Configuring OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
June 11, 2024

Table of Contents

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**.

Copyright information

Trademark information