソースシステムと同時に動作する場合、リストアされたシステムがソースシステムから分離されたネットワーク上にあることを確認してください。たとえば、運用システムのバックアップからテストシステムを作成した場合、テストシステムは運用システムから分離されたネットワーク上にある必要があります。テストシステムと運用システムが同じネットワーク上にあると、2 台のサーバーがクラスターを作成し互いに作用する場合があります。これはデータの破損や損失につながる場合があります。

さらに、リストアされたシステムのクラスタリングを以下の手順でオフにすることが重要です。

- 1 リストアされたサーバーで、「C:¥Program Files (x86)¥Agilent Technologies¥OpenLAB Data Store¥tomcat¥shared¥classes¥alfresco-global.properties」を開きます。
- 2 `alfresco.cluster.enabled` プロパティを検索し、以下のように `false` に設定します。
`alfresco.cluster.enabled=false`
- 3 AlfrescoTomcat サービスを再開します。

バリデーション

既存のインストールにリストアしたら、リストアが正しく実行されたことを確認することもできます。バリデーションレポートは
C:\ProgramData\Agilent\Restore\Verification に保存されます。

リストア手順のトラブルシューティング

リストアユーティリティのログは、%ProgramData%\Agilent\LogFiles\Restore フォルダーに保存されます。リストア中にすべてのステップが確認され、失敗したステップでリストア手順が停止します。失敗したステップのリンクから、現在のリストアログファイルを開き、失敗の原因を特定します。リストアコンフィグレーション中に各ページでバリデーションされ、資格情報の誤り、コンテンツおよびアーカイブロケーションへのアクセス権の欠如、形式の誤り、その他の一般的なコンフィグレーションの問題など、発生する可能性があるエラーが防止されます。

PostgreSQL または Microsoft SQL データベース搭載のシステムのリストア

リストアユーティリティを使用して、PostgreSQL または MS SQL Server データベース搭載のサポートされる OpenLab Server/ECM XT システムをリストアします。リストアユーティリティでサポートするトポロジのリストについては、59 ページの「バックアップおよびリストアユーティリティの使用」を参照してください。

すべての場合、105 ページの「OpenLab Server/ECM XT Server の手動リストア手順」で説明する手動リストア手順に従ってください。

リストア中に各ページでバリデーションが実施され、資格情報の誤り、コンテンツおよびアーカイブロケーションへのアクセス権の欠如、形式の誤り、その他の一般的なコンフィグレーションの問題など、発生する可能性があるエラーが防止されます。

サポートされるトポロジの場合、以下の手順でリストアユーティリティを使用してシステムをリストアします。

注意

バックアップが作成されたシステムと同じ OpenLab Server/ECM XT の更新プログラムがインストールされている必要があります。これは、リストアされたデータベースのパッチレベルがアプリケーションのパッチレベルと一致している必要があるためです。

注記

リストアユーティリティによって、バックアップユーティリティで作成されたコールドバックアップとホットバックアップからシステムをリストアできます。リストアユーティリティは、OpenLab Server/ECM XT がインストールされたシステムやクリーンなシステム上で実行できます（79 ページの「**OpenLab Server/ECM XT がインストールされていないクリーンなマシン上のリストア**」を参照）。

注記

リストアユーティリティは、セキュリティで保護された接続用のカスタム証明書をリストアしません。リストア後のシステムは内部証明書を使用して設定されます。カスタム証明書を設定するには、29 ページの「**OpenLab Server/ECM XT リバースプロキシの設定**」の**ステップ 4**に従ってください。4 サーバーまたはスケラブルシステムのインデックスサーバーの場合、37 ページの「**インデックスサーバーコンフィグレーション - 4 サーバーシステムのみ**」を参照してください。

注記

リストアユーティリティは Oracle データベースのリストアをサポートしていません。Oracle データベースのリストア方法は、Oracle のドキュメントを参照してください。

注記

Sample Scheduler を使用する場合、リストア手順の後に Sample Scheduler サービスを再起動する必要があります。

注記

バックアップされたシステムの PostgreSQL の差分バックアップ設定でデフォルト以外のパスを使用している場合は、リストア後に 71 ページの「**差分コンフィグレーションツールを使用する差分バックアップの設定**」の指示に従ってください。

OpenLab Server/ECM XT がインストールされたシステムのリストアユーティリティの使用

以下の手順のように、バックアップユーティリティを使用してバックアップされたインストール済みシステムをリストアします。

注意

リストアプロセスを実行する前に、OpenLab Server/ECM XT のすべての操作を停止してください。リストア中は、クライアント、機器、またはシステムのその他の部分がサーバーを使用しないようにしてください。

リストアユーティリティを使用した既存のインストールへのリストア

ステップ	オプション	注記
1 [スタート] > [Agilent Technologies] > [リストアユーティリティ] からリストアユーティリティを開始します。		リストアユーティリティを実行するには、システム管理者権限を持っている必要があります。
2 [バックアップロケーション] ページで、バックアップロケーションを選択します。	- バックアップがローカルまたは Windows 共有に配置されている場合、[ファイルシステム] を [バックアップロケーション] として選択します。バックアップユーティリティで使用されたバックアップフォルダーを選択し、[次へ] をクリックします。 - バックアップが Amazon AWS S3 ストレージに配置されている場合、[AWS S3] を [バックアップロケーション] として選択します。AWS S3 バックアップのバケットリージョンおよびバケット名、キーを指定し、[次へ] をクリックします。 - デフォルトでは、[リストアとバリデーション] が選択されています。通常の復旧は、[リストアのみ] を選択します。	- リストアユーティリティはまず Current フォルダーからフルバックアップをリストアして、次に Incremental フォルダーから差分バックアップをリストアします。 - OpenLab ソフトウェアがインストール済みのシステムでのみバリデーションを利用できます。 [バリデーションのみ] を選択した場合、次に [レビュー] ページ、[処理中] ページの順に表示されます。
3 [データベースサーバー] ページの設定は、バックアップされたシステムに基づいて自動入力されています。	- バックアップ以降に現在の環境状態が変化している場合、これらの設定を変更します。 - SQL Server の場合、サーバー名とデータベース管理者資格情報を入力します。 - PostgreSQL の場合、接続設定とデータベース管理者資格情報を入力します。 - リストア中の再コンフィグレーションの詳細については、81 ページの「リストア中の再設定」を参照してください。	Oracle データベースのリストアはサポートされていないため、手動でリストアする必要があります。Oracle データベースのリストア方法は、Oracle のドキュメントを参照してください。
4 [アクセス資格情報] ページの設定は、バックアップされたシステムに基づいて自動入力されています。	- バックアップ以降に現在の環境状態が変化している場合、これらの設定を変更します。 [確認] をクリックして、入力した資格情報が有効であることを確認します。	

リストアユーティリティを使用した既存のインストールへのリストア（続き）

ステップ	オプション	注記
5 [コンテンツパス] ページの設定は、バックアップされたシステムに基づいて自動入力されています。	- この画面は、ファイルシステムストレージロケーションのみ変更できます。 [確認] をクリックして、入力した資格情報が有効であることを確認します。	複数のコンテンツおよびアーカイブロケーションがサポートされています。
6 設定をレビューし、[適用] をクリックします。		[リストア] ページで進行状況が確認できます。
7 [リストア] ページでリストア手順の進行状況を確認できます。	サーバーコンフィグレーションユーティリティの実行ステップで促されたら、Shared Services 管理者の資格情報を入力します。	「リストアとバリデーション」または「バリデーションのみ」を選択した場合、最後にバリデーションのステップが表示されます。バリデーションのステータスにある [完了] リンクをクリックすると、バリデーションレポートが開きます。
8 リストア手順が完了したら、[完了] をクリックします。		
9 リストア後にシステムを再起動します。	システムをすぐに再起動するには、[はい] をクリックします。 再起動を後で手動で実行するには、[いいえ] をクリックします。	インストール済みのシステムでリストアを完了した後は、システムを再起動することをお勧めします。
10 111 ページから開始されるステップ 6 - ステップ 7 を実行します。		

OpenLab Server/ECM XT がインストールされていないクリーンなマシン上のリストア

この手順を使用して、バックアップされた OpenLab Server/ECM XT システムを、OpenLab Server/ECMXT がインストールされていないマシンへリストアします。

注記

MS SQL データベースを使用する場合、リストア手順を実行する前に MS SQL Server をインストールする必要があります。そうしないと、データベースサーバーの設定中にエラーが発生し、リストアプロセスを続行できません。

PostgreSQL の場合、ユーティリティはすべての PostgreSQL データベースを他の ECM XT データと併せてクリーンなシステムにリストアします。リストア完了後にソフトウェアをインストールする必要があります。

クリーンなマシンでリストアユーティリティを使用したリストア手順

ステップ	オプション	注記
1 OpenLab Server/ECM XT Server のインストールメディアから、 [Setup] > [Tools] > [RestoreTool] へ移動し、RestoreUtility.exe を起動します。		ソフトウェアインストールメディアのダウンロードおよび解凍方法については、『OpenLab Server/ECM XT インストールガイド』を参照してください。
2 [バックアップロケーション] ページで、バックアップロケーションを選択します。	- バックアップがローカルまたは Windows 共有に配置されている場合、[ファイルシステム] を [バックアップロケーション] として選択します。バックアップユーティリティによって使用したバックアップロケーションを選択します。 - バックアップが Amazon AWS S3 ストレージに配置されている場合、[AWS S3] を [バックアップロケーション] として選択します。AWS S3 バックアップのバケットリージョンおよびバケット名、キーを指定します。	OpenLab Server/ECM XT がインストールされていないマシンにリストアすると、バリデーションは利用できません。
3 [データベースサーバー] ページの設定は、バックアップされたシステムに基づいて自動入力されています。	- PostgreSQL Server を PostgreSQL がインストールされていないマシンにリストアすると、リストアプロセスを続行するか確認が促されます。[はい] をクリックして続行します。リストア手順が完了して OpenLab Server/ECM XT がインストールされた後に、PostgreSQL がインストールされます。 - Microsoft SQL データベースがコンフィグレーションされている場合、リストア手順を続行するには MS SQL Server がインストールされている必要があります。	- リストア中の再設定の詳細については、81 ページの「リストア中の再設定」を参照してください。 - 自動入力されたサーバー設定を変更しないでください。
4 [アクセス資格情報] ページの設定は、バックアップされたシステムに基づいて自動入力されています。	バックアップ以降に現在の環境状態が変化している場合、これらの設定を変更できます。	
5 [コンテンツパス] ページの設定は、バックアップされたシステムに基づいて自動入力されています。	この画面は、ファイルシステムストレージロケーションのみ変更できます。	複数のコンテンツおよびアーカイブロケーションがサポートされています。
6 設定をレビューし、[適用] をクリックします。		

5 バックアップとリストアの手順

リストア中の再設定

クリーンなマシンでリストアユーティリティを使用したリストア手順（続き）

ステップ	オプション	注記
7 [リストア] ページでリストア手順の進行状況を確認できます。リストア手順が完了したら、[完了] をクリックします。		OpenLab Server/ECM XT ソフトウェアがインストールされたら、「バリデーションのみ」オプションを選択してリストアユーティリティを実行します。これによりデータが確認され、バリデーションレポートが作成されます。

リストア手順が成功したら、OpenLab Server/ECM XT の標準インストールを進めます。リストア手順中にレビューおよび設定されたすべての値は OpenLab Server/ECM XT のインストール中に自動的に取り込まれますので、プロセス中に変更しないでください。

リストア中の再設定

再設定が必要な場合があります。

- データベースのサーバーが別のコンピューターに移動した。
- ポートまたは管理者資格情報が変更された。
- ユーザーが別のサーバーからバックアップをリストアする。
- データベースがサーバー上の別のインスタンスへ移動した。
- ストレージロケーションが変更された。
- Content Management インデックスパスが変更された。

リストア手順中に PostgreSQL および MS SQL の設定を再設定できます。[データベースサーバー] ページで、データベースへの接続に関する読み込み済みの情報が表示されます。このページで変更を行う場合、その情報が正しいことを必ず確認してください。ユーティリティが値を確認し、問題がある場合は詳細なメッセージが表示されます。Oracle データベースの設定の再設定はサポートされていないため、手動で実行する必要があります。

PostgreSQL データベースサーバーの再設定

[データベースサーバー] ページで、サーバー名、ポート、スーパーユーザー、パスワードを変更および確認できます。別のユーザーが使用されている場合、デフォルトのスーパーユーザー（postgres）と同じ権限を持っている必要があります。

入力した値を確認するには、**[確認]** または **[次へ]** をクリックします。

PostgreSQL のデータリポジトリのパスワード再設定

「データベースサーバー」 ページで、PostgreSQL データベースのデータリポジトリのスーパーユーザーのパスワードを変更および確認できます。

入力した値を確認するには、**【確認】** または **【次へ】** をクリックします。

MS SQL データベースサーバーの再設定

「データベースサーバー」 ページで、サーバー名、名前付きインスタンス、ポート、スーパーユーザー、パスワードを変更および確認できます。別のユーザーが使用されている場合、デフォルトのスーパーユーザー（sa）と同じ権限を持っている必要があります。

名前付きインスタンスは、MS SQL Server のインストール時にユーザーが指定する名前です（デフォルトと異なる場合）。

Windows ユーザーを使用する場合、MS SQL Server のセキュリティ設定に追加する必要があります。『OpenLab Server/ECM XT インストールガイド』の「リモートデータベースサーバーのコンフィグレーションに関するセクション」を参照してください。

入力した値を確認するには、**【確認】** または **【次へ】** をクリックします。

アクセス資格情報の再設定

このページで、すべてのコンテンツストレージパスにアクセスするために使用されているアカウントを変更できます。このアカウントが ECM XT Server とデータベースサーバー両方のマシンで **Administrators グループ** にあることを確認してください。

個々のストレージロケーションでの個別のアカウントはサポートされていません。

ユーザーが「サービスとしてログオン」権限を持っていることを確認してください。

入力した値を確認するには、**【確認】** または **【次へ】** をクリックします。

コンテンツパスの再設定

[コンテンツパス] ページで、リストアロケーションに新しいパスを入力して、リストアされたデータのストレージロケーションを変更できます。

リストアロケーションに新しいパスを入力して、新しいインデックスロケーションを指定することもできます。インデックスパスは絶対パスまたは UNC パスである必要があります。

注記

インデックスロケーションにネットワークドライブはサポートされていません。

入力した値を確認するには、**[確認]** または **[次へ]** をクリックします。

リストアのレビューおよび開始

[レビュー] ページで、コンフィグレーションする **OpenLab Server** 設定のサマリーをレビューします。

すべて正しければ、**[適用]** をクリックしてリストアプロセスを開始します。変更する場合は **[戻る]** をクリックします。

バックアップおよびリストアスクリプトの使用

何らかの理由でシステムのバックアップおよびリストアユーティリティが使用できない場合、バックアップおよびリストアスクリプトを使用してバックアップやリストアができます。

オールインワン、2 台のサーバーおよび 4 台のサーバーを使用するトポロジの場合、以降のセクションで説明するバックアップとリストアの各スクリプトを使用してください。スケーラブルトポロジのバックアップおよびリストアは、95 ページの「**手動バックアップとリストアの手順**」で説明する手動バックアップとリストアの手順を使用してください。以下の表に、バックアップおよびリストアスクリプトでサポートされる OpenLab Server/ECM XT のトポロジを記載しています。

表 6 バックアップおよびリストアスクリプトでサポートされる OpenLab Server/ECM XT のトポロジ

トポロジ	バックアップスクリプト	リストアスクリプト	注記
オールインワン	+	+	
2 サーバー	+	+	Oracle データベースのバックアップとリストアは手動で実行
4 サーバー	+	+	Oracle データベースのバックアップとリストアは手動で実行
スケーラブルシステム	手動のみ	手動のみ	

4 サーバートポロジは以下のサーバー構成です。

- OpenLab Server/ECM XT Content Management サーバー（Content Management サーバー）
- OpenLab インデックスサーバー（インデックスサーバー）
- データベースサーバー
- Windows ファイルサーバーおよび / または AWS S3 ストレージ

バックアップおよびリストアスクリプトは以下をサポートします。

- PostgreSQL および Microsoft SQL データベース
- ファイルシステムおよび AWS S3 ストレージ
- ファイルシステムのバックアップ先およびリストア元
- 即時フルバックアップのみ

バックアップやリストア操作を実行する前に、以下のセクションを確認してください。

- 55 ページの「バックアップとリストアに関する重要な情報」
- 57 ページの「障害復旧プランの作成」

注記

Oracle データベースの場合、データベースのバックアップ / リストアはスキップされるため、手動で実行する必要があります。Oracle データベースのバックアップとリストア方法は、Oracle のドキュメントを参照してください。Oracle データベースのバックアップは、システムの他のバックアップより前に実行してください。Oracle データベースの場合、リストア手順は同じ順序で行ってください。

注意

バックアップおよびリストアスクリプトは、システムを保護するためのカスタム証明書をサポートしていません。カスタム証明書を使用した場合、手動でバックアップし、リストアプロセスで使用できるようにセキュリティで保護された場所に保存してください。カスタム証明書は、`C:\Program Files\OpenLab Reverse Proxy\Apache2\conf\ssl\custom` にあります。

リストア後のシステムは、内部証明書を使用して設定されます。カスタム証明書をリストアするには、バックアップしたカスタム証明書を使用し、29 ページの「OpenLab Server/ECM XT リバースプロキシの設定」のステップ 4 に従ってください。4 サーバーまたはスケーラブルシステムのインデックスサーバーの場合、37 ページの「インデックスサーバーコンフィグレーション - 4 サーバーシステムのみ」を参照してください。

システム準備

バックアップおよびリストアスクリプトを開始する前に、システムを構成してください。システムの構成は、以下の説明に従ってください。

- 1 Content Management サーバーで、C:\ProgramData\Agilent Technologies\OpenLab Platform\Data Repository\postgresql\14\data\pg_hba.conf ファイルに以下の行を追加します。
 - host replication postgres 127.0.0.1/32 md5
 - host replication postgres ::1/128 md5
- 2 PostgreSQL の場合、データベースサーバーで、C:\ProgramData\Agilent\PostgreSQLData-14-OLCM\pg_hba.conf ファイルに以下の行を追加します。
 - host replication postgres <CM Node IPv4>/<CM Node IPv4 CIDR> md5
 - host replication postgres <CM Node IPv6>/<CM Node IPv6 CIDR> md5
- 3 インデックスおよびデータベースサーバーで、[セキュリティが強化された Windows Defender ファイアウォール] > [受信の規則] へ移動し、以下の規則を有効にします。
 - ファイルとプリンターの共有 (SMB 受信)
 - ファイルとプリンターの共有 (エコー要求 - ICMPv4 受信)
- 4 Content Management およびインデックスサーバーで、
 - a [セキュリティが強化された Windows Defender ファイアウォール] > [受信の規則] > [新しい規則] へ移動します。
 - b 次のオプションを選択します。**ポート**、**UDP**、**137** を選択し、他のオプションはデフォルト値のままにします。
 - c 名前を設定し、[終了] をクリックします。
 - d 新しい規則が有効になっていることを確認します。
- 5 署名されたスクリプトを実行するよう PowerShell を設定します。
 - a [スタート] > [Windows PowerShell] へ移動します。
 - b [Windows PowerShell] を右クリックし、[その他] > [管理者として実行] を選択します。
 - c 開いた PowerShell ウィンドウで、コマンドを実行します：
Set-ExecutionPolicy -ExecutionPolicy AllSigned -Scope LocalMachine [実行ポリシーを変更しますか?] という質問が表示された場合、**A** を入力して **Enter** をクリックします。

注意

バックアップ / リストアスクリプトの開始ユーザーは、Content Management、データベース、およびインデックスサーバーの管理者である必要があります。ユーザーは、コンテンツおよびアーカイブのストレージロケーションと、さらにバックアップロケーションにアクセスできる（読み取りおよび書き込み権限が付与されている）必要があります。

注記

バックアップおよびリストアスクリプトは .zip アーカイブとして提供されます。Content Management サーバーに .zip ファイルをアップロードしてください。展開する前にファイルを右クリックし、**【プロパティ】** > **【全般】** へ移動して、**【セキュリティ】** セクションに **【ブロック解除】** のチェックボックスがないことを確認してください。**【セキュリティ】** セクションに **【ブロック解除】** チェックボックスが表示されている場合、**【ブロック解除】** チェックボックスをオンにして **【適用】** をクリックしてください。

バックアップスクリプトを使用する OpenLab Server/ECM XT のバックアップ

サポートされるバックアップシナリオ

システムでバックアップスクリプト（Secure_OpenLABCDS_backup.ps1）を実行して、以下のデータをバックアップできます。

- Content Management およびインデックスサーバーのコンフィグレーションファイル
- Shared Services、Content Management、およびデータリポジトリのデータベース
- Solr インデックス
- コンテンツおよびアーカイブストレージ
- Alfresco キャッシュ
- Certificate Service の証明書

必要な領域

バックアップ処理に必要な空き領域は、サーバーコンフィグレーション、バックアップロケーション、データベースのバックアップサイズなど、さまざまな要因によって異なります。最もリソースの消費量が多いケースでは、バックアップのロケーションの空き領域が、すべてのオンプレミスファイルストレージとデータベースサイズの合計の少なくとも 2 倍あることを確認してください。以前成功したバックアップが、何らかの理由で途中で終了したバックアップに上書きされるのを避けるために必要です。

バックアップスクリプトの使用手順

Content Management サーバーで Windows PowerShell を使用して、Secure_OpenLABCDS_backup.ps1 スクリプトを実行してバックアップ手順を実行します。

- 1 [スタート] > [Windows PowerShell] へ移動し、[Windows PowerShell] を右クリックして、[その他] > [別のユーザーとして実行] を選択します。
- 2 ダイアログウィンドウが開いたら、バックアップを実行するユーザーのログインとパスワードを設定します。[OK] をクリックします。
- 3 PowerShell ウィンドウに以下のコマンドを入力して、権限モードでスクリプトを実行します。

```
Start-Process -FilePath "powershell" -Verb RunAs
```

 ユーザーアカウント制御アクセスのリクエストが表示された場合、[はい] をクリックします。
- 4 PowerShell ウィンドウが新たに開いたら、バックアップスクリプトがあるフォルダーへ移動します（デフォルトでは、C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts）。
 たとえば、コマンド：cd "C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts" を使用します。
- 5 Secure_OpenLABCDS_backup.ps1 スクリプトを実行します。パラメータを入力します。

```
.\Secure_OpenLABCDS_backup.ps1 -backupDestinationDir "<destination_path>" [-hotBackup]
```

以下のパラメータを使用します。

- <destination path> - バックアップ先のパス。例：C:\BackupDir スクリプトでは絶対ローカルフォルダーおよびネットワーク共有パスがサポートされます。
 - [hotBackup] - ホットバックアップまたはコールドバックアップセットを選択するためのオプションのパラメータ。デフォルトでは、パラメータはなく、コールドバックアップが実行されます。ホットバックアップの場合、バックアップ中もシステムは稼働したままとなります。コールドバックアップの場合、バックアップが開始する前にすべての OpenLab Server/ECM XT の操作が自動的に停止し、バックアップが完了した後に実行されます。
- 6 バックアップスクリプトが終了するまでお待ちください。バックアップが成功した場合、「Backup has completed」というメッセージが表示され、バックアップフォルダーが<destination_path> ロケーションに作成されます。

バックアップが失敗した場合、バックアップロケーションの Temp フォルダにバックアップの一部が保存されます。バックアップが失敗することで、Current フォルダにある以前成功したバックアップが上書きされたり壊れたりすることはありません。

バックアップのトラブルシューティング

バックアップスクリプトを実行すると、%AppData%\Agilent\LogFiles\Backup フォルダに "Backup_log_" の接頭語と末尾にタイムスタンプが付いて実行ログが書き込まれます。スクリプトが失敗した場合、「The backup has failed.」というメッセージがログに表示され、現在の実行のログファイルパスが提供されます。現在のバックアップログファイルは問題を特定するのに役立ちます。バックアップが失敗した場合、バックアップロケーションの Temp フォルダにバックアップの一部が保存されます。

スクリプト実行エラーが発生した場合、以下の手順に従ってください。

- 1 バックアップ手順を実行する前に、必要なシステムコンポーネントである 86 ページの「**システム準備**」のすべてのアクションが実行されていることを確認します。
- 2 86 ページの「**システム準備**」に従って、スクリプトを実行するユーザーが適切な権限を持っていることを確認します。
- 3 すべてのマシンが作動し、スクリプトを実行したマシンからアクセスできることを確認します（データベースサーバー、インデックスサーバー、Windows ファイルサーバーなど）。
- 4 データベースサーバーアカウントに、データベース管理者権限 / スーパーユーザーがあることを確認します。
- 5 ウィルス対策スキャンによってバックアップが正常に完了できなくなっていないことを確認します。定期的 / スケジュール済みスキャンとリアルタイム保護の両方でバックアップロケーションを除外します。
- 6 Content Management およびデータベースサーバーに C ドライブのスペースが十分あることを確認します。C ドライブに一時的なデータベースバックアップ用の十分なスペースがない場合、他のローカルドライブをこのために使用できます。これを行うには、94 ページの「**バックアップとリストア手順の一時的なデータベースロケーションの変更**」の説明に従います。
- 7 上記のステップで問題が解決しない場合、%AppData%\Agilent\LogFiles\Backup フォルダからログファイルを取得し、Agilent のサポート部門にご相談ください。

リストアスクリプトを使用する OpenLab Server/ECM XT のリストア

このセクションでは、リストアスクリプトを使用するオールインワン、2 サーバー、および 4 サーバートポロジのリストア方法について説明します。

サポートされるリストアシナリオ

リストアスクリプト（Secure_OpenLABCDS_restore.ps1）は、以下の環境で実行できます。

- 障害が発生した後に既存のシステムをリストアするため、バックアップ時点のデータにリストアする
- 新しいクリーンな（OpenLab/ECM XT サーバーがインストールされていない）システムにバックアップからシステムをリストアする
- 新しくインストールした環境にバックアップからシステムをリストアする
- サポートされるすべてのケースで、追加のソフトウェアをインストールせずにスクリプトを実行できます。

注意

データベースサーバー、インデックスノード、およびデータストレージサーバーは、バックアップの時点と同じ名前にしてください。バックアップから `installation¥configuration.xml` ファイルを確認して、データベースサーバー、インデックスノード、およびストレージロケーションの名前を取得できます。

リストアスクリプトの使用手順

サポートされるトポロジのリストア手順を実行するには、Content Management サーバーとして使用しているマシンで Windows PowerShell を使用して Secure_OpenLABCDS_restore.ps1 スクリプトを実行します。

注記

リストア手順を実行する前に、必要なシステムコンポーネントである 86 ページの「**システム準備**」のすべてのアクション実行されていることを確認します。

- 1 [スタート] > [Windows PowerShell] へ移動し、[Windows PowerShell] を右クリックして、[その他] > [別のユーザーとして実行] を選択します。
- 2 ダイアログウィンドウが開いたら、バックアップを実行するユーザーのログインとパスワードを設定します。[OK] をクリックします。

- 3 PowerShell ウィンドウに以下のコマンドを入力して、権限モードでスクリプトを実行します。
`Start-Process -FilePath "powershell" -Verb RunAs`
ユーザーアカウント制御アクセスのリクエストが表示された場合、**[はい]**をクリックします。
- 4 PowerShell ウィンドウが新たに開いたら、リストアスクリプトがあるフォルダーへ移動します（インストール済みシステムのデフォルトでは、C:¥Program Files (x86)¥Agilent Technologies¥OpenLab Backup Utility¥Backup and Restore Scripts）。
たとえば、コマンド：cd "C:¥Program Files (x86)¥Agilent Technologies¥OpenLab Backup Utility¥Backup and Restore Scripts" を使用します。
クリーンなシステムにリストアする場合、以下のメディアでスクリプトを検索します。¥Setup¥Scripts¥Server Restore
- 5 Secure_OpenLABCDS_restore.ps1 スクリプトを実行し、バックアップロケーションを指定します。
¥Secure_OpenLABCDS_restore.ps1 -backupDir "<path_to_backup>"
<path_to_backup> は、保存されたバックアップのファイルシステムパスです。スクリプトでは絶対ローカルフォルダーおよびネットワーク共有パスがサポートされます。
- 6 スクリプトが終了するまでお待ちください。リストアが成功した場合、「The restore has completed」というメッセージが表示されます。
- 7 システムを再起動します。

注記

ECM XT サーバーがインストール済みのシステムでリストア手順を実行する場合、サーバーコンフィグレーションユーティリティの実行中に ECM XT 管理者資格情報を要求するウィンドウが表示される可能性があります。このウィンドウは、前回のサーバーコンフィグレーションユーティリティの実行以降に ECM XT 管理者資格情報を変更した場合に表示されます。

注記

4 サーバーまたはスケーラブルシステムの場合、リストア後にインデックスサーバーに対してシステムコンフィグレーションユーティリティを実行してシステム設定を適用してください。

注記

インストール済みの ECM XT サーバーでリストアする場合で、Content Management サーバー名がバックアップで使った名前と異なる場合、以下を行う必要があります。

- Shared Services コントロールパネルを開き、Content Management サーバーで新しいサーバー名で Content Management をアクティブ化します。
- インデックスノードマシンへ移動し、サーバーコンフィギュレーションユーティリティを実行してシステム設定を適用します。

注記

-backupDir パラメータが指定されていない場合、スクリプトにバックアップのパスを指定するよう促されます。バックアップのパスを入力して **Enter** を押します。

リストアのトラブルシューティング

リストアスクリプトを実行すると、%AppData%\Agilent\LogFiles\Restore フォルダに "Restore_log_" の接頭語と末尾にタイムスタンプが付いて実行ログが書き込まれます。スクリプトが失敗した場合、「The restore procedure has failed.」というメッセージがログに印刷され、現在の実行のログファイルパスが提供されます。

スクリプト実行エラーが発生した場合、以下の手順に従ってください。

- 1 リストア手順を実行する前に、必要なシステムコンポーネントである 86 ページの「**システム準備**」のすべてのアクション実行されていることを確認します。
- 2 86 ページの「**システム準備**」に従って、スクリプトを実行するユーザーが適切な権限を持っていることを確認します。
- 3 すべてのマシンが作動し、スクリプトを実行したマシンからアクセスできることを確認します（データベースサーバー、インデックスサーバー、Windows ファイルサーバーなど）。
 - データベースサーバー、インデックスサーバー、および Windows ファイルサーバーは、バックアップ時と同じ名前にしてください。バックアップから Installation\configuration.xml ファイルを確認して、データベースサーバー、インデックスサーバー、およびストレージロケーションの名前を取得できます。
- 4 バックアップ時に使用されたデータベースサーバーアカウントがデータベースサーバーと同じ資格情報で存在し、データベース管理者権限 / スーパーユーザーを持っていることを確認します。

- 5 Content Management およびデータベースサーバーの C ドライブに十分なスペースがあることを確認します。C ドライブに一時的なデータベースバックアップ用の十分なスペースがない場合、他のローカルドライブをこのために使用できます。これを行うには、94 ページの「**バックアップとリストア手順の一時的なデータベースロケーションの変更**」の説明に従います。

トラブルシューティングのステップで問題が解決しない場合、
%AppData%\Agilent\LogFiles\Restore フォルダーからログファイルを取得し、
Agilent のサポート部門にご相談ください。

バックアップとリストア手順の一時的なデータベースロケーションの変更

デフォルトでは、バックアップ / リストアスクリプトは C:\ProgramData\Agilent\Backup および C:\ProgramData\Agilent\Restore フォルダを使用し、バックアップ / リストア手順時にデータベースのバックアップを保存します。データベースバックアップには、C ドライブに一時的なロケーション用の十分な空き領域が必要です。C ドライブのスペースが十分な大きさでなく、このためにバックアップ / リストアが失敗した場合、別のローカルドライブを使用できます。これを行うには、LinkTempFolderForBackupAndRestoreDatabase.ps1 スクリプトを実行します。デフォルトで C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts にあります。

注記

リモート MSSQL の場合、"LinkTempFolderForBackupAndRestoreDatabase.ps1" スクリプトはデータベースサーバーで実行されます。それ以外の場合は、Content Management サーバーで実行されます。スクリプトは 1 回実行されます。

LinkTempFolderForBackupAndRestoreDatabase.ps1 スクリプトを使用して一時的なデータベースバックアップロケーションを変更するには、

- 1 [スタート] > [Windows PowerShell] へ移動し、[Windows PowerShell] を右クリックして、[その他] > [管理者として実行] を選択します。
- 2 PowerShell ウィンドウが開いたら、スクリプトがあるフォルダへ移動します（デフォルトでは、C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Scripts）。

たとえば、コマンド：cd "C:\Program Files (x86)\Agilent Technologies\OpenLab Backup Utility\Backup and Restore Script" を使用します。

- 3 以下のコマンドを実行します。
 .\LinkTempFolderForBackupAndRestoreDatabase.ps1
 -tempFolderForBackupAndRestoreDatabase "<new_temporary_DB_path>"

以下のパラメータを使用します。

<tempFolderForBackupAndRestoreDatabase> - 新しい一時的なデータベースバックアップロケーション。ローカルパスのみサポートされます。例："E:\New temp folder"

- 4 スクリプトが終了するまでお待ちください。

6

手動バックアップとリストアの手順

OpenLab Server/ECM XT Server の手動バックアップ手順 96

OpenLab Server/ECM XT Server の手動リストア手順 105

異なるサーバー間の手動バックアップの データ移行 115

OpenLab Server/ECM XT Server の手動バックアップ手順

すべての OpenLab Server/ECM XT Server を必ず定期的にバックアップしてください。定期的なフルバックアップと、フルバックアップの間に実行する差分バックアップは、OpenLab Server/ECM XT Server 管理者が作成する必要があります。これらのバックアップは、ハードウェアまたはソフトウェアの不具合が発生したときに OpenLab Server/ECM XT Server をリストアする唯一の方法です。

致命的なシステム障害が発生した場合、バックアップはデータ損失量を軽減します。バックアップを実施することで、バックアップの時点で収容されたデータをリストアすることができるよう保証されます。アップロード待ちでまだ収容されていないデータや、バックアップを実施した後にシステムに追加または更新されたデータは、バックアップをリストアしても修復できません。

バックアップが正しく実施され、リストアに使用できることを確認するには、必ずリストア手順（105 ページの「**OpenLab Server/ECM XT Server の手動リストア手順**」）もテストする必要があります。有効なリストアを実行するには、障害復旧プランの作成が必要です。

OpenLab Server/ECM XT は、ファイルとインデックスをサーバーのファイルシステムに保存します。フォルダーの場所は、製品のインストール時に決定します。フォルダー情報、監査証跡、署名などのその他のデータは、リレーショナルデータベースに保存されます。

フルバックアップは、アップロードしたファイルやそのデータベースも含めて、OpenLab Server/ECM XT 内のすべてのデータを取り込みます。差分バックアップは、前回のフルバックアップ以降に発生した変更だけをバックアップします。差分バックアッププロセスは、変更された要素だけをバックアップするので、フルバックアップよりも短時間で行えます。

サーバーをアップグレードする場合は、アップグレードする前にマシンで以下の手順を実行してください。アップグレードの前に、すべての作業領域とファイルアップロードキューをクリアしてください。異なる OS へのアップグレードを実行する場合は、キューにデータがないようにしてください。すべてのファイルアップロードを完了してください。アップグレードの前に、ファイルバッファアアップロードキューをクリアしてください。

手動システムバックアップの実行

ステップ 1：データベース、コンテンツフォルダー、インデックスフォルダーの確認

OpenLab Server/ECM XT のバックアップやリストアを行うには、データベースの名前、保存されているコンテンツフォルダーの場所、保存されているインデックスフォルダーの場所、インストールやコンフィグレーションに関するその他の情報を確認する必要があります。

バックアップする必要があるデータベースは 2 つあります。OpenLab Server/ECM XT Server のデータベースと、Shared Services データベースです。これらのデータベースの名前は、[サーバーコンフィグレーション] ページから取得できます。

同様に、コンテンツフォルダーのパスも、サーバーのインストール時に指定するパラメータの 1 つです。以下の手順からパスを確認できます。

- 1 OpenLab Server/ECM XT Server マシンに移動します。
- 2 [スタート] > [Agilent Technologies] > [サーバーコンフィグレーションビューア] をクリックします。

ウェブページが表示され、Content（コンテンツストア）、Index（インデックス）、Archive（オフラインアーカイブ）のパスが提供されます。

Content Management Content Summary	
Server Configuration	Content Management with Index and Search Services
Primary Content Storage Location	C:\DataStoreContent
Secondary Content Storage Location(s)	None
Primary Archive Storage Location	C:\DataStoreArchive
Secondary Archive Storage Location(s)	None
Index Path	C:\DataStoreIndex
Index hostname	

図 3 OpenLab Server/ECM XT Server コンテンツサマリー

注記

トポロジーに個別のインデックスノードサーバーがある場合、そのインデックスノードサーバーにインデックスパスがある場合があります。

リポジトリに複数のコンテンツストアがある場合、追加の各コンテンツストアをバックアップする必要があります。システムに複数のコンテンツストアがあるかどうかと、それらの場所を確認するには：

- 1 <INSTALLATION PATH>%OpenLab Data Store%tomcat%shared%classes から **alfresco-global.properties** ファイルを開きます（デフォルトの場所は、OpenLab Server/ECM XT Server の C:\Program Files (x86)\Agilent Technologies\OpenLab Data Store\tomcat\shared\classes ディレクトリです）。

- 2 **dir.root** プロパティを検索します。複数のコンテンツストアがある場合、下記のように一覧表示されます。ここでは2つのコンテンツストアが定義されています。

```
dir.root=¥¥¥¥HA-ContentStore¥¥ContentStore# content store 1
dir2.root=¥¥¥¥HA-ContentStore¥¥ContentStore2 # content store 2 (current)
```

ステップ 2：OpenLab Server/ECM XT サービスの停止

Windows サービス (services.msc) を開いて、次のサービスを停止します。

- Agilent OpenLab Content Management Search service
無効になっている場合はこのサービスをスキップします。
- alfrescoTomcat
- Agilent OpenLab Shared Services
- olcm-postgresql-x64-14 (OpenLab Server/ECM XT 用 PostgreSQL データベースを使用している場合のみ)。データベースが別のホスト上にある場合はこのサービスをスキップします。

注記

トポロジーに複数の ECM XT Server または個別のインデックスノードサーバーがある場合、すべての ECM XT Server でこれらのサービスを停止してください。

MSSQL サーバーまたは Oracle の場合、サービスの停止方法に関するベンダーのデータベースドキュメントを参照してください。データベースが別のホスト上にある場合は、そのホスト上でこのステップを実行する必要があります。

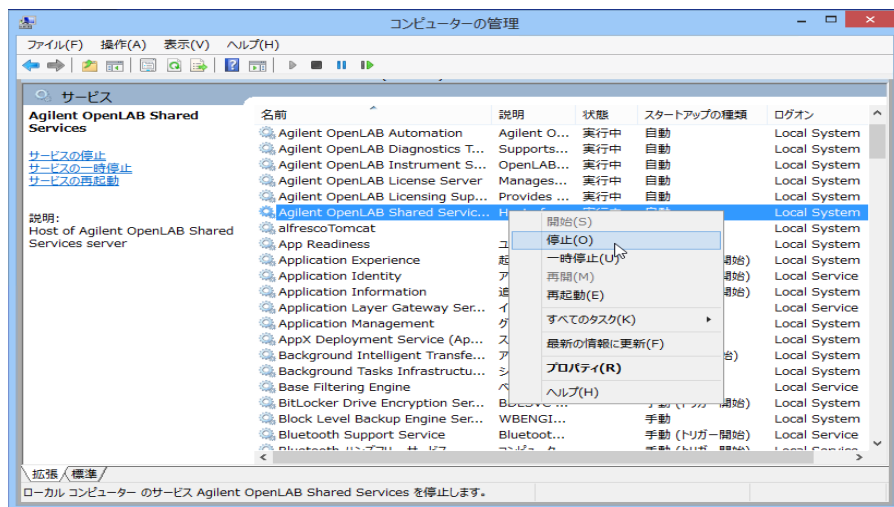


図4 OpenLab Server/ECM XT サービスの停止

ステップ 3：データベースのバックアップ

このセクションでは、データベースをバックアップする簡単にインタラクティブな方法について説明します。その他のオプション（プロセスを自動化できる方法など）については、PostgreSQL、MS SQL Server または Oracle のドキュメントを参照してください。

PostgreSQL での手順 データベースファイルの保存場所は、サーバーのインストール時に指定済みです。ローカル PostgreSQL データベースの場合、デフォルトでは、C:\ProgramData\Agilent\PostgreSqlData-14-OLCM です。インストール時にカスタマイズした場合は、保存場所の情報はサーバーコンフィグレーションで確認できます（[スタート] > [Agilent Technologies] > [サーバーコンフィグレーションビューア]）。

この情報は、次の場所にある Windows レジストリにも記録されています。

```
"HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\Installations\postgresql-x64-14\Data Directory".
```

リモート PostgreSQL データベースの場合、この情報は次の場所にある Windows レジストリに記録されています。

```
"HKEY_LOCAL_MACHINE\SOFTWARE\PostgreSQL\Installations\postgresql-x64-14\Data Directory"
```

PostgreSQL データベースをバックアップするために、

Windows Server バックアップなどの好みのツールを使ってデータベースフォルダー（C:\ProgramData\Agilent\PostgreSqlData-14-OLCM）をバックアップします。

注意

PostgreSQL 14.1 より前のバージョンを使用しているサーバーで、システムを同じロケーションで最新バージョンにアップグレードした場合、PostgreSQL データベースはバージョン 14.1 にアップグレードされ、データベースのデータは C:\ProgramData\Agilent\PostgreSqlData-14-OLCM に移行されます。バックアップとリストアアクティビティはアップグレードしたシステムで行ってください。

MS SQL Server での手順 MSSQL サービスが起動されていることを確認します。**SQL Server Management Studio** を使用して、Shared Services データベース（OLSharedServices）と OpenLab Server/ECM XT Server データベース（DataStore）をバックアップします。このツールを使用すると、**フルバックアップ**と**差分バックアップ**の両方を実施できます。

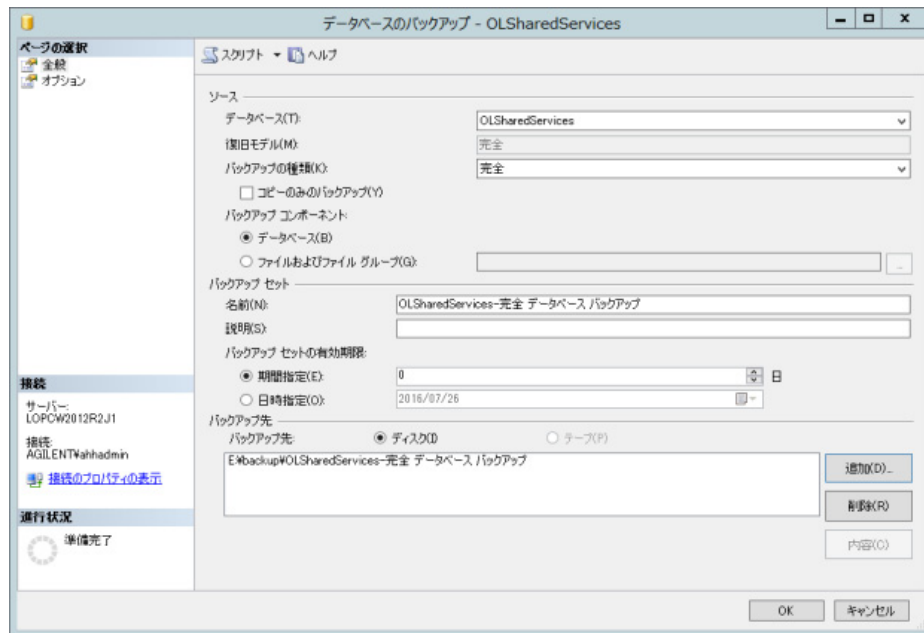


図 5 SQL Server Management Studio を使用したバックアップ

Oracle サーバーでの手順 Oracle データベースのバックアップについては、Oracle のドキュメントを参照してください。

ステップ 4：コンテンツフォルダー、インデックスフォルダー、およびアーカイブフォルダーのバックアップ

Windows Server バックアップなど、好みのツールを使って、OpenLab Server/ECM XT のコンテンツフォルダー（C:¥DataStoreContent）、インデックスフォルダー

（C:¥DataStoreIndex）、およびアーカイブフォルダー

（C:¥DataStoreArchive）をバックアップします。

トポロジーに個別のインデックスノードサーバーがある場合、そのインデックスノードからインデックスをバックアップします。

複数のコンテンツストアがある場合、追加のコンテンツフォルダー（D:¥DataStoreContent2）ごとにバックアップする必要があります。

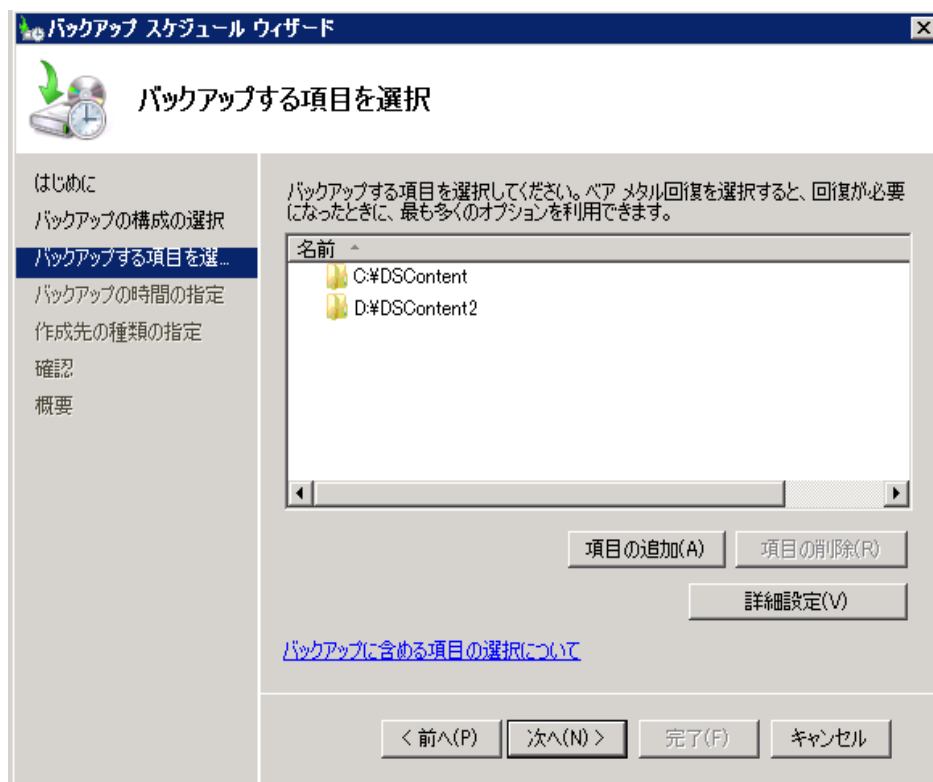


図 6 Windows Server バックアップの使用

ステップ 5：OpenLab Server/ECM XT Server コンフィグレーション情報のバックアップ

- 1 <Installation Directory>%OpenLab Data Store%\tomcat%\temp%\com.agilent.datastore.cache ファイルを、 C:%ProgramData%\Agilent%\Installation フォルダーにコピーします。

<Installation Directory> は、[サーバーコンフィグレーション] ページの [Installation Summary] で確認できます。

- 2 C:%ProgramData%\Agilent%\Installation フォルダーをバックアップします。これは、後でシステムを再構成するために使用されます。

注記

トポロジーに個別のインデックスノードサーバーがある場合、そのインデックスノードサーバーにインデックスパスがある場合があります。

注記

トポロジーに複数の ECM XT Server または個別のインデックスノードサーバーがある場合、すべての ECM XT およびインデックスノードサーバーからこれらのファイルをバックアップします。

ステップ 6：カスタム証明書のバックアップ

セキュリティで保護された接続用にカスタム証明書を使用している場合、これらの証明書をバックアップします。 C:%Program Files%\OpenLab Reverse Proxy%\Apache24%\conf%\ssl%\custom% フォルダーをバックアップロケーションにコピーします。

ステップ 7：OpenLab 証明書サーバーのバックアップ

C:%ProgramData%\Agilent%\OpenLab Certificate Service フォルダーをバックアップロケーションにコピーします。

ステップ 8：OpenLab Server/ECM XT サービスの開始

Windows サービス (services.msc) を開いて、次のサービスを開始します。

- olcm-postgresql-x64-14 (OpenLab Server/ECM XT 用 PostgreSQL データベースを使用している場合のみ)。データベースが別のホスト上にある場合はこのサービスをスキップします。
データベースが別のホスト上にある場合は、そのホスト上でこのステップを実行する必要があります。
- Agilent OpenLab Shared Services
- alfrescoTomcat
- Content Management Search service 無効になっている場合はこのサービスをスキップします。

注記

Sample Scheduler を使用する場合、リストア手順の後に Sample Scheduler サービスを再起動する必要があります。

注記

トポロジーに複数の ECM XT Server または個別のインデックスノードサーバーがある場合、すべての ECM XT およびインデックスノードサーバーでこれらのサービスを開始します。

データリポジトリデータベースの手動バックアップ

データリポジトリは、PowerShell スクリプトによる自動バックアップと手動での回復をサポートしています。データリポジトリのバックアップとリストア手順では、圧縮されたカスタムバックアップファイルへのフルデータベースバックアップと、そのカスタムバックアップファイルからのフルデータベースリストアが可能です。この手順は、組み込みコマンド `pg_dump` および `pg_restore` に依存しています。

スケジュールされたバックアップをサポートするため、Data Repository 1.4 ではユーザー資格情報を暗号化形式で Windows Registry に保存します。

この手順を完了するには、以下が必要となります。

- データリポジトリの権限内でインストールおよび構成された PostgreSQL データベース
- すべてのデータベースオブジェクトの読み取り権限
- バックアップターゲットフォルダーへの書き込み権限

注記

スクリプト実行時の不要なエラーを回避するために、制限しないモードで PowerShell を実行してください。以下のコマンドを使用すると、強制的に制限されないスクリプト実行となります。

```
PowerShell.exe Set-ExecutionPolicy UnRestricted -Force
```

管理者は、グループポリシーを使用して実行ポリシーのバイパスを防ぐことができます。この場合は、PowerShell スクリプトは実行できません。

注記

トポロジーに複数の ECM XT Server または個別のインデックスノードサーバーがある場合、すべての ECM XT Server でこれらのサービスを停止してください。

バックアップの作成

データリポジトリのバックアップスクリプトは、以下のデータリポジトリインストールフォルダーにあります。

```
C:\Program Files (x86)\Agilent Technologies\OpenLab Platform\Data
Repository\Data Repository\Service\Scripts\PostgreSQL\Backup
\dr-db-backup.ps1
```

SYNOPSIS

Agilent Technologies - OpenLab Data Repository Backup Utility

SYNTAX

```
dr-db-backup.ps1
[[-hostname] <String>]
[[-port] <String>]
[[-database] <String>]
[[-path] <String>]
```

DESCRIPTION

実行中の PostgreSQL データベースのバックアップを pg_dump カスタム圧縮形式で作成します。

PARAMETERS

```
-hostname <String>
    PostgreSQL サーバーを指定します。
-port <String>
    PostgreSQL サーバーポートを指定します。
-database <String>
    PostgreSQL データベースを指定します。
-path <String>
    バックアップディレクトリを指定します。
```

バックアップの呼び出し例

```
./dr-db-backup -path c:\temp
```

バックアップ出力

このスクリプトでは、組み込みコマンド **pg_dump** を使用して完全な PostgreSQL バックアップを作成し、カスタムバックアップ（ファイル形式 **.bakpgdc**）に結果を保存します。これは、目次を含めたすべてのデータベースオブジェクトの圧縮されたアーカイブファイルです。

バックアップ操作が成功した場合、終了コードは **0** になります。バックアップディレクトリが無効の場合、終了コードは **2** になります。その他のエラーではエラーコードは **1** になります。

OpenLab Server/ECM XT Server の手動リストア手順

ハードウェアやソフトウェアの不具合により OpenLab Server/ECM XT Server が操作不能になった場合、次の手順を実行して既存のバックアップファイルからシステムをリストアします。

サーバーをアップグレードする場合、アップグレード後に以下の手順を実行してください。

リストア手順は、成功したバックアップで取り込まれたコミット済みデータのみリストアします。アップロード待ちでまだ収容されていないデータや、バックアップを実施した後にシステムに追加または更新されたデータは、バックアップをリストアしても修復できません。

ステップ 1：データベースのリストア

PostgreSQL サーバーでの手順 データベースフォルダー（例えば **C:\ProgramData\Agilent\PostgreSqlData-14-OLCM**）を特定し、バックアップからそのフォルダーに PostgreSQL データベースをリストアします。その後の設定を簡単にするため、オリジナルのパスを維持することをお勧めします。

注意

PostgreSQL 14.1 より前のバージョンを使用しているサーバーで、システムを同じロケーションで最新バージョンにアップグレードした場合、PostgreSQL データベースはバージョン 14.1 にアップグレードされ、データベースのデータは **C:\ProgramData\Agilent\PostgreSqlData-14-OLCM** に移行されます。バックアップとリストアアクティビティはアップグレードしたシステムで行ってください。

MS SQL サーバーでの手順 次の手順を使用してデータベースをリストアし、リストアされた各データベースの設定を変更します。

データベースのリストア

SQL Management Studio を使用して、Shared Services データベース（OLSharedServices）と OpenLab Server/ECM XT Server のデータベース（DataStore）をリストアします。

SQL Management Studio を使用した Shared Services データベース設定の構成

- 1 **[Shared Services データベース] > [セキュリティ] > [ユーザー]**
でデータベースユーザーを確認します（ユーザーをレビューして既存のユーザーを再使用するか、ユーザーを削除して新しいユーザーを作成します）。
- 2 ステップ 1 で使用したデータベースユーザーに db_owner が付与されているか確認します。
- 3 MS SQL Server ログインの確認
 - a **[セキュリティ] > [ログイン]** に移動します。
 - b Shared Service ログインユーザーが MS SQL Server 上に存在することを確認します（必要な場合は作成します）。

MS SQL Server 認証を使用したインストール手順のステップ 2 で使用したログインが存在することを確認してください。

インストール手順のステップ 2 で Windows 認証を使用した場合、以下の定義されたログインユーザーを確認してください。
 - ローカル MS SQL Server データベースの場合（MS SQL Server と ECM XT Server が同じマシンにインストールされている）、'NT AUTHORITY\SYSTEM' ログインを使用します。
 - リモート MS SQL Server データベースの場合（MS SQL Server と ECM XT Server が 2 台の別のマシンにインストールされている）、Windows ログインから 'DOMAIN\ECM XT Server machine name\$' を使用します。（たとえば、ドメインが Agilent で ECM XT Server が 'ECMServer' のマシンにインストールされている場合、Windows ログインから 'Agilent\ECMServer\$' を使用 / 作成してください）。
- 4 MS SQL Server ログインで Shared Service ユーザーをマッピングします。
 - a OLSharedServices データベースの **[マップ]** を選択します。
 - b MS SQL ログインをステップ 1 の Shared Services データベースユーザーにマッピングします。

SQL Management Studio を使用した、DataStore データベース設定の構成

- 1 **[DataStore データベース] > [セキュリティ] > [ユーザー]** でデータベースユーザーを確認します（ユーザーをレビューして既存のユーザーを再使用するか、ユーザーを削除して新しいユーザーを作成します）。
- 2 ステップ 1 で使用したデータベースユーザーに db_owner が付与されているか確認します。
- 3 MS SQL Server ログインを確認します。
 - a **[セキュリティ] > [ログイン]** に移動します。
 - b インストール手順のステップ 2 で使用した DataStore ログインユーザーが MS SQL Server 上に存在することを確認します（必要な場合は作成します。）

- 4 MS SQL Server ログインで DataStore ユーザーをマッピングします。
 - a DataStore データベースの **【マップ】** を選択します。
 - b MS SQL ログインをステップ 1 の DataStore データベースユーザーにマッピングします。

Oracle サーバーでの手順 バックアップファイルからのデータベースのリストアについては、Oracle のドキュメントを参照してください。

データリポジトリデータベースのリストア この手順を完了するには、以下が必要となります。

- データリポジトリを使用してインストールおよび構成された PostgreSQL データベース
- 指定されたバックアップの対象となっているすべてのアプリケーションが、それらのドキュメントに従ってインストールされ データリポジトリに登録されている
- バックアップディレクトリへの読み取りおよび書き込み権限

バックアップのリストア データリポジトリのリストアスクリプトは、以下のデータリポジトリインストールフォルダーにあります。

C:¥Program Files (x86)¥Agilent Technologies¥OpenLab Platform¥Data Repository¥Data Repository¥Service¥Scripts¥PostgreSQL¥Backup

SYNOPSIS

Agilent Technologies - OpenLab Data Repository Restore Utility

SYNTAX

```
dr-db-restore.ps1
[[-hostname] <String>]
[[-port] <String>]
[[-database] <String>]
[-path] <String>
[-quiet]
```

DESCRIPTION

実行中の PostgreSQL データベースのバックアップを pg_dump カスタム圧縮形式を使用してリストアします。

PARAMETERS

```
-hostname <String>
    PostgreSQL サーバーを指定します。
    - optional, default: 'localhost'
-port <String>
    PostgreSQL サーバーポートを指定します。
    - optional, default: 5433
-database <String>
    PostgreSQL データベースを指定します。
    - optional, default: 'datarepo'
-path <String>
    バックアップディレクトリを指定します。
-quiet
    ユーザーの操作なしでリストアが実行されます。
    - optional
```

リストアの呼び出し例 `./dr-db-restore -path c:¥temp`

リストア出力 データリポジトリでは、組み込みコマンド **pg_restore** を使用し、ターゲットディレクトリパスにある最新のバックアップファイルから開始して、カスタム PostgreSQL データベースのバックアップ **pg_dump** をリストアします。

パラメータ **-quiet** を指定すると、データリポジトリはユーザーの操作なしで最新のバックアップをリストアします。

バックアップ操作が成功した場合、終了コードは **0** になります。バックアップディレクトリが無効の場合、終了コードは **2** になります。その他のエラーではエラーコードは **1** になります。

ステップ 2：コンテンツフォルダー、インデックスフォルダーおよびアーカイブフォルダーのリストア

OpenLab Server/ECM XT のコンテンツフォルダー（**C:¥DataStoreContent**）、インデックスフォルダー（**C:¥DataStoreIndex**）、およびアーカイブフォルダー（**C:¥DataStoreArchive**）の場所を指定し、バックアップからそれらのフォルダーをリストアします。その後の設定を簡単にするため、オリジナルのパスを使用することをお勧めします。

複数のコンテンツ保存がある場合、追加のコンテンツ保存ごとにそれぞれの場所にリストアする必要があります。

ストレージが共有ネットワークリソースにあるトポロジーの場合、ストレージをリストアした後、サーバーに対するアクセス許可をリストアするか、それらの許可が問題なく利用できるか確認する必要があります。

アクティビティログインデックスの再構築 アクティビティログテーブルまたはデータが破損した場合や Shared Services データベースが既存の OpenLab インストールでリストアされている場合に、次の手順で OpenLab Shared Services アクティビティログインデックスを再構築します。

アクティビティログインデックスは以下の状況で自動的に再構築されます。

- Firebird データベースを用いたファイルベースのワークステーションコンフィグレーションを使用している
- Shared Services データベースが新たなインストールでリストアされている
- データを移行またはアップグレードしている

インデックスの再構築に要する時間は、データベースのタイプとアクティビティログレコード数によって異なります。数時間かかることもあります。処理中は、アプリケーションでアクティビティログの検索はできません。

アクティビティログを再構築するには、

- 1 管理者としてコマンドプロンプトを開始します。
- 2 以下のコマンドを実行します。

```
net stop SharedServicesHost && del /s /f /q
%ProgramData%\Agilent\OLSS¥Index¥ActivityLog && net start
SharedServicesHost
```

以下のエラーが発生する可能性があります。

- **メッセージ**

Agilent OpenLab Shared Services サービスは開始されていません。 *NET HELPMSG 3521* と入力すると、より詳しい説明が得られます。

解決策

以下のコマンドを使用します。

```
del /s /f /q %ProgramData%\Agilent\OLSS\Index\ActivityLog &&  
net start SharedServicesHost
```

- **メッセージ**

システムエラー 5 が発生しました。アクセスが拒否されました。

解決策

コマンドプロンプトを管理者として実行してください。

ステップ 3：OpenLab Server/ECM XT のコンフィグレーション情報のリストア

インストール / コンフィグレーション関連のファイルを

C:\ProgramData\Agilent\Installation にリストアします。

スケーラブルシステムの場合、ノードごとにこのフォルダーをリストアします。

ステップ 4：OpenLab 認証サービスのリストア

バックアップした認証サービスフォルダーを

"C:\ProgramData\Agilent\OpenLab Certificate Service" フォルダーにコピーします。

ステップ 5：オリジナルコンフィグレーションを使用した OpenLab Server/ECM XT のインストール

インストール手順に従って、マシンに OpenLab Server/ECM XT をインストールし、新しい OpenLab Server/ECM XT を構成します。以下の手順では、PostgreSQL データベースを例に、リストア済み情報を使用して OpenLab Server/ECM XT をインストールする方法について説明します。この手順は他のデータベースの場合も同様です。

- 1 インストーラで、**【ステップ 1 - ソフトウェアに必要なコンポーネントのインストールおよびアップグレード】** を実行します。
- 2 データベースタイプ画面で、**【PostgreSQL Server (v14)】** が選択されているのを確認し、**【次へ】** をクリックしてください。
- 3 **【PostgreSQL】** 画面で、デフォルトのサーバー名とポートを変更せず、**【次へ】** をクリックします。
- 4 **PostgreSQL 設定**画面では、PostgreSQL インストールパスを変更しないでください。データベースファイルの場所が、データベースファイルがリストアされた場所と対応していることを確認してください。
- 5 **スーパーユーザーのパスワード**を入力し、前提条件のインストールを完了します。
- 6 インストーラで、**【ステップ 2 - データベーススキーマの作成および更新】** を実行します。
- 7 データベースサーバー画面で、**【既存の OpenLab Server データベースに接続してアップグレード】** を選択し、**【次へ】** をクリックしてください。
- 8 データベーススキーマのコンフィグレーションを完了します。
- 9 **【ステップ 3 - OpenLab Content Management のインストールおよびアップグレード】** を実行します。
- 10 **【ステップ 4 - OpenLab Content Management の構成】** を実行します。このステップ中に、Shared Services admin の資格情報を入力できるようにしておいてください。
- 11 **コンテンツパス**画面で、すべてのデータベースファイルのロケーションが実際のデータフォルダーの場所と一致していることを確認します。**【確認】** をクリックし、**【次へ】** をクリックします。
- 12 コンフィグレーションサマリーを注意深くレビューしてください。OK であれば、**【適用】** をクリックします。

ステップ 6：OpenLab Control Panel でのライセンスサーバーの変更

ライセンスサーバーを別の名前のコンピューターへ移動した場合は次の手順に従ってください。

- 1 管理者として OpenLab Control Panel にログインします。
- 2 **[管理]** > **[ライセンス]** > **[サーバーの変更]** をクリックします。
- 3 ライセンスサーバーの名前を入力します。
- 4 **[ping]** をクリックして、新しいサーバーが正しいことを確認します。
- 5 **[OK]** をクリックします。
- 6 マシンを再起動します。

ステップ 7：OpenLab Server/ECM XT のアクティブ化

同じホスト名でリストアを実行する場合は、OpenLab Server/ECM XT を再度アクティブにする必要はありません。ただし、サーバーを新しいマシンに移動した場合、OpenLab Server/ECM XT の再アクティブ化が必要になることがあります。

- 1 **[OpenLab Control Panel]** > **[管理]** を開きます。
- 2 **[システムコンフィグレーション]** > **[システム設定の編集]** をクリックします。
- 3 認証プロバイダーに対して **[内部]** または **[Windows ドメイン]** を選択します。これらの値のいずれかがすでにコンフィグレーションされている場合は、**[現在のコンフィグレーションを維持]** を選択できます。
[Windows ドメイン] を選択した場合は、46 ページの **「Windows ドメイン」** を参照してください。
- 4 **[Content Management]** をストレージタイプとして選択し、**[次へ]** をクリックします。
- 5 認証プロバイダーに対して現在のコンフィグレーションを維持しなかった場合、管理者アカウントの **認証パラメータ** を入力します。
- 6 **[次へ]** をクリックします。

- 7 **【サーバーの変更】** を選択し、OpenLab Server/ECM XT URL を指定した後、**【ライセンス認証】** をクリックし、OpenLab Server/ECM XT の同期を再度アクティブにします。

図 7 OpenLab Server/ECM XT のアクティブ化

- 8 **【次へ】** をクリックし、**【適用】** をクリックします。

注記

Sample Scheduler を使用する場合、リストア手順の後に Sample Scheduler サービスを再起動する必要があります。

ステップ 8：クライアントコンフィグレーション

OpenLab Server/ECM XT Server が別のホストにリストアされた場合、セットアップですべてのクライアントをこの新しい OpenLab Server/ECM XT Server に設定する必要があります。各クライアントマシンからこの手順を繰り返す必要があります。

- 1 Windows の **［スタート］** > **［Agilent Technologies］** > **［メンテナンスユーティリティ］** を選択します。
- 2 **［サーバー設定］** タブをクリックします。
- 3 **［サーバーの追加］** をクリックし、サーバー名とオプションで説明を入力します。
- 4 **［サーバー］** フィールドに新しいホスト名を入力し、**［テスト接続］** をクリックします。
- 5 **［OK］** をクリックし、このサーバーをデフォルトとして設定します。これでコントロールパネルにログインできます。

ステップ 9：カスタム証明書のリストア

バックアップにカスタム証明書のあるフォルダーが含まれる場合、29 ページの「**OpenLab Server/ECM XT リバースプロキシの設定**」の**ステップ 4**に従って設定します。4 サーバーまたはスケラブルシステムのインデックスサーバーの場合、37 ページの「**インデックスサーバーコンフィグレーション - 4 サーバースystemのみ**」を参照してください。

ステップ 10：コントロールパネルでライセンスの確認

サーバーのアップグレード時にサーバー Mac アドレスが変更された場合、新しいサーバーのライセンスは古いサーバーとは異なります。

- 1 コントロールパネルから **［管理］** > **［ライセンス］** を選択します。
- 2 **［ライセンス］** ツールバーで **［ライセンスの表示］** をクリックします。インターネットウィンドウに情報が表示されます。

必要に応じて、ライセンスを再適用します。詳細については、コントロールパネルのヘルプを参照してください。

異なるサーバー間の手動バックアップの データ移行

このセクションでは、異なるサーバー間の手動データバックアップによるデータ移行について説明します。OpenLab Server/ECM XT v2.4 システム（Windows Server 2012）から、新しいオペレーティングシステム（Windows Server 2016、Windows Server 2019、または Windows Server 2022）を搭載した v2.7 サーバーへアップグレードする場合にこの手順を使用します。

以下のステップは、オールインワン OpenLab Server/ECM XT 2.4 サーバーに適用されます。

注記

データを継承する新しいサーバーは Windows Server 2022 など、OpenLab Server/ECM XT v2.7 でサポートされるサーバーオペレーティングシステム上になければなりません。

- 1 オールインワン OpenLab Server/ECM XT 2.4 およびソフトウェアアップデートを新しいサーバーにインストールします。
- 2 2.4 の『OpenLab Server および ECM XT 管理者ガイド』の「手動システムバックアップの実行」セクションに従って、サーバーデータをバックアップします。
- 3 Windows Server バックアップなど、好みのツールを使用して、新しいサーバーにデータを転送してリストアします。
- 4 C: ドライブのフォルダーおよびファイルをバックアップフォルダーおよびファイルに手動で置き換えます。
 - a 以下のサービスを停止します。これは C: フォルダーを正常に置き換えるために必要です。
 - AlfrescoTomcat
 - Agilent OpenLab Content Management Search service
 - Agilent OpenLab Shared Services
 - olcm-postgressql-x64-10

- b C: フォルダーおよびファイルを対応するバックアップデータに置き換えます。
 - PostgreSQLData-10-OLCM -
C:¥ProgramData¥Agilent¥PostgreSQLData-10-OLCM
 - DataStoreContent - **C:¥DataStoreContent**
 - DataStoreIndex - **C:¥DataStoreIndex**
 - DataStoreArchive - **C:¥DataStoreArchive**
 - インストールフォルダー - **C:¥ProgramData¥Agilent¥Installation**
 - c サービスを逆の順序で再起動します。
 - olcm-postgressql-x64-10
 - Agilent OpenLab Shared Services
 - Agilent OpenLab Content Management Search service
 - AlfrescoTomcat
- 5 OpenLab Server/ECM XT v2.4 インストーラのステップ 2 とステップ 4 を実行して、元のスキーマで新しいサーバーを再コンフィグレーションします。
 - ステップ 2 で、**【既存の OpenLab Content Management データベースに接続してアップグレード】** を選択し、古いサーバーログインスキーマでデータベースに接続していることを確認します。
 - ステップ 4 で、すべてのデータベースファイルのロケーションが実際のデータフォルダーの場所と一致していることを確認します。**【確認】** をクリックし、ステップが順調に進んでいることを確認します。
- 6 OpenLab Control Panel で Content Management を再度アクティブ化します。
 この時点では、Content Management は古いサーバーロケーションを指しているため、変更する必要があります。
 - a 管理者ユーザーとして OpenLab Control Panel にログインします。
 - b **【管理】 > 【システムコンフィグレーション】 > 【システム設定の編集】** から、**【システム設定の編集】** にアクセスします。
 - c Content Management の下のドロップダウンメニューを選択し、**【Content Management】** を選択します。
 - d **【次へ】** をクリックします。
 - e Content Management サーバーの現在のロケーションが古いサーバー名を指している場合、**【サーバーの変更】** チェックボックスをオンにします。
 Content Management URL を変更します。
 <新規サーバー名> に置き換えます。
【ライセンス認証】 をクリックして、問題なくライセンス認証が成功したことを確認します。

- f [次へ] をクリックします。
 - g [適用] をクリックして設定を保存します。
- 7 Content Management ウェブサイトから、すべてのデータが移行できたことを確認します。
- 8 最新の v2.7 インストーラをダウンロードして OpenLab Server/ECM XT にアップグレードします。

バックアップのガイドライン 119

概要 120

Solr インデックスのバックアップ 121

データベースの手動バックアップ 125

データリポジトリのバックアップ 137

コンテンツストアの手動バックアップ 138

OpenLab Server/ECM XT Server および インデックスサーバーコンフィグレーション情報の手動バックアップ 139

バックアップファイルの保存 140

システムの手動リストア 141

本章は、データベースのバックアップとメンテナンスに精通し、Apache Tomcat に関する知識をある程度お持ちの管理者を対象としています。Solr インデックス、データベース、コンテンツストア、およびコンフィグレーション情報のホットバックアップを含む、OpenLab Server/ECM XT システムのホットバックアップを実行するために必要な情報を記載しています。システムのリストア方法に関する情報も含まれます。

注記

バックアップおよびリストアユーティリティをサポートしているシステムでホットバックアップが利用できます。Agilent では、可能な限りバックアップおよびリストアユーティリティを使用することをお勧めします。バックアップおよびリストアユーティリティの使用方法については、54 ページの「**バックアップとリストアの手順**」を参照してください。

バックアップのガイドライン

- システムをバックアップするときは、必ず 120 ページの「概要」の説明で指定された順序に従ってください。
- ホットバックアップは、システム上でユーザーがアクティブな状態で実行するよう設計されていると同時に、パフォーマンスへの影響があります。アーカイブが実行中でないときやアップロード速度が標準または標準未満のレベルのときなど、システムアクティビティが低下している間に実行することをお勧めします。

概要

ホットバックアップでは、システムの操作を続行したまま、OpenLab Server/ECM XT からすべてのデータを一貫性のある状態でコピーすることができます。バックアップ手順を以下の順序で実行することが重要です。

- 1 **Solr インデックス** - Solr インデックスを最初に（データベースの前に）バックアップします。リストア時に、システムはデータバーストランザクションデータから不明なインデックスエントリを検出し、必要に応じてそれらのエントリを作成します。
- 2 **Data Repository** - トポロジに複数の ECM XT Server または個別のインデックスノードサーバーがある場合、すべての ECM XT Server から Data Repository をバックアップします。
- 3 **データベース** - データベースとコンテンツストアとの一貫性を確保するため、ファイルをバックアップする前にデータベースのバックアップを完了する必要があります。データベースのバックアップを実行するときは、OpenLab Server/ECM XT で使用するよう設定された、データベースベンダーが提供するバックアップツールを使用してください。
- 4 **コンテンツストア** - 最終的なステップで、実際のファイルをバックアップします。このために任意のファイルバックアップツールを使用できます。
- 5 **カスタム証明書** - セキュリティで保護された接続用にカスタム証明書を使用している場合、これらの証明書のバックアップを作成します。このために任意のファイルバックアップツールを使用できます。
- 6 **コンフィグレーション情報** - 最終ステップでは、ソフトウェアの再インストールが簡略化できるようにコンフィグレーションファイルをバックアップします。このために任意のファイルバックアップツールを使用できます。

注記

スケーラブルな環境では、データベースとコンテンツストア（ファイルシステム）が共有され、Solr インデックスはインデックスサーバーに保存されません。システムをリストアするときは、インデックスサーバーにインデックスをリストアします。

注記

バックアップが完了したら、インデックス、データベース、およびコンテンツストアのバックアップを1つのユニットとして一緒に保存することが重要です。これらはセットとしてリストアする必要があるため、そのようにしないとシステムが正しく動作しません。

Solr インデックスのバックアップ

OpenLab Server/ECM XT の実行中に OS ファイルシステムコピーを使用して solr6/ インデックスサブディレクトリを直接バックアップしようとししないでください。Solr インデックスが破損します。

Solr の推奨されるバックアップ方法は、スケジュール済みの Solr バックアップジョブです。自動バックアップを有効にする手順については、「**定期的なバックアップ**」を参照してください。OpenLab Server/ECM XT では、定期的な Solr インデックスバックアップをスケジュールでき、これはシステムプロパティから設定します。

定期的なバックアップ

以下の手順で、自動バックアップを有効にします。

Content Management サーバーのみの OpenLab Server/ECM XT

オールインワンまたは 2 台のサーバーソリューションなど、個別のインデックスサーバーがなく、インデックスおよび検索サービスが Content Management サーバーローカルのコンフィグレーションでは、以下で定期的なインデックスのバックアップをスケジュールしてください。

- 1 サーバーコンフィグレーションアプリケーションを開いてインデックスのロケーションを見つけてます（Windows の [スタート] > [Agilent Technologies] > [サーバーコンフィグレーション ビューア]）。
- 2 [Content Management Content Summary] に、インデックスパス（Index Path）が表示されます。たとえば、以下の例のインデックスパスが C:\DataStoreIndex と表示され、インデックスフォルダーが C:\DataStoreIndex\solr6\index\alfresco にあることが示されます。

表 7 Solr インデックス Content Management コンテンツサマリー

サーバー設定	インデックスおよび検索サービス搭載の Content Management
Primary content storage location	C:\DataStoreContent
Secondary content storages	None

表 7 Solr インデックス Content Management コンテンツサマリー

Primary archive storage location	C:\DataStoreArchive
Secondary archive storage locations	None
Index path	C:\DataStoreIndex
Index hostname	

- 定期的なインデックスバックアップを有効にするようシステムプロパティを設定します（124 ページの「システムプロパティの変更」を参照）。たとえば、インデックスパスが C:\DataStoreIndex の場合、バックアップの場所を次のように設定する必要があります。
¥DataStoreIndex¥solr6Backup¥alfresco:

表 8 システムプロパティの設定

プロパティ	説明
solr.backup.alfresco.remoteBackupLocation=C:\DataStoreIndex¥solr6Backup¥alfresco	インデックスバックアップの場所
solr.backup.alfresco.numberToKeep=3	最新のバックアップに加えて前の 3 つのバックアップを維持
solr.backup.alfresco.cronExpression=0 0 2 ** ?	デフォルトは 1 日 1 回 2:00 a.m. に実行。ページ 51 の「Cron 記法」を参照。

- フォルダー C:\DataStoreIndex¥solr6Backup¥alfresco を作成します。
- Content Management サーバーを再起動して設定を有効にします。

注記

リストアすると、インデックスバックアップディレクトリのコンテンツ（ディレクトリ構造とファイル）が、インストール時に指定した検索サービスの <solr6¥index> ディレクトリにコピーされます。デフォルトのロケーションは C:\DataStoreIndex です。

注記

インデックスバックアップは、3 日後に自動的に削除される前に定期的に保存する必要があります。一致するコンテンツとデータベースバックアップとのセットとして保存してください。インデックスをリストアするときは、データベースのバックアップ後に作成された Solr インデックスは使用しないでください。データベースのバックアップ時間に最も近いものを使用し、バックアップ後のものは使用しないでください。

インデックスサーバーのある OpenLab Server/ECM XT

4 台のサーバーまたはスケーラブルなトポロジなど、個別のインデックスサーバーがあるコンフィグレーションでは、以下を行って定期的なインデックスのバックアップをスケジュールしてください。

- 1 [サーバーコンフィグレーション アプリケーション (Windows の [スタート] > [Agilent Technologies] > [サーバーコンフィグレーション ビュア]) でインデックスサーバーのインデックスロケーションを確認します。
- 2 [Content Management Content Summary] に、インデックスパスが表示されます。たとえば、以下の例のインデックスパスが
C:\DataStoreIndex と表示され、インデックスフォルダーが
C:\DataStoreIndex\solr6\index\alfresco にあることが示されます。

表 9 Content Management コンテンツサマリー

サーバー設定	インデックスおよび検索サービス搭載の Content Management
Primary content storage location	C:\DataStoreContent
Secondary content storages	None
Primary archive storage location	C:\DataStoreArchive
Secondary archive storage locations	None
Index path	C:\DataStoreIndex
Index hostname	

- 3 定期的なインデックスバックアップを有効にするようインデックスサーバーのシステムプロパティを設定します。(124 ページの「**システムプロパティの変更**」を参照。) たとえば、インデックスパスが
C:\DataStoreIndex の場合、バックアップロケーションを
C:\DataStoreIndex\solr6Backup\alfresco に設定し、バックアップフォルダーがインデックスフォルダー C:\DataStoreIndex\solr6\index\alfresco に近くなるようにする必要があります。

表 10 システムプロパティの設定

プロパティ	説明
solr.backup.alfresco.remoteBackupLocation=C:\DataStoreIndex\solr6Backup\alfresco	インデックスサーバー上のインデックスバックアップの場所
solr.backup.alfresco.numberToKeep=3	最新のバックアップに加えて前の 3 つのバックアップを維持
solr.backup.alfresco.cronExpression=0 0 2 * * ?	デフォルトは 1 日 1 回 2:00 a.m. に実行

- 4 フォルダー C:\DataStoreIndex\solr6Backup\alfresco を作成します。
- 5 その他すべての Content Management サーバーに同じ設定を適用します。
- 6 インデックスサーバーのみ再起動して設定を有効にします。他の Content Management サーバーを再起動する必要はありません。

注記

インデックスサーバーで適用した同じ設定を他のすべての Content Management サーバーに適用して、すべてのサーバーが一貫して動作するようにすることが重要です。これらのサーバーがすべて同じデータベースおよびインデックスサーバーを指しているためです。スケジュール化されたジョブは、インデックスサーバー自体を含む任意のサーバーによって呼び出すことができます（どのサーバーになるかは保証されません）。インデックスサーバー上のインデックスに対してバックアップが行われるため、remoteBackupLocation はインデックスサーバーが認識できるロケーションである必要があります。サーバーごとに異なる設定にすると、矛盾した動作や予期しない動作を引き起こします。

注記

リストアすると、インデックスバックアップディレクトリのコンテンツ（ディレクトリ構造とファイル）が、インストール時に指定したインデックスサーバーの <solr6\index> ディレクトリにコピーされます。デフォルトのロケーションは C:\DataStoreIndex です。

注記

インデックスバックアップは、3 日後に自動的に削除される前に定期的に保存する必要があります。一致するコンテンツとデータベースバックアップとのセットとして保存してください。インデックスをリストアするときは、データベースのバックアップ後に作成された Solr インデックスは使用しないでください。データベースのバックアップ時間に最も近いものを使用し、バックアップ後のものは使用しないでください。

システムプロパティの変更

- 1 alfresco-global.properties ファイルを
<INSTALLATION PATH>\OpenLAB Data Store\tomcat\shared\classes から開きます
（デフォルトのロケーションは、ECM XT サーバーの C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\tomcat\shared\classes ディレクトリです）。
- 2 変更するプロパティを検索するか、プロパティが存在しない場合は追加します。変更を行ってファイルを保存します。次回サーバーを再起動すると変更が有効になります。

データベースの手動バックアップ

OpenLab Server/ECM XT システムでは、ホットバックアップのサポート機能は、OpenLab Server/ECM XT で使用するよう設定されたデータベース製品のホットバックアップ機能により異なります。ホットバックアップを行うには、使用しているデータベース製品が、一貫性のあるバージョンの OpenLab Server/ECM XT のデータベースを「スナップショット」できるツールを備えている必要があります。（つまり、OpenLab Server/ECM XT データベース内のすべてのテーブルのトランザクションが一貫したコピーを取得する必要があります。）さらに、バックアップの実行中に動作している OpenLab Server/ECM XT システムのパフォーマンスに関する重大な問題を回避するには、この「スナップショット」操作を、OpenLab Server/ECM XT データベースでロックを確立せずに実施するか、迅速に（数秒以内に）完了しなければなりません。

バックアップ機能は、リレーショナルデータベース製品間で大きく異なります。バックアップ手順を運用環境に導入する前に、適正な資格を持つ経験豊富なデータベース管理者によってこれらの手順が検証されるようにしてください。

データベースをバックアップするには、以下を行います。

1 データベースが

『Agilent OpenLab ECM Server および ECM XT インストールガイド』に従ってインストールおよびコンフィグレーションされていることを確認します。

Oracle データベースを使用している場合、Fast Recovery Area（FRA）が定義され、データベースモードが ARCHIVELOG に設定され、保持ポリシーが実施されているようにします。

2 インストール時に指定されたコンテンツデータベースおよび Shared Services データベースの名前を特定します。これらの名前は以下のように確認できます。

- a サーバーコンフィグレーションアプリケーションを実行します
(Windows の [スタート] > [Agilent Technologies] > [サーバーコンフィグレーションビューア])。これによりサーバーコンフィグレーションのサマリーが確認できます。

- b** Shared Services データベースサマリーに、Shared Services のデータベース名が表示されます。

表 11 Shared Services データベースサマリー

データベースタイプ	PostgreSQL
サーバー名	localhost
サーバーインスタンス	該当なし
サーバーポート	5432
データベース名	OLSharedServices
データベース管理者	postgres
データベースユーザー	Olss

- c** Content Management データベースサマリーにコンテンツデータベースのデータベース名が表示されます。

表 12 Content Management データベースサマリー

データベースタイプ	PostgreSQL
サーバー名	localhost
サーバーインスタンス	該当なし
サーバーポート	5432
データベース名	DataStore
データベース管理者	postgres
データベースユーザー	DSAdmin

- 3** データベース名を取得したら、適切なデータベースバックアップの方法およびツールを使用してすべてのテーブルをバックアップします。

SQL サーバーデータベースのバックアップ

このセクションでは、MS SQL Server OpenLab Server/ECM XT データベースのホットバックアップ作成について詳しく説明しています。

システムで提供されるスクリプトによって、以下のタイプのデータベースオブジェクトのフルバックアップが作成されます。

- SQL サーバースystemデータベース（master、msdb、model など）
- OpenLab Server/ECM XT データベース（DataStore、OLSharedServices）
- 実行中のトランザクションを含むトランザクションログのアクティブな部分

前提条件

データベースをバックアップする前に、以下の前提条件を確認してください。

- システム管理者権限のあるユーザー資格情報
- SQL Server Management Studio（SSMS）または SQL スクリプトを実行するためのその他のツール
- SQLCMD
- バックアップファイルを保存するための非ローカルドライブ上のフォルダー（¥¥NetworkBackups¥Database など）
- バックアップファイル作成用のローカルフォルダー（C:¥Backup¥Database など）このロケーションは一時的にしてください。バックアップファイルはバックアップの完了後にストレージロケーションへ移動します。

ホットバックアップの実行

SQL Server Management Studio（SSMS）を使用して、システムで提供されるバックアップスクリプトを実行できます。デフォルトのインストールの場合、スクリプトは **C:¥Program Files (x86)¥Agilent Technologies¥OpenLAB Data Store¥Backup Scripts¥Hot Backup¥SQLServer¥** に保存されます。

SSMSを開き、[ファイル] > [開く] メニューで、実行するバックアップスクリプトを選択します。ツールバーの [実行] ボタンをクリックしてスクリプトを実行します。

実行するスクリプトごとに、用語 “TO DISK =” を、作成したローカルバックアップフォルダーを指すよう変更します。以下のスクリプトが用意されています。

手動ホットバックアップ手順

SQL サーバーデータベースのバックアップ

ECMDBHotBackup.sql このスクリプトは、DataStore および OLSharedServices ユーザーデータベースのバックアップを作成します。

```
-----
ALTER DATABASE OLSharedServices SET RECOVERY FULL
```

```
BACKUP DATABASE OLSharedServices TO DISK =
'C:¥Backup¥Database¥OLSharedServices.bak'
```

```
WITH INIT
```

```
ALTER DATABASE DataStore SET RECOVERY FULL
```

```
BACKUP DATABASE DataStore TO DISK =
'C:¥Backup¥Database¥DataStore.bak'
```

```
WITH INIT
-----
```

SystemDBHotBackup.sql このスクリプトは、SQL サーバースystemデータベースのバックアップを作成します。

```
-----
ALTER DATABASE Master SET RECOVERY SIMPLE
```

```
BACKUP DATABASE Master TO DISK =
'C:¥Backup¥Database¥MSSQLBackupMaster.bak'
```

```
WITH INIT
```

```
ALTER DATABASE MSDB SET RECOVERY FULL
```

```
BACKUP DATABASE MSDB TO DISK = 'C:¥Backup¥Database¥
MSSQLBackupMsdb.bak'
```

```
WITH INIT
```

```
ALTER DATABASE Model SET RECOVERY FULL
```

```
BACKUP DATABASE Model TO DISK = 'C:¥Backup¥Database¥
MSSQLBackupModel.bak'
```

```
WITH INIT
-----
```


手動ホットバックアップ手順

PostgreSQL データベースのバックアップ

バックアップに関する追加の検討事項

- ・ オフラインバックアップ - 保護を強化するため、バックアップファイルをオフサイトロケーションへコピーしてください。
- ・ **BACKUP** コマンドの **"WITH INIT"** パラメータによって、以前のバージョンのバックアップが削除されます。つまり、1 つバージョンのデータのみが維持されます。各データベースのバックアップ後に、コンテンツファイルおよび **solr** インデックスのバックアップと併せて別の場所にファイルをコピーすることで、一致するセットが維持されるようにしてください。
- ・ 暗号化 - データをさらに保護するために、バックアップファイルを暗号化できません。
- ・ データベースバックアップジョブのスケジュール - 管理 / メンテナンスプラン機能を使用して、バックアップジョブを **SSMS** でスケジュールできます。
- ・ ログバックアップ - フルバックアップの間にログバックアップを行わないと、前回のバックアップ以降に行ったデータベースへの変更が失われます。ログバックアップをバックアップスクリプトに追加すべきか検討してください。
- ・ ログの切り詰め - ログエントリを定期的に削除して、ログファイルが大きくなりすぎないようにしてください。
- ・ ローカルのフォルダーロケーションから非ローカルのバックアップストレージロケーションへバックアップファイルをコピーしてください。

PostgreSQL データベースのバックアップ

このセクションでは、OpenLab Server/ECM XT PostgreSQL コンポーネントの基本的なデータベースホットバックアップとリストア方法について説明します。これらの方法は、総合的なデータベースのバックアップ戦略に代わるものと見なしてはなりません。このような戦略は、適正な資格を持つ PostgreSQL の専門家が作成する必要があります。

これらの方法は、以下のタイプのデータベースオブジェクトのフルバックアップを作成するためのものです。

- ・ システムデータベース
- ・ OpenLab Server/ECM XT データベース（DataStore、OLSharedServices）
- ・ Work-ahead-log のアクティブな部分

前提条件

データベースのバックアップを開始する前に以下の前提条件を確認してください。

- postgres ユーザー admin のパスワード
- pg_hba.conf へのユーザーエントリ。ホットバックアップスクリプトの注記を参照してください。
- gzip 圧縮 TAR ファイルを解凍できるユーティリティ
- バックアップファイルを保存するためのフォルダー。保存場所は PostgreSQL データベースファイルを保存する同じデバイス上にしないことをお勧めします。

ホットバックアップの実行

この方法では、ユーザーがシステムでの操作を続行中に PostgreSQL データベースをバックアップすることができます。ホットバックアップを実行すると、バックアップの実行中はシステムパフォーマンスが低下する場合があります、またバックアップが開始される前に入力したデータのみバックアップファイルに保存されることが保証されます。

データベースバックアップを作成するための高度な手順は以下のとおりです。

- 1 「バックアップファイルを保存するためのフォルダーの作成」。
- 2 131 ページの 「ホットバックアップスクリプトの実行」。

バックアップファイルを保存するためのフォルダーの作成

PostgreSQL データベースを含まないデバイス上にフォルダーを作成します。データベースのサイズに基づいて、バックアップ戦略で要求されるバックアップの作成数を保持するのに十分なスペースが割り当てられているようにしてください。バックアップスクリプトによってバックアップファイルは圧縮されます。

バックアップスクリプトの設定

デフォルトのインストールの場合、バックアップスクリプトを **C:\Program Files (x86)\Agilent Technologies\OpenLAB Data Store\Backup Scripts\Hot Backup\Postgres\postgresqlHotBackup.bat** で見つけ、テキストエディタを使用して環境に合わせてスクリプトをカスタマイズします。

- 1 上記で作成したフォルダーへのパスでバックアップ先を編集します。

表 13 バックアップ先

ツール	プロパティ	注記
テキスト エディタ	backupdestination=<Path¥to¥backupfolder> を設定 または、 backupdestination=<¥¥Path¥to¥backupfolder> を設定	デフォルトでは、フォルダーをサー バルードライブの ¥PostgreSQLBackup フォルダーに配置 しますが、別のデバイスに保存するこ とをお勧めします。 バックアップ先が UNC パスの場合、こ のフォーマットを使用してください。

- 2 パス環境変数に次のロケーションを追加します：C:¥Program Files (x86)¥PostgreSQL-11-OLCM¥bin。これによりホットバックアップスクリプトの実行時に PostgreSQL バックアップコマンドが見つかるようになります。

ホットバックアップスクリプトの実行

デフォルトのインストールの場合、バックアップスクリプトを **C:¥Program Files (x86)¥Agilent Technologies¥OpenLAB Data Store¥Backup Scripts¥Hot Backup¥Postgres¥** フォルダーで、コマンドを実行します。「postgres」ユーザーのパスワードが求められます。

表 14 バックアップ先

ツール	プロパティ	注記
Windows コマンド ライン	postgresqlHotBackup.bat	バックアップを実行すると、ジョブの進行状況 が報告されます。

バックアップスクリプトを実行するたびに、新しいサブフォルダーがバックアップ先に作成されます（Backup-2019-06-28_10_45_14 など）。作成されたフォルダー内には、2 つの gzip 圧縮アーカイブがあります。

- base.tar.gz – このファイルは、データベースに追加されたすべてのデータを保持します。
- pg_wal.tar.gz – このファイルには pg_wal フォルダーが含まれ、このフォルダーは write-ahead-log (wal) レコードを保持します。各レコードには、データベースに変更が適用される前に書き込まれた一連のデータベースの変更が保存されます。このメカニズムによって、不具合が発生した場合にデータベースが保護されます。

ホットバックアップスクリプト注記

pg_hba.conf

ホットバックアップスクリプトは「postgres」ユーザーアカウントを使用して実行されます。このアカウントは、システム管理者権限を持っており、またデフォルトではレプリケーション（バックアップ）権限を持っています。レプリケーション権限を持つユーザーは、pg_hba.conf ファイルで一致するエントリも持っている必要があります。既存のファイルに以下の 2 つのラインを追加し、olcm-postgresql-x64-11 Windows サービスを再開してください。

ファイルへのデフォルトパスは、
C:\ProgramData\Agilent\PostgreSqlData-11-OLCM です。

表 15 バックアップ先

# タイプ	データベース	ユーザー	アドレス	メソッド
ホスト	レプリケーション	postgres	127.0.0.1/32	md5
ホスト	レプリケーション	postgres	::1/128	md5

バックアップに関する追加の検討事項

- ・ オフラインバックアップ – 保護を強化するため、バックアップファイルをオフサイトロケーションへコピーしてください。少なくとも、PostgreSQL データベースファイルとは別のデバイス上にバックアップを保存してください。
- ・ 保持するよう選択したデータベースごとに、コンテンツファイルおよび Solr インデックスのバックアップと併せて別のロケーションにデータベースバックアップファイルをコピーして、一致するセットが維持されるようにしてください。
- ・ 暗号化 – データをさらに保護するために、バックアップファイルを暗号化できます。
- ・ データベースバックアップジョブのスケジュール – Windows スケジューラなどを使用して、バックアップジョブをスケジュールできます。

Oracle データベースのバックアップ

以下の方法では、以下のタイプのデータベースオブジェクトのフルバックアップを作成します。

- Oracle システム表領域
- OpenLab Server/ECM XT データベース（DataStore、OLSharedServices）
- 実行中のトランザクションを含むトランザクションログのアクティブな部分

前提条件

『*Agilent OpenLab ECM Server* および *ECM XT* インストールガイド』に、Oracle のホットバックアップ機能を有効にするためのワンタイムの設定手順を記載しています。この設定手順は、このドキュメントのホットバックアップを実行する前に完了する必要があります。

データベースのバックアップを開始する前に以下の前提条件を確認してください。

- システム管理者権限のある Oracle ユーザー資格情報
- Oracle Recovery Manager（RMAN）。136 ページの「**RMAN をデータベースに接続する方法**」を参照してください。
- SQL コマンドを実行するための SQL*Plus またはその他のツール。136 ページの「**SQL*Plus をデータベースに接続する方法**」を参照してください。
- Oracle のインストール時に設定されたインスタンス名。

注記

すべての RMAN および SQL コマンドには、コマンドの最後にセミコロン (;) が必要です。

注記

SQL または RMAN コマンドを実行する前に、データベースへの接続を最初に確立する必要があります。「**RMAN をデータベースに接続する方法**」および 136 ページの「**SQL*Plus をデータベースに接続する方法**」を参照してください。前のコマンドで接続を閉じた場合（SHUTDOWN IMMEDIATE など）、SQL または RMAN コマンドを実行する前にデータベース接続を再度確立することが必要な場合があります。

ホットバックアップの実行

この方法では、ユーザーがシステムでの操作を続行中に Oracle データベースをバックアップすることができます。ホットバックアップを実行すると、バックアップの実行中はシステムパフォーマンスが低下する場合があります。

データベースバックアップを作成するための高度な手順は以下のとおりです。

- 1 「データベースとアーカイブログのバックアップ」。
- 2 134 ページの「SPFILE の保存」。

データベースとアーカイブログのバックアップ

表 16 データベースのバックアップ

ツール	コマンド
該当なし	RMAN をデータベースに接続します。136 ページの「 RMAN をデータベースに接続する方法 」を参照してください。
RMAN	BACKUP AS BACKUPSET DATABASE PLUS ARCHIVELOG データベースとアーカイブログがバックアップされ、Fast Recovery Area（FRA）に配置されます。

設定された FRA ロケーションを、次の SQL SHOW コマンドを使用して表示できます：

SHOW PARAMETER DB_RECOVERY_FILE_DEST。

SQL コマンドを実行するには、SQL*Plus をデータベースに接続します。方法については、「RMAN をデータベースに接続する方法」を参照してください。

SPFILE の保存

SPFILE は Oracle コンフィグレーション情報を保存し、不具合が発生した場合にサーバーを回復するために使用されます。ファイルの初期バックアップを作成し、コンフィグレーションが変更された場合に再保存するか、バックアップを取るたびに保存を検討することで、常に最新バージョンを保持するようにしてください。

表 17 SPFILE の保存

ツール	コマンド
該当なし	SPFILE をコピーし、バックアップと一緒に保存します。デフォルトのロケーション： <Oracle Installation>%database%SPFILE<YOURINSTANCENAME>.ORA コマンドに <> を含めないでください。例： C:\app\%orcladmin%\product\12.2.0\dbhome_1\database

利用可能なすべてのバックアップを表示するには、以下のコマンドを実行します。 RMAN> LIST BACKUP SUMMARY

バックアップに関するその他の検討事項

- ・ オフラインバックアップ – 保護を強化するため、バックアップファイルをオフサイトロケーションへコピーしてください。少なくとも、Oracle データベースファイルとは別のデバイス上にバックアップを保存してください。バックアップは、上記で作成した Fast Recovery Area (FRA) に保存されます。FRA フォルダー全体を保存します。
- ・ 上記で設定した保持ポリシーによって、バックアップが 7 日間保持されます。このため、これらのバックアップが自動的に削除される前に別のロケーションへコピーすることを検討してください。保持するよう選択したデータベースごとに、Solr インデックス、コンテンツファイル、およびコンフィグレーションのバックアップと併せて別のロケーションにデータベースバックアップファイルをコピーして、一致するセットが維持されるようにしてください。
- ・ 暗号化 – データをさらに保護するために、バックアップファイルを暗号化できます。
- ・ データベースバックアップジョブのスケジュール – Oracle Enterprise Manager や Windows スケジューラなどを使用して、バックアップジョブをスケジュールできます。
- ・ ログバックアップのサイズ変更 – Fast-recovery-area とログアーカイブ先に十分なスペースを割り当てて、システムの中断を回避することが重要です。適切なサイズ変更については DBA にご相談ください。
- ・ ログバックアップ – 前回のフルバックアップ以降に行ったデータベースへの変更がログに保存されます。作業が失われる事態を防ぐには、フルバックアップの間にアーカイブログのバックアップを毎日（またはより頻繁に）行うことが欠かせません。Oracle では、回復性向上のため、複数のロケーションに同時にログアーカイブをコピーすることをサポートしていますが、それには追加のストレージスペースと設定が必要です。
- ・ ログアーカイブメンテナンス – 不要なログを定期的に削除して、ログディレクトリが大きくなりすぎないようにしてください。完全アーカイブを行うとシステムが中断します。

RMAN をデータベースに接続する方法

表 18 RMAN をデータベースに接続

ツール	コマンド
Windows コマンドライン	<pre>rman TARGET SYS@<YOURINSTANCENAME> nocatalog</pre> Oracle インスタンス名を置換します。コマンドに <> を含めないでください。 例： <pre>rman TARGET SYS@OPENLAB nocatalog</pre>

SQL*Plus をデータベースに接続する方法

表 19 SQL*Plus をデータベースに接続

ツール	コマンド
Windows コマンドライン	<pre>sqlplus/NOLOG</pre>
SQL	<pre>CONNECT SYS/<THEPASSWORD> AS SYSDBA</pre>

データリポジトリのバックアップ

103 ページの「データリポジトリデータベースの手動バックアップ」の手順を使用してデータリポジトリをバックアップします。

コンテンツストアの手動バックアップ

コンテンツストアをバックアップするには、任意のファイルバックアップユーティリティを使用できます。差分バックアップを実行できるものを使用することをお勧めします。それにより、コンテンツストア全体を毎回バックアップする必要はなく、差分バックアップを行うだけで済みます。インデックス、データベース、およびファイルコンテンツストアを一貫性のある状態でリストアできることが重要です。コンテンツファイルをバックアップするには、コンテンツストアのロケーションを特定する必要があります。コンテンツストアのロケーションを見つけるには、以下を行います。

- 1 OpenLab Server/ECM XT Server マシンに移動します。スケーラブルな環境では、任意のノードに接続できます。
- 2 Windows の **【スタート】 > 【Agilent Technologies】 > 【サーバーコンフィグレーション ビューア】** の順にクリックします。ウェブページが表示され、コンテンツストアとアーカイブパスが確認できます。

表 20 Content Management Content Summary

Primary content storage location	C:\DataStoreContent
Secondary content storages	None
Primary archive storage location	C:\DataStoreArchive
Secondary archive storage locations	None

- 3 リポジトリに複数のコンテンツストアがある場合、追加の各コンテンツストアもバックアップする必要があります。
- 4 すべてのコンテンツストアのロケーションを特定したら、ファイルバックアップツールを使用してそれらをバックアップします。

OpenLab Server/ECM XT Server および インデックスサーバーコンフィグレーション 情報の手動バックアップ

OpenLab Server/ECM XT Server およびインデックスサーバーごとに、以下の手順を実行してください。

1 <Installation Directory>%OpenLAB Data

Store%tomcat%temp%com.agilent.datastore.cache ファイルを、
C:%ProgramData%Agilent%Installation フォルダにコピーします。

<Installation Directory> は、[サーバーコンフィグレーション] ページの
[Installation Summary] で確認できます。

2 C:%ProgramData%Agilent%Installation フォルダをバックアップします。

これは、後でシステムを再構成するために使用されます。

カスタム証明書のバックアップ

セキュリティで保護された接続用にカスタム証明書を使用している場合、これらの証明書のバックアップを作成します。 C:%Program Files%OpenLab Reverse Proxy%Apache24%conf%ssl%custom% フォルダをバックアップロケーションにコピーします。

バックアップファイルの保存

データベース、コンテンツ、インデックスファイルのセットが一貫性を持つようにするには、これらのバックアップステップの出力を毎日保存して整理するプロセスを実施することで、システムをリストアする必要が生じた場合に一致したセットが見つかるようにする必要があります。同じセットのファイルを一緒に保存するか、以下のバックアップの必須順序に留意して、セットを見つける手順を文書化するかを選択できます。

- 1 Solr インデックス
- 2 データベース
- 3 データリポジトリ
- 4 コンテンツおよびアーカイブストア
- 5 コンフィグレーション情報

Solr のバックアップはあらかじめ決められたスケジュールで実行され、オンデマンドでは実行されないため、リストアが必要な場合に備えて、データベースのバックアップを最新の Solr バックアップと一緒に保存してください。

システムの手動リストア

バックアップの時点で使用中のコンフィグレーションと一貫性のあるシステムを設定します。これは、最初に行った設定およびコンフィグレーション手順に加えて、それ以降に行った追加の手順にすべて従うことで、手動で行うことができます。このほかに、完全なシステムバックアップをベースとして行って、コンフィグレーションの更新時にそのバックアップを更新する方法があります。障害復旧プランをどのように設定するかはお客様次第です。ただし、データセットをリストアしてシステムを動作させるには、適切なコンフィグレーションから開始する必要があります。

データをリストアするには、動作中のシステムから開始し、サービスを停止して、インデックス、データベース、データリポジトリ、コンテンツおよびアーカイブストア、サーバーコンフィグレーションファイルをリストアします。リストアする順序は問題ではありません。重要なのは、一貫性のある完全なデータセットをリストアすることです。これを行うには、以下のことを検討してください。

- リストアする前に、既存のファイルやフォルダーをインデックスフォルダーに残しておかないでください。空のディレクトリから開始してください。インデックススナップショットを適切なディレクトリ構造に必ず配置してください（例：<DataStoreIndex¥solr6¥index>）。その他のディレクトリはスタートアップ時に作成されます。
- 既存のデータをデータベースに残しておかないでください。空のデータベースから開始してください。
- リストアを開始するときにコンテンツストアが空になっているようにしてください。複数のコンテンツストアを使用している場合、各ロケーションに正しいファイルセットを配置してください。

すべてのデータをリストアしたら、サーバーを再起動すると、システムが最終的な一貫性チェックを行います。必要に応じてインデックスを更新し、スタートアップしてください。

注記

以降のセクションのスクリプトでは、スクリプトを実行する前に、データベースバックアップファイルの実際のロケーションを指定するようにしてください。

注記

バックアップにカスタム証明書のあるフォルダーが含まれる場合、29 ページの「**OpenLab Server/ECM XT リバースプロキシの設定**」の**ステップ 4**に従って設定します。4 サーバーまたはスケラブルシステムのインデックスサーバーの場合、37 ページの「**インデックスサーバーコンフィグレーション - 4 サーバースystemのみ**」を参照してください。

Solr インデックスのリストア

バックアップから Solr インデックスをリストアするには、以下の手順を実行します。

- 1 リストアするインデックスバックアップを見つけます。リストアするデータベースと一致するバックアップを必ず使用してください。

インデックスバックアップは、snapshot.xxxxxxxxxxxxxxxx という名前のフォルダーに保存されています。例：snapshot.20190708231001373。

- 2 **Agilent OpenLab Content Management Search service** を停止します。
- 3 サーバーコンフィグレーションでインデックスパスにより指定されたロケーションに “snapshot” フォルダーをコピーします。デフォルトは C:\¥DataStoreIndex¥solr6¥index¥alfresco です。
 - a このパスがすでに存在する場合、
C:\¥DataStoreIndex¥solr6¥index¥alfresco¥index にあるインデックスファイルを削除し、バックアップのファイルに置き換えます。
 - b このパスが存在しない場合、パス
C:\¥DataStoreIndex¥solr6¥index¥alfresco を作成し、“snapshot” フォルダーをコピーします。“snapshot” フォルダーの名前を “index” に変更し、C:\¥DataStoreIndex¥solr6¥index¥alfresco¥index のパスを作成します。
- 4 **Agilent OpenLab Content Management Search service** を開始します。

SQL サーバーデータベースをバックアップからリストア

システムを回復する必要が生じた場合、すべてのデータタイプ（データベース、コンテンツファイル、インデックス）を同じセットから回復することで、システムのデータの一貫性を確保する必要があります。

データベースのリストア用に以下のスクリプトが提供されています。

ECMDBRestore.sql このスクリプトは、DataStore および OLSharedServices ユーザーデータベースのデータをバックアップファイルのデータに置き換えます。

SQL サーバーの新たなインストールにリストアする場合（ECM XT がまだインストールされていない場合など）、少なくとも、OpenLab Server/ECM XT インストーラのステップ 1 とステップ 2 を最初に行い、DataStore および OLSharedServices データベースを作成する必要があります。リストアする前にこれらのデータベースが存在しない場合、以下のメッセージが送付されます。

「ユーザーにデータベース 'OLSharedServices' を変更する権限がないか、データベースが存在しない、またはデータベースがアクセスチェックが可能な状態にありません。」

OpenLab Server/ECM XT がすでにインストールされている場合、ECM XT インストーラのステップ 1 とステップ 2 を実行せずに続行できます。

リストアする前に OpenLab Server/ECM XT をインストール済みであるかどうかにかかわらず、リストア全体が完了したら OpenLab Server/ECM XT インストーラのステップ 4 を実行して、システム自体が再コンフィグレーションできるようにする必要があります。そうしないとシステムが正しく動作しません。

注記

バックアップファイルの実際のロケーションをスクリプトで使用するようにしてください。

```
-----
ALTER DATABASE [DataStore ] SET SINGLE_USER WITH ROLLBACK
IMMEDIATE

RESTORE DATABASE DataStore FROM DISK =
'¥¥NetworkBackup¥Database¥DataStore.bak' WITH RECOVERY, REPLACE

ALTER DATABASE [DataStore] SET MULTI_USER WITH ROLLBACK IMMEDIATE

ALTER DATABASE [OLSharedServices] SET SINGLE_USER WITH ROLLBACK
IMMEDIATE

RESTORE DATABASE OLSharedServices FROM DISK =
'¥¥NetworkBackup¥Database¥OLSharedServices.bak' WITH RECOVERY,
REPLACE

ALTER DATABASE [OLSharedServices] SET MULTI_USER WITH ROLLBACK
IMMEDIATE
-----
```

SystemDBRestore.sql このスクリプトは、SQL サーバーシステムデータベースのデータをバックアップファイルのデータに置き換えます。

```
-----
ALTER DATABASE [MSDB] SET SINGLE_USER WITH ROLLBACK IMMEDIATE
RESTORE DATABASE MSDB FROM DISK =
'¥¥NetworkBackup¥Database¥MSSQLBackupMsd.bak'
WITH RECOVERY, REPLACE
ALTER DATABASE [MSDB] SET MULTI_USER WITH ROLLBACK IMMEDIATE

ALTER DATABASE [Model] SET SINGLE_USER WITH ROLLBACK IMMEDIATE
RESTORE DATABASE Model FROM DISK =
'¥¥NetworkBackup¥Database¥MSSQLBackupModel.bak'
WITH RECOVERY, REPLACE
ALTER DATABASE [Model] SET MULTI_USER WITH ROLLBACK IMMEDIATE
-----
```

注記

システムデータベースをリストアするには、リストアするサーバー上の SQL サーバーのバージョンが、バックアップの取得元のバージョンと正確に一致している必要があります。不一致の状態が存在する場合、メッセージ 3168 が SQL サーバーによって作成されます。この状況が生じた場合、ターゲットサーバーをアップグレードまたはダウングレードして、バージョンが一致するようにしてください。3168 エラーメッセージには、ターゲットサーバーとバックアップファイルのバージョン番号が記載されています。この情報を使用して、ターゲットサーバーを正しいバージョンに設定してください。

MasterDBRestore.bat このスクリプトは、SQL サーバーマスターデータベースのデータをバックアップファイルのデータに置き換えます。このスクリプトは、Windows コマンドラインから SQLCMD ユーティリティを使用して実行されます。以下のステップを実行します。

注記

SQL サーバーバイナリフォルダーへのパスは、SQL サーバーのバージョンによって異なります。スクリプトで使用したパスを必ず確認してください。

- 1 Windows の [システムのプロパティ] ダイアログを開き、[環境変数] を選択します。(Windows 内で “sysdm.cpl” を検索し、コマンドを実行します。[詳細設定] タブで [環境変数] を選択します。)
- 2 パス環境変数を編集し、以下のパスを追加します。 C:¥Program Files¥Microsoft SQL Server¥MSSQL14.MSSQLSERVER¥MSSQL¥Binn
- 3 マスターデータベースをリストアする前に、サーバーをシングルユーザーモードに設定します。
 - a SQL Server Configuration Manager を使用して、SQL Server Services アイコンをクリックしてサービスのリストを表示します。SQL Server (MSSQLSERVER) サービスを右クリックし、[スタートアップパラメータ] タブを選択して以下を追加します。 -mSQLCMD
- 4 SQL Server Configuration Manager で SQL Server (MSSQLSERVER) サービスを再開します。
- 5 リストアスクリプトを実行します。
 - a Windows コマンドラインを使用して、MasterDBRestore.bat を実行します。システム管理者 (SA) のパスワードを入力するよう促されます。バッチファイルコンテンツをコマンドラインにコピーしてコマンドを実行することもできます。
- 6 マスターデータベースのリストアが完了したら：
 - a スタートアップスクリプトから -mSQLCMD パラメータを削除します。
 - b SQL Server サービスを再開します。

 以下を含む Windows コマンドラインから MasterDBRestore.bat を実行します。

```
sqlcmd -U SA -S localhost -Q "RESTORE DATABASE Master FROM DISK
= '¥¥NetworkBackup¥Database¥MSSQLBackupMaster.bak' WITH
REPLACE "
```

PostgreSQL データベースをバックアップからリストア

システムを回復する必要がある場合、すべてのデータタイプ（データベース、コンテンツファイル、インデックス）を同じセットから回復することで、システムのデータの一貫性を確保する必要があります。バックアップからリストアする原因となったデータベースの不具合に応じて、必要な手順が異なることがあります。このドキュメントの目的のために、不具合は PostgreSQL データベースの完全な消失と想定しています（ユーザーおよびシステムデータベースファイルと再試行ログが存在していない、など）。この場合、前回のバックアップ以降に行った変更は失われます。

リストアに関する検討事項

- 正常にリストアされるようにするには、リストアするサーバー上の PostgreSQL のバージョンが、バックアップの取得元のバージョン以降である必要があります。
- OpenLab Server/ECM XT がインストールされていない新しいサーバーにリストアする場合、バックアップファイルからデータベースをリストアする前に、OpenLab Server/ECM XT インストーラのステップ 1 から 4 を実行する必要があります。

データベースのリストア

以下のステップを実行してデータベースをリストアします。

- 1 **alfrescoTomcat** サービスを停止します。
- 2 **olcm-postgresql-x64-11** サービスを停止します。
- 3 <PostgreSQL Installation> ディレクトリからすべてのコンテンツを削除します。デフォルトは、C:\ProgramData\Agilent\PostgreSqlData-11-OLCM です。
- 4 base.tar.gz アーカイブのコンテンツを <PostgreSQL Installation> フォルダーへ抽出します。
- 5 <PostgreSQL Installation> フォルダー内で **pg_wal** フォルダーを見つけます。
- 6 **pg_wal.tar.gz** アーカイブのコンテンツを pg_wal フォルダーへ抽出します。
- 7 **alfrescoTomcat** サービスを再開します。
- 8 **Agilent OpenLab Shared Services** サービスを再開します。

最後のコマンドが実行されると、データベースがリストアされ、ユーザーアクティビティに使用できるようになります。

Oracle データベースをバックアップからリストア

バックアップファイルから Oracle データベースへのリストア方法は、Oracle のドキュメントを参照してください。

- 1 以下のコマンドを実行してデータベースをリストアします。

表 21 データ損失後の Oracle データベースのリストア

ツール	コマンド
SQL	SHUTDOWN IMMEDIATE
該当なし	保存された SPFILE を <Oracle Installation>%database% ヘコピー
SQL	CREATE PFILE='<Oracle Installation>%database%PFIL<YOURINSTANCENAME>.ORA' FROM SPFILE='<Oracle Installation>%database%SPFILE<YOURINSTANCENAME>.ORA
テキストエディタ	tnsnames.ora を編集して (UR = A) 句を追加 デフォルトのロケーション: <Oracle Installation>%network%admin%tn snames.ora <YOURINSTANCENAME> = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = YourServerName) (PORT = 1521))) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = <YOURINSTANCENAME>) (UR = A)))
SQL	STARTUP NOMOUNT データベースがすでに実行中の場合は、代わりに SHUTDOWN IMMEDIATE。次に、STARTUP NOMOUNT を実行し、RMAN と SQL を再接続します。

- 2 最後のコマンドが実行されたら、データベースをシャットダウンし Windows server を再起動します。

リストアに関する検討事項

システムを回復する必要がある場合、すべてのデータタイプ（インデックス、データベース、コンテンツ、コンフィグレーションファイル）を同じセットから回復することで、システムのデータの一貫性を確保する必要があります。バックアップからリストアする原因となったデータベースの不具合に応じて、必要な手順が異なることがあります。

データリポジトリのリストア

105 ページの「**OpenLab Server/ECM XT Server の手動リストア手順**」に記載された手順に従ってデータリポジトリをリストアします。

アクティビティログインデックスの再構築

アクティビティログテーブルまたはデータが破損した場合や Shared Services データベースが既存の OpenLab インストールでリストアされている場合に、次の手順で OpenLab Shared Services アクティビティログインデックスを再構築します。

アクティビティログインデックスは以下の状況で自動的に再構築されます。

- Firebird データベースを用いたファイルベースのワークステーションコンフィグレーションを使用している
- Shared Services データベースが新たなインストールでリストアされている
- データを移行またはアップグレードしている

インデックスの再構築に要する時間は、データベースのタイプとアクティビティログレコード数によって異なります。数時間かかることもあります。処理中は、アプリケーションでアクティビティログの検索はできません。

アクティビティログを再構築するには、

- 1 管理者としてコマンドプロンプトを開始します。
- 2 以下のコマンドを実行します。

```
net stop SharedServicesHost && del /s /f /q  
%ProgramData%\Agilent\OLSS\Index\ActivityLog && net start  
SharedServicesHost
```

手動ホットバックアップ手順

アクティビティログインデックスの再構築

以下のエラーが発生する可能性があります。

- **メッセージ**

Agilent OpenLab Shared Services サービスは開始されていません。 *NET HELPMSG 3521* と入力すると、より詳しい説明が得られます。

解決策

以下のコマンドを使用します。

```
del /s /f /q %ProgramData%\Agilent\OLSS\Index\ActivityLog &&  
net start SharedServicesHost
```

- **メッセージ**

システムエラー 5 が発生しました。アクセスが拒否されました。

解決策

コマンドプロンプトを管理者として実行してください。

8

アップグレードと再設定

オペレーティングシステムを変更した場合の OpenLab Server/ECM XT Server
のアップグレード 151

OpenLab Server/ECM XT Server の再設定 151

オペレーティングシステムを変更した場合の OpenLab Server/ECM XT Server のアップグレード

- 1 新しいオペレーティングシステムを搭載した新しいマシンに OpenLab Server/ECM XT をインストールします。
- 2 古いマシンで、手動システムバックアップを実行します。62 ページの「**バックアップユーティリティを使用する OpenLab Server/ECM XT のバックアップ**」または 96 ページの「**OpenLab Server/ECM XT Server の手動バックアップ手順**」を参照してください。
- 3 新しいマシンで、サーバーリストア手順を実行します。75 ページの「**リストアユーティリティを使用する OpenLab Server/ECM XT のリストア**」または 105 ページの「**OpenLab Server/ECM XT Server の手動リストア手順**」を参照してください。

OpenLab Server/ECM XT Server の再設定

このセクションでは、以下のような一般的なシナリオを対象としています。

- データベースサーバー（ローカルまたはリモート）を使用した OpenLab Server/ECM XT をインストール済みで、データベースサーバーソフトウェアを新しいバージョンにアップグレードするかハードウェアをアップグレードするため、データベースサーバーソフトウェアを新しいマシンに再配置する必要がある。OpenLab Server/ECM XT に新しいデータベースサーバーへの接続を設定し、引き続き機能するようにする必要がある。
- ファイルサーバーの空き容量が不足しているため、コンテンツストレージを別のハードウェアに移動することにした。
- 企業のセキュリティポリシーの変更により、OpenLab Server/ECM XT によって使用されるシステムユーザーやパスワードを変更する必要がある。

以降で、OpenLab Server のコンフィグレーションユーティリティ (OSCU) を使用してこれらのタスクを実行する方法について説明します。

一般に、プロセスは 4 つのステップで構成されます。

- 1 152 ページの「OpenLab Server/ECM XT の停止」
- 2 152 ページの「インフラストラクチャへの変更」
- 3 159 ページの「OpenLab Server のコンフィグレーションユーティリティの実？」
- 4 163 ページの「OpenLab Server/ECM XT の起動」

コンテンツまたはアーカイブストアを追加したい場合は、164 ページの「追加のコンテンツまたはアーカイブストア設定」を参照してください。

OpenLab Server/ECM XT の停止

以下の順序でサービスを停止します。

- 1 Agilent OpenLab Content Management Search service
- 2 alfrescoTomcat
- 3 Agilent OpenLab Shared Services

インフラストラクチャへの変更

DB サーバーの移動

OpenLab Server/ECM XT および Shared Services データベースを新しいサーバーへ再配置します。このステップは、使用する DB タイプに固有のものとなります。『*Agilent OpenLab Server* および *OpenLab ECM XT* ハードウェアおよびソフトウェア要件ガイド』を参照してください。SQL Server および Oracle データベースについては、ベンダーのドキュメントを参照してください。

PostgreSQL データベースの移動 移動先と移動元のデータベースサーバーバージョンが同じである必要があります。メジャーバージョンとマイナーバージョンの数字が等しくなければなりません。例：14.x.x. この例では、

- Server1 が移動元マシン
- Server2 が移動先マシン

- 1 Server1 で、PostgreSQL サービスを停止します（バージョン 14 の場合：**olcm-postgresql-x64-14**）。
- 2 **[スタート]** > **[Agilent Technologies]** > **[サーバーコンフィギュレーションビューア]** をクリックします。
- 3 **[Installation Summary]** セクションで **PostgreSQL Database Folder** を確認し、バックアップを作成してください。
- 4 Server2 で、PostgreSQL データフォルダーを解凍します。このフォルダーに **PG_DATA_NEW** という名前を付けます。
- 5 PostgreSQL インストーラを実行します。データフォルダーを指定するよう要求されたら、**PG_DATA_NEW** と入力します。
- 6 **[Next]** をクリックし、インストールを完了させます。
- 7 再設定を行った場合、PostgreSQL サーバーは OpenLab Server/ECM XT をインストールしたマシンとは別のマシンへ移動するため、次のステップに従います。再設定を行っていない場合は、**ステップ 8**に進みます。

PostgreSQL データベースユーザーを使用して PostgreSQL へのリモート接続を行うには：

- a Server1、Server2、および OpenLab Server/ECM XT Server がすべて同じドメインに接続されていることを確認します。
- b **PG_DATA_NEW** フォルダーから **pg_hba.conf** を開き、以下のラインが含まれていることを確認します。

```
host all "postgres" 172.16.0.111/32 md5
host all "postgres" ::1/128 md5
host all "SYSTEM" 127.0.0.1/32 sspi
host all "SYSTEM" ::1/128 sspi
host all all 127.0.0.1/32 md5
host all all ::1/128 md5
```

IPv4 アドレスが 172.16.0.111 で IPv6 アドレスが fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed の OpenLab Server/ECM XT サーバーに以下の行を追加します。

```
host all "postgres" 172.16.0.111/32 md5
host all "postgres"
fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128 md5
host all all 172.16.0.111/32 md5
host all all fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128
md5
```

外部 PostgreSQL サーバーの設定方法の詳細については、『*Agilent OpenLab Server/ECM XT インストールガイド*』の「リモート PostgreSQL データベースサーバーのコンフィグレーション」セクションを参照してください。ネットワーク管理者に問い合わせ、お使いのネットワークに最適なオプションを見つけてください。

- c PG_DATA_NEW** フォルダーから **pg_ident.conf** を開き、以下のラインを追加します。

```
# MAPNAME    SYSTEM-USERNAME    PG-USERNAME
datastore    Server1$            SYSTEM
```

ここで、**Server1\$** は、PostgreSQL によって割り当てられたリモートシステムユーザー名です。通常、システムユーザー名は、OpenLab Server/ECM XT が実行されているマシンの NetBIOS 名の後にドル記号 (\$) が付いたものと一致します。

ユーザー名が一致せず OpenLab ECM XT のコンフィグレーションが失敗した場合、**PG_DATA_NEW > pg_log** フォルダー内の最新のメッセージを確認して、以下と同様のメッセージがないか確認してください。

```
2015-06-02 10:05:34 PDT FATAL:SSPI authentication failed for
user "SYSTEM"
```

```
2015-06-02 10:05:37 PDT LOG: provided user name (SYSTEM) and
authenticated user name (WIN-ITGSOV7UQM2$) do not match
```

ここで、WIN-ITGSOV7UQM2\$ は、**pg_ident.conf**に入力しなければならない SYSTEM_USERNAME です。

セキュリティ機能に関する詳細については、PostgreSQL の公式ドキュメントを参照してください。

SQL 認証を使用して PostgreSQL へのリモート接続を行うには：

PG_DATA_NEW フォルダーから **pg_hba.conf** を開き、IPv4 アドレスが 172.16.0.111 で IPv6 アドレスが fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed の OpenLab Server/ECM XT サーバーに以下の行が含まれていることを確認します。

```
host    all    "postgres"    172.16.0.111/32    md5
host    all    "postgres"
        fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128    md5
host    all    all    172.16.0.111/32    md5
host    all    all    fc00:1ac4:65fb:34cb:e71c:db64:c33:e1ed/128
        md5
```

pg_hba.conf で単一の IP アドレスではなくサブネット範囲を定義することができます。以下の例では、アドレス範囲 172.16.0.0 から 172.16.0.255 およびアドレス範囲 fc00:1ac4:65fb:34cb::/64 IPv6 からの PostgreSQL データベースサーバーへのすべての接続を許可しています。

```
host all "postgres" 172.16.0.0/24 md5
host all "postgres" fc00:1ac4:65fb:34cb::/64 md5 0.0/24 md5
host all all fc00:1ac4:65fb:34cb::/64 md5
```

セキュリティ機能に関する詳細については、PostgreSQL の公式ドキュメントを参照してください。

- 8 変更を適用するには、PostgreSQL サービスを再起動します。

1つのコンテンツストレージロケーションの変更

この手順では、1つのコンテンツストレージロケーションのみ対象としています。複数のコンテンツストレージをセットアップした場合は、156 ページの「**複数のコンテンツストレージロケーションの変更**」を参照してください。

- 1 コンテンツストレージ、インデックスストレージ、およびアーカイブストレージ用のフォルダーを作成します。ストレージロケーションは絶対パスまたは UNC パスである必要があります。ネットワークドライブはサポートされていません。

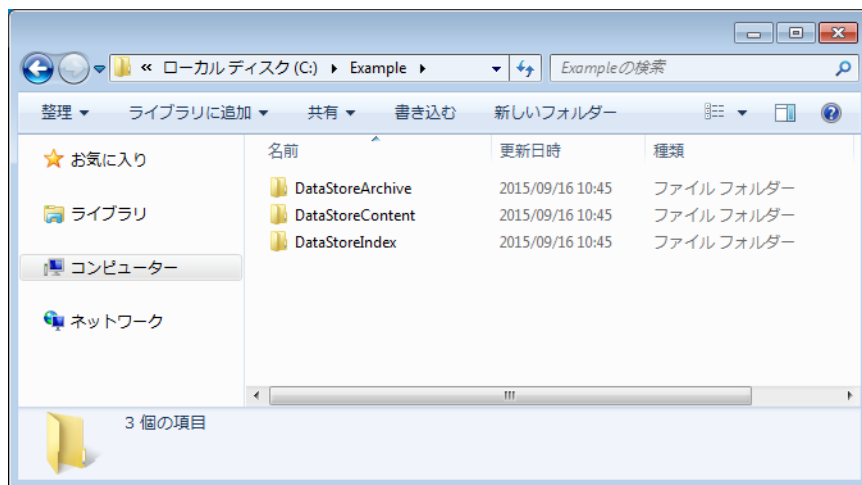


図 8 OpenLab ECM XT のストレージフォルダー

- 2 ストレージフォルダーがすでに存在する場合は、既存の各ストレージロケーションから新しいロケーションへコンテンツを移動します。

例：

- コンテンツストレージの既存のフォルダーロケーションが
C:¥DataStoreContent
- コンテンツストレージの新しいフォルダーロケーションが
C:¥Example¥DataStoreContent

C:¥DataStoreContent フォルダーからすべてのコンテンツを
C:¥Example¥DataStoreContent へ移動します。必要に応じて、インデックス
ストレージおよびアーカイブストレージフォルダーのコンテンツも移動し
ます。

複数のコンテンツストレージロケーションの変更

- 1 コンテンツストレージ、インデックスストレージ、およびアーカイブストレージ用のフォルダーを作成します。ストレージロケーションは絶対パスまたは UNC パスである必要があります。ネットワークドライブはサポートされていません。
- 2 ストレージフォルダーがすでに存在する場合は、既存の各ストレージロケーションから新しいロケーションへコンテンツを移動します。

例：

- コンテンツストレージの既存のフォルダーロケーションが
C:¥DataStoreContent
- コンテンツストレージの新しいフォルダーロケーションが
C:¥Example¥DataStoreContent

C:¥DataStoreContent フォルダーからすべてのコンテンツを
C:¥Example¥DataStoreContent へ移動します。必要に応じて、インデックス
ストレージおよびアーカイブストレージフォルダーのコンテンツも移動し
ます。

- 3 **alfresco-global.properties** を開きます。デフォルトのロケーションは、
**C:¥Program Files (x86)¥Agilent Technologies¥OpenLab Data
Store¥tomcat¥shared¥classes** です。
- 4 すべてのコンテンツストアパスを更新します。例：

```
dir.root=C:¥¥Example¥¥DataStoreContent
dir2.root=C:¥¥Example¥¥DataStoreContent
dir3.root=C:¥¥Example¥¥DataStoreContent
```

OpenLab ECM XT ユーザーまたはパスワードの変更

データベースユーザーのパスワードを変更したり、ユーザーを作成して OpenLab Server/ECM XT で使用できるように設定できます。

既存のデータベースユーザーのパスワードのみ変更する場合は、MS SQL Server Management Studio、pgAdmin III、Oracle Developer など、ソフトウェアの標準手順を使用したデータベース統合開発環境 (IDE) を使用します。詳細については、公式ドキュメントを参照してください。PostgreSQL パスワードを変更すると、データベースへのバックアップユーティリティアクセスに影響する場合があります。

新しいユーザーの作成

- 1 ユーザーを作成します。
- 2 データベーステーブルでユーザー認証を付与します。

たとえば、Shared Services データベース用の「テスト」ユーザーを作成した場合、以下のスクリプトを実行して、すべてのデータベーステーブルで権限を付与します。

```
DO
$$
DECLARE
    r information_schema.tables%rowtype;
    user_name VARCHAR = 'test'; -- specify username
BEGIN
    FOR r IN SELECT * FROM information schema.tables WHERE tab
schema='public'
        LOOP
            RAISE NOTICE 'EXECUTE "ALTER TABLE % OWNER TO
%";',r.table_name, user_name; -- for debug
            EXECUTE 'ALTER TABLE \' || quote_ident(r.table_name) || ' OWNER
TO \' || user_name || ';' ;
        END LOOP;
END
$;$;
```

MS SQL Server データベース用の新しいユーザーを作成 MS SQL Server Management Studio を使用して、データベースログインマッピングを指定します。そのユーザーが、必要なデータベースのデータベースロール **db_datareader** および **db_datawriter** のメンバーであることを確認します。データベース管理者資格情報を用いてクエリーを実行する必要があります。

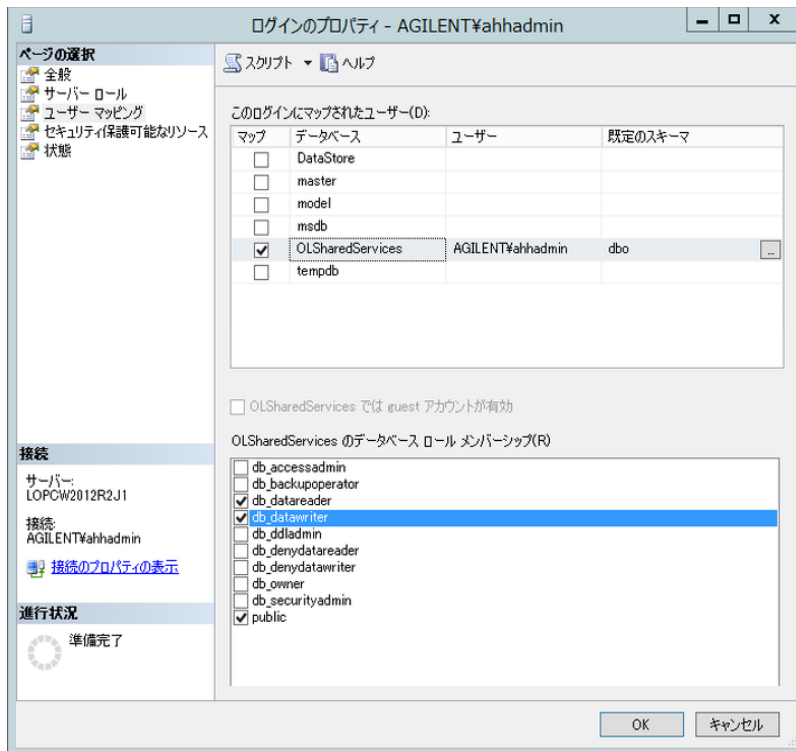


図 9 MS SQL Server Management Studio

Oracle データベース用のユーザーを作成

すべてのデータベースオブジェクト（制約付きテーブル、シーケンス、トリガーなど）を、古いスキーマ（ユーザー）から新しいスキーマ（ユーザー）へ移行します。これは Power Designer を使用して行えます（データベースのスキーマをデータと一緒にインポートし、調整済みスキーマを展開します）。

データベースタイプによっては、その他の許可を付与することが必要な場合があります。詳細については、DB サーバーマニュアルを参照してください。

OpenLab Server のコンフィグレーションユーティリティの実行

OpenLab Server のコンフィグレーションユーティリティはサーバーにインストールされ、インストーラなしで単独で実行できます。コンフィグレーションユーティリティは、Agilent のスタートアップメニューに追加されます。

注意

OpenLab Server のコンフィグレーションユーティリティ（OSCU）のすべての画面はデフォルトで自動入力されており、実際の OpenLab Server/ECM XT のコンフィグレーションを反映したものとなっています。152ページの「[インフラストラクチャへの変更](#)」で変更したフィールドのみ、それを反映してください。その他の値は編集しないようにしてください。その他のフィールドを変更すると、構成がクラッシュする可能性があります。

- 1 Windows の [スタート] メニューから、[Agilent Technologies] > [サーバーコンフィグレーションユーティリティ] をクリックします。
- 2 ようこそ画面で [次へ] をクリックします。
- 3 [データベースタイプ] 画面で、使用しているデータベースが選択されています。[次へ] をクリックします。
- 4 [データベースサーバー] 画面に表示される情報は、OpenLab Server/ECM XT Server に対して選択されたデータベースタイプにより異なります。表示されたデータベースサーバー接続情報を確認し、新しい構成に応じて変更を行います。

この画面は、データベースサーバー接続情報（サーバー名やポート番号など）が変更されている場合のみ編集してください。

[確認] をクリックして、入力した値を確認し、[次へ] をクリックします。

- 5 データベースユーザーまたはパスワードが変更されている場合のみ、[スキーマ情報] 画面で情報を編集します。

[確認] をクリックして、入力した値を確認し、[次へ] をクリックします。

6 **【サーバー設定】** タブで、コンフィグレーション情報を入力し、**【次へ】** をクリックします。

- オールインワンシステムコンフィグレーションを使用する場合は、**Content Management（インデックスおよび検索サービスを含む）** を選択します。デフォルトは、この選択です。
- 拡張可能（スケーラブル）なシステムトポロジーマたは 4 サーバートポロジーを使用し Content Management ウェブサービスを実行するサーバーを作成する場合は、**Content Management のみ**を選択します。
- 拡張可能（スケーラブル）なシステムトポロジーマたは 4 サーバートポロジーを使用し インデックスおよび検索サービスを実行するサーバーを作成する場合は、**インデックスおよび検索サービスのみ**を選択します。Content Management がインストールされたサーバーの完全修飾ドメイン名を入力し、**【確認】** をクリックします。

【次へ】 をクリックします。

7 **【アカウント資格情報】** 画面で、アカウントのアクセス資格情報を入力します。4 サーバートポロジーマたは スケーラブルトポロジーマたは 外部の PostgreSQL データベースサーバーを使用する場合、Windows ドメインユーザーをサービスアカウントとして使用します。このユーザーは「サービスとしてログオン」権限を持っている必要があります。

【確認】 をクリックして、資格情報を確認し、**【次へ】** をクリックします。

8 [コンテンツパス] 画面で、コンテンツストレージ、アーカイブストレージ、およびインデックスロケーションの情報を確認します。

- すべてのロケーションパスは一意にしてください。たとえば、コンテンツロケーションとアーカイブロケーションに同じパスを使用することはできません。
- UNC パスが使用されている場合、マニュアルでパスを検証する必要があります。この検証では、ユーザーに UNC パスの読み取りおよび書き込みのアクセス権があるかどうかは確認しません。
- サーバーが **Content Management のみ**または**インデックスおよび検索のみ**としてコンフィグレーションされている場合、すべてのサーバーでコンテンツストレージロケーション用の共有ストレージロケーションの UNC パスを使用するよう同じコンテンツストレージロケーションをコ構成してください。

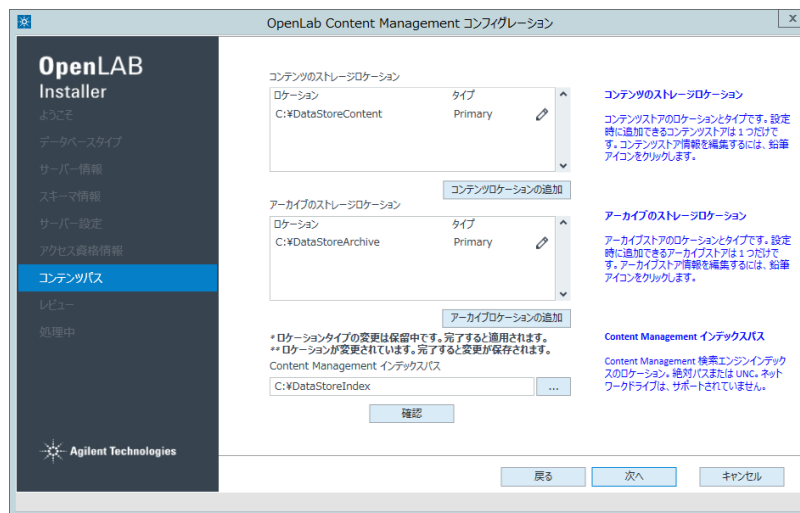


図 10 OpenLab Installer コンテンツパス 画面

コンテンツまたはアーカイブのストレージロケーションを編集するには、

- ロケーションの **[編集]** アイコン（鉛筆）をクリックします。
- ロケーション情報を必要に応じて編集し、**[完了]** をクリックします。

ダブルアスタリスク (**) インジケーターがロケーションの名前の横に表示されます。

新しいコンテンツまたはアーカイブのストレージロケーションを追加するには、

- a **【コンテンツロケーションの追加】** または **【アーカイブロケーションの追加】** をクリックします。新しいロケーションは一度に 1 つしか追加できません。
- b ロケーションのタイプとして、ファイルシステムまたは Amazon S3 (AWS S3) を選択します。
- c 必要な情報を入力します。S3 の場合、追加する前にロケーションを作成しアクセス可能にする必要があります。
- d ロケーションを追加してロケーションリストに戻るには、**【完了】** をクリックします。新しいロケーションの追加をキャンセルするには、**【キャンセル】** をクリックします。

新しいロケーションが、リストの最初のアイテムとして表示されます。ロケーションタイプ (Primary) の横にアスタリスク (*) が表示され、この新しいロケーションがファイルの書き込み先となることが示されます。

この新しいロケーションを削除するには、**【削除】** アイコン (ゴミ箱) をクリックします。

前のプライマリロケーションのロケーションタイプの横にアスタリスク (*) が表示されます。これは、このロケーションがセカンダリ

(Secondary) と見なされ、読み取り専用になっていることを示します。このロケーションからデータを取得できますが、新しいデータを保存することはできません。

コンテンツロケーションおよびアーカイブロケーション用の以下のストレージロケーションの組み合わせが Amazon S3 でサポートされています。

表 22 ストレージロケーションの組み合わせ

プライマリ	セカンダリ
S3	on-prem
on-prem	on-prem
S3	(セカンダリなし)

サーバーがインデックスおよび検索を含む Content Management か、インデックスおよび検索のみのサーバーとしてコンフィグレーションされている場合は、インデックスロケーションがパスになります。

サーバーが Content Management のみのサーバーとしてコンフィグレーションされている場合は、パスの代わりに OpenLab インデックスサーバーのホスト名が提供されます。確認時に OpenLab インデックスサーバーの電源が投入されている必要があり、ICMP エコー要求が許可されていなければなりません。

【確認】をクリックして、ロケーションを確認し、【次へ】をクリックします。

- 9 デフォルトでは、Agilent OpenLab 内部証明書がインストールされます。インストールされていない場合、【既存のカスタム証明書を使用する】を選択し、証明書情報を入力します。次に、【次へ】をクリックします。
- 10 更新したコンフィグレーションサマリーを確認して、【適用】をクリックします。
- 11 コンフィグレーションが完了したら、【完了】をクリックします。
- 12 新しいストレージロケーションにコンテンツを移動します。

OpenLab Server/ECM XT の起動

OSCU プロセスが完了すると、OpenLab Server/ECM XT が作動します。

新しいコンフィグレーションが正常に取得されたことを確認するには、

- 1 コントロールパネルにログインし、【管理】 > 【Content Management】 > 【同期】をクリックします。

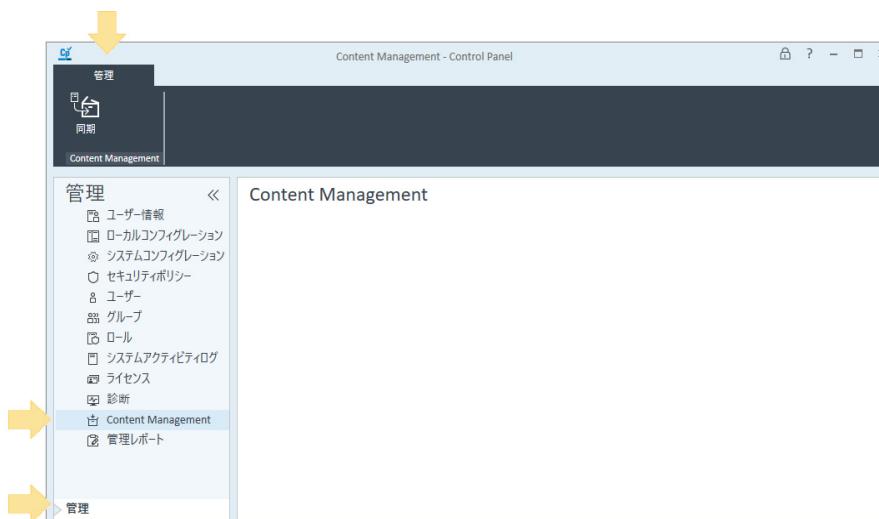


図 11 コントロールパネル Content Management の同期

- 2 Content Management にログインし、すべてのコンテンツが所定の場所にあることを確認します。

追加のコンテンツまたはアーカイブストア設定

OpenLab Server のコンフィグレーションユーティリティを使用して、追加のコンテンツまたはアーカイブストアを OpenLab Server/ECM XT Server に設定します。詳細については、159 ページの「**OpenLab Server のコンフィグレーションユーティリティの実 ?**」を参照してください。

営業およびサポートのお問い合わせ先 166

営業およびサポートのお問い合わせ先

営業およびサポートのお問い合わせ先については、以下のウェブサイトを確認してください。

<https://www.chem-agilent.com/contents.php?id=1001827>

アジレントコミュニティ（英語サイト）

1万人以上のユーザーが参加するアジレントコミュニティで、疑問が解消されるかもしれません。プラットフォーム技術によって構成された、厳選されたサポート資料をご覧ください。同業者や協力者に質問することができます。作業に関連した新しいビデオやドキュメント、ツール、ウェビナーで通知を受けられます。

<https://community.agilent.com>

www.agilent.com

© Agilent Technologies, Inc. 2024
文書番号 D0013947ja Rev. C.00
2024 年 2 月

