Installation and Setup for Windows

OnCommand Workflow Automation 5.1

NetApp
May 03, 2022

Table of Contents

Installation and Setup for Windows

Overview of OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) is a software solution that helps to automate storage management tasks, such as provisioning, migration, decommissioning, data protection configurations, and cloning storage. You can use WFA to build workflows to complete tasks that are specified by your processes. WFA supports both ONTAP and Data ONTAP operating in 7-Mode.

A workflow is a repetitive and procedural task that consists of sequential steps, including the following types of tasks:

- Provisioning, migrating, or decommissioning storage for databases or file systems
- Setting up a new virtualization environment, including storage switches and datastores
- Setting up storage for an application as part of an end-to-end orchestration process

Storage architects can define workflows to follow best practices and meet organizational requirements, such as the following:

- Using required naming conventions
- Setting unique options for storage objects
- Selecting resources
- Integrating internal configuration management database (CMDB) and ticketing applications

WFA features

- Workflow design portal to build workflows

  The workflow design portal includes several building blocks, such as commands, templates, finders, filters, and functions, that are used to create workflows. The designer enables you to include advanced capabilities to workflows such as automated resource selection, row repetition (looping), and approval points.

  The workflow design portal also includes building blocks, such as dictionary entries, cache queries, and data source types, for caching data from external systems.

- Execution portal to execute workflows, verify status of workflow execution, and access logs
- Administration/Settings option for tasks such as setting up WFA, connecting to data sources, and configuring user credentials
- Web service interfaces to invoke workflows from external portals and data center orchestration software
- Storage Automation Store to download WFA packs. The ONTAP 9.7.0 pack is bundled with WFA 5.1.

WFA license information

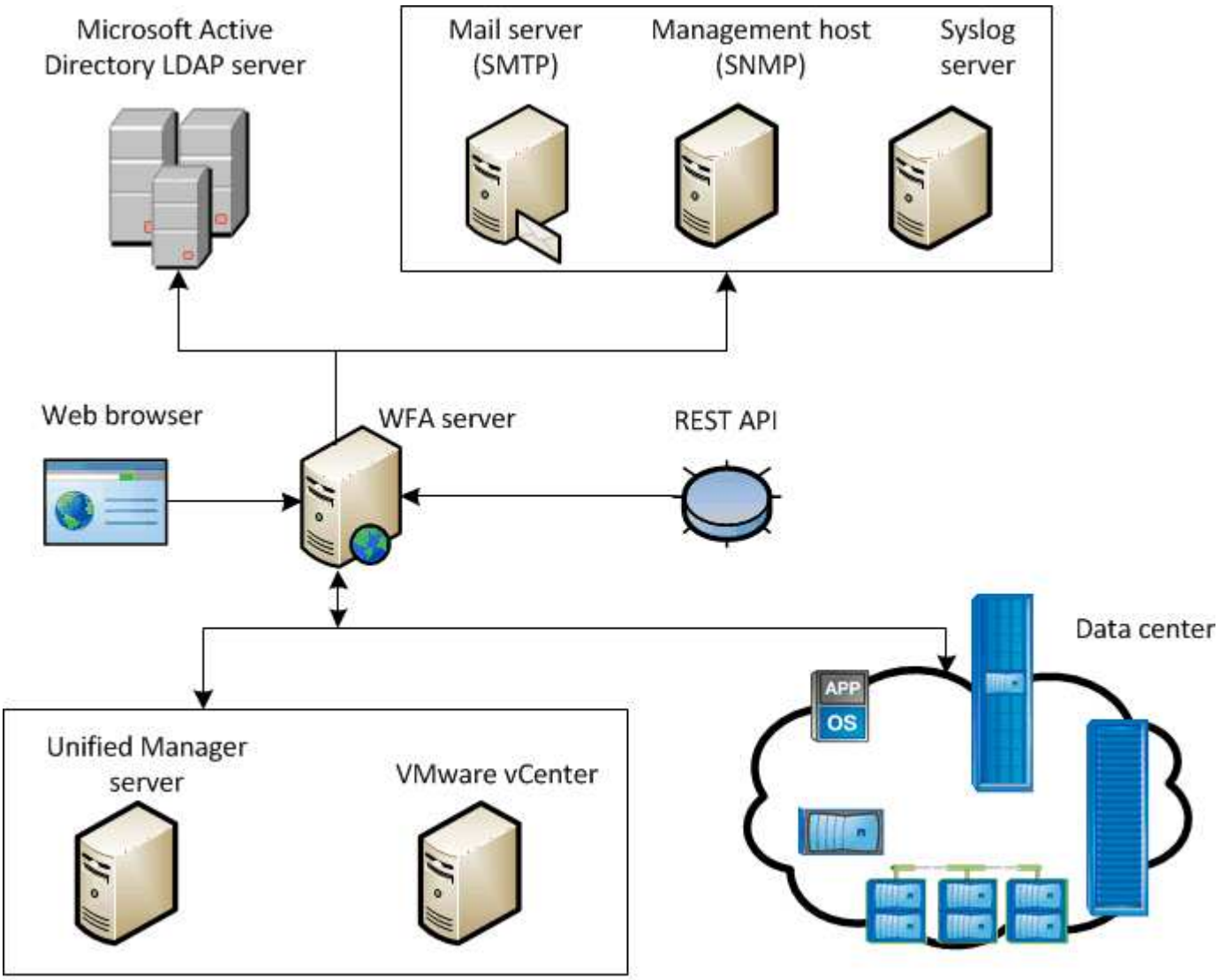
No license is required for using the OnCommand Workflow Automation server.

OnCommand Workflow Automation deployment architecture

OnCommand Workflow Automation (WFA) server is installed to orchestrate the workflow operations across several datacenters.

You can centrally manage your automation environment by connecting your WFA server to several Active IQ Unified Manager deployments and VMware vCenters.

The following illustration shows a deployment example:

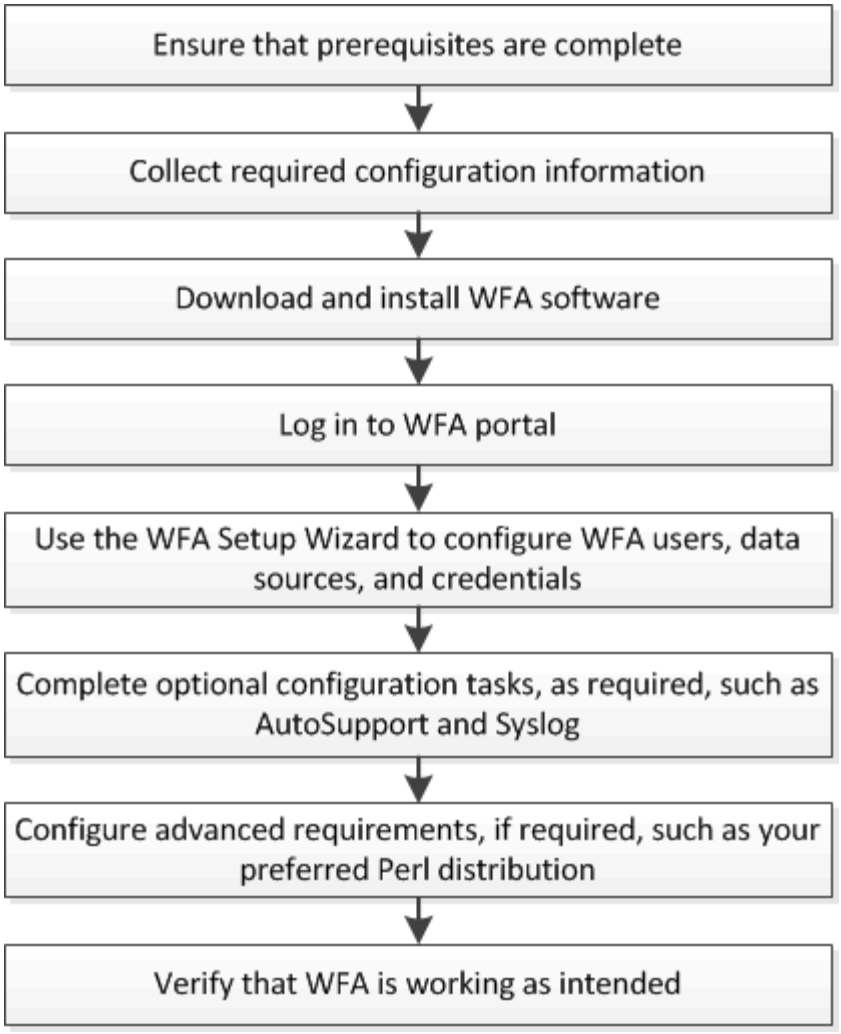


OnCommand Workflow Automation (WFA) deployment

OnCommand Workflow Automation installation and setup overview

Installing OnCommand Workflow Automation (WFA) includes performing tasks such as preparing for the installation, downloading the WFA installer, and running the installer. After the installation is complete, you can configure WFA to meet your requirements.

The following flowchart illustrates the installation and configuration tasks:



Known limitations and enhancements

OnCommand Workflow Automation (WFA) 5.1 includes some limitations and unsupported features that you should be aware of before you install and configure WFA.

- **Creating category names**
  - When a hyphen (-) is used in a category name, it is replaced with a space once the category is saved. For example, if the category name "abc-xyz" is provided, the category name is saved as "abc xyz", with the hyphen removed. To avoid this issue, do not use hyphens in category names.
  - When a colon (:) is used in a category name, the text string before the colon is ignored once the category is saved. For example, if the category name "abc : xyz" is provided, the category name is saved as "xyz", with the "abc" string removed. To avoid this issue, do not use colons in category names.
  - There is no check to prevent two categories having the same name. However, this causes a problem when selecting these categories from the navigation pane. To avoid this issue, make sure that each category name is unique.

System requirements for installing OnCommand Workflow Automation

You must be aware of the OnCommand Workflow Automation (WFA) hardware and software requirements before installing WFA.

Hardware requirements for installing WFA

The following table lists the minimum hardware requirements and the recommended hardware specifications for the WFA server.

Component	Minimum requirements	Recommended specifications
CPU	2.27 GHz or faster, 4 core, 64-bit	2.27 GHz or faster, 4 core, 64-bit
RAM	4 GB	8 GB
Free disk space	5 GB	20 GB

If you are installing WFA on a virtual machine (VM), you should reserve the required memory and CPU so that the VM has sufficient resources. The installer does not verify the CPU speed.

Software requirements for installing WFA

WFA runs on a 64-bit Windows operating system, and should be installed on dedicated physical machines or VMs. You must not install any other application on the server that runs WFA.

WFA runs from Microsoft Windows Server 2012 Enterprise Edition to Microsoft Windows Server 2016 (all editions). Enterprise Edition is the recommended Windows operating system.

For Windows 2012 servers, .NET Framework version 4.5.2 must be installed on your Windows system. If .NET Framework version 4.5.2 is not installed, WFA 5.1 installation fails.

- One of the following supported browsers:
  - Mozilla Firefox
  - Microsoft Internet Explorer
  - Google Chrome
- PowerShell 3.0
- VMware PowerCLI version 5

The PowerShell extension for VMware APIs is required only if you are using WFA to execute workflows on VMware vSphere.

Antivirus applications might prevent WFA services from starting.

To avoid this issue, configure antivirus scanning exclusions for the following WFA directories:

- The directory where you have installed WFA
- The directory where you have installed Perl
- The directory where you have installed OpenJDK
- The MySQL Data Directory

For more details, see the Interoperability Matrix Tool.

Related information

NetApp Interoperability Matrix Tool

Ports required for Workflow Automation

If you are using a firewall, you must be aware of the required ports for Workflow Automation (WFA).

The default port numbers are listed in this section. If you want to use a non-default port number, you must open that port for communication. For more details, see the documentation on your firewall.

The following table lists the default ports that should be open on the WFA server:

Port	Protocol	Direction	Purpose
80, 443	HTTP, HTTPS	Incoming	Opening WFA and logging in
80, 443, 22	HTTP, HTTPS, SSH	Outgoing	Command execution (ZAPI, PowerCLI)
445, 139, 389, 636	Microsoft-DS, NetBIOS-ssn, AD LDAP, AD LDAPS	Outgoing	Microsoft Active Directory LDAP authentication
161	SNMP	Outgoing	Sending SNMP messages on the status of workflows
3306	MySQL	Incoming	Caching read-only user
25	SMTP	Outgoing	Mail notification
80, 443, 25	HTTP, HTTPS, SMTP	Outgoing	Sending AutoSupport messages
514	Syslog	Outgoing	Sending logs to a syslog server

The following table lists the default ports that should be open on the Unified Manager server:

Port	Protocol	Direction	Purpose
2638	Sybase	Incoming	Caching data from Active IQ Unified Manager earlier than 6.0
3306	MySQL	Incoming	Caching data from Active IQ Unified Manager 6.0 and later
8088, 8488	HTTP, HTTPS	Incoming	Caching data from Performance Advisor, which is a part of Active IQ Unified Manager earlier than 6.0

The following table lists the default port that should be open on the VMware vCenter:

Port	Protocol	Direction	Purpose
443	HTTPS	Incoming	Caching data from VMware vCenter

The following table lists the default port that should be open on the SNMP host machine:

Port	Protocol	Direction	Purpose
162	SNMP	Incoming	Receiving SNMP messages on the status of workflows

Prerequisites for installing Workflow Automation

Before installing OnCommand Workflow Automation (WFA), you must ensure that you have the required information and you have completed certain tasks.

Before you install WFA on a system, you must have completed the following tasks:

- Downloading the WFA installation file from the NetApp Support Site and copying the file to the server on which you want to install WFA

  You must have valid credentials to log in to the NetApp Support Site. If you do not have valid credentials, you can register on the NetApp Support Site to obtain the credentials.

- Verifying that the system has access to the following, as applicable:
  - Storage controllers
  - Active IQ Unified Manager
  - VMware vCenter

If your environment requires Secure Shell (SSH) accessibility, you must ensure that SSH is enabled on the target controllers.

- Verifying that PowerShell 3.0 or later is installed
- Ensuring that VMware Power CLI is installed, if you are using WFA to execute workflows on VMware vSphere
- Collecting the required configuration information
- Ensuring that the MySQL .Net connector is installed, if you are using the Invoke-MysqlQuery cmdlet

Required configuration information

Unit or system	Details	Purpose
Arrays	• IP address • User name and password	Perform operations on storage systems Root or admin account credentials are required for storage (arrays).
vSphere	• IP address • User name and password of an admin for vCenter server	Acquire data Perform operations by using VMware APIs You must have installed VMware Power CLI.
External repositories such as OnCommand Balance and custom databases	• IP address • User name and password of a read-only user account	Acquire dataYou must create the relevant WFA content, such as dictionary entries and cache queries for the external repositories, in order to acquire data from the external repositories.
Mail server	• IP address • User name and password User name and password are required if your mail server requires authentication.	Receive WFA notifications through email

Unit or system	Details	Purpose
AutoSupport server	• Mail host	Send AutoSupport messages through SMTPIf you do not have a mail host configured, you can use HTTP or HTTPS to send AutoSupport messages.
Microsoft Active Directory (AD) LDAP server	• IP address • User name and password • Group name	Authenticate and authorize using AD LDAP or AD LDAPS
SNMP management application	• IP address • Port	Receive WFA SNMP notifications
Syslog server	• IP address	Send log data

Related information

NetApp Support

Managing high availability

You can configure a high-availability setup to provide constant support for network operations. If one of the components fail, the mirrored component in the setup takes over the operation and provides uninterrupted network resources. You can also back up the WFA database and supported configurations so that you can recover the data in case of a disaster.

Set up Workflow Automation in MSCS for high availability

You can install and configure Workflow Automation (WFA) in a Microsoft Cluster Service (MSCS) environment to set up high availability and provide failover. Before you install WFA, you must verify that all the required components are configured correctly.

A high-availability setup provides constant support for application operations. If one of the components fails, the mirrored component in the setup takes over the operation and provides uninterrupted network resources.

MSCS is the only clustering solution that is supported by WFA in Windows.

Configure MSCS to install Workflow Automation

Before you install Workflow Automation (WFA) in Microsoft Cluster Server (MSCS), you must configure your MSCS environment.

- MSCS must be installed from the server manager.
- Optional: SnapDrive for Windows must be installed.

The minimum supported version is Windows 2012.

- The same version of WFA must be installed using the same path on both the cluster nodes.
- Both the cluster nodes must be added to the same domain.

You must complete this task by using Cluster Manager in the MSCS interface.

Steps

1. Log in to Cluster Manager as a domain admin.
2. Verify that the LUNs are accessible to both the nodes using one of the following options:
   - Managing the LUNs natively.
   - By using SnapDrive for Windows:
     i. Install and configure SnapDrive for Windows on both the nodes.
     ii. Create a LUN using SnapDrive for Windows and configure the LUN for both the nodes.
3. From Failover Cluster Manager, add the disk to the cluster.

Install OnCommand Workflow Automation on Windows

You can install OnCommand Workflow Automation (WFA) to create and customize storage workflows for automating the storage tasks that are performed in your environment.

- You must have reviewed the installation prerequisites.

  Prerequisites for installing Workflow Automation

- If you are installing WFA on a system where WFA was previously installed and then uninstalled, you must ensure that there are no WFA services on that system.
- You must have downloaded the WFA installer from the NetApp Support Site.
- If you are installing WFA on a virtual machine (VM), the name of the VM must not include the underscore (_) character.
- ActiveState ActivePerl is installed before you install WFA.

  This installation does not affect any other instances of ActivePerl that you have installed on your WFA server.

- Before you reinstall WFA 4.2 or later, you must delete MySQL data directory if you have uninstalled MySQL.

Steps

1. Log in to Windows using an account with administrative permissions.
2. Open Windows Explorer, and then navigate to the directory where the installation file is located.
3. Install WFA:
   - Interactive installation
     i. Right-click and run the WFA installer executable (.exe) file as an admin user.
     ii. Click **Next**.

iii. Enter the credentials for the default admin user, and then click **Next**.

The default admin password must satisfy the following criteria:

- Minimum of eight characters
- One uppercase character
- One lowercase character
- One numeral
- One special character
- The following special characters are not supported in a password and cause installation failure:

`" ; < > , = & ^ |

You must note the credentials of the admin user.

iv. Enter a user name and password for the WFA service logon. For a domain user provide a user name in the format DOMAIN\USER. For a local system user the format is just a user name. The default user name is "wfa".

WFA installer creates a local user if one does not exist. If a local user exists and the password entered is different than the existing password, WFA updates the password.

Ensure the password conforms to the password policy configured for local users on the system. If the password does not conform to the password policy, the install fails.

v. Select the ports for the WFA configuration, and then click **Next**.

vi. Enter a site name and your company name, and then click **Next**.

The site name can include the location of the WFA installation, for example, Pittsburgh, PA.

vii. If you want to change the default installation location, select the location where you want to install WFA, and then click **Next**.

viii. If you want to change the default installation location for third party products, select the location where you want to install third party products, and then click **Next**.

ix. If you do not want to change the default location of the WFA database, click **Next**.

x. Click **Install** to continue the installation.

xi. Click **Finish** to complete the installation.

xii. Verify that WFA was installed successfully by choosing one of the following actions:

- Access WFA through a web browser.
- Use the Windows Services console to verify that the NetApp WFA Server service and the NetApp WFA Database service are running.

◦ Silent installation (from the command prompt):

```
WFA-version_number-build_number.exe /s
/v"WFA_ADMIN_USERNAME=wfa_username WFA_ADMIN_PASSWORD=password
WFA_ADMIN_CONFIRM_PASSWORD=confirm admin password /
WFA_MYSQL_PASS=password CONFIRM_WFA_MYSQL_PASS=confirm MySQL password
WFA_INSTALL_SITE=site WFA_INSTALL_ORGANIZATION=organization_name
WFA_HTTP_PORT=port WFA_HTTPS_PORT=port INSTALLDIR=install_directory
JDKINSTALLDIR=jdk_directory PerlDir=perl_directory
MySqlInstallDir=mysql_directory WFA_SERVICE_LOGON_USERNAME=wfa
service logon username WFA_SERVICE_LOGON_PASSWORD=wfa service logon
user password MYSQL_DATA_DIR= mysql data directory /qr /l*v
C:\install.log"
```

Example

WFA-x64-V5.1.0.0.1-B5355278.exe /s /v"WFA_ADMIN_USERNAME=admin WFA_ADMIN_PASSWORD=Company*123 WFA_ADMIN_CONFIRM_PASSWORD=Company*123 WFA_MYSQL_PASS=MySQL*123 CONFIRM_WFA_MYSQL_PASS=MySQL*123 WFA_INSTALL_SITE=nb WFA_INSTALL_SITE=nb WFA_INSTALL_ORGANIZATION=netapp WFA_HTTP_PORT=80 WFA_HTTPS_PORT=443 INSTALLDIR=\"C:\Program Files\NetApp\WFA\" JDKINSTALLDIR=\"C:\Program Files\NetApp\" PerlDir=\"C:\Perl64\" MySqlInstallDir=\"C:\Program Files\MySQL\"WFA_SERVICE_LOGON_USERNAME=wfa WFA_SERVICE_LOGON_PASSWORD=Wfa*1234\NetApp\WFA\" MYSQL_DATA_DIR=\"C:\Program Files\NetApp\WFA\Database\" /qr /l*v C:\install.log"

The /qn option is not supported by WFA.

The command parameters are as follows:

Parameter	Description
WFA_ADMIN_USERNAME	Admin user name Optional parameter. If you do not specify a value, the value defaults to admin.
WFA_ADMIN_PASSWORD	Admin user password Mandatory parameter. The default admin password must satisfy the following criteria: • Minimum of eight characters • One uppercase character • One lowercase character • One numeral • One special character • The following characters are not allowed and cause password input to fail: `" ; < > , = & ^ |

Parameter	Description
WFA_ADMIN_CONFIRM_PASSWORD	Admin user password Mandatory parameter
WFA_MYSQL_PASS	MySQL user password Mandatory parameter
CONFIRM_WFA_MYSQL_PASS	MySQL user password Mandatory parameter
WFA_INSTALL_SITE	Organizational unit where WFA is being installed Mandatory parameter
WFA_INSTALL_ORGANIZATION	Organization or company name where WFA is being installed Mandatory parameter
WFA_HTTP_PORT	HTTP port Optional parameter. If you do not specify a value, the value defaults to 80.
WFA_HTTPS_PORT	HTTPS port Optional parameter. If you do not specify a value, the value defaults to 443.
INSTALLDIR	Installation directory path Optional parameter. If you do not specify a value, the path defaults to "C:\Program Files\NetApp\WFA\".
JDKINSTALLDIR	JDK installation directory path Optional parameter. If you do not specify a value, the path defaults to "C:\Program Files\NetApp\".
PerlDir	Perl installation directory path Optional parameter. If you do not specify a value, the path defaults to "C:\Perl64\".
MySqlInstallDir	MySQL installation directory path Optional parameter. If you do not specify a value, the path defaults to "C:\Program Files\MySQL\".

Parameter	Description
WFA_SERVICE_LOGON_USERNAME	User name for WFA service logon Optional parameter. If you do not specify a value, the default user name is "wfa". For a domain user provide a user name in the format DOMAIN\USER. For a local system user the format is just a user name. WFA installer creates a local user if one does not exist. If a local user exists and the password entered is different than the existing password, WFA updates the password. Ensure the password conforms to the password policy configured for local users on the system. If the password does not conform to the password policy, the install fails.
WFA_SERVICE_LOGON_PASSWORD	Password for WFA service logon Mandatory parameter
MYSQL_DATA_DIR	Directory for MYSQL data Optional parameter. If you do not specify a value, the path defaults to "C:\ProgramData\MySQL\MySQLServerData" Available for fresh install only.

Related information

NetApp Support

Configure Workflow Automation with MSCS

After you install Workflow Automation (WFA) in Microsoft Cluster Server (MSCS), you must configure WFA for high availability in MSCS using configuration scripts.

You must have created a backup of WFA.

Before you start your configuration make sure that the WFA encryption key is set consistently on both MSCS cluster nodes. If it is not set on both nodes, then when failover occurs, the credentials cannot be decrypted on the second node causing workflow failures.

Steps

1. Log in to the first node of the MSCS cluster, and perform the following steps:

For…	Do this…
Windows 2012, Windows 2016, Windows 2019	a. From the Failover Cluster Manager, right-click **Service Roles**. b. Select **Create Empty Service Role**, and then rename the role to “WFA”. c. Add the IP address resource to the newly created “WFA” role: i. From the Failover Cluster Manager, right-click the newly created “WFA” role. ii. Select **Resource** > **More Resources** > **IP Address**. iii. Configure the cluster IP address.

2. Edit the `mscs_data_parameters.xml` file and set the relative path to the MySQL data directory:

```
<dir>
    <description>Data directory</description>
    <srcpath>..\..\..\..\..\ProgramData\MySQL\MySQLServerData</srcpath>
    <destpath>wfa</destpath>
</dir>
```

3. Edit the `mscs_resource_properties.xml` file and make the following updates:
   a. Perform a find/replace for the `NA_WFA_DB` service name and update it to `MYSQL57`.
   b. Set the `vip_res <prettyname>` to the virtual IP address name:

```
<resource>
    <type>essential</type>
    <id>vip_res</id>
    <prettyname>WFA IP address</prettyname>
</resource>
```

   c. Set the `data_res <prettyname>` to the disk name assigned to the share disk resource:

```
<resource>
    <type>essential</type>
    <id>datadisk_res</id>
    <prettyname>Cluster Disk 2</prettyname>
</resource>
```

   d. Copy the XML files from the first node to the second node:

```
copy "\\node1\D$\Program Files\NetApp\WFA\bin\ha\*xml" "D:\Program
Files\NetApp\WFA\bin\ha"
```

e. Run the command to join the second node to the cluster:

```
D:\Program Files\NetApp\WFA\bin\ha>perl ha_setup.pl --join -t mscs -f E:\
```

4. At the command prompt, run the ha_setup.pl script to move the WFA data to the shared location and to configure WFA with MSCS for failover. The script is available at WFA_install_location\WFA\bin\ha\.

```
perl ha_setup.pl --first [-t type_of_cluster_vcs] [-g cluster_group_name] [-i
IP_address_name] [-n cluster_name] [-k shared_disk_resource_name] [-f
shared_drive_path]
```

The ha_setup.pl script expects an input using the IP Address resource for the MSCS cluster. When installing on MSCS 2016, the resource needs to be added by name, not IP address, `WFA IP address`. For example:

```
perl ha_setup.pl --first -t mscs -g WFA -i "WFA IP address" -n wfa_cluster -k
"Cluster Disk 2" -f E:\
```

5. Verify that the MSCS resources are created, by checking for the successfully configured message in the output.

```
Successfully configured MSCS cluster resources on this node
```

6. Stop the WFA services from the Failover Cluster Manager:

For…	Do this…
Windows 2012, Windows 2016, Windows 2019	a. Select **Service Roles**, and then select the newly created “WFA” role. b. In the Resource pane, right-click **MYSQL57**, and then select **Take Offline**. c. In the Resource pane, right-click **NA_WFA_SRV**, and then select **Take Offline**.

The WFA database service and the WFA server service must be taken offline. The WFA services must not be stopped from the Windows services.

1. Manually move the WFA resources to the secondary node.
2. Verify that the shared disk is accessible from the second node.
3. At the command prompt, run the ha_setup.pl script on the secondary node of the cluster to configure WFA for using the data from the shared location:

```
perl ha_setup.pl --join [-t type_of_cluster_mscs] [-f shared_drive_path]
```

The ha_setup.pl script is available at WFA_install_location\WFA\bin\ha\.

```
perl ha_setup.pl --join -t mscs -f E:\
```

4. From the Failover Cluster Manager, bring the WFA resources online:

For…	Do this…
Windows 2012, Windows 2016, Windows 2019	a. Right-click the newly created “WFA” role, and then select **Start Role**. The role must be in the Running status, and the individual resources must be in the Online state.

5. Manually switch to the second node of the MSCS cluster.
6. Verify that the WFA services start properly on the second node of the cluster.

Configure earlier versions of OnCommand Workflow Automation for high availability

You can configure OnCommand Workflow Automation (WFA) versions earlier than 3.1 for high availability.

Steps

1. Upgrade the existing version of WFA to the latest available version of WFA.

   Upgrade WFA

   This upgraded version of WFA is the primary node of the cluster.

2. Create a backup of the WFA database.

   Backing up the WFA database

   If any of the parameters were changed manually, you must create a backup of the WFA database, uninstall the existing WFA installation, install the latest available version of WFA, restore the backup, and then proceed with the Microsoft Cluster Service (MSCS) configuration.

3. Configure MSCS to install WFA on the primary node.

   Configure MSCS to install WFA

4. Install the latest available version of WFA on the secondary node.

   Install WFA

5. Configure WFA in MSCS.

   Configure WFA in MSCS

   The WFA server is configured for high availability.

Uninstall Workflow Automation in an MSCS environment

You can uninstall Workflow Automation (WFA) from a cluster by deleting all the WFA

services from the cluster nodes.

This task applies to Windows Server 2012.

Steps

1. Take the services offline by using Failover Cluster Manager:
   a. Right-click the role.
   b. Select **Stop Role**.
2. Uninstall WFA on the first node, and then uninstall WFA on the second node.

   Uninstall OnCommand Workflow Automation
3. Delete the cluster resources from Failover Cluster Manager:
   a. Right-click the role.
   b. Select **Remove**.
4. Manually delete the data in the shared location.

Back up and restore the OnCommand Workflow Automation database and configurations on Windows

You can back up and restore the OnCommand Workflow Automation (WFA) database and supported configurations so that you can recover the data in case of a disaster. The supported configurations include data access, HTTP timeout, and SSL certificates.

You must have admin privileges or architect credentials.

You must create the backup in a secure location because restoring the backup will provide access to all the storage systems that are accessed by WFA.

You can use only the CLI commands or REST APIs for comprehensive backup and restore operations during disaster recovery. You cannot use the web UI to create a backup during disaster recovery in a high-availability environment.

Steps

1. Back up your existing databases and configurations.

   Backing up the OnCommand Workflow Automation database
2. Restore a previous backup of your databases and configurations.

   Restoring the OnCommand Workflow Automation database

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 versions earlier than 6.0, you must have run the latest version of the ocsetup tool on the Unified Manager server to enable and configure remote read-only access to the database.
- For Active IQ Unified Manager6.0 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
2638	5.x	Sybase SQL Anywhere database server
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 versions earlier than 6.0	Enter the user name and password that you used for overriding the default credentials while running ocsetup tool.
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.

For…	Do this…
Performance Advisor for (Active IQ Unified Manager versions earlier than 6.0)	Enter the credentials of an Active IQ Unified Manager user with a minimum role of GlobalRead. 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"/>
```

Upgrade OnCommand Workflow Automation

If you have installed a previous version of OnCommand Workflow Automation (WFA), you can upgrade to the latest version of WFA to use the new features and enhancements.

- You can upgrade to WFA 5.1 from either WFA 5.0 or 4.2 only.

  If you are currently running WFA 4.1 or earlier versions of WFA, then you must first upgrade to either WFA 5.0 or 4.2 and then upgrade to WFA 5.1.

- You can restore a backup taken on either WFA 5.0 or 4.2 on WFA 5.1. A WFA database backup can only be restored to a system that is running the same version or a later version of WFA.

  For example, if you created a backup on a system that is running WFA 4.2, the backup can be restored only to systems that are running WFA 4.2 or later.

- You cannot install MySQL on your own when upgrading from versions earlier than WFA 4.2.

  However, you can install MySQL on your own:

  - During a fresh installation of WFA 4.2 and later or
  - When you are upgrading from WFA 4.2 to later versions of WFA.
    1. Back up the WFA database by using one of the following options:
  - WFA web portal
  - PowerShell script If you want to revert to the same version of WFA, you can use the backup that you created to restore your WFA database.
    1. Uninstall the existing version of WFA.
    2. Install the latest version of WFA.
    3. Restore the WFA database.

You can review the restored content for completeness in functionality—for example, you can check the functioning of your custom workflows.

Upgrade from OnCommand Workflow Automation 3.1 or later versions

You can perform an in-place upgrade from OnCommand Workflow Automation (WFA) 3.1 or later versions to the latest available versions of WFA to use the new features and enhancements.

You must have downloaded the .exe binary file from the NetApp Support Site to the WFA host machine.

The WFA 5.1 cluster connection needs to accept the SSL certificate. When updating from an earlier version of WFA to WFA 5.1, you need to certify the cluster connection. Save the cluster connection details for cluster certification after the in-place upgrade.

You cannot install MySQL on your own when upgrading from earlier versions of WFA. However, you can install MySQL on your own:

- During a fresh installation of WFA 4.2 and later or
- When you are upgrading from WFA 4.2 to later versions of WFA.

Step

1. Upgrade from WFA 3.1 or later versions by choosing one of the following methods:
   - Interactive installation

i. Navigate to the .exe binary file in the WFA host machine, and then run the file.

ii. Follow the on-screen instructions in the wizard to complete the upgrade.

- Silent installation

  Enter the following at the command prompt:

  ```
  WFA-version_number-build_number.exe /s /v"WFA_ADMIN_USERNAME_UP=wfa username
  WFA_ADMIN_PASSWORD_UP=password /qr /l*v C:\upgrade.log"
  ```

  Example:

  ```
  WFA-x64-v4.2.0.0.0-B2973881.exe /s /v"WFA_ADMIN_USERNAME_UP=admin
  WFA_ADMIN_PASSWORD_UP=password*123 /qr /l*v C:\upgrade.log"
  ```

  The /qn option is not supported by WFA.

  If you want to perform a silent upgrade, then you must include values for all of the command parameters:

  - WFA_ADMIN_USERNAME_UP is the user name of a WFA user who has permission to create a WFA database backup.
  - WFA_ADMIN_PASSWORD_UP is the password of the user.

Pack identification during upgrade

During the upgrade process, OnCommand Workflow Automation (WFA) identifies and classifies the entities into a pack. If you had deleted any entity of a pack before the upgrade, the pack will not be identified during the upgrade.

During the upgrade process, WFA compares the packs in the database with the list of packs that were released in the Storage Automation Store to identify the packs that were installed before the upgrade. Pack identification thus classifies existing packs in the database.

WFA performs the following processes to identify and classify packs:

- Maintains a list of packs released in the Storage Automation Store to compare and identify the packs that were installed before the upgrade.
- Classifies the entities in a pack as part of the Storage Automation Store synchronization, if Storage Automation Store is enabled.
- Classifies the entities into packs using the updated list.

Pack identification is applicable only to NetApp-certified packs that were downloaded from the Storage Automation Store.

If a pack is not identified during upgrade, you can re-import the pack to get it identified in WFA. The wfa.log files provide details about the entities that were not identified as a pack during the upgrade.

Upgrading third-party products

You can upgrade third-party products on OnCommand Workflow Automation (WFA) such

as OpenJDK, MySQL, and ActiveState Perl in Windows. Third-party products like Open JDK, MYSQL, and so on, report security vulnerabilities. Starting from this release of WFA, you can now upgrade third-party products on your own.

Upgrade OpenJDK

Oracle JRE is no longer supported in OnCommand Workflow Automation. In this release, OpenJDK replaces Oracle JRE for Windows. You can upgrade new versions of OpenJDK for OnCommand Workflow Automation (WFA) on the Windows server. You can upgrade to a newer version of OpenJDK to get fixes for security vulnerabilities on the Windows server.

You must have Windows admin privileges on the WFA server.

You can update OpenJDK releases within release families. For example, you can upgrade from OpenJDK 11.0.1 to OpenJDK 11.0.2, but you cannot update directly from OpenJDK 11 to OpenJDK 12.

Steps

1. Log in as an admin user on the WFA host machine.
2. Download the latest version of OpenJDK 11 (64-bit) to the target system.
3. Use the Windows Services console to stop the WFA server and WFA Database services.
4. Extract the downloaded version of OpenJDK 11 to the folder where you have installed open JDK.
5. Use the Windows Services console to start the WFA services.

Upgrade MySQL

You can upgrade new versions of MySQL for OnCommand Workflow Automation (WFA) on the Windows server. You can upgrade to a newer version of MySQL to get fixes for security vulnerabilities on the Windows server.

You must have Windows admin privileges and the password for MYSQL root user on the WFA server.

Before reinstalling WFA 4.2 or later, you must have deleted the MySQL data directory if you have uninstalled MySQL.

You should be aware of the following limitations:

- You can upgrade within any version of MySQL 5.7.

  For example, you can upgrade from MySQL 5.7.1 to MySQL 5.7.2.

- You cannot upgrade from MySQL 5.7 to MySQL 5.8

Steps

1. Log in as the admin user on the WFA host machine.
2. Download the appropriate version of MySQL to the target system.
3. Use the Windows Services console to stop the following WFA services:
   - NetApp WFA Database or MYSQL57

- NetApp WFA Server

4. Click on the MYSQL msi package to invoke the upgrade of MySQL.
5. Follow the instructions on the screen to complete MySQL installation.
6. Start the WFA services by using the Windows Services console.

Upgrade ActiveState Perl

OnCommand Workflow Automation (WFA) works with the Enterprise edition of ActiveState Perl on Windows. You can upgrade to a newer version of ActiveState Perl to get fixes for security vulnerabilities on the Windows server.

You must have Windows admin privileges on the WFA server. ActiveState Perl does not support “in-place” upgrades.

WFA 5.1 uses the Enterprise edition of ActiveState Perl.

You can upgrade from ActiveState Perl 5.26.3 to later builds. You cannot upgrade to a major release of ActiveState Perl.

Steps

1. Log in as the admin user on the WFA host machine.
2. Download the latest version of 64-bit ActiveState Enterprise Edition 5.26.3 to the target system.
3. Use the Windows Services console to stop the following WFA services:
   - WFA Database or MYSQL57
   - WFA Server
4. Uninstall the current version of ActiveState Perl on the target system from the control panel.
5. Perform a backup of the C:\Perl64\site\lib folder.
6. Install the new ActiveState Enterprise Edition on the target machine.
7. Restore the \site\lib folder of ActiveState Enterprise Edition whose backup you created in step 5.
8. Restart the WFA services by using the Windows Services console.

Backing up the OnCommand Workflow Automation database

A backup of the OnCommand Workflow Automation (WFA) database includes the system configuration settings and cache information, including the playground database. You can use the backup for restoration purposes on the same system or on a different system.

An automatic backup of the database is created daily at 2 a.m. and is saved as a .zip file in the following location: wfa_install_location/WFA-Backups.

WFA saves up to five backups in the WFA-Backups directory, and replaces the oldest backup with the latest backup. The WFA-Backups directory is not deleted when you uninstall WFA. You can use the automatically created backup for restoration if you did not create a backup of the WFA database while uninstalling WFA.

You can also manually back up the WFA database when you have to save specific changes for restoration; for

example, if you want to back up the changes that you have made before the automatic backup occurs.

- You can restore a WFA database backup only to a system that is running the same version or a later version of WFA.

  For example, if you created a backup on a system that is running WFA 4.2, the backup can be restored only to systems that are running WFA 4.2 or later.

- You cannot use the web UI to back up the WFA database during disaster recovery in a high-availability setup.

Backup and restoration of user credentials

The backup of the WFA database includes the WFA user credentials.

The WFA database is also included in the AutoSupport data; however, the password of any WFA user is not included in the AutoSupport data.

When a WFA database is restored from a backup, the following items are preserved:

- The admin user credentials that were created during the current WFA installation.
- If a user with admin privileges other than the default admin user restores the database, the credentials of both the admin users.
- All other user credentials of the current WFA installation are replaced with the user credentials from the backup.

Back up the WFA database from the web portal

You can back up the OnCommand Workflow Automation (WFA) database from the web portal and use the backup file for data recovery purposes. You cannot perform a full backup from the web portal.

You must have admin or architect credentials to perform this task.

A WFA user with backup role cannot log in to the web portal to perform a backup. The WFA users with backup role can only perform remote or scripted backups.

Steps

1. Log in to the WFA web GUI as an admin.
2. Click **Settings** and under **Maintenance**, click **Backup & Restore**.
3. Click **Backup**.
4. In the dialog box that opens, select a location, and then save the file.

Back up the WFA database using the PowerShell script

If you want to back up the OnCommand Workflow Automation (WFA) database frequently, you can use the PowerShell script that is provided with the WFA installation package.

You must have admin user credentials, architect credentials, or backup user credentials.

For more information, see the REST documentation.

Steps

1. Open Windows PowerShell as an admin user, and then back up the WFA database: `<WFA_install_location\WFA\bin\Backup.ps1> -User user_name -Password password -Path backup_file_path`
   - WFA_install_location is the WFA installation directory.
   - user_name is the user name of the admin user, architect, or backup user.
   - password is the password of the admin user, architect, or backup user.
   - backup_file_path is the complete directory path for the backup file.

   The backup file is a zip file with the name in the following format: wfa_backup_servername_.zip

- wfa_backup_ is a fixed portion of the file name, which is the name of the backup server.
- servername is extracted from the environment of the Windows server.
- _.zip is a fixed portion of the file name. `C:\Program Files\NetApp\WFA\bin\Backup.ps1 -User backup -Password MyPassword123 -Path C:\WFA_backups\backup_10_08_12`

  After the backup is complete, the following output is displayed: C:\WFA_backups\backup_10*08_12\wfa_backup_myserver*.zip . Verify that the backup file was created at the specified location.

Backing up the WFA database using the CLI

If you want to back up the OnCommand Workflow Automation (WFA) database frequently, you can use the WFA command-line interface (CLI) provided with the WFA installation package.

The following are the two backup types:

- Full backup
- Regular backup

Back up (full) the WFA database using the CLI

You can perform a full backup of the OnCommand Workflow Automation (WFA) database by using the WFA command-line interface (CLI). In a full backup, the WFA database, WFA configuration, and key are backed up.

You must have admin user credentials or architect credentials.

In a high-availability environment, you should create scheduled backups by using REST APIs. You cannot create backups by using the CLI when WFA is in failover mode.

For more information, see the REST documentation.

Steps

1. At the shell prompt, navigate to the following directory on the WFA server: `WFA_install_location\WFA\bin.`

   WFA_install_location is the WFA installation directory.

2. Back up the WFA database:

   ```
   .\wfa --backup --user=USER [--password=PASS] [--location=PATH] [--full]
   ```

   - user is the user name of the backup user.
   - password is the password of the backup user.

     If you have not provided the password, you must enter the password when prompted.

   - path is the complete directory path to the backup file.

3. Verify that the backup file was created at the specified location.

Back up (regular) the WFA database using the CLI

You can perform a regular backup of the OnCommand Workflow Automation (WFA) database by using the WFA command-line interface (CLI). In a regular backup, only the WFA database is backed up.

You must have admin user credentials, architect credentials, or backup user credentials.

In a high-availability environment, you should create scheduled backups by using REST APIs. You cannot create backups by using the CLI when WFA is in failover mode.

For more information, see the REST documentation.

Steps

1. At the shell prompt, navigate to the following directory on the WFA server: `WFA_install_location\WFA\bin.`

   WFA_install_location is the WFA installation directory.

2. Back up the WFA database:

   ```
   .\wfa --backup --user=USER [--password=PASS] [--location=PATH]
   ```

   - user is the user name of the backup user.
   - password is the password of the backup user.

     If you have not provided the password, you must enter the password when prompted.

   - path is the complete directory path to the backup file.

3. Verify that the backup file was created at the specified location.

Backing up the WFA database using REST APIs

You can back up the OnCommand Workflow Automation (WFA) database by using the

REST APIs. If WFA is in the failover mode in a high-availability environment, you can use the REST APIs to create scheduled backups. You cannot use the command-line interface (CLI) to create backups during a failover.

The following are the two types of backup:

- Full backup
- Regular backup

Perform a full backup of the WFA database using REST APIs

You can perform a full back up of the OnCommand Workflow Automation (WFA) database by using the REST APIs. In a full backup, the WFA database, WFA configuration, and key are backed up.

You must have admin or architect credentials.

Step

1. Enter the following URL in your web browser: `https://IP address of the WFA server/rest/backups?full=true`

   For more information, see the REST documentation.

Perform a regular backup of the WFA database using REST APIs

You can perform a regular backup of the OnCommand Workflow Automation (WFA) database by using the REST APIs. In a regular backup, only the WFA database is backed up.

You must have admin, architect, or backup credentials.

Step

1. Enter the following URL in your web browser: `https://IP address of the WFA server/rest/backups`

   For more information, see the REST documentation.

Restoring the OnCommand Workflow Automation database

Restoring the OnCommand Workflow Automation (WFA) database includes restoring the system configuration settings and cache information, including the playground database.

- Restoring a WFA database erases the current WFA database.
- You can restore a WFA database backup only to a system that is running the same version or a later version of WFA.

  For example, if you created a backup on a system that is running WFA 4.2, the backup can be restored only to systems that are running WFA 4.2 or later.

- After the restore operation is complete, the WFA SSL certificate is replaced with the SSL certificate in the backup file.

- A comprehensive restore operation of WFA databases and configurations is required during disaster recovery, and can be used in both standalone and high-availability environments.
- A comprehensive backup cannot be created by using the web UI.

  You can use only the CLI commands or REST APIs to backup and restore the WFA database comprehensively during disaster recovery.

Restore the WFA database

You can restore the OnCommand Workflow Automation (WFA) database that you backed up previously.

- You must have created a backup of the WFA database.
- You must have admin or architect credentials.
- Restoring a WFA database erases the current database.
- You can restore a WFA database backup only to a system running the same or a later version of OnCommand Workflow Automation.

  For example, if you created a backup on a system running OnCommand Workflow Automation 4.2, the backup can be restored only to systems running OnCommand Workflow Automation 4.2 or later.

Steps

1. Log in to the WFA web GUI as an admin.
2. Click **Settings** and under **Maintenance**, click **Backup & Restore**.
3. Click **Choose file**.
4. In the dialog box that opens, select the WFA backup file, and click **Open**.
5. Click **Restore**.

You can review the restored content for completeness in functionality—for example, the functioning of your custom workflows.

Restoring the WFA database using the CLI

During a disaster, while recovering data you can restore the OnCommand Workflow Automation (WFA) database and supported configurations that you backed up previously using the command-line interface (CLI). The supported configurations include data access, HTTP timeout, and SSL certificates.

The following are the two types of restore:

- Full restore
- Regular restore

Restore (full) WFA database using the CLI

You can do a full restore of the OnCommand Workflow Automation (WFA) database by using the command-line interface (CLI). In a full restore, you can restore the WFA database, WFA configuration, and key.

- You must have created a backup of the WFA database.
- You must have admin or architect credentials.

Steps

1. At the shell prompt, navigate to the following directory on the WFA server: WFA_install_location\WFA\bin

   wfa_install_location is the WFA installation directory.

2. Perform the restore operation:

   ```
   wfa.cmd --restore --full --user=user_name [--password=password] [--
   location=path] --restart
   ```

   - user_name is the user name of the admin or architect user.
   - password is the password of the user.

     If you have not provided the password, you must enter the password when prompted.

   - path is the complete directory path to the restore file.
3. Verify that the restore operation is successful and WFA is accessible.

Restore (regular) WFA database using the CLI

You can do regular restore of the OnCommand Workflow Automation (WFA) database by using the REST APIs. In a regular restore, you can only backup the WFA database.

- You must have created a backup of the WFA database.
- You must have admin credentials, architect credentials, or backup user credentials.

Steps

1. At the shell prompt, navigate to the following directory on the WFA server: WFA_install_location\WFA\bin

   wfa_install_location is the WFA installation directory.

2. Perform the restore operation:

   ```
   wfa.cmd --restore --user=user_name [--password=password] [--location=path]
   ```

   - user_name is the user name of the admin or architect user.
   - password is the password of the user.

     If you have not provided the password, you must enter the password when prompted.

   - path is the complete directory path to the restore file.
3. Verify that the restore operation is successful and WFA is accessible.

Restoring the WFA database using REST APIs

You can restore the OnCommand Workflow Automation (WFA) database by using REST APIs. You cannot use the command-line interface (CLI) to restore the WFA database during a failover.

The following are the two types of restore:

- Full restore
- Regular restore

Restore (full) the WFA database using REST APIs

You can do a full restore of the OnCommand Workflow Automation (WFA) database by using REST APIs. In a full restore, you can restore the WFA database, WFA configuration, and key.

- You must have created a .zip backup of the WFA database.
- You must have admin or architect credentials.
- If you are restoring the database as a part of the migration procedure, you must do a full restore.

Steps

1. Enter the following URL in the REST client browser: `https://IP address of WFA server/rest/backups?full=true`
2. In the Backup window, select the **POST** method.
3. In the **Part** drop-down list, select **Multipart Body**.
4. In the **File** field, enter the following information:
   a. In the **Content type** drop-down list, select **multi-part/form-data**.
   b. In the **Charset** drop-down list, select **ISO-8859-1**.
   c. In the **File name** field, enter the name of the backup file you created and that you want to restore.
   d. Click **Browse**.
   e. Select the location of the .zip backup file.
5. Navigate to the WFA_install_location\wfa\bin directory, and restart the WFA services:
6. Restart the **NetApp WFA Database** and **NetApp WFA Server** service:

   ```
   wfa --restart
   ```

7. Verify that the restore operation is successful and WFA is accessible.

Restore (regular) the WFA database using REST APIs

You can do a regular restore of the OnCommand Workflow Automation (WFA) database by using REST APIs. In a regular restore, you can only restore the WFA database.

- You must have created a .zip backup of the WFA database.
- You must have admin or architect credentials.

- If you are restoring the database as a part of the migration procedure, you must do a full restore.

Steps

1. Enter the following URL in the REST client browser: `https://IP address of WFA server/rest/backups`
2. In the Backup window, select the **POST** method.
3. In the **Part** drop-down list, select **Multipart Body**.
4. In the **File** field, enter the following information:
   a. In the **Content type** drop-down list, select **multi-part/form-data**.
   b. In the **Charset** drop-down list, select **ISO-8859-1**.
   c. In the **File name**field, enter the name of the backup file as backupFile.
   d. Click **Browse**.
   e. Select the location of the .zip backup file.
5. Navigate to the WFA_install_location\wfa\bin directory, and restart the WFA services:
6. Verify that the restore operation is successful and WFA is accessible.

Reset the admin password created during installation

If you have forgotten the password of the admin user that you created during OnCommand Workflow Automation (WFA) server installation, you can reset the password.

- You must have admin privileges for the Windows system on which you have installed WFA.
- The WFA services must be running.
- This procedure resets only the password of the admin user that was created during the WFA installation.

  You cannot reset the password of other WFA admin users that you created after the WFA installation.

- This procedure does not enforce the password policy that you have configured.

  You must either enter a password that complies with your password policy or change the password from the WFA user interface after you have reset the password.

Steps

1. Open a command prompt and navigate to the following directory: `WFA_install_location\WFA\bin\`
2. Enter the following command:

   ```
   wfa --admin-password [--password=PASS]
   ```

   If you do not provide a password in the command, you must enter the password when prompted.

3. At the command prompt, follow the on-screen instructions to reset the admin password.

Import OnCommand Workflow Automation content

You can import user-created OnCommand Workflow Automation (WFA) content such as workflows, finders, and commands. You can also import content that is exported from another WFA installation, content that is downloaded from the Storage Automation Store or the WFA community, as well as packs, including Data ONTAP PowerShell toolkits and Perl NMSDK toolkits.

- You must have access to the WFA content that you want to import.
- The content that you want to import must have been created on a system that is running the same version or an earlier version of WFA.

  For example, if you are running WFA 2.2, you cannot import content that was created using WFA 3.0.
- You can import content developed on N-2 versions of WFA only into WFA 5.1.
- If the .dar file references NetApp-certified content, the NetApp-certified content packs must be imported.

  The NetApp-certified content packs can be downloaded from the Storage Automation Store. You must refer to the documentation of the pack to verify that all requirements are met.

Steps

1. Log in to WFA through a web browser.
2. Click **Settings**, and under **Maintenance** click **Import Workflows**.
3. Click **Choose File** to select the .dar file that you want to import, and then click **Import**.
4. In the Import Success dialog box, click **OK**.

Related information

NetApp community: OnCommand Workflow Automation

Considerations while importing OnCommand Workflow Automation content

You must be aware of certain considerations when you import user-created content, content that is exported from another OnCommand Workflow Automation (WFA) installation, or content that is downloaded from the Storage Automation Store or the WFA community.

- WFA content is saved as a .dar file and can include the entire user-created content from another system or specific items such as workflows, finders, commands, and dictionary terms.
- When an existing category is imported from a .dar file, the imported content is merged with the existing content in the category.

  For example, consider there are two workflows WF1 and WF2 in category A in the WFA server. If workflows WF3 and WF4 in category A are imported to the WFA server, category A will contain workflows WF1, WF2, WF3, and WF4 after the import.
- If the .dar file contains dictionary entries, then the cache tables corresponding to the dictionary entries are automatically updated.

If the cache tables are not updated automatically, an error message is logged in the wfa.log file.

- When importing a .dar file that has a dependency on a pack that is not present in the WFA server, WFA tries to identify whether all the dependencies on the entities are met.
  - If one or more entities are missing or if a lower version of an entity is found, the import fails and an error message is displayed.

    The error message provides details of the packs that should be installed in order to meet the dependencies.

  - If a higher version of an entity is found or if the certification has changed, a generic dialog box about the version mismatch is displayed, and the import is completed.

    The version mismatch details are logged in a wfa.log file.

- Questions and support requests for the following must be directed to the WFA community:
  - Any content downloaded from the WFA community
  - Custom WFA content that you have created
  - WFA content that you have modified

Migrate the OnCommand Workflow Automation installation

You can migrate an OnCommand Workflow Automation (WFA) installation to maintain the unique WFA database key that is installed during the WFA installation. For example, you can migrate the WFA installation from a Windows 2012 server to a Windows 2016 server.

- You must perform this procedure only when you want to migrate a WFA installation that includes the WFA database key to a different server.
- A WFA database restore does not migrate the WFA key.
- Migrating a WFA installation does not migrate the SSL certificates.
- 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. Access WFA through a web browser as an admin.
2. Back up the WFA database.
3. Open a command prompt on the WFA server and change directories to the following location:
   `c:\Program Files\NetApp\WFA\bin`
4. Enter the following at the command prompt to obtain the database key:

   ```
   wfa.cmd -key
   ```

5. Note the database key that is displayed.
6. Uninstall WFA.
7. Install WFA on the required system.
8. Open the command prompt on the new WFA server and change directories to the following location:

```
c:\Program Files\NetApp\WFA\bin
```

9. Enter the following at the command prompt to install the database key:

   ```
   wfa.cmd -key=yourdatabasekey
   ```

   yourdatabasekey is the key that you noted from the previous WFA installation.

10. Restore the WFA database from the backup that you created.

Uninstall OnCommand Workflow Automation

You can uninstall OnCommand Workflow Automation (WFA) using Microsoft Windows Programs and Features.

Steps

1. Log in to Windows using an account with admin privileges.
2. Click **All Programs** > **Control Panel** > **Control Panel** > **Programs and Features**.
3. Uninstall WFA by choosing one of the following options:
   - Select **NetApp WFA** and click **Uninstall**.
   - Right-click **NetApp WFA** and select **Uninstall**.
4. If the uninstallation process stops responding before it is complete, stop the **NetApp WFA Database** service from the Windows Services console and try to uninstall again.

Managing OnCommand Workflow Automation SSL certificate

You can replace the default OnCommand Workflow Automation (WFA) SSL certificate with a self-signed certificate or a certificate signed by a Certificate Authority (CA).

The default self-signed WFA SSL certificate is generated during the installation of WFA. When you are upgrading, the certificate for the previous installation is replaced with the new certificate. If you are using a non-default self-signed certificate or a certificate signed by a CA, you must replace the default WFA SSL certificate with your certificate.

Replace the default Workflow Automation SSL certificate

You can replace the default Workflow Automation (WFA) SSL certificate if the certificate has expired or if you want to increase the validity period of the certificate.

You must have Windows admin privileges on the WFA server.

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. Log in as the admin user on the WFA host machine.
2. Use the Windows Services console to stop the following WFA services:

- NetApp WFA Database
- NetApp WFA Server

3. Delete the wfa.keystore file from the following location:

   ```
   <WFA_install_location>\WFA\jboss\standalone\configuration\keystore
   ```

4. Open a command prompt on the WFA server, and change directories to the following location:<OpenJDK_install_location>\bin
5. Obtain the database key:

   ```
   keytool -keysize 2048 -genkey -alias "ssl keystore" -keyalg RSA -keystore
   "<WFA_install_location>\WFA\jboss\standalone\configuration\keystore\wfa.keysto
   re" -validity xxxx
   ```

   xxxx is the number of days for the new certificate's validity.

6. When prompted, provide the password (default or new).

   changeit is the default password. If you do not want to use the default password, you must change the password attribute of the SSL element in the standalone-full.xml file from the following location: <WFA_install_location>\WFA\jboss\standalone\configuration\

   ```
   <ssl name="ssl" password="new_password" certificate-key-
   file="${jboss.server.config.dir}/keystore/wfa.keystore"
   ```

7. Enter the required details for the certificate.
8. Review the displayed information, and enter `Yes`.
9. Press **Enter** when prompted by the following message: Enter key password for <SSL keystore> <RETURN if same as keystore password>.
10. Restart the WFA services by using the Windows Services console.

Create a certificate signing request for Workflow Automation

You can create a certificate signing request (CSR) in Windows so that you can use the SSL certificate that is signed by a Certificate Authority (CA) instead of the default SSL certificate for Workflow Automation (WFA).

- You must have Windows admin privileges on the WFA server.
- You must have replaced the default SSL certificate that is provided by WFA.

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

Steps

1. Log in as an admin user on the WFA host machine.
2. Open a command prompt on the WFA server, and then change directories to the following location: <OpenJDK_install_location>\bin

3. Create a CSR:

   ```
   keytool -certreq -keystore
   WFA_install_location\WFA\jboss\standalone\configuration\keystore\wfa.keystore
   -alias "ssl keystore" -file C:\file_name.csr
   ```

   file_name is the name of the CSR file.

4. When prompted, provide the password (default or new).

   changeit is the default password. If you do not want to use the default password, you must change the password attribute of the SSL element in the standalone-full.xml file from the WFA_install_location\WFA\jboss\standalone\configuration\ location.

   ```
   <ssl name="ssl" password="new_password" certificate-key-
   file="${jboss.server.config.dir}/keystore/wfa.keystore"
   ```

5. Send the file_name.csr file to the CA to obtain a signed certificate.

   See the CA web site for details.

6. Download a chain certificate from the CA, and then import the chain certificate to your keystore: `keytool -import -alias "ssl keystore CA certificate" -keystore "WFA_install_location\WFA\jboss\standalone\configuration\keystore\wfa.keystore" -trustcacerts -file C:\chain_cert.cer`

   C:\chain_cert.cer is the chain certificate file that is received from the CA. The file must be in the X.509 format.

7. Import the signed certificate that you received from the CA:

   ```
   keytool -import -alias "ssl keystore" -keystore
   "WFA_install_location\WFA\jboss\standalone\configuration\keystore\wfa.keystore
   " -file C:\certificate.cer
   ```

   C:\certificate.cer is the chain certificate file that is received from the CA.

8. Start the following WFA services:
   - NetApp WFA Database
   - NetApp WFA Server

Managing Perl and Perl modules

OnCommand Workflow Automation (WFA) supports Perl commands for workflow operations. ActivePerl 5.26.3 is installed and configured on the WFA server when you install WFA. You can install and configure your preferred Perl distribution and Perl modules.

In addition to ActivePerl, the required Perl modules from the NetApp Manageability SDK are also installed when you install WFA. The NetApp Manageability SDK Perl modules are required for successful execution of

Perl commands.

Configure your preferred Perl distribution

By default, ActivePerl is installed with OnCommand Workflow Automation (WFA). If you want to use another Perl distribution, you can configure your preferred Perl distribution to work with WFA.

You must have installed the required Perl distribution on the WFA server.

You must not uninstall or overwrite the default ActivePerl installation. You must install your preferred Perl distribution at a separate location.

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 CustomPerl -PerlPath CustomPerlPath

   Set-WfaConfig -Name CustomPerl -PerlPath C:\myperl\perl.exe
   ```

4. When prompted, restart the WFA services.

Manage site-specific Perl modules

You can use the ActiveState Perl Package Manager (PPM) to manage your site-specific Perl modules. You must install your site-specific Perl modules outside the OnCommand Workflow Automation (WFA) installation directory to avoid deletion of your Perl modules during a WFA upgrade.

Using the PERL5LIB environment variable, you can configure the Perl interpreter installed on the WFA server to use your Perl modules.

Installation of the Try-Tiny Perl module in the user area at c:\Perl is used as an example in this procedure. This user area is not deleted when you uninstall WFA, and you can reuse the area after WFA is reinstalled or upgraded.

Steps

1. Set the PERL5LIB environment variable to the location where you want to install your Perl modules.

   ```
   c:\>echo %PERL5LIB% c:\Perl
   ```

2. Verify that the Perl module area is not initialized by using `ppm area list`.

   ```
   c:\Program Files\NetApp\WFA\Perl64\bin>ppm area list
   ```

```
┌──────────┬──────┬──────────────────────────────────────────────────────────────┐
│ name     │ pkgs │ lib                                                          │
├──────────┼──────┼──────────────────────────────────────────────────────────────┤
│ (user)   │  n/a │ C:/Perl                                                      │
│  site*   │  0   │ C:/Program Files/NetApp/WFA/Perl64/site/lib                  │
│  perl    │  229 │ C:/Program Files/NetAPP/WFA/Perl64/lib                       │
└──────────┴──────┴──────────────────────────────────────────────────────────────┘
```

3. Initialize the Perl module area by using `ppm area init user`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm area init user
```

```
Syncing user PPM database with .packlists...done
```

4. Verify that the Perl module area is initialized by using `ppm area list`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm area list
```

```
┌──────────┬──────┬──────────────────────────────────────────────────────────────┐
│ name     │ pkgs │ lib                                                          │
├──────────┼──────┼──────────────────────────────────────────────────────────────┤
│  user    │  0   │ C:/Perl                                                      │
│  site*   │  0   │ C:/Program Files/NetApp/WFA/Perl64/site/lib                  │
│  perl    │  229 │ C:/Program Files/NetAPP/WFA/Perl64/lib                       │
└──────────┴──────┴──────────────────────────────────────────────────────────────┘
```

5. Add the required repositories and install the required packages.
   a. Add the required repository by using `ppm repo add`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm repo add
http://ppm4.activestate.com/MSWin32-x64/5.16/1600/package.xml
```

```
Downloading ppm4.activestate.com packlist...done
Updating ppm4.activestate.com database...done
Repo 1 added.
```

   b. Verify that the required repository is added by using `ppm repo list`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm repo list
```

```
┌──────────┬──────┬──────────────────────────────────────────────────────────┐
│ id       │ pkgs │ name                                                     │
├──────────┼──────┼──────────────────────────────────────────────────────────┤
│  1       │17180 │ ppmr.activestate.com                                     │
└──────────┴──────┴──────────────────────────────────────────────────────────┘
 (1 enabled repository)
```

c. Install the required Perl module by using `ppm install`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm install Try-Tiny --area user
```

```
Downloading ppm4.activestate.com packlist...done
Updating ppm4.activestate.com database...done
Downloading Try-Tiny-0.18...done
Unpacking Try-Tiny-0.18...done
Generating HTML for Try-Tiny-0.18...done
Updating files in user area...done
   2 files installed
```

d. Verify that the required Perl module is installed by using `ppm area list`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm area list
```

```
┌──────────┬──────┬──────────────────────────────────────────────────────────┐
│ name     │ pkgs │ lib                                                      │
├──────────┼──────┼──────────────────────────────────────────────────────────┤
│  user    │  1   │ C:/Perl                                                  │
│  site*   │  0   │ C:/Program Files/NetApp/WFA/Perl64/site/lib              │
│  perl    │  229 │ C:/Program Files/NetAPP/WFA/Perl64/lib                   │
└──────────┴──────┴──────────────────────────────────────────────────────────┘
```

Repair the ActivePerl installation

ActiveState ActivePerl is installed on your OnCommand Workflow Automation (WFA) server when you install WFA. ActivePerl is required for the execution of Perl commands. If you inadvertently uninstall ActivePerl from the WFA server or if the ActivePerl

installation is corrupted, you can manually repair the ActivePerl installation.

Steps

1. Back up the WFA database using one of the following options:
   - WFA web portal
   - PowerShell script
2. Uninstall WFA.
3. Install the version of WFA that you uninstalled.

   ActivePerl is installed when you install WFA.

4. Restore the WFA database.

You can review the restored content for completeness in functionality—for example, the functioning of your custom workflows.

Troubleshooting installation and configuration issues

You can troubleshoot issues that might occur while installing and configuring OnCommand Workflow Automation (WFA).

Cannot open the OnCommand Workflow Automation login page

If you have installed .Net 3.5, the Internet Information Services (IIS) is installed with it. The IIS occupies port 80, which is used by WFA.

Ensure that either the IIS role is removed or IIS is disabled in the WFA server.

Cannot view Performance Advisor data in WFA

If you cannot view Performance Advisor data in WFA or if the data acquisition process from the Performance Advisor data source fails, you should perform certain actions to troubleshoot the issue.

- Ensure that you have specified the credentials of an Active IQ Unified Manager user with a minimum role of GlobalRead when configuring Performance Advisor as a data source in WFA.
- Ensure that you have specified the correct port when configuring Performance Advisor as a data source in WFA.

  By default, Active IQ Unified Manager uses port 8088 for an HTTP connection and port 8488 for an HTTPS connection.

- Ensure that performance data is collected by the Active IQ Unified Manager server.

OnCommand Workflow Automation (WFA) displays a blank page on Windows 2012

A blank page might be displayed if you have downloaded and installed Adobe Flash Player separately from the Adobe website. You must not download and install the Flash Player separately because it is bundled with Internet Explorer in Windows 2012. Updates

for the Flash Player are installed through Windows updates.

If you have downloaded and installed the Flash Player separately, you must perform the following steps:

Steps

1. Uninstall the Flash Player that you have already installed.
2. In Windows, open **Server Manager** > **Local Server** > **ROLES AND FEATURES** > **TASKS** and select **Add Roles and Features**.
3. In the Add Roles and Features Wizard, click **Features** > **User Interface and Infrastructure**, select **Desktop Experience** and then complete adding the feature.

   Adding Desktop Experience adds the Flash Player to Windows.

4. Restart Windows.

Related documentation for OnCommand Workflow Automation

There are additional documents and tools to help you learn to perform more advanced configuration of your OnCommand Workflow Automation (WFA) server.

Other references

The Workflow Automation space within the NetApp community provides additional learning resources, including the following:

- **NetApp community**

  NetApp community: Workflow Automation (WFA)

Tool references

- **Interoperability Matrix**

  Lists supported combinations of hardware components and software versions.

  Interoperability Matrix