OnCommand® Workflow Automation 5.1

Installation and Setup Guide for Linux®

November 2019 | 215-14031_2019-11_en-us
doccomments@netapp.com

NetApp®

Contents

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 ONTAP.

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

WFA license information

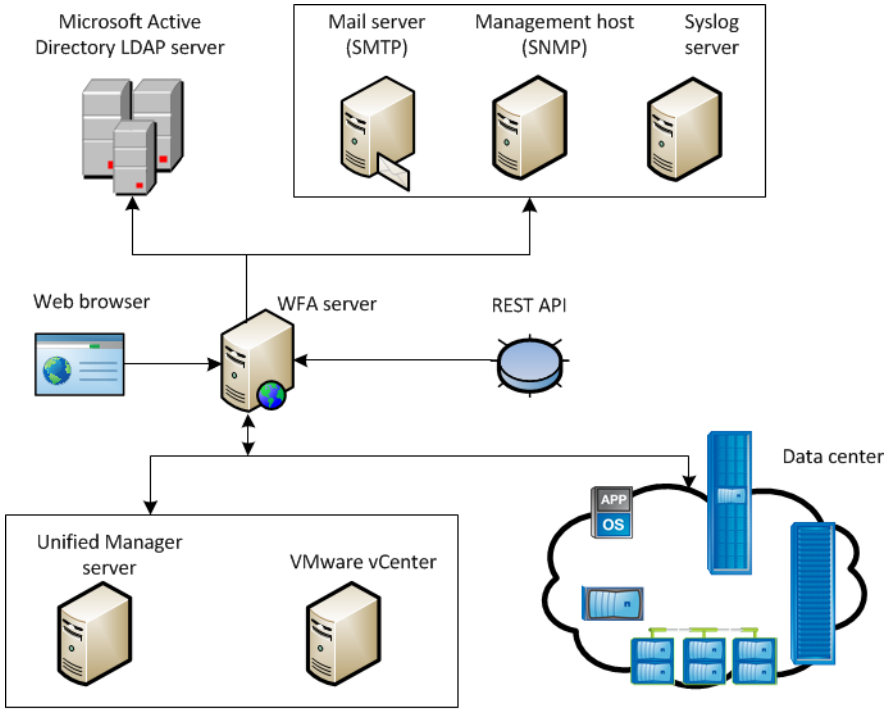
No license is required for using the OnCommand Workflow Automation server.

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:

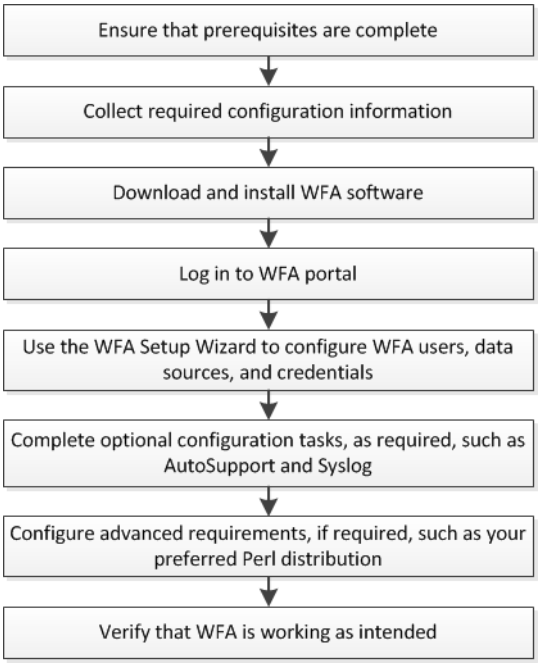


OnCommand Workflow Automation (WFA) deployment

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 for OnCommand Workflow Automation

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

LDAP authentication

- You can use only Microsoft Active Directory Lightweight Directory Access Protocol (LDAP) server for LDAP authentication.
- You must not use an LDAP user name that is part of a hierarchical structure of multiple domains for authentication or notification.

  Note: Microsoft Active Directory Lightweight Directory Services (AD LDS) is not supported.

WFA data sources types

OnCommand Unified Manager 6.0, 6.1, and 6.2 data source types are deprecated in the WFA 4.1 release, and these data source types will not be supported in future releases.

WFA installed on Linux

- Certified content from Data ONTAP operating in 7-Mode is currently not available.
- Commands that include only PowerShell code are not compatible with Linux.
- Certified commands for 7-Mode and VMware are currently not ported to Perl, and are therefore not compatible with Linux.

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

Note: 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

The following table lists all the operating system versions compatible with the WFA server.

Operating System	Version
Red Hat Enterprise Linux	7.0, 7.1, 7.2, 7.3, 7.4, 7.5 and 7.6 64-bit operating systems
CentOS	7.1, 7.2, 7.3, 7.4, 7.5, and 7.6 64-bit operating systems

Note: WFA should be installed on dedicated physical machines or VMs. You must not install any other application on the server that runs WFA.

Other minimum required software

- One of the following supported browsers:
  - Mozilla Firefox
  - Microsoft Internet Explorer
  - Google Chrome
- Perl v5.x
  You can obtain information about the Perl modules that should be installed by using the `./WFA-`*`version_number`*`.bin -l` command.

For more details, see the *Interoperability Matrix Tool*.

Note: 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

Related references

Ports required for Workflow Automation on page 9

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

Port	Protocol	Direction	Purpose
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

  Note: 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

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

- Verifying that Perl v5.10.1 is installed

Required configuration information

Unit or system	Details	Purpose
Arrays	• IP address • User name and password	Perform operations on storage systems **Note:** Root or admin account credentials are required for storage (arrays).
External repositories such as OnCommand Balance and custom databases	• IP address • User name and password of a read-only user account	Acquire data You 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 **Note:** User name and password are required if your mail server requires authentication.	Receive WFA notifications through email
AutoSupport server	• Mail host	Send AutoSupport messages through SMTP If you do not have a mail host configured, you can use HTTP or HTTPS to send AutoSupport messages.

Unit or system	Details	Purpose
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 references

Ports required for Workflow Automation on page 9

Related information

NetApp Support

Installing Perl modules on CentOS and RHEL

Some Perl modules are not included by default with the Perl package for Linux.

About this task

During WFA installation, the WFA installer verifies that all of the Perl modules are available in the system, and then proceeds when this requirement is met. You must install the Perl modules before installing OnCommand Workflow Automation (WFA).

Note: The WFA installer attempts to install the perl modules automatically if the perl-modules are available in the yum repositories configured on the system. If the perl modules are not available, the installer prompts the user to install the perl modules manually. The one exception is the "perl-core" module. This module is not installed on the system automatically even if it is available in the yum repositories configured on the system. This is a known issue.

Table 1: Required Perl modules for WFA

Perl Module	RPM Package Name
Perl core modules	perl-core
DBI	per-DBI
XML::DOM	perl-XML-DOM
Term::ReadKey	perl-TermReadKey
HTTP::Request	perl-libwww-perl
XML::LibXML perl-XML-LibXML	perl-XML-LibXML
DBD::mysql	perl-DBD-MySQL
URI::URL	perl-URI
HTTP::Response	perl-libwww-perl

Perl Module	RPM Package Name
HTTP::Headers	perl-libwww-perl
Net::SSLeay	perl-Net-SSLeay
URI::Escape	perl-URI
LWP::Protocol::https perl-LWP-Protocol-https	perl-LWP-Protocol-https
XML::Parser	perl-XML-Parser
LWP::UserAgent	perl-libwww-perl
Net::LDAP	perl-LDAP
Date::Calc	perl-Date-CalcXML

Steps

1. Log in to the Linux server as a `root` user.
2. Verify that all of the Perl modules required for WFA are installed on the system:

   `./WFA-4.2.0.0.0.bin -l`
3. If any Perl modules are not detected, check whether they are available in the configured repository:

   `yum search Perl-module-name`

   #### Example

   If the `DBD::mysql` module is not detected:

   `yum search perl-DBD-MySQL`
4. If any Perl modules are not in the repository, configure the repository that contains the Perl module, or download the Perl module from the Internet.
5. Install any missing Perl modules from the configured repository:

   `yum -y install Perl-module-name`

   #### Example

   Install the `DBD::mysql` module from the configured repository:

   `yum -y install perl-DBD-MySQL`

Installing OnCommand Workflow Automation on Linux

You can install OnCommand Workflow Automation (WFA) by using the command-line interface (CLI).

Before you begin

- You must have reviewed the installation prerequisites.
  Installation prerequisites on page 11
- You must have downloaded the WFA installer from the NetApp Support Site.

About this task

If you are installing WFA on a virtual machine (VM), the name of the VM must not include the underscore (_) character.

You can change the default installation location at the shell prompt:

`./WFA-`*`version_number`*`.bin [-i `*`WFA_install_directory`*`] [-d `*`mysql_data_directory`*`]`

If you change the default installation location, the `MySQL data` directory is not deleted when you uninstall WFA. You must manually delete the directory.

Note: Before reinstalling WFA 4.2 or later, you must delete the `MySQL` data directory if you have uninstalled MySQL.

Steps

1. Log in to the Linux server as a `root` user.
2. Navigate to the directory where the executable `.bin` file is located.
3. Install WFA by choosing one of the following methods:
   - Interactive installation
     a. Start the interactive session: **`./WFA-`*`version_number`*`.bin`**
     b. Enter the credentials for the default admin user, and then press Enter.
        You must note the credentials for the admin user and ensure that the password meets the following criteria:
        - Minimum of eight characters
        - One uppercase character
        - One lowercase character
        - One numeral
        - One special character
     c. Accept the default ports for WFA configuration or provide custom ports, and then press Enter.
     d. Specify your company name and a site name, and then press Enter.

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

e. Verify that WFA is installed successfully by choosing one of the following actions:

- Access WFA through a web browser.
- Verify that the NetApp WFA Server service and the NetApp WFA Database service are running:

  ```
  service wfa-server status
  ```

  ```
  service wfa-db status
  ```

- Silent installation

  At the shell prompt:

  ```
  ./WFA-version_number.bin [-u admin_user_ name] [-p admin_user_password] [-m https_port] [-n http_port] [-c company_name] [-s site_name] [-i install_directory] [-d mysql_data_directory][-y] [-b]
  ```

  If you want to perform a silent installation, you must specify values for all of the command options. The command options are as follows:

Option	Description
`-y`	Option to skip Skips the installation confirmation
`-b`	Option to skip Skips creating a backup of the WFA database during an upgrade
`-u`	Admin user name
`-p`	Admin user password The admin user password must satisfy the following criteria: ◦ Minimum of eight characters ◦ One uppercase character ◦ One lowercase character ◦ One numeral ◦ One special character
`-m`	HTTPS port
`-n`	HTTP port
`-s`	Site name
`-c`	Company name
`-i`	Installation directory path
`-d`	MySQL data directory
`-h`	Option to display Displays the Help

Related references

Prerequisites for installing Workflow Automation on page 11

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.

Setting up Workflow Automation in VCS for high availability

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

About this task

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.

Note: VCS is the only clustering solution that is supported by WFA on Linux.

Steps

1. Configuring VCS to install OnCommand Workflow Automation on page 17
2. Installing OnCommand Workflow Automation on Linux on page 18
3. Configuring Workflow Automation in VCS on page 20

Configuring VCS to install OnCommand Workflow Automation

Before you install OnCommand Workflow Automation (WFA) in Veritas Cluster Server (VCS), you must ensure that the cluster nodes are properly configured to support WFA.

Before you begin

- VCS must be installed on both nodes of the cluster according to the instructions in the *Veritas Cluster Server 6.1.1 Installation Guide*.
- To receive notifications about cluster events, VCS software must be configured for SNMP and SMTP according to the instructions in the *Veritas Cluster Server Administrator's Guide*.
- All requirements and guidelines for configuring cluster servers must be met according to the VCS documentation.
- SnapDrive for UNIX must be installed if you want to create LUNs using SnapDrive for UNIX.
- Both the cluster nodes must be running a supported version of the operating system.
  The minimum supported operating systems are Red Hat Enterprise Linux 7.0 and VCS 6.1.1.
- The same version of WFA must be installed using the same path on both the cluster nodes.
- The WFA server must be connected to the storage system through Fibre Channel (FC) or iSCSI.
- The latency must be minimum between the WFA server and the storage system.
- The FC link must be active, and the LUNs that are created must be accessible to both the cluster nodes.

- A minimum of two network interfaces must be set up on each system: one for node-to-node communication and the other for node-to-client communication.
- The name of the network interface used for node-to-client communication should be the same on both the systems.
- A separate heartbeat link must be established between the cluster nodes; otherwise, the network interface is used to communicate between the cluster nodes.
- A shared location must be created for high availability.
  You can use SnapDrive for UNIX to create the shared location.
  You can also manage the LUNs using SnapDrive or the storage system command-line interface.
  See the SnapDrive for UNIX compatibility matrix for more information.

Steps

1. Verify that VCS is installed correctly:

   `hastatus –summary`

   Both the nodes must be online, and the VCS service must be running on both the nodes.
2. Verify that the LUNs are accessible to both the nodes by using one of the following options:
   - Manage the LUNs natively.
   - Use SnapDrive for UNIX:
     a. Install SnapDrive for UNIX on both the nodes.
     b. Configure SnapDrive for UNIX on both nodes.
     c. From the first node, run the **`snapdrive storage create`** command to create a LUN.
     d. Verify that the LUN created on the first node is visible on the second node by running the **`snapdrive storage show –all`** command.

Installing OnCommand Workflow Automation on Linux

You can install OnCommand Workflow Automation (WFA) by using the command-line interface (CLI).

Before you begin

- You must have reviewed the installation prerequisites.
  Installation prerequisites on page 11
- You must have downloaded the WFA installer from the NetApp Support Site.

About this task

If you are installing WFA on a virtual machine (VM), the name of the VM must not include the underscore (_) character.

You can change the default installation location at the shell prompt:

`./WFA-`*`version_number`*`.bin [-i `*`WFA_install_directory`*`] [-d `*`mysql_data_directory`*`]`

If you change the default installation location, the `MySQL data` directory is not deleted when you uninstall WFA. You must manually delete the directory.

Note: Before reinstalling WFA 4.2 or later, you must delete the `MySQL` data directory if you have uninstalled MySQL.

Steps

1. Log in to the Linux server as a `root` user.
2. Navigate to the directory where the executable `.bin` file is located.
3. Install WFA by choosing one of the following methods:
   - Interactive installation
     a. Start the interactive session: **`./WFA-version_number.bin`**
     b. Enter the credentials for the default admin user, and then press Enter.
     You must note the credentials for the admin user and ensure that the password meets the following criteria:
        - Minimum of eight characters
        - One uppercase character
        - One lowercase character
        - One numeral
        - One special character
     c. Accept the default ports for WFA configuration or provide custom ports, and then press Enter.
     d. Specify your company name and a site name, and then press Enter.
     The site name can include the location of the WFA installation, for example, Pittsburgh, PA.
     e. Verify that WFA is installed successfully by choosing one of the following actions:
        - Access WFA through a web browser.
        - Verify that the NetApp WFA Server service and the NetApp WFA Database service are running:

          ```
          service wfa-server status
          service wfa-db status
          ```
   - Silent installation
     At the shell prompt:

     `./WFA-version_number.bin [-u admin_user_ name] [-p admin_user_password] [-m https_port] [-n http_port] [-c company_name] [-s site_name] [-i install_directory] [-d mysql_data_directory][-y] [-b]`

     If you want to perform a silent installation, you must specify values for all of the command options. The command options are as follows:

Option	Description
`-y`	Option to skip Skips the installation confirmation
`-b`	Option to skip Skips creating a backup of the WFA database during an upgrade
`-u`	Admin user name

Option	Description
`-p`	Admin user password The admin user password must satisfy the following criteria: ◦ Minimum of eight characters ◦ One uppercase character ◦ One lowercase character ◦ One numeral ◦ One special character
`-m`	HTTPS port
`-n`	HTTP port
`-s`	Site name
`-c`	Company name
`-i`	Installation directory path
`-d`	MySQL data directory
`-h`	Option to display Displays the Help

Related references

Prerequisites for installing Workflow Automation on page 11

Related information

NetApp Support

Configuring Workflow Automation in VCS

After you install Workflow Automation (WFA) in VCS, you must configure WFA in VCS using configuration scripts for high availability.

Before you begin

- You must have installed the same version of WFA on both the cluster nodes.
- You must have the same installation path for both the nodes.
- You must create a backup of WFA.

Steps

1. Log in to the first node of the cluster.
2. Use Cluster Manager to verify that the HA state of both nodes is **`running`**.
3. At the shell prompt, run the `ha_setup.pl` script to move the WFA data to the shared location and to configure WFA with VCS for failover:

   `perl ha_setup.pl --first [-t type_of_cluster_vcs] [-g cluster_group_name] [-e NIC_card_name] [-i IP_address] [-m Netmask] [-n`

_cluster_name_] [-f _mount_point_of_shared_LUN_] [-v _name_of_logical_volume_] [-d _disk_group_name_] [-l _install_directory_]

For the default installation location, the script is available at `/opt/netapp/wfa/bin/ha/`.

Example

```
perl ha_setup.pl --first -t vcs -g WFA -e eth0 -i 10.238.170.3 -m
255.255.255.0 -n wfa_cluster -f /mnt/wfa_mount/ -v lun_volume -d lun_dg
-l /opt/netapp/wfa
```

4. Use Cluster Manager to verify that the WFA services, mount point, virtual IP, NIC, and volume group are added to the cluster group.
5. Use Cluster Manager to move the WFA resources to the secondary node:
   a. Select and right-click the cluster group.
   b. Select **Switch To** > **Secondary Node**.
6. Verify that the data mount, virtual IP, volume group, and NIC cards are up on the second node of the cluster.
7. Take the WFA services offline by using Cluster Manager:
   a. Select **WFA** > **Application** > **wfa-server**.
   b. Right-click and select **Offline**.
   c. Select **WFA** > **Application** > **wfa-db**.
   d. Right-click and select **Offline**.
8. At the shell prompt, run the `ha_setup.pl` script on the secondary node of the cluster to configure WFA to use the data from the shared location:

   perl ha_setup.pl --join [-t _type_of_cluster_vcs_] [-f _mount_point_of_shared_LUN_]

   For the default installation location, the script is available at `/opt/netapp/wfa/bin/ha/`.

   Example

   ```
   perl ha_setup.pl --join -t vcs -f /mnt/wfa_mount/
   ```

9. Go to Cluster Manager and click **Cluster Group** > **Online** > **Server**.

   It might take a while before Cluster Manager shows that the application resources are online. You can also right-click the application resources and verify whether the resources are online.
10. Ensure that WFA is accessible through the IP address used during this configuration.

Configuring an earlier version 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.

   Upgrading WFA on page 38

   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 on page 42

   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 Veritas Cluster Server (VCS) configuration.

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

   Configuring VCS to install WFA on page 17

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

   Installing WFA on page 14

5. Configure WFA in VCS.

   Configuring WFA in VCS on page 20

   The WFA server is configured for high availability.

Uninstalling Workflow Automation in a VCS environment

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

Steps

1. Take the services offline by using Cluster Manager:
   a. Right-click the cluster group.
   b. Select **Offline**, and then select the node.
2. Uninstall WFA on the first node, and then uninstall WFA on the second node.

   Uninstalling OnCommand Workflow Automation on page 54

3. Delete the cluster resources from Cluster Manager:
   a. Right-click the cluster group.
   b. Select **Delete**.
4. Manually delete the data in the shared location.

Backing up and restoring the OnCommand Workflow Automation database and configurations on Linux

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.

Before you begin

You must have administrator privileges or architect credentials.

About this task

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.

Note:

- A comprehensive backup of WFA databases and configurations is required during disaster recovery and can be used in both standalone and high-availability environments.
- 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 for backing up or restoring the WFA database during disaster recovery.

Steps

1. Back up the OnCommand Workflow Automation database.

   Backing up the OnCommand Workflow Automation database on page 42

2. Restore a previous backup of the OnCommand Workflow Automation database.

   Restoring the OnCommand Workflow Automation database on page 46

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.

Related concepts

OnCommand Workflow Automation data sources on page 24
Configuring OnCommand Workflow Automation on page 31

Related tasks

Setting up a data source on page 27
Configuring the credentials of a target system on page 30
Creating local users on page 29

Accessing OnCommand Workflow Automation

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

Before you begin

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. Optional: In the **Settings** > **Setup** menu, set up the credentials and a data source.
4. Optional: 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.

Configuring 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.

   Note: 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.

Configuring 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.

   ### Example

   `/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.

   Note: 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 *****
   ```

Setting 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.

Before you begin

- 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 Manager 6.0 and later, you must have created a database user account on the Unified Manager server.
  See the *OnCommand Unified Manager Online Help* for details.
- The TCP port for incoming connections on the Unified Manager server must be open.
  See the documentation on your firewall for details.
  The following are the default TCP port numbers:

TCP port number	Unified Manager server version	Description
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.
- 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.

About this task

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*.

Note: 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.
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. **Note:** 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.

6. Click **Save**.

7. Optional: In the Data Sources table, select the data source, and click  on the toolbar.

8. Verify the status of the data acquisition process.

Related tasks

Configuring a database user by running ocsetup on Windows on page 25
Configuring a database user by running ocsetup on Linux on page 26

Adding 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. Optional: 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.

Creating 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.

Before you begin

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

About this task

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.

  Note: 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**.

Related tasks

Configuring the credentials of a target system on page 30
Configuring authentication settings on page 32

Configuring 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.

About this task

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
     You can use regular expression syntax 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.
7. Test the connectivity by performing the following action:

If you selected the following match type...	Then...
Exact	Click **Test**.

If you selected the following match type...	Then...
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**.

Related tasks

Accessing OnCommand Workflow Automation on page 24
Configuring protocols for connecting to remote systems on page 35

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

Related tasks

Configuring AutoSupport on page 31
Configuring authentication settings on page 32
Configuring email notifications on page 33
Configuring SNMP on page 34
Configuring Syslog on page 34
Accessing OnCommand Workflow Automation on page 24

Configuring 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

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

6. Optional: 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. Optional: Test the sending of an AutoSupport message to the specified destination by clicking **Send Now**.
8. Click **Save**.

Configuring 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.

Before you begin

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

About this task

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.

Note: 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. Add a list of Active Directory group names to the required roles.

   Note: You can add a list of AD group names to the required roles in the Active Directory Groups Window.

   Active Directory Groups window on page 33

3. Click **Administration > WFA Configuration**.
4. In the **WFA Configuration** dialog box, click the **Authentication** tab, and then select the **Enable Active Directory** check box.
5. Enter the required information in the fields:

a. Optional: If you want to use the *user@domain* format for domain users, replace `sAMAccountName` with `userPrincipalName` in the **User name attribute** field.

b. Optional: If unique values are required for your environment, edit the required fields.

6. Click **Add** to add the Active Directory in the Active Directory Servers table with a URI format:

   `ldap://active_directory_server_address[:port]`

   Example

   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]`

7. Optional: Provide the credentials to bind the LDAP server and the base DN.

8. Optional: Test the authentication of the given user:

   a. Enter the user name and password.

   b. Click **Test Authentication**.

   Note: You must have added the Active Directory Group to test the authentication of the given user in WFA.

9. Click **Save**.

Adding 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**.

Configuring email notifications

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

Before you begin

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. Optional: 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**.

Configuring SNMP

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

About this task

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.

Note: 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.

Configuring 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.

Before you begin

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**.

Configuring 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**.

Disabling 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.

Before you begin

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

About this task

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

2. Enter the following command:

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

Modifying the default password policy

OnCommand Workflow Automation (WFA) is configured to enforce a password policy for local users. You can modify the default password policy.

Before you begin

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

About this task

- 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.
- The command for the default password policy is `./wfa --password-policy=default`.
  The default is “minLength=true,8;specialChar=true,1;digitalChar=true,1;lowercaseChar=true, 1;uppercaseChar=true,1;whitespaceChar=false” . This indicates that the default password policy must have a minimum length of eight characters, must contain at least 1 special character, 1 digit, 1 lowercase character, 1 uppercase character, and no spaces.

Steps

1. At the shell prompt, navigate to the following directory on the WFA server:
   `WFA_install_location``/wfa/bin/`
2. Modify the default password policy by entering the following command:

   `./wfa --password-policy=`*`PasswordPolicyString`*` --restart=WFA`

Enabling or disabling remote access to the OnCommand Workflow Automation database

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

Before you begin

- You must have logged in to the WFA host system as a root user.
- If a firewall is installed on the WFA host system, you must have configured your firewall settings to allow access to the MySQL port (3306) from the remote system.

About this task

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. Navigate to the following directory on the WFA server: *`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`

Related references

Ports required for Workflow Automation on page 9

Modifying 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.

Before you begin

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

About this task

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. At the shell prompt, navigate to the following directory on the WFA server:
   WFA_install_location/wfa/bin/
2. Enter the following command:
   ./wfa --txn-timeout[=*TIMEOUT*] --restart=WFA

   Example

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

Configuring 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 of 180 seconds.

About this task

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. You cannot set the timeout value from the WFA web GUI.

Steps

1. Log in as a root user on the WFA host machine.
2. Set the timeout value:
   installdir* bin/wfa -S=*timeout value in minutes

Upgrading from OnCommand Workflow Automation 3.1 or later

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

Before you begin

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

About this task

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

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. You can install MySQL on your own:

- When you are upgrading from WFA 4.2 to later versions of WFA.
- Upgrade from WFA 3.1 or later by choosing one of the following methods:
  - Interactive installation
    1. Navigate to the `.bin` binary file in the WFA host machine, and then run the file.
    2. Follow the on-screen instructions to complete the upgrade.
  - Silent installation
    At the shell prompt:

    `./WFA-`*`version_number-build_number`*`.bin [-y] [-u `*`admin_user_name`*`] [-p `*`admin_user_password`*`]`

    Example:

    `./WFA-3.1-Z3234343435.bin -y -u admin -p Company*234`

    During the silent upgrade, you must include values for all of the following command options:

    - `-y` skips the installation confirmation.
    - `-u` specifies the admin user name.
    - `-p` specifies the admin user password.
      If you have not provided the admin user password, then you must enter the password when prompted.

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 Workflow Automation (WFA) such as OpenJDK and MySQL in Linux.

Related tasks

Upgrading OpenJDK on page 40
Upgrading MySQL on page 40

Upgrading OpenJDK

Oracle JRE is no longer supported in OnCommand Workflow Automation. In this release, OpenJDK replaces Oracle JRE for Linux. You can upgrade to a newer version of OpenJDK on the Linux server on which OnCommand Workflow Automation is installed to obtain fixes for security vulnerabilities.

Before you begin

You must have root privileges for the Linux system on which WFA is installed.

About this task

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 a root user on the WFA host machine.
2. Install the latest version of OpenJDK 11 from the yum repository on the target system.
3. At the shell prompt, stop the WFA server.
4. Restart the WFA server.

Upgrading MySQL on Linux

You can upgrade to a newer version of MySQL on the Linux server on which OnCommand Workflow Automation is installed to obtain fixes for security vulnerabilities.

Before you begin

You must have root privileges for the Linux system on which WFA is installed.

Note: Before you reinstall WFA 4.2, you must delete the MySQL data directory if you have uninstalled MySQL.

About this task

You can only upgrade to minor updates of MySQL 5.7, for example, 5.7.22 to 5.7.26. You cannot upgrade to major versions of MySQL, for example, version 5.8.

Steps

1. Log in as a root user on the WFA host machine.
2. Download the latest MySQL Community Server `.rpm` bundle on the target system.
3. Untar the bundle to a directory on the target system.
4. You will get multiple `.rpm` packages in the directory after untarring the bundle, but WFA only needs the following rpm packages:
   - mysql-community-client-5.7.x
   - mysql-community-libs-5.7.x
   - mysql-community-server-5.7.x
   - mysql-community-common-5.7.x
   - mysql-community-libs-compat-5.7.x

   Delete all other `.rpm` packages. Installing all packages in an rpm bundle will not cause any problems.
5. At the shell prompt, stop the WFA database and server services:

   ```
   service wfa-db stop
   service wfa-server stop
   ```
6. Invoke the upgrade of MySQL by using the following command:

   ```
   rpm -uvh *.rpm
   ```

   `*.rpm` refers to the `.rpm` packages in the directory where you downloaded the newer version of MySQL.
7. Start the WFA services:

   ```
   service wfa-db start
   service wfa-server start
   ```

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.

Note:

- 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.

Note: 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.

Choices

- Backing up the WFA database from the web portal on page 43
- Backing up the WFA database using the CLI on page 43
- Backing up the WFA database using REST APIs on page 44

Backing 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.

Before you begin

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

About 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.

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

Backing 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.

Before you begin

You must have admin user credentials or architect credentials.

About this task

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. Optional: Verify that the backup file was created at the specified location.

Backing 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.

Before you begin

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

About this task

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. Optional: 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

Performing 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.

Before you begin

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.

Performing 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.

Before you begin

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.

Note:

- 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.

Restoring the WFA database

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

Before you begin

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

About this task

- 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**.

After you finish

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

Related concepts

Backing up the OnCommand Workflow Automation database on page 42

Related tasks

Migrating the OnCommand Workflow Automation installation on page 53
Modifying the transaction timeout setting of OnCommand Workflow Automation on page 37

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

Restoring (full) the WFA database using the CLI

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

Before you begin

- 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. Restore the WFA database:

   `wfa --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.

Restoring (regular) the WFA database using the CLI

You can do a regular restore of the OnCommand Workflow Automation (WFA) database that you backed up previously by using the command-line interface (CLI). In a regular restore, you can only restore the WFA database.

Before you begin

- 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. Restore the WFA database:

   wfa --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

Restoring (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.

Before you begin

- 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 `/opt/netapp/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.

Restoring (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.

Before you begin

- 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 `/opt/netapp/wfa/bin` directory, and restart the WFA services:
6. Verify that the restore operation is successful and WFA is accessible.

Resetting the admin password created during installation

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

Before you begin

- You must have root privileges for the Linux system on which you have installed WFA.
- The WFA services must be running.

About this task

- This procedure resets only the password of the admin user 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 you have configured.
  Therefore, you must 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. As a root user, log in to the Linux system on which WFA is installed.
2. At the shell prompt, navigate to the following directory on the WFA server:
   WFA_install_location`/wfa/bin/`
3. Enter the following command:

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

   If you have not provided a password, you must enter the password when prompted.
4. At the shell prompt, follow the on-screen instructions.

Importing 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.

Before you begin

- 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 Management Software
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

Migrating 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.

About this task

- 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 shell prompt on the WFA server and change directories to the following location:
   WFA_install_location`/wfa/bin/`
4. Enter the following at the shell prompt to obtain the database key: **`./wfa -key`**
5. Note the database key that is displayed.
6. Uninstall WFA.
7. Install WFA on the required system.
8. Open a shell prompt on the WFA server and change the directories to the following location:
   WFA_install_location`/wfa/bin/`
9. At the shell prompt, install the database key by entering the following command:

   **`./wfa -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.

Related concepts

Backing up the OnCommand Workflow Automation database on page 42

Related tasks

Backing up the WFA database from the web portal on page 43
Backing up (full) the WFA database using the CLI on page 43
Uninstalling OnCommand Workflow Automation on page 54
Installing OnCommand Workflow Automation on Linux on page 14
Restoring the WFA database on page 46
Importing OnCommand Workflow Automation content on page 51

Uninstalling OnCommand Workflow Automation

You can uninstall OnCommand Workflow Automation (WFA) from your Red Hat Enterprise Linux machine using a single command.

Before you begin

You must have root user access to the Red Hat Enterprise Linux machine from which want to uninstall WFA.

Steps

1. Log in as root user to the Red Hat Enterprise Linux machine from which you want to uninstall WFA.
2. At the shell prompt, enter the following command:

   ```
   rpm -e wfa
   ```

   If the default installation location was changed, the `MySQL data` directory is not deleted when you uninstall WFA. You must manually delete the directory.

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.

Replacing 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.

Before you begin

You must have root privileges for the Linux system on which you have installed WFA.

About this task

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 a root user on the WFA host machine.
2. At the shell prompt, navigate to the following directory on the WFA server: *WFA_install_location*/wfa/bin
3. Stop the WFA database and server services:

   ./wfa --stop=WFA

   ./wfa --stop=DB
4. Delete the wfa.keystore file from the following location: *WFA_install_location*/wfa/jboss/standalone/configuration/keystore.
5. Open a shell prompt on the WFA server, and then change directories to the following location: <*OpenJDK_install_location*>/bin
6. Obtain the database key:

   keytool -keysize 2048 -genkey -alias "ssl keystore" -keyalg RSA -keystore "*WFA_install_location*/wfa/jboss/standalone/configuration/keystore/wfa.keystore" -validity *xxxx*

   xxxx is the number of days for the validity of the new certificate.
7. 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

Example

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

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

    ./wfa --start=DB

    ./wfa --start=WFA

Related tasks

Creating a certificate signing request for Workflow Automation on page 56

Creating a certificate signing request for Workflow Automation

You can create a certificate signing request (CSR) in Linux 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).

Before you begin

- You must have root privileges for the Linux system on which you have installed WFA.
- You must have replaced the default SSL certificate that is provided by WFA.

About this task

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 a root user on the WFA host machine.
2. Open a shell prompt on the WFA server, and then change directories to the following location: `<OpenJDK_install_location>/bin`
3. Create a CSR file:

   keytool -certreq -keystore *WFA_install_location*/wfa/jboss/standalone/configuration/keystore/wfa.keystore -alias "ssl keystore" -file /root/*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.

Example

```
<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" -trustcacerts -file C:\certificate.cer

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

8. Start the WFA services:

   ./wfa --start=DB

   ./wfa --start=WFA

Related tasks

Replacing the default Workflow Automation SSL certificate on page 55

Managing Perl and Perl modules

OnCommand Workflow Automation (WFA) supports Perl commands for workflow operations. You can install and configure your preferred Perl distribution and Perl modules.

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.

You can install additional Perl modules, if required, from the Red Hat package repositories or from the CPAN repositories.

Configuring your preferred Perl distribution

The Perl package installed on your system is used by OnCommand Workflow Automation. If you want to use another Perl distribution, you can configure your preferred Perl distribution to work with WFA.

Before you begin

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

Steps

1. At the shell prompt, navigate to the following directory on the WFA server:
   WFA_install_location/wfa/bin/
2. Enter the following command:

   /wfa --custom-perl[=*PERL_PATH*] --restart=WFA

   Example

   /wfa --custom-perl=/usr/local/perl5-11/bin/perl --restart=WFA

Troubleshooting installation and configuration issues

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

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.

Creating a support case for OnCommand Workflow Automation

You can create support cases for OnCommand Workflow Automation (WFA) issues that require assistance from technical support. You must use the technical triage template for creating a support case.

About this task

The technical triage template for WFA provides all the required information for creating a support case. You must use the questions and information in the technical triage template to construct your issue, which helps in improving the time required for the resolution of your case.

Steps

1. Access the WFA technical triage template.

   NetApp KB Article 1013484: Triage Template - How to Troubleshoot OnCommand Workflow Automation

2. Use the template to construct and send your case to technical support.

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

Copyright

Trademark

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277