SQL サーバの強化

SQL サーバの強化に関する検討事項

SQL の強化に関する検討事項の上位

SQL の強化に関する検討事項の上位：

1. Active Directory ドメインコントローラに SQL サーバをインストールしないでください。
2. Microsoft サイトから SQL サーバの最新の累積アップデートをインストールします：https://www.microsoft.com/en-us/download/details.aspx?id=56128。
3. ICM をインストールする前に、sa アカウントの強力なパスワードを設定します。
4. 最小権限のアカウントを使用して実行するには、常に SQL サーバサービスをインストールします。組み込みのローカルシステムアカウントを使用して、SQL サーバをインストールして実行してはなりません。代わりに、バーチャルアカウントを使用します。

   詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html の「*Cisco Unified ICM/Contact Center Enterprise* ステージング ガイド」を参照してください。
5. SQL サーバエージェントサービスを有効にして、Unified ICM でのデータベースメンテナンスのために [Automatic（自動）] に設定します。

（注） Microsoft から SQL サーバの最新の累積更新をインストールするには、SQL サーバエージェントサービスを無効にする必要がある場合があります。そのため、累積更新のインストールを実行する前に、このサービスを無効にリセットします。インストールが完了したら、サービスを停止して有効に戻します。

6. SQL ゲストアカウントを無効にします。
7. Unified ICM の管理者に sysadmin のメンバーを制限します。
8. 管理&データサーバがロガーと同じセキュリティゾーンにない限り、ネットワーク ファイアウォールで TCP ポート 1433 と UDP ポート 1434 をブロックします。
9. Microsoft SQL サーバサービスのリカバリアクションを変更し、失敗後に再起動します。
10. すべてのサンプルデータベースを削除します。
11. サインインの失敗に対する監査を有効にします。

次の表に、SQL 強化の設定と対応するデフォルト値とサポートされる値を示します。

設定名	デフォルト値（Default Value）	サポートされる値
起動手順のスキャン	無効 |0|	0 または 1 がサポートされています。Unified CCE では、有効にする必要はありません。ただし、有効にすることで問題は発生しません。
アドホック分散クエリ	無効 |0|	0 または 1 がサポートされています。0 の方が安全です。

関連トピック

SQL サーバのユーザと認証 （2 ページ）
バーチャル アカウント （5 ページ）

SQL サーバのユーザと認証

SQL サーバアカウント用にユーザを作成する場合は、SQL サーバサービスを実行するための最も弱い権限を持つ Windows アカウントを作成します。SQL サーバのインストール中にアカウントを作成します。

インストール中は、SQL サーバデータベースエンジンが Windows 認証モードまたは SQL サーバと Windows 認証モードのいずれかのモードに設定されます。インストール中に Windows 認証モードを選択した場合、sa ログインは無効になります。後で認証モードを SQL サーバと Windows 認証モードに変更した場合、sa ログインは無効な状態のままです。sa ログインを有効にするには、ALTER LOGIN ステートメントを使用します。詳細については、https://msdn.microsoft.com/en-us/library/ms188670.aspx を参照してください。

SQL サーバサービスアカウント用に作成されたローカルユーザまたはドメインユーザアカウントは、それぞれ Windows またはドメインパスワードポリシーに従います。厳格なパスワードポリシーをこのアカウントに適用します。ただし、パスワードの有効期限は設定しないでください。パスワードの有効期限が切れると、SQL サーバサービスは機能しなくなり、管理 & データサーバが失敗します。

サイトの要件は、パスワードとアカウント設定を適用できます。次のような最小設定を検討してください。

表 *1*: パスワードとアカウント設定

設定	値
パスワード履歴の強制	24 個のパスワードを記憶
パスワードの最小文字数	12 文字
パスワードの複雑度	有効
最短パスワード変更間隔	1 日
アカウントロックアウト時間	15 分
アカウントロックアウトしきい値	無効なログイン試行 3 回
アカウントロックアウトカウンタのリセット	15 分

混在モード認証は、SQL サーバの自動強化によって強制されます。

自動化された SQL サーバの強化中に、sa パスワードが空白だった場合は、sa アカウントを保護するために、ランダム生成の強力なパスワードが生成されます。

インストール後に sa アカウントのパスワードをリセットするには、Windows ローカル管理者アカウントを使用して SQL サーバにログインします。

SQL サーバのセキュリティに関する検討事項

Microsoft SQL サーバは、設計、デフォルト、および導入により、以前のバージョンよりもはるかに安全です。これにより、はるかに詳細なアクセス制御と、攻撃対象領域を管理する新しいユーティリティが提供され、より低い権限で実行されます。セキュリティ機能を実装する際は、データベース管理者が次のセクションのガイドラインに従う必要があります。

自動 SQL サーバの強化

SQL サーバセキュリティの自動強化ユーティリティでは、次の作業を実行します。

- 混在モード認証を適用します。
- 名前付きパイプ（np）が SQL サーバクライアント ネットワーク プロトコル順序の TCP/IP（tcp）の前にリストされることを確認します。
- SQLWriter および SQLBrowser サービスを無効にします。
- 空白の場合、SQL サーバユーザの「sa」のパスワードを強制的に設定します。

SQL サーバのセキュリティ強化ユーティリティ

SQL サーバのセキュリティ強化ユーティリティを使用すると、ロガーと管理サーバおよびデータサーバ/HDS コンポーネントの SQL サーバセキュリティの強化またはロールバックを可能にします。強化オプションにより、不要なサービスや機能が無効になります。最新バージョンのセキュリティ設定が既に適用されている場合は、[強化（Harden）] オプションは何も変更しません。[ロールバック（Rollback）] オプションでは、最後の強化を適用する前に存在していた SQL サービスと機能の状態に戻ります。

必要に応じて、Unified CCE のインストールとアップグレードの一部として、またはセキュリティ ウィザード ツールを使用して SQL サーバのセキュリティ強化を適用できます。このユーティリティは、Windows PowerShell スクリプト ICMSQLSecurity.ps1 を実行して内部で管理されます。PowerShell スクリプトを直接実行して、強化を適用することもできます。

（注） 管理者としてセキュリティ ウィザード ツールまたは Windows PowerShell スクリプトを実行します。

ユーティリティの場所

このユーティリティは次の場所にあります。

```
%SYSTEMDRIVE%\CiscoUtils\SQLSecurity
```

HARDEN コマンド

Windows PowerShell コマンドラインで、次の値を入力します。

```
Powershell .\ICMSQLSecurity.ps1 HARDEN
```

（注） 現在の SQL サーバの構成は、ユーティリティが SQL サーバの強化を適用する前に、<ICMInstallDrive>:\CiscoUtils\SQLSecurity\icmsqlsecuritybkp.xml にバックアップされています。

ROLLBACK コマンド

前に強化が適用された場合、ROLLBACK コマンドは以前の SQL サーバ構成にロールバックします。

以前の SQL サーバ構成にロールバックするには、次のコマンドを入力します。

```
Powershell .\ICMSQLSecurity.ps1 ROLLBACK
```

（注） Unified CCE が正常に機能するには、次の設定が必要です。自動ロールバックを実行すると、元の状態には戻りません。

1. SQL サーバ クライアント ネットワーク プロトコル順序の TCP/IP（tcp）の前にリストされている名前付きパイプ（np）。
2. 混合モードの認証。

コマンドのヘルプ

コマンドラインで引数を使用しない場合、ヘルプが表示されます。

出力ログ

すべての出力ログがファイルに保存されます。

```
%SYSTEMDRIVE%\CiscoUtils\SQLSecurity\Logs\ICMSQLSecurity.log
```

手動 SQL サーバの強化

デフォルトでは、SQL サーバ は VIA エンドポイントを無効にし、専用管理者接続（DAC）をローカルアクセスに制限します。また、デフォルトでは、すべてのログインが、共有メモリ、名前付きパイプ、TCP/IP、および VIA エンドポイントを使用して CONNECT に対する GRANT 権限を持っています。Unified ICM には、名前付きパイプエンドポイントと TCP/IP エンドポイントだけが必要です。

手順

- SQL サーバのセットアップ中に、名前付きパイプエンドポイントと TCP/IP エンドポイントの両方を有効にします。名前付きパイプエンドポイントの優先順位が TCP/IP よりも高くなるようにしてください。

（注） SQL サーバセキュリティ強化ユーティリティは、これらのエンドポイントの可用性と順序を確認します。

- すべての不要なエンドポイントへのアクセスを無効にします。たとえば、データベースにアクセスできるすべてのユーザ/グループに対して、VIA エンドポイントへの接続権限を拒否します。

バーチャル アカウント

バーチャル アカウント、前者のセキュリティレベルが高いため、SQL サービスのネットワークまたはローカルサービスアカウントよりも優先されます。バーチャルアカウントは最小限の

権限で実行されます。CCE のインストーラは、ボリューム メンテナンス タスクの実行権限を SQLアカウントに追加します。この権限は、データベースの作成や拡張などのデータベース関連の操作を実行するために必要です。

社内ポリシーでこの権限の使用が許可されていない場合は、削除できます。ただし、データベースの作成や拡張などのデータベース関連の操作を実行すると、（データベースのサイズによっては）時間が長くなります。