Setting up OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
June 11, 2024

Table of Contents

Setting up OnCommand Workflow Automation . . . 1
- Access OnCommand Workflow Automation . . . 1
- OnCommand Workflow Automation data sources . . . 1
- Create local users . . . 6
- Configure the credentials of a target system . . . 7
- Configuring OnCommand Workflow Automation . . . 8
- Disable the default password policy . . . 14
- Modify the default password policy for Windows . . . 14
- Enable remote access to the OnCommand Workflow Automation database on Windows . . . 15
- Restrict access rights of OnCommand Workflow Automation on the host . . . 15
- Modify the transaction timeout setting of OnCommand Workflow Automation . . . 16
- Configure the timeout value for Workflow Automation . . . 16
- Enabling ciphers and adding new ciphers . . . 17

Setting up OnCommand Workflow Automation

After you complete installing OnCommand Workflow Automation (WFA), you must complete several configuration settings. You have to access WFA, configure users, set up data sources, configure credentials, and configure WFA.

Access OnCommand Workflow Automation

You can access OnCommand Workflow Automation (WFA) through a web browser from any system that has access to the WFA server.

You must have installed Adobe Flash Player for your web browser.

Steps

1. Open a web browser and enter one of the following in the address bar:
   - `https://wfa_server_ip`

     wfa_server_ip is the IP address (IPv4 or IPv6 address) or the fully qualified domain name (FQDN) of the WFA server.

   - If you are accessing WFA on the WFA server: `https://localhost/wfa` If you have specified a non-default port for WFA, you must include the port number as follows:
   - `https://wfa_server_ip:port`
   - `https://localhost:port` port is the TCP port number you have used for the WFA server during installation.
2. In the Sign in section, enter the credentials of the admin user that you have entered during installation.
3. In the **Settings** > **Setup** menu, set up the credentials and a data source.
4. Bookmark the WFA web GUI for ease of access.

OnCommand Workflow Automation data sources

OnCommand Workflow Automation (WFA) operates on data that is acquired from data sources. Various versions of Active IQ Unified Manager and VMware vCenter Server are provided as predefined WFA data source types. You must be aware of the predefined data source types before you set up the data sources for data acquisition.

A data source is a read-only data structure that serves as a connection to the data source object of a specific data source type. For example, a data source can be a connection to an Active IQ Unified Manager database of an Active IQ Unified Manager 6.3 data source type. You can add a custom data source to WFA after defining the required data source type.

For more information about the predefined data source types, see the Interoperability Matrix.

Related information

NetApp Interoperability Matrix Tool

Configuring a database user on DataFabric Manager

You must create a database user on DataFabric Manager 5.x to configure read-only access of the DataFabric Manager 5.x database to OnCommand Workflow Automation.

Configure a database user by running ocsetup on Windows

You can run the ocsetup file on the DataFabric Manager 5.x server to configure read-only access of the DataFabric Manager 5.x database to OnCommand Workflow Automation.

Steps

1. Download the wfa_ocsetup.exe file to a directory in the DataFabric Manager 5.x server from the following location: *https*://WFA_Server_IP/download/wfa_ocsetup.exe.

   WFA_Server_IP is the IP address (IPv4 or IPv6 address) of your WFA server.

   If you have specified a non-default port for WFA, you must include the port number as follows: *https*://wfa_server_ip:port/download/wfa_ocsetup.exe.

   port is the TCP port number that you have used for the WFA server during installation.

   If you are specifying an IPv6 address, you must enclose it with square brackets.

2. Double-click the wfa_ocsetup.exe file.
3. Read the information in the setup wizard and click **Next**.
4. Browse or type the OpenJDK location and click **Next**.
5. Enter a user name and password to override the default credentials.

   A new database user account is created with access to the DataFabric Manager 5.x database.

   > If you do not create a user account, the default credentials are used. You must create a user account for security purposes.

6. Click **Next** and review the results.
7. Click **Next**, and then click **Finish** to complete the wizard.

Configure a database user by running ocsetup on Linux

You can run the ocsetup file on the DataFabric Manager 5.x server to configure read-only access of the DataFabric Manager 5.x database to OnCommand Workflow Automation.

Steps

1. Download the wfa_ocsetup.sh file to your home directory on the DataFabric Manager 5.x server using the following command in the terminal:

   ```
   wget https://WFA_Server_IP/download/wfa_ocsetup.sh
   ```

   WFA_Server_IP is the IP address (IPv4 or IPv6 address) of your WFA server.

   If you have specified a non-default port for WFA, you must include the port number as follows:

`wget https://wfa_server_ip:port/download/wfa_ocsetup.sh`

port is the TCP port number that you have used for the WFA server during installation.

If you are specifying an IPv6 address, you must enclose it with square brackets.

2. Use the following command in the terminal to change the wfa_ocsetup.sh file to an executable: `chmod +x wfa_ocsetup.sh`
3. Run the script by entering the following in the terminal:

   `./wfa_ocsetup.sh OpenJDK_path`

   OpenJDK_path is the path to OpenJDK.

   /opt/NTAPdfm/java

   The following output is displayed in the terminal, indicating a successful setup:

```
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. Enter a user name and password to override the default credentials.

   A new database user account is created with access to the DataFabric Manager 5.x database.

   If you do not create a user account, the default credentials are used. You must create a user account for security purposes.

   The following output is displayed in the terminal, indicating a successful setup:

```
***** 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 *****
```

Configure a database user on Active IQ Unified Manager

You must create a database user on Active IQ Unified Manager to configure read-only

access of the Active IQ Unified Manager database to OnCommand Workflow Automation.

Steps

1. Log in to Active IQ Unified Manager with administrator credentials.
2. Click **Settings** > **Users**.
3. Click **Add a New User**.
4. Select **Database User** as the type of user.

   The same user should be used in OnCommand Workflow Automation while adding Active IQ Unified Manager as a data source in OnCommand Workflow Automation.

Set up a data source

You must set up a connection with a data source in OnCommand Workflow Automation (WFA) to acquire data from the data source.

- For Active IQ Unified Manager 6.0 and later, you must have created a database user account on the Unified Manager server.

  See the *OnCommand Unified Manager Online Help* for details.

- The TCP port for incoming connections on the Unified Manager server must be open.

  See the documentation on your firewall for details.

  The following are the default TCP port numbers:

TCP port number	Unified Manager server version	Description
3306	6.x	MySQL database server

- For Performance Advisor, you must have created an Active IQ Unified Manager user account with a minimum role of GlobalRead.

  See the *OnCommand Unified Manager Online Help* for details.

- For VMware vCenter Server, you must have created a user account on the vCenter Server.

  See the VMware vCenter Server documentation for details.

  You must have installed VMware PowerCLI. If you want to execute workflows only on vCenter Server data sources, setting up Unified Manager server as a data source is not required.

- The TCP port for incoming connections on the VMware vCenter Server must be open.

  The default TCP port number is 443. See the documentation on your firewall for details.

You can add multiple Unified Manager server data sources to WFA using this procedure. However, you must not use this procedure if you want to pair Unified Manager server 6.3 and later with WFA and use the protection functionality in Unified Manager server.

For more information about pairing WFA with Unified Manager server 6.x, see the *OnCommand Unified Manager Online Help*.

> While setting up a data source with WFA, you must be aware that Active IQ Unified Manager 6.0, 6.1, and 6.2 data source types are deprecated in the WFA 4.0 release, and these data source types will not be supported in future releases.

Steps

1. Access WFA using a web browser.
2. Click **Settings**, and under **Setup** click **Data Sources**.
3. Choose the appropriate action:

To…	Do this…
Create a new data source	Click on the toolbar.
Edit a restored data source if you have upgraded WFA	Select the existing data source entry, and click on the toolbar.

   If you have added a Unified Manager server data source to WFA and then upgraded the version of the Unified Manager server, WFA will not recognize the upgraded version of the Unified Manager server. You must delete the previous version of the Unified Manager server and then add the upgraded version of the Unified Manager server to WFA.

4. In the New Data Source dialog box, select the required data source type, and enter a name for the data source and the host name.

   Based on the selected data source type, the port, user name, password, and timeout fields might be automatically populated with the default data, if available. You can edit these entries as required.

5. Choose an appropriate action:

For…	Do this…
Active IQ Unified Manager 6.3 and later	Enter the credentials of the Database User account that you created on the Unified Manager server. See *OnCommand Unified Manager Online Help* for details on creating a database user account. You must not provide the credentials of an Active IQ Unified Manager Database User account that was created using the command-line interface or the ocsetup tool.
VMware vCenter Server (only for windows)	(only for windows) Enter the user name and password of the user that you created on the VMware vCenter server.

6. Click **Save**.

7. In the Data Sources table, select the data source, and click on the toolbar.
8. Verify the status of the data acquisition process.

Add an upgraded Unified Manager server as a data source

If Unified Manager server (5.x or 6.x) is added as a data source to WFA and then the Unified Manager server is upgraded, you must add the upgraded Unified Manager server as a data source because the data that is associated with the upgraded version is not populated in WFA unless it is manually added as a data source.

Steps

1. Log into the WFA web GUI as an admin.
2. Click **Settings** and under **Setup**, click **Data Sources**.
3. Click on the toolbar.
4. In the New Data Source dialog box, select the required data source type, and then enter a name for the data source and the host name.

   Based on the selected data source type, the port, user name, password, and timeout fields might be automatically populated with the default data, if available. You can edit these entries as required.
5. Click **Save**.
6. Select the previous version of the Unified Manager server, and click on the toolbar.
7. In the Delete Data Source Type confirmation dialog box, click **Yes**.
8. In the Data Sources table, select the data source, and then click on the toolbar.
9. Verify the data acquisition status in the History table.

Create local users

OnCommand Workflow Automation (WFA) enables you to create and manage local WFA users with specific permissions for various roles, such as guest, operator, approver, architect, admin, and backup.

You must have installed WFA and logged in as an admin.

WFA enables you to create users for the following roles:

- **Guest**

  This user can view the portal and the status of a workflow execution, and can be notified of a change in the status of a workflow execution.

- **Operator**

  This user is allowed to preview and execute workflows for which the user is given access.

- **Approver**

  This user is allowed to preview, execute, approve, and reject workflows for which the user is given access.

It is recommended to provide the email ID of the approver. If there are multiple approvers, you can provide a group email ID in the **E-mail** field.

- **Architect**

  This user has full access to create workflows, but is restricted from modifying global WFA server settings.

- **Admin**

  This user has complete access to the WFA server.

- **Backup**

  This is the only user who can remotely generate backups of the WFA server. However, the user is restricted from all other access.

Steps

1. Click **Settings**, and under **Management** click **Users**.
2. Create a new user by clicking on the toolbar.
3. Enter the required information in the New User dialog box.
4. Click **Save**.

Configure the credentials of a target system

You can configure the credentials of a target system in OnCommand Workflow Automation (WFA) and use the credentials to connect to that specific system and execute commands.

After initial data acquisition, you must configure the credentials for the arrays on which the commands are run. PowerShell WFA controller connection works in two modes:

- With credentials

  WFA tries to establish a connection using HTTPS first, and then tries using HTTP. You can also use Microsoft Active Directory LDAP authentication to connect to arrays without defining credentials in WFA. To use Active Directory LDAP, you must configure the array to perform authentication with the same Active Directory LDAP server.

- Without credentials (for storage systems operating in 7-Mode)

  WFA tries to establish a connection using domain authentication. This mode uses the remote procedure call protocol, which is secured using the NTLM protocol.

- WFA checks the Secure Sockets Layer (SSL) certificate for ONTAP systems. Users might be prompted to review and accept/deny the connection to ONTAP systems if the SSL certificate is not trusted.
- You must reenter the credentials for ONTAP, NetApp Active IQ and Lightweight Directory Access Protocol (LDAP) after you restore a backup or complete an in-place upgrade.

Steps

1. Log in to WFA through a web browser as an admin.

2. Click **Settings**, and under **Setup** click **Credentials**.
3. Click on the toolbar.
4. In the New Credentials dialog box, select one of the following options from the **Match** list:
   - **Exact**

     Credentials for a specific IP address or host name
   - **Pattern**

     Credentials for the entire subnet or IP range

     The use of regular expression syntax is not supported for this option.
5. Select the remote system type from the **Type** list.
6. Enter either the host name or the IPv4 or IPv6 address of the resource, the user name, and the password.

   WFA 5.1 verifies the SSL certificates of all resources added to WFA. As certificate verification might prompt you to accept the certificates, using wildcards in credentials is not supported. If you have multiple clusters using the same credentials, you cannot add them all at once.
7. Test the connectivity by performing the following action:

If you selected the following match type…	Then…
Exact	Click **Test**.
Pattern	Save the credentials and choose one of the following: • Select the credential and click on the toolbar. • Right-click and select **Test Connectivity**.

8. Click **Save**.

Configuring OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) enables you to configure various settings—for example, AutoSupport and notifications.

When configuring WFA, you can set up one or more of the following, as required:

- AutoSupport for sending AutoSupport messages to technical support
- Microsoft Active Directory Lightweight Directory Access Protocol (LDAP) server for LDAP authentication and authorization for WFA users
- Mail for email notifications about workflow operations and sending AutoSupport messages
- Simple Network Management Protocol (SNMP) for notifications about workflow operations

- Syslog for remote data logging

Configure AutoSupport

You can configure several AutoSupport settings such as the schedule, content of the AutoSupport messages, and the proxy server. AutoSupport sends weekly logs of the content that you selected to technical support for archiving and issue analysis.

Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Settings**, and under **Setup** click **AutoSupport**.
3. Ensure that the **Enable AutoSupport** box is selected.
4. Enter the required information.
5. Select one of the following from the **Content** list:

If you want to include…	Then choose this option…
Only configuration details such as users, workflows, and commands of your WFA installation	`send only configuration data`
WFA configuration details and data in WFA cache tables such as the scheme	`send configuration and cache data` (default)
WFA configuration details, data in WFA cache tables, and data in the installation directory	`send configuration and cache extended data`

The password of any WFA user is *not* included in the AutoSupport data.

6. Test that you can download an AutoSupport message:
   a. Click **Download**.
   b. In the dialog box that opens, select the location to save the .7z file.
7. Test the sending of an AutoSupport message to the specified destination by clicking **Send Now**.
8. Click **Save**.

Configure authentication settings

You can configure OnCommand Workflow Automation (WFA) to use a Microsoft Active Directory (AD) Lightweight Directory Access Protocol (LDAP) server for authentication and authorization.

You must have configured a Microsoft AD LDAP server in your environment.

Only Microsoft AD LDAP authentication is supported for WFA. You cannot use any other LDAP authentication methods, including Microsoft AD Lightweight Directory Services (AD LDS) or Microsoft Global Catalog.

During communication, LDAP sends the user name and password in plain text. However, LDAPS (LDAP secure) communication is encrypted and secure.

Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Settings**, and under **Setup** click **Authentication**.
3. Select the **Enable Active Directory** check box.
4. Enter the required information in the fields:
   a. If you want to use the user@domain format for domain users, replace sAMAccountName with userPrincipalName in the **User name attribute** field.
   b. If unique values are required for your environment, edit the required fields.
   c. Enter the AD server URI as follows: `ldap://active_directory_server_address\[:port\]`

      ldap://NB-T01.example.com[:389]

      If you have enabled LDAP over SSL, you can use the following URI format: `ldaps://active_directory_server_address\[:port\]`
   d. Add a list of AD group names the required roles.

      You can add a list of AD group names to the required roles in the Active Directory Groups Window.
5. Click **Save**.
6. If LDAP connectivity to an array is required, configure the WFA service to log on as the required domain user:
   a. Open the Windows services console by using services.msc.
   b. Double-click the **NetApp WFA Server** service.
   c. In the NetApp WFA Server Properties dialog box, click the **Log On** tab, and then select **This account**.
   d. Enter the domain user name and password, and then click **OK**.

Add Active Directory groups

You can add Active Directory groups in OnCommand Workflow Automation (WFA).

Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Settings** and under **Management**, click **Active Directory Groups**.
3. In the Active Directory Groups window, click the **New** icon.
4. In the New Active Directory Group dialog box, enter the required information.

   If you select **Approver** from the **Role** drop down list, it is recommended provide the email ID of the approver. If there are multiple approvers, you can provide a group email ID in the **E-mail** field. Select the different events of the workflow for which the notification is to be sent to the particular Active Directory group.

5. Click **Save**.

Configure email notifications

You can configure OnCommand Workflow Automation (WFA) to send you email notifications about workflow operations—for example, workflow started or workflow failed.

You must have configured a mail host in your environment.

Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Settings**, and under **Setup** click **Mail**.
3. Enter the required information in the fields.
4. Test the mail settings by performing the following steps:
   a. Click **Send test mail**.
   b. In the Test Connection dialog box, enter the email address to which you want to send the email.
   c. Click **Test**.
5. Click **Save**.

Configure SNMP

You can configure OnCommand Workflow Automation (WFA) to send Simple Network Management Protocol (SNMP) traps about the status of workflow operations.

WFA now supports SNMP v1 and SNMP v3 protocols. SNMP v3 provides additional security features.

The WFA .mib file provides information about the traps that are sent by the WFA server. The .mib file is located in the <WFA_install_location>\wfa\bin\wfa.mib directory on the WFA server.

The WFA server sends all the trap notifications with a generic object identifier (1.3.6.1.4.1.789.1.1.12.0).

You cannot use SNMP community strings such as community_string@SNMP_host for SNMP configuration.

Configure SNMP Version 1

Steps

1. Log in to WFA through a web browser as an admin user, and then access the WFA server.
2. Click **Settings**, and under **Setup** click **SNMP**.
3. Select the **Enable SNMP** check box.
4. In the **Version**drop-down list, select **Version 1**.
5. Enter an IPv4 or IPv6 address or the host name, and the port number of the management host.

   WFA sends SNMP traps to the specified port number. The default port number is 162.

6. In the Notify On section, select one or more of the following check boxes:

- Workflow execution started
- Workflow execution completed successfully
- Workflow execution failed/partially successful
- Workflow execution waiting for approval
- Acquisition failure

7. Click **Send Test Notification** to verify the settings.
8. Click **Save**.

Configure SNMP Version 3

You can also configure OnCommand Workflow Automation (WFA) to send Simple Network Management Protocol (SNMP) Version 3 traps about the status of workflow operations.

Version 3 offers two additional security options:

- Version 3 with Authentication

  Traps are sent unencrypted over the network. SNMP management applications, which are configured by the same authentication parameters as SNMP trap messages, can receive traps.

- Version 3 with Authentication and Encryption

  Traps are sent encrypted over the network. To receive and decrypt these traps, you must configure SNMP management applications with the same authentication parameters and encryption key as the SNMP traps.

Steps

1. Log in to WFA through a web browser as an admin user, and then access the WFA server.
2. Click **Settings**, and under **Setup** click **SNMP**.
3. Select the **Enable SNMP** check box.
4. In the **Version** drop-down list, select one of the following options:
   - Version 3
   - Version 3 with Authentication
   - Version 3 with Authentication and Encryption
5. Select the SNMP configuration options that correspond to the specific SNMP Version 3 option you chose in Step 4.
6. Enter an IPv4 or IPv6 address or the host name, and the port number of the management host. WFA sends SNMP traps to the specified port number. The default port number is 162.
7. In the Notify On section, select one or more of the following check boxes:
   - Workflow planning started/failed/completed
   - Workflow execution started
   - Workflow execution completed successfully
   - Workflow execution failed/ partially successful
   - Workflow execution waiting for approval

- Acquisition failure

8. Click **Send Test Notification** to verify the settings.
9. Click **Save**.

Configure Syslog

You can configure OnCommand Workflow Automation (WFA) to send log data to a specific Syslog server for purposes such as event logging and log information analysis.

You must have configured the Syslog server to accept data from the WFA server.

Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Settings**, and under **Maintenance** click **Syslog**.
3. Select the **Enable Syslog** check box.
4. Enter the Syslog host name and select the Syslog log level.
5. Click **Save**.

Configure protocols for connecting to remote systems

You can configure the protocol used by OnCommand Workflow Automation (WFA) to connect to remote systems. You can configure the protocol based on your organization's security requirements and the protocol supported by the remote system.

Steps

1. Log in to WFA through a web browser as an admin.
2. Click **Data Source Design** > **Remote System Types**.
3. Perform one of the following actions:

If you want to…	Do this…
Configure a protocol for a new remote system	a. Click  . b. In the New Remote System Type dialog box, specify the details such as name, description, and version.
Modify the protocol configuration of an existing remote system	a. Select and double-click the remote system that you want to modify. b. Click  .

4. From the Connection Protocol list, select one of the following:
   - HTTPS with fallback to HTTP (default)
   - HTTPS only
   - HTTP only

    - Custom
5. Specify the details for the protocol, default port, and default timeout.
6. Click **Save**.

Disable the default password policy

OnCommand Workflow Automation (WFA) is configured to enforce a password policy for local users. If you do not want to use the password policy, you can disable it.

You must have logged in to the WFA host system as an admin.

The default WFA installation path is used in this procedure. If you changed the default location during installation, you must use the changed WFA installation path.

Steps

1. Open Windows Explorer and navigate to the following directory: `WFA_install_location\WFA\bin\.`
2. Double-click the ps.cmd file.

   A PowerShell command-line interface (CLI) prompt opens with ONTAP and WFA modules loaded in it.
3. At the prompt, enter the following:

   ```
   Set-WfaConfig -Name PasswordPolicy -Enable $false
   ```
4. When prompted, restart the WFA services.

Modify the default password policy for Windows

OnCommand Workflow Automation (WFA) enforces a password policy for local users. You can modify the default password policy to set a password as per your requirement.

You must be logged in to the WFA host system as a root user.

- The default WFA installation path is used in this procedure.

  If you changed the default location during installation, you must use the custom WFA installation path.
- The command for modifying the default password policy is .\wfa --password-policy=default.

  The default setting is “minLength=true,8;specialChar=true,1;digitalChar=true,1;lowercaseChar=true,1;uppercaseChar=true,1;whitespaceChar=false”. Per this setting for the default password policy, the password must have a minimum length of eight characters, must contain at least one special character, one digit, one lowercase character, and one uppercase character, and must not contain spaces.

Steps

1. At the command prompt, navigate to the following directory on the WFA server:

   ```
   WFA_install_location/wfa/bin/
   ```

2. Modify the default password policy:

```
.\wfa --password-policy=PasswordPolicyString --restart=WFA
```

Enable remote access to the OnCommand Workflow Automation database on Windows

By default, the OnCommand Workflow Automation (WFA) database can be accessed only by clients that are running on the WFA host system. You can change the default settings if you want to access the WFA database from a remote system.

- You must have logged in to the WFA host system as an admin user.
- If a firewall is installed on the WFA host system, you must have configured your firewall settings to allow access from the remote system.

The default WFA installation path is used in this procedure. If you changed the default location during installation, you must use the custom WFA installation path.

Steps

1. Open Windows Explorer, and navigate to the following directory: WFA_install_location\WFA\bin
2. Perform one of the following actions:

To…	Enter the following command…
Enable remote access	`.\wfa --db-access=public --restart`
Disable remote access	`.\wfa --db-access=default --restart`

Restrict access rights of OnCommand Workflow Automation on the host

By default, OnCommand Workflow Automation (WFA) executes the workflows as the admin of the host system. You can restrict WFA rights on the host system by changing the default settings.

You must have logged in to the WFA host system as an admin.

Steps

1. Create a new Windows user account with permissions to open sockets and to write to the WFA home directory.
2. Open the Windows services console by using services.msc and double-click **NetApp WFA Database**.
3. Click the **Log On** tab.
4. Select **This account** and enter the credentials of the new user you have created, and then click **OK**.
5. Double-click **NetApp WFA Server**.

6. Click the **Log On** tab.
7. Select **This account** and enter the credentials of the new user you have created, and then click **OK**.
8. Restart the **NetApp WFA Database** and the **NetApp WFA Server** services.

Modify the transaction timeout setting of OnCommand Workflow Automation

The OnCommand Workflow Automation (WFA) database transaction times out in 300 seconds by default. You can increase the default timeout duration when restoring a large-sized WFA database from a backup to avoid potential failure of the database restoration.

You must have logged in to the WFA host system as an admin.

The default WFA installation path is used in this procedure. If you changed the default location during installation, you must use the changed WFA installation path.

Steps

1. Open Windows Explorer and navigate to the following directory:

   ```
   WFA_install_location\WFA\bin
   ```

2. Double-click the ps.cmd file.

   A PowerShell command-line interface (CLI) prompt opens with ONTAP and WFA modules loaded in it.

3. At the prompt, enter the following:

   ```
   Set-WfaConfig -Name TransactionTimeOut -Seconds NumericValue
   ```

   ```
   Set-WfaConfig -Name TransactionTimeOut -Seconds 1000
   ```

4. When prompted, restart the WFA services.

Configure the timeout value for Workflow Automation

You can configure the timeout value for the Workflow Automation (WFA) web GUI, instead of using the default timeout value.

The default timeout value for WFA web GUI is 180 minutes. You can configure the timeout value to meet your requirements through CLI. You cannot set the timeout value from the WFA web GUI.

The timeout value that you set is an absolute timeout rather than a timeout related to inactivity. For example, if you set this value to 30 minutes, then you are logged out after 30 minutes, even if you are active at the end of this time.

Steps

1. Log in as the administrator on the WFA host machine.
2. Set the timeout value:

```
installdir bin/wfa -S=timeout value in minutes
```

Enabling ciphers and adding new ciphers

OnCommand Workflow Automation 5.1 supports a number of ciphers out of the box. Also, you can add additional ciphers as required.

The following ciphers can be enabled out of the box:

```
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"
```

Additional ciphers can be added to this configuration in the `standalone-full.xml` file. This file is located at: `<installdir>/jboss/standalone/configuration/standalone-full.xml`.

The file can be modified to support additional ciphers as follows:

```
<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"/>
```

Copyright information

Trademark information