# OnCommand Workflow Automation をセットアップしています

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

# 目次

# OnCommand Workflow Automation をセットアップしています

OnCommand Workflow Automation （ WFA ）のインストールが完了したら、いくつかの設定を完了する必要があります。WFA にアクセスし、ユーザを設定し、データソースをセットアップし、クレデンシャルを設定し、 WFA を設定する必要があります。

## OnCommand Workflow Automation にアクセスします

OnCommand Workflow Automation （ WFA ）には、 Web ブラウザを使用して、 WFA サーバにアクセスできる任意のシステムからアクセスできます。

使用している Web ブラウザに対応した Adobe Flash Player がインストールされている必要があります。

手順

1. Web ブラウザを開き、アドレスバーに次のいずれかを入力します。
   - 「 + https://wfa_server_ip+` 」と入力します

     wfa_server_ip は、 WFA サーバの IP アドレス（ IPv4 または IPv6 アドレス）または完全修飾ドメイン名（ FQDN ）です。

   - WFA サーバ上の WFA にアクセスしている場合：「 + https://localhost/wfa+` 」 WFA にデフォルト以外のポートを指定した場合は、次のようにポート番号を含める必要があります。
   - 「 + https://wfa_server_ip:port+` 」と入力します
   - 「 + https://localhost:port+` port 」は、インストール時に WFA サーバに使用した TCP ポート番号です。
2. サインインセクションで、インストール時に入力した admin ユーザのクレデンシャルを入力します。
3. [ * 設定 * > * 設定 * ] メニューで、資格情報とデータソースを設定します。
4. WFA Web GUI をブックマークに登録してアクセスを簡単にします。

## OnCommand Workflow Automation データソース

OnCommand Workflow Automation （ WFA ）は、データソースから取得されたデータに対して機能します。WFA の定義済みのデータソースの種類として、 Active IQ Unified Manager および VMware vCenter Server のさまざまなバージョンが用意されています。データ収集用のデータソースを設定する前に、事前に定義されているデータソースのタイプを確認しておく必要があります。

データソースは、特定のデータソースタイプのデータソースオブジェクトへの接続として機能する読み取り専用のデータ構造です。たとえば、データソースは、 Active IQ Unified Manager 6.3 データソースタイプの Active IQ Unified Manager データベースに接続できます。WFA にカスタムデータソースを追加するには、必要なデータソースのタイプを定義します。

事前定義されたデータソースの種類の詳細については、 Interoperability Matrix を参照してください。

- 関連情報 *

"NetApp Interoperability Matrix Tool で確認できます"

## DataFabric Manager でデータベースユーザを設定する

DataFabric Manager 5.x データベースの OnCommand Workflow Automation への読み取り専用アクセスを設定するには、データベースユーザを DataFabric Manager 5.x で作成する必要があります。

### Windows で ocsetup を実行して、データベースユーザを設定します

DataFabric Manager 5.x サーバで ocsetup ファイルを実行して、 DataFabric Manager 5.x データベースの OnCommand Workflow Automation への読み取り専用アクセスを設定することができます。

手順

1. 次のサイトから、 DataFabric Manager 5.x サーバのディレクトリに wfa_ocsetup.exe ファイルをダウンロードします。

   + https://WFA_Server_IP/download/wfa_ocsetup.exe.+

   _wfa_Server_IP_is は、 WFA サーバの IP アドレス（ IPv4 または IPv6 アドレス）です。

   WFA にデフォルト以外のポートを指定した場合は、次のようにポート番号を含める必要があります。

   + https://wfa_server_ip:port/download/wfa_ocsetup.exe.+

   _port_は 、インストール時に WFA サーバに使用した TCP ポート番号です。

   IPv6 アドレスを指定する場合は、角かっこで囲む必要があります。

2. wfa_ocsetup.exe ファイルをダブルクリックします。
3. セットアップ・ウィザードの情報を読み、 * 次へ * をクリックします。
4. OpenJDK の場所を参照するか入力し、 * Next * をクリックします。
5. ユーザ名とパスワードを入力して、デフォルトクレデンシャルを上書きします。

   DataFabric Manager 5.x データベースへのアクセス用に新しいデータベースユーザアカウントが作成されます。

   > ユーザアカウントを作成しない場合は、デフォルトクレデンシャルが使用されます。セキュリティ上の理由からユーザアカウントを作成する必要があります。

6. 「 * 次へ * 」をクリックして結果を確認します。
7. [ 次へ * ] をクリックし、 [ * 完了 * ] をクリックしてウィザードを完了します。

**Linux** で **ocsetup** を実行してデータベースユーザを設定します

## DataFabric Manager 5.x サーバで ocsetup ファイルを実行して、 DataFabric Manager 5.x データベースの OnCommand Workflow Automation への読み取り専用アクセスを設定することができます。

手順

1. ターミナルで次のコマンドを使用して、 DataFabric Manager 5.x サーバのホームディレクトリに wfa_ocsetup.sh ファイルをダウンロードします。

   「 + wget 」と入力します https://WFA_Server_IP/download/wfa_ocsetup.sh+`

   _wfa_Server_IP_is は、 WFA サーバの IP アドレス（ IPv4 または IPv6 アドレス）です。

   WFA にデフォルト以外のポートを指定した場合は、次のようにポート番号を含める必要があります。

   「 + wget 」と入力します https://wfa_server_ip:port/download/wfa_ocsetup.sh+`

   _port_は 、インストール時に WFA サーバに使用した TCP ポート番号です。

   IPv6 アドレスを指定する場合は、角かっこで囲む必要があります。

2. wfa_ocsetup.sh ファイルを実行可能ファイルに変更するには、端末で次のコマンドを使用します。

   chmod +x wfa_ocsetup.sh

3. ターミナルに次のように入力して、スクリプトを実行します。

   wfa_ocsetup.sh OpenJDK パス

   OpenJDK は OpenJDK のパスです。

   /opt/NTAPdfm/java

   次の出力が端末に表示され、セットアップが完了したことが示されます。

   ```
   Verifying archive integrity... All good.
   Uncompressing WFA OnCommand Setup.....
   *** Welcome to OnCommand Setup Utility for Linux ***
       <Help information>
   *** Please override the default credentials below ***
   Override DB Username [wfa] :
   ```

4. ユーザ名とパスワードを入力して、デフォルトクレデンシャルを上書きします。

   DataFabric Manager 5.x データベースへのアクセス用に新しいデータベースユーザアカウントが作成されます。

ユーザアカウントを作成しない場合は、デフォルトクレデンシャルが使用されます。セキュリティ上の理由からユーザアカウントを作成する必要があります。

次の出力が端末に表示され、セットアップが完了したことが示されます。

```
***** Start of response from the database *****
>>> Connecting to database
<<< Connected
*** Dropped existing 'wfa' user
=== Created user 'username'
>>> Granting access
<<< Granted access
***** End of response from the database *****
***** End of Setup *****
```

## データソースを設定

データソースからデータを取得するには、 OnCommand Workflow Automation （ WFA ）でデータソースとの接続をセットアップする必要があります。

- Active IQ Unified Manager 6.0 以降では、 Unified Manager サーバでデータベースユーザアカウントを作成しておく必要があります。

  詳細については、 OnCommand Unified Manager オンラインヘルプを参照してください。

- Unified Manager サーバで受信接続用の TCP ポートが開いている必要があります。

  詳細については、ファイアウォールのマニュアルを参照してください。

  デフォルトの TCP ポート番号は次のとおりです。

| **TCP** ポート番号 | **Unified Manager** サーバのバージョン | 説明 |
|---|---|---|
| 3306 | 6.x | MySQL データベースサーバ |

- Performance Advisor の場合、 GlobalRead の最小ロールを持つ Active IQ Unified Manager ユーザーアカウントを作成しておく必要があります。

  詳細については、 OnCommand Unified Manager オンラインヘルプを参照してください。

- VMware vCenter Server で受信接続用の TCP ポートが開いている必要があります。

  デフォルトの TCP ポート番号は 443 です。詳細については、ファイアウォールのマニュアルを参照してください。

この手順 を使用して、 Unified Manager サーバのデータソースを WFA に複数追加できます。ただし、

Unified Manager サーバ 6.3 以降を WFA とペアリングし、 Unified Manager サーバの保護機能を使用する場合は、この手順 を使用しないでください。

WFA と Unified Manager サーバ 6.x のペアリングの詳細については、 OnCommand Unified Manager オンラインヘルプを参照してください。

> WFA を使用してデータソースをセットアップするときは、 WFA 4.0 リリースでは Active IQ Unified Manager 6.0 、 6.1 、 6.2 のデータソースタイプが廃止され、以降のリリースではこれらのデータソースタイプがサポートされないことに注意してください。

手順

1. Web ブラウザを使用して WFA にアクセスします。
2. [ * 設定 * ] をクリックし、 [ * 設定 * ] で [ * データソース * ] をクリックします。
3. 適切なアクションを選択します。

| 目的 | 手順 |
| --- | --- |
| 新しいデータソースを作成します | をクリックします をクリックします。 |
| WFA をアップグレードした場合は、リストアしたデータソースを編集します | 既存のデータソースエントリを選択し、をクリックします をクリックします。 |

Unified Manager サーバのデータソースを WFA に追加してから Unified Manager サーバのバージョンをアップグレードした場合、アップグレード後の Unified Manager サーバのバージョンは WFA で認識されません。以前のバージョンの Unified Manager サーバを削除してから、アップグレード後のバージョンの Unified Manager サーバを WFA に追加する必要があります。

4. [ 新しいデータソース ] ダイアログボックスで、必要なデータソースの種類を選択し、データソースの名前とホスト名を入力します。

   選択したデータソースのタイプに基づいて、ポート、ユーザ名、パスワード、およびタイムアウトの各フィールドにデフォルトのデータが自動的に入力される場合があります。これらのエントリは必要に応じて編集できます。

5. 適切なアクションを選択します。

| 用途 | 手順 |
| --- | --- |
| Active IQ Unified Manager 6.3 以降 | Unified Manager サーバで作成したデータベースユーザアカウントのクレデンシャルを入力します。データベースユーザアカウントの作成の詳細については、 OnCommand Unified Manager オンラインヘルプを参照してください。<br><br>コマンドラインインターフェイスまたは ocsetup ツールを使用して作成された Active IQ Unified Manager データベースユーザアカウントのクレデンシャルは指定しないでください。 |

6. [ 保存（ Save ） ] をクリックします。
7. [ データソース ] テーブルで、データソースを選択し、をクリックします をクリックします。
8. データ取得プロセスのステータスを確認します。

## アップグレードした **Unified Manager** サーバをデータソースとして追加します

WFA のデータソースとして Unified Manager サーバ（ 5.x または 6.x ）を追加したあと、 Unified Manager サーバをアップグレードした場合は、 アップグレード後のバージョンに関連付けられているデータは、手動でデータソースとして追加しないかぎり WFA に取り込まれないため、アップグレードした Unified Manager サーバをデータソースとして追加する必要があります。

手順

1. WFA Web GUI に管理者としてログインします。
2. [ * 設定 * ] をクリックし、 [ * 設定 * ] で [ * データソース * ] をクリックします。
3. をクリックします をクリックします。
4. [ 新しいデータソース ] ダイアログボックスで、必要なデータソースの種類を選択し、データソースの名前とホスト名を入力します。

   選択したデータソースのタイプに基づいて、ポート、ユーザ名、パスワード、およびタイムアウトの各フィールドにデフォルトのデータが自動的に入力される場合があります。これらのエントリは必要に応じて編集できます。

5. [ 保存（ Save ） ] をクリックします。
6. 以前のバージョンの Unified Manager サーバを選択し、をクリックします をクリックします。
7. [ データソースタイプの削除 ] 確認ダイアログボックスで、 [ はい *] をクリックします。
8. [ データソース ] テーブルで、データソースを選択し、をクリックします をクリックします。
9. History テーブルでデータ取得ステータスを確認します。

# ローカルユーザを作成する

## OnCommand Workflow Automation （ WFA ）を使用すると、ゲスト、オペレータ、承認者、アーキテクト、 admin 、 backup のいずれかです。

WFA をインストールし、 admin としてログインしておく必要があります。

WFA では、次のロールのユーザを作成できます。

- * ゲスト *

  このユーザーは、ポータルとワークフロー実行のステータスを表示し、ワークフロー実行のステータスの変更を通知できます。

- * 演算子 *

  このユーザーは、ユーザーにアクセス権が付与されているワークフローをプレビューおよび実行できます。

- * 承認者 *

  このユーザーは、ユーザーにアクセス権が与えられているワークフローをプレビュー、実行、承認、および却下することができます。

  > 承認者の E メール ID を指定することを推奨します。複数の承認者がいる場合は、 [ 電子メール *] フィールドにグループ電子メール ID を入力できます。

- * 建築家 *

  このユーザには作成ワークフローへのフルアクセスが許可されますが、 WFA サーバのグローバル設定の変更は禁止されています。

- * 管理者 *

  このユーザには WFA サーバへの完全なアクセス権があります。

- * バックアップ *

  WFA サーバのバックアップをリモートで生成できる唯一のユーザです。ただし、ユーザは他のすべてのアクセスから制限されます。

手順

1. [ * 設定 * ] をクリックし、 [ * 管理 * ] で [ * ユーザー * ] をクリックします。
2. をクリックして新しいユーザを作成します をクリックします。
3. [ 新規ユーザー ] ダイアログボックスに必要な情報を入力します。
4. [ 保存（ Save ） ] をクリックします。

# ターゲットシステムのクレデンシャルを設定します

OnCommand Workflow Automation （ WFA ）でターゲットシステムのクレデンシャルを設定し、そのクレデンシャルを使用して特定のシステムに接続し、コマンドを実行できます。

初回のデータ取得が完了したら、コマンドを実行するアレイのクレデンシャルを設定する必要があります。PowerShell WFA コントローラの接続には、次の 2 つのモードがあります。

- クレデンシャルあり

  WFA は、最初に HTTPS を使用して接続を確立しようとし、次に HTTP を使用しようとします。また、WFA でクレデンシャルを定義しなくても、 Microsoft Active Directory LDAP 認証を使用してアレイに接続できます。Active Directory LDAP を使用するには、同じ Active Directory LDAP サーバで認証を実行するようにアレイを設定する必要があります。

- クレデンシャルなし（ストレージシステム 7-Mode の場合）

  WFA は、ドメイン認証を使用して接続を確立しようとします。このモードでは、 NTLM プロトコルを使用して保護されたリモート手順 コールプロトコルが使用されます。

- WFA は、 ONTAP システムの Secure Sockets Layer （ SSL ）証明書をチェックします。ONTAP 証明書が信頼されていない場合、ユーザにはシステムへの接続を確認して許可または拒否するように求められることがあります。
- バックアップのリストア後またはインプレースアップグレードの完了後に、 ONTAP 、 NetApp Active IQ 、および Lightweight Directory Access Protocol （ LDAP ）のクレデンシャルを再入力する必要があります。

手順

1. Web ブラウザから admin として WFA にログインします。
2. [ * 設定 * ] をクリックし、 [ * 設定 * ] で [ * クリデンシャル * ] をクリックします。
3. をクリックします をクリックします。
4. [New Credentials] ダイアログボックスで、 **match** リストから次のいずれかのオプションを選択します。

   - * EXACT *

     特定の IP アドレスまたはホスト名のクレデンシャル

   - * パターン *

     サブネットまたは IP 範囲全体のクレデンシャル

     このオプションでは、正規表現の構文の使用はサポートされていません。

5. [* タイプ * （ * Type * ） ] リストからリモートシステムタイプを選択します。
6. リソースのホスト名、 IPv4 アドレス、または IPv6 アドレス、ユーザ名、およびパスワードを入力します。

WFA 5.1 は、 WFA に追加されたすべてのリソースの SSL 証明書を検証します。証明書の検証では証明書の受け入れが求められる場合があるため、ワイルドカードを使用したクレデンシャルはサポートされていません。同じクレデンシャルを使用するクラスタが複数ある場合、一度に追加することはできません。

7. 次の操作を実行して接続をテストします。

| 選択した一致タイプ | 作業 |
| --- | --- |
| • EXACT * | [ * テスト * ] をクリックします。 |
| • パターン * | クレデンシャルを保存して、次のいずれかを選択します。<br>• クレデンシャルを選択し、をクリックします をクリックします。<br>• 右クリックして、 * 接続のテスト * を選択します。 |

8. [ 保存（ Save ） ] をクリックします。

# OnCommand Workflow Automation を設定しています

OnCommand Workflow Automation （ WFA ）を使用すると、 AutoSupport や通知など、さまざまな設定を行うことができます。

WFA を設定する際には、必要に応じて次の作業を 1 つ以上セットアップできます。

- AutoSupport ：テクニカルサポートに AutoSupport メッセージを送信するために使用します
- Microsoft Active Directory の Lightweight Directory Access Protocol （ LDAP ）サーバ： WFA ユーザの LDAP 認証と許可に使用されます
- ワークフロー処理および AutoSupport メッセージの送信に関する E メール通知用のメールです
- Simple Network Management Protocol （ SNMP ；簡易ネットワーク管理プロトコル）。ワークフローの処理に関する通知に使用します
- リモートデータロギング用の syslog

## AutoSupport を設定します

スケジュール、 AutoSupport メッセージの内容、プロキシサーバなど、複数の AutoSupport 設定を行うことができます。AutoSupport は、選択したコンテンツの週次ログをアーカイブと問題 分析のためにテクニカルサポートに送信します。

手順

1. Web ブラウザから admin として WFA にログインします。
2. [ * 設定 * ] をクリックし、 [ * 設定 * ] で [ * AutoSupport * ] をクリックします。

3. [* AutoSupport を有効にする * ] ボックスが選択されていることを確認します。
4. 必要な情報を入力します。
5. [* コンテンツ * （ Content * ） ] リストから次のいずれかを選択します。

| 含める項目 | 選択するオプション |
|---|---|
| WFA インストールのユーザ、ワークフロー、コマンドなど、設定の詳細のみを表示します | 設定データのみを送信します |
| WFA の設定の詳細と、スキームなどの WFA キャッシュテーブル内のデータ | 設定データとキャッシュデータを送信（デフォルト） |
| WFA の設定の詳細、 WFA のキャッシュテーブル内のデータ、インストールディレクトリ内のデータ | 設定およびキャッシュの拡張データを送信します |

WFA ユーザのパスワードは、 AutoSupport データに _not_included です。

6. AutoSupport メッセージをダウンロードできることをテストします。
   a. [ * ダウンロード ] をクリックします。
   b. 表示されたダイアログボックスで、 .7z ファイルの保存場所を選択します。
7. [ 今すぐ送信 ] をクリックして、指定した宛先への AutoSupport メッセージの送信をテストします。
8. [ 保存（ Save ） ] をクリックします。

## 認証を設定

### OnCommand Workflow Automation （ WFA ）では、 Microsoft Active Directory （ AD ）の Lightweight Directory Access Protocol （ LDAP ）サーバを認証と許可に使用するように設定できます。

環境内に Microsoft AD LDAP サーバを設定しておく必要があります。

WFA でサポートされるのは Microsoft AD LDAP 認証のみです。Microsoft AD ライトウェイトディレクトリサービス (AD LDS) や Microsoft グローバルカタログなど、他の LDAP 認証方法は使用できません。

通信中、 LDAP はユーザ名とパスワードをプレーンテキストで送信します。ただし、 LDAPS （ LDAP セキュア）通信は暗号化されて安全に保護されます。

手順

1. Web ブラウザから admin として WFA にログインします。
2. 必要なロールに Active Directory グループ名のリストを追加します。

Active Directory Groups ウィンドウで、必要なロールに AD グループ名のリストを追加できます。

Active Directory グループウィンドウ

3. [ * Administration * ] > [* WFA Configuration * ] をクリックします。
4. WFA 設定ダイアログボックスで、 * 認証 * タブをクリックし、 * Active Directory の有効化 * チェックボックスをオンにします。
5. 各フィールドに必要な情報を入力します。
   a. ドメインユーザに user@domain 形式を使用する場合は、 [ ユーザ名属性 *] フィールドで sAMAccountName を userPrincipalName に置き換えます。
   b. 環境に固有の値を指定する必要がある場合は、必要なフィールドを編集します。
6. [**Add**] をクリックして、 Active Directory サーバテーブルに URI 形式で Active Directory を追加します。「 ldap://active_director_server_address\[:port\]] 」

   LDAP ： // NB-T01.example.com[:389]

   LDAP over SSL を有効にしている場合は、「 ldaps ： // active_director_server_address \ [ ： port\]] 」という URI 形式を使用できます
7. LDAP サーバとベース DN をバインドするためのクレデンシャルを指定します。
8. 指定されたユーザの認証をテストします。
   a. ユーザ名とパスワードを入力します。
   b. ［ * 認証のテスト * ］ をクリックします。

   WFA で指定されたユーザの認証をテストするために、 Active Directory グループを追加しておく必要があります。
9. [ 保存（ Save ） ] をクリックします。

## Active Directory グループを追加します

Active Directory グループは、 OnCommand Workflow Automation （ WFA ）で追加できます。

手順

1. Web ブラウザから admin として WFA にログインします。
2. [ * 設定 * ] をクリックし、 [ * 管理 * ] の下にある [ * Active Directory グループ * ] をクリックします。
3. Active Directory Groups （ Active Directory グループ）ウィンドウで、 * New * （新規）アイコンをクリックします。
4. [ 新しい Active Directory グループ ] ダイアログボックスで、必要な情報を入力します。

   [*Role] ドロップダウンリストから [*Approver] を選択した場合は、承認者の電子メール ID を指定することをお勧めします。複数の承認者がいる場合は、 [ 電子メール *] フィールドにグループ電子メール ID を入力できます。特定の Active Directory グループに通知を送信するワークフローのさまざまなイベントを選択します。
5. [ 保存（ Save ） ] をクリックします。

## E メール通知を設定

ワークフローの処理に関する E メール通知を送信するように OnCommand Workflow Automation （ WFA ）を設定できます。たとえば、ワークフローが開始された場合やワークフローが失敗した場合などです。

環境でメールホストを設定しておく必要があります。

手順

1. Web ブラウザから admin として WFA にログインします。
2. [ * 設定 * ] をクリックし、 [ * 設定 * ] で [ * メール * ] をクリックします。
3. 各フィールドに必要な情報を入力します。
4. 次の手順を実行してメール設定をテストします。
   a. [ テストメールの送信 ] をクリックします。
   b. [ 接続のテスト ] ダイアログボックスで、電子メールの送信先の電子メールアドレスを入力します。
   c. [ * テスト * ] をクリックします。
5. [ 保存（ Save ） ] をクリックします。

## SNMP を設定する

ワークフロー処理のステータスに関する簡易ネットワーク管理プロトコル（ SNMP ）トラップを送信するように OnCommand Workflow Automation （ WFA ）を設定できます。

WFA では現在、 SNMP v1 および SNMP v3 プロトコルがサポートされています。SNMP v3 は、追加のセキュリティ機能を提供します。

wfa_mib ファイルには、 WFA サーバから送信されるトラップに関する情報が格納されます。MIB ファイルは WFA サーバの <wfa_install_location >\WFA\bin\wfa_mib ディレクトリにあります。

> WFA サーバは、すべてのトラップ通知を汎用のオブジェクト ID （ 1.3.6.1.4.1.789.1.12.0 ）で送信します。

SNMP 設定に community_string@snmp_host などの SNMP コミュニティストリングは使用できません。

## syslog を設定します

イベントロギングやログ情報の分析などの目的で、ログデータを特定の syslog サーバに送信するように OnCommand Workflow Automation （ WFA ）を設定できます。

WFA サーバのデータを受け入れるように syslog サーバを設定しておく必要があります。

手順

1. Web ブラウザから admin として WFA にログインします。
2. [ * 設定 * ] をクリックし、 [ * メンテナンス * ] で [ * Syslog * ] をクリックします。

3. [Enable Syslog* （ syslog を有効にする） ] チェックボックスを選択します。
4. Syslog ホスト名を入力し、 Syslog ログレベルを選択します。
5. [ 保存（ Save ） ] をクリックします。

## リモートシステムに接続するためのプロトコルを設定します

リモートシステムへの接続に OnCommand Workflow Automation （ WFA ）で使用するプロトコルを設定できます。プロトコルは、組織のセキュリティ要件とリモートシステムでサポートされるプロトコルに基づいて設定できます。

手順

1. Web ブラウザから admin として WFA にログインします。
2. [ * データソースデザイン **>** リモートシステムタイプ * ] をクリックします。
3. 次のいずれかを実行します。

| 状況 | 手順 |
| --- | --- |
| 新しいリモートシステムのプロトコルを設定します | a. をクリックします 。<br>b. [ 新しいリモートシステムタイプ ] ダイアログボックスで、名前、概要 、バージョンなどの詳細を指定します。 |
| 既存のリモートシステムのプロトコル設定を変更する | a. 変更するリモートシステムを選択してダブルクリックします。<br>b. をクリックします 。 |

4. [ 接続プロトコル ] リストから、次のいずれかを選択します。
   - HTTPS を HTTP にフォールバック（デフォルト）
   - HTTPS のみ
   - HTTP のみ
   - カスタム
5. プロトコル、デフォルトポート、およびデフォルトタイムアウトの詳細を指定します。
6. [ 保存（ Save ） ] をクリックします。

# デフォルトのパスワードポリシーを無効にします

OnCommand Workflow Automation （ WFA ）は、ローカルユーザにパスワードポリシーを適用するように設定されています。パスワードポリシーを使用しない場合は、無効にすることができます。

WFA ホストシステムに root ユーザとしてログインしておく必要があります。

WFA のデフォルトのインストールパスは、この手順 で使用されます。インストール時にデフォルトの場所を変更した場合は、変更した WFA のインストールパスを使用する必要があります。

手順

1. シェルプロンプトで、 WFA サーバの次のディレクトリに移動します。 wfa_install_location /wfa/bin/
2. 次のコマンドを入力します。

   `./wfa — password-policy = none — restart=wfa

# デフォルトのパスワードポリシーを変更します

## OnCommand Workflow Automation （ WFA ）は、ローカルユーザにパスワードポリシーを適用するように設定されています。デフォルトのパスワードポリシーを変更できます。

WFA ホストシステムに root ユーザとしてログインしておく必要があります。

- WFA のデフォルトのインストールパスは、この手順 で使用されます。

  インストール時にデフォルトの場所を変更した場合は、変更した WFA のインストールパスを使用する必要があります。

- デフォルトのパスワードポリシーのコマンドは、 ./wfa --password-policy = default です。

  デフォルトは "minLength=true,8;specialChar=true,1; digitalChar=true,1; lowercaseChar=true,1; casupperChar=true,1; whitespaceChar=false`" です。デフォルトのパスワードポリシーは、 8 文字以上で、 1 文字以上の特殊文字、 1 桁、 1 文字以上の小文字、 1 文字以上の大文字、およびスペースを含まない必要があります。

手順

1. シェルプロンプトで、 WFA サーバの次のディレクトリに移動します。 wfa_install_location /wfa/bin/
2. 次のコマンドを入力して、デフォルトのパスワードポリシーを変更します。

   `./wfa — password-policy=PasswordPolicyString — restart=wfa

# **OnCommand Workflow Automation** データベースへのリモートアクセスを有効または無効にします

## デフォルトでは、 OnCommand Workflow Automation （ WFA ）データベースには、WFA ホストシステムで実行中のクライアントからのみアクセスできます。リモートシステムから WFA データベースへのアクセスを有効にする場合は、デフォルトの設定を変更できます。

- WFA ホストシステムに root ユーザとしてログインしておく必要があります。
- WFA ホストシステムにファイアウォールがインストールされている場合は、リモートシステムから MySQL ポート（ 3306 ）にアクセスできるようにファイアウォールを設定しておく必要があります。

WFA のデフォルトのインストールパスは、この手順 で使用されます。インストール時にデフォルトの場所を変更した場合は、変更した WFA のインストールパスを使用する必要があります。

手順

1. WFA サーバの次のディレクトリに移動します。 wfa_install_location /wfa/bin/
2. 次のいずれかを実行します。

| 目的 | 入力するコマンド |
|---|---|
| リモートアクセスを有効にします | `./wfa --db-access = public－restart` |
| リモートアクセスを無効にします | `./wfa --db-access=default－restart` |

# OnCommand Workflow Automation のトランザクションタイムアウト設定を変更します

OnCommand Workflow Automation （ WFA ）データベースのトランザクションは、デフォルトで 300 秒以内にタイムアウトします。大容量の WFA データベースをバックアップからリストアする際には、データベースのリストアが失敗する可能性を回避するために、デフォルトのタイムアウト期間を延長できます。

WFA ホストシステムに root ユーザとしてログインしておく必要があります。

WFA のデフォルトのインストールパスは、この手順 で使用されます。インストール時にデフォルトの場所を変更した場合は、変更した WFA のインストールパスを使用する必要があります。

手順

1. シェルプロンプトで、 WFA サーバの次のディレクトリに移動します。 wfa_install_location /wfa/bin/
2. 次のコマンドを入力します。

   `./wfa --txn-timeout[=timeout] — -restart=wfa

   `./wfa --txn-timeout=1000 --restart=wfa

# Workflow Automation のタイムアウト値を設定します

Workflow Automation （ WFA） Web GUI のタイムアウト値を設定できます。デフォルトのタイムアウト値である 180 秒を使用する必要はありません。

設定するタイムアウト値は、非アクティブ時のタイムアウトではなく、絶対タイムアウトです。たとえば、この値を 30 分に設定すると、この時間の終わりにアクティブな場合でも、 30 分後にログアウトされます。WFA の Web GUI からタイムアウト値を設定することはできません。

手順

1. WFA ホストマシンに root ユーザとしてログインします。

2. タイムアウト値を設定します。

   `installdir bin/wfa -S = タイムアウト値 ( 分

# 暗号を有効にして新しい暗号を追加する

OnCommand Workflow Automation 5.1 では、標準で用意されている多数の暗号がサポートされています。必要に応じて暗号を追加することもできます。

事前に有効にできる暗号は次のとおりです。

```
enabled-cipher-suites=
"TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,T
LS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA25
6,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA38
4,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA25
6,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384"
```

この構成には ' standalone-full.xml' ファイルに暗号を追加できますこのファイルは、「 <installdir>/jboss/standalone/configuration/standalone-full.xml 」にあります。

このファイルは、次のように追加の暗号をサポートするように変更できます。

```
<https-listener name="https" socket-binding="https" max-post-
size="1073741824" security-realm="SSLRealm"
enabled-cipher-suites="**< --- add additional ciphers here ---\>**
enabled-protocols="TLSv1.1,TLSv1.2"/>
```