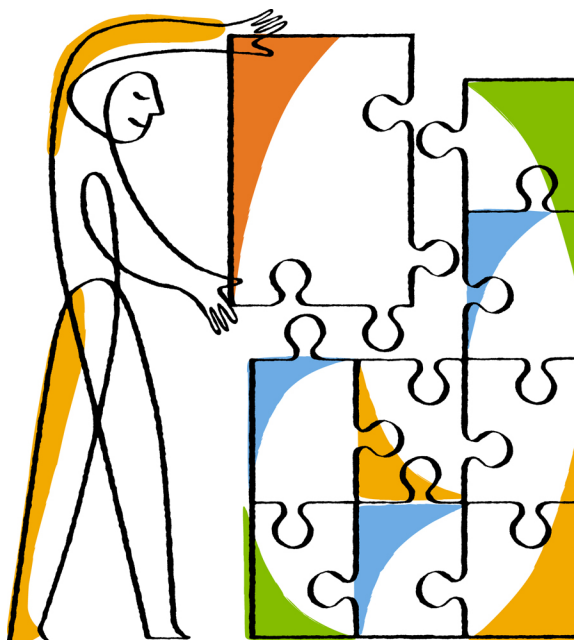




Release Candidate Documentation - Contents Subject To Change

OnCommand® Workflow Automation 2.2

Installation and Setup Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-08682_A0
January 2014

Contents

Overview of OnCommand Workflow Automation	5
OnCommand Workflow Automation deployment architecture	5
OnCommand Workflow Automation installation and setup overview	6
System requirements for OnCommand Workflow Automation	8
Ports required for Workflow Automation	9
Prerequisites for installing Workflow Automation	11
Installing OnCommand Workflow Automation	13
Setting up OnCommand Workflow Automation	15
Accessing OnCommand Workflow Automation	15
Setting up WFA using the Setup Wizard	16
Creating users	17
OnCommand Workflow Automation data sources	18
Configuring a database user on OnCommand Unified Manager	18
Setting up a data source	20
Configuring the credentials of a target system	22
Configuring OnCommand Workflow Automation	23
Configuring AutoSupport	24
Configuring LDAP	24
Configuring email notifications	25
Configuring SNMP	25
Configuring Syslog	26
Enabling remote access to the OnCommand Workflow Automation database	27
Restricting access rights of OnCommand Workflow Automation on the host	27
Modifying the transaction timeout setting of OnCommand Workflow Automation	28
Enabling HTTPS-only access to OnCommand Workflow Automation	29
Upgrading OnCommand Workflow Automation	30
Backing up the OnCommand Workflow Automation database	31
Backing up the WFA database from the web portal	32
Backing up the WFA database using PowerShell script	32
Restoring the OnCommand Workflow Automation database	34
Importing OnCommand Workflow Automation content	35

Migrating the OnCommand Workflow Automation installation	36
Uninstalling OnCommand Workflow Automation	38
Managing OnCommand Workflow Automation SSL certificate	39
Replacing the default Workflow Automation SSL certificate	39
Creating a certificate signing request for Workflow Automation	40
Managing Perl and Perl modules	42
Configuring your preferred Perl distribution	42
Managing site-specific Perl modules	43
Repairing the ActivePerl installation	46
Troubleshooting installation and configuration issues	47
Related documentation for OnCommand Workflow Automation	48
Copyright information	49
Trademark information	50
How to send your comments	51
Index	52

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, and cloning storage. You can use WFA to build workflows to complete tasks specified by your processes. WFA supports both clustered Data ONTAP and Data ONTAP operating in 7-Mode.

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

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

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

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

WFA features

WFA includes the following features:

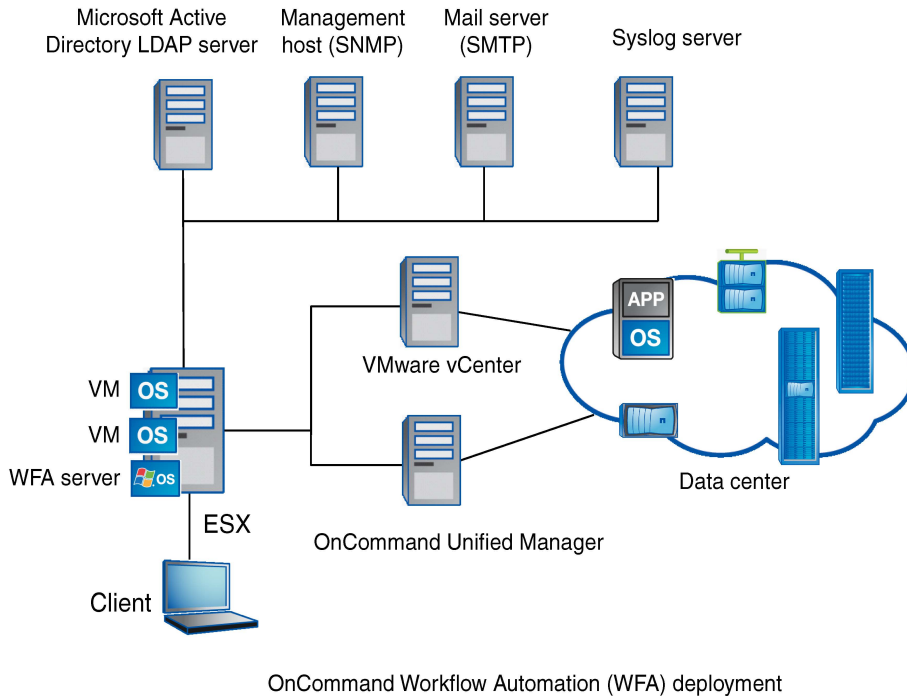
- Designer portal to build workflows
The designer portal includes several building blocks, such as commands, templates, finders, filters, and functions, that are used to create workflows. The designer enables workflows to include advanced capabilities such as automated resource selection, row repetition (looping), and approval points.
- Execution portal to execute workflows, verify status of workflow execution, and access logs
- Administration portal for tasks such as setting up WFA, connecting to data sources, and configuring user credentials
- Web services interfaces to invoke workflows from external portals and data center orchestration software

OnCommand Workflow Automation deployment architecture

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

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

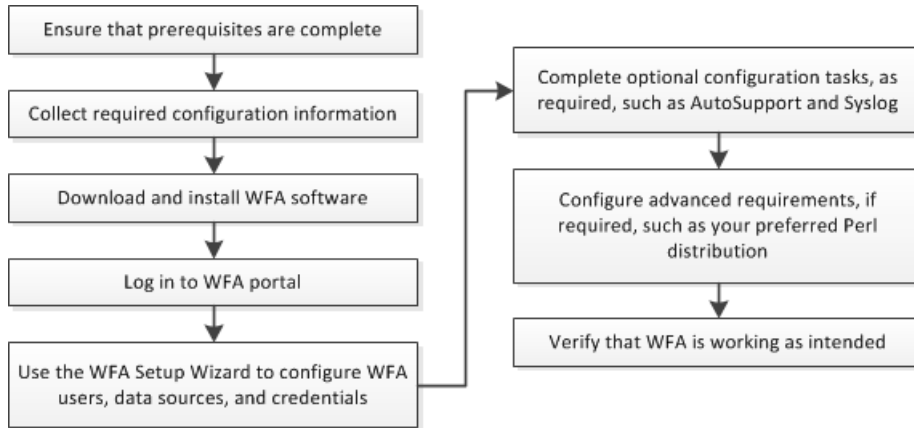
The following illustration shows an example deployment:



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:



System requirements for 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 recommended hardware requirements for the WFA server:

Component	Recommended
CPU	2.27 GHz or faster, 2 core, 64-bit
RAM	4 GB
Free disk space	20 GB

Software requirements for installing WFA

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

Microsoft Windows Server 2008 R2 EE is the recommended Windows operating system for WFA.

Other minimum required software

- One of the following supported browsers:
 - Mozilla Firefox
 - Microsoft Internet Explorer
 - Google Chrome
- The latest version of Adobe Flash Player for your browser
- PowerShell 2.0
- .NET Framework 3.5
- VMware Power CLI version 5

Note: The PowerShell extension for VMware APIs is required only if you are integrating WFA with VMware vSphere.

For more details, see the Interoperability Matrix.

Related references

[Ports required for Workflow Automation](#) on page 9

Related information

[Interoperability Matrix: support.netapp.com/matrix](https://support.netapp.com/matrix)

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:

TCP 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	Microsoft-DS, NetBIOS-ssn	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:

TCP port	Protocol	Direction	Purpose
2638	Sybase	Incoming	Caching data from OnCommand Unified Manager earlier than 6.0

TCP port	Protocol	Direction	Purpose
3306	MySQL	Incoming	Caching data from OnCommand Unified Manager 6.0 and later
8088, 8488	HTTP, HTTPS	Incoming	Caching data from Performance Advisor

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

TCP 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:

TCP 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 complete 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 should contact technical support.

- Verifying that the system has access to the following, as applicable:

- Storage controllers
- OnCommand Unified Manager
- VMware vCenter

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

- Installing all the .NET Framework 3.5 run-time patches on the system
- Verifying that PowerShell 2.0 is installed
- Ensuring that VMware Power CLI is installed, if you are integrating WFA with VMware vSphere
- Collecting the required configuration information

Required configuration information

The following table lists the required information, as applicable, to your environment.

Unit or system	Details	Purpose
Arrays	• IP address • User name and password	Perform operations on storage systems Note: The root or administrator account credentials are required for storage (arrays).
vSphere	• IP address • User name and password of an administrator for vCenter server	Data acquisition Perform operations by using VMware APIs

Unit or system	Details	Purpose
External repositories, such as OnCommand Balance and custom databases	- IP address - User name and password of a read-only user account	Data acquisition You must create the relevant WFA content, such as finders and commands for the external repositories, 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.
Microsoft Active Directory (AD) LDAP server	- IP address - User name and password - Group name You should use an LDAP bind account with read-only privilege.	Authenticate and authorize using AD LDAP server
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 Site: support.netapp.com](http://support.netapp.com)

Installing OnCommand Workflow Automation

You can use the installation wizard to install OnCommand Workflow Automation (WFA).

Before you begin

- You must have reviewed all of the [installation prerequisites](#) on page 11.
- You must have downloaded the WFA installer from the NetApp Support Site.
- You must ensure that ActiveState ActivePerl is not installed on the computer where you are installing WFA.

About this task

- If you are installing WFA on a virtual machine (VM), the name of the VM must not include the underscore (_) character.
- ActiveState ActivePerl is installed when you install WFA.

Steps

1. Log in to Windows using the default administrator account.

Note: You must not install WFA using any other Windows user accounts, including the user accounts that have administrator privileges, for security purposes.

2. Open Windows Explorer and navigate to the directory where the installation file is located.
3. Right-click the WFA installer executable file and run the .exe file as an administrator.
4. Click **Next**.
5. Accept the license agreement and click **Next**.
6. Accept the default ports for WFA configuration and click **Next**.

If PowerShell and .NET Framework are not found in your system, the installer prompts you to download and install the software.

7. Click **Next** and enter a site name and your company name, and click **Next**.
8. Enter the credentials for the default administrator user and click **Next**.

You must note the credentials of the administrator user.

9. Optional: If you want to change the default installation location, select the location where you want to install WFA and click **Next**.
10. Click **Install** to continue the installation.
11. Review the information displayed by the setup wizard and click **Next**.
12. Click **Finish** to complete the installation.

14 | Installation and Setup Guide

13. Optional: You can verify that WFA is installed successfully by choosing one of the following actions:
- Access WFA through a web browser.
 - Use the Windows Services console to ensure that the NetApp WFA Server service and the NetApp WFA Database service are running.

Related tasks

[Upgrading OnCommand Workflow Automation](#) on page 30

Related references

[Prerequisites for installing Workflow Automation](#) on page 11

Related information

[NetApp Support Site: support.netapp.com](http://support.netapp.com)

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 18

[Configuring OnCommand Workflow Automation](#) on page 23

Related tasks

[Setting up a data source](#) on page 20

[OnCommand Workflow Automation data sources](#) on page 18

[Configuring the credentials of a target system](#) on page 22

[Setting up WFA using the Setup Wizard](#) on page 16

[Creating users](#) on page 17

Accessing OnCommand Workflow Automation

You can access OnCommand Workflow Automation (WFA) through a web browser.

Before you begin

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

About this task

You can access WFA through a web browser from any system that has access to the WFA server.

Steps

1. Open a web browser and enter one of the following in the address bar:
 - **`http://wfa_server_ip/wfa`**
`wfa_server_ip` is the IP address or the fully qualified domain name (FQDN) of the WFA server.
 - **`http://localhost/wfa`**, if you are accessing WFA on the WFA server

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

- **`http://wfa_server_ip:port/wfa`**
- **`http://localhost:port/wfa`**

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 administrator user that you have entered during installation.
3. Optional: In the **WFA Setup Wizard**, set up the credentials and a data source.
The wizard is displayed only at the first login.
4. Optional: Bookmark the WFA page in the web browser for ease of access.

Setting up WFA using the Setup Wizard

You can use the WFA Setup Wizard to easily set up WFA by connecting to OnCommand Unified Manager and configuring an OnCommand Unified Manager data source, a Performance Advisor data source, and the credentials.

Before you begin

You must have installed OnCommand Workflow Automation (WFA).

About this task

- Only one OnCommand Unified Manager data source and one Performance Advisor data source can be added to WFA using the setup wizard.
- If you have defined data sources and credentials, running the wizard deletes the existing data sources and credentials.
- If you are integrating WFA with a Unified Manager server 6.1 for workflow execution, you must not use the setup wizard to add that Unified Manager server as a data source.
For more information about integrating WFA with the Unified Manager server, see the *OnCommand Unified Manager Online Help*.

Steps

1. Log in to WFA through a web browser as an administrator.
2. Click **Administration > Setup Wizard**.
3. Follow the on-screen instructions to enable access to OnCommand Unified Manager, configure data sources and credentials, and execute your first workflow.

Note: If you had overridden the default credentials when running `ocsetup` on a Unified Manager server earlier than 6.0, you must provide the credentials that you used for the override to configure the data sources.

Related concepts

[OnCommand Workflow Automation data sources](#) on page 18

Related tasks

[Accessing OnCommand Workflow Automation](#) on page 15

[Setting up a data source](#) on page 20

Creating users

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

Before you begin

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

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.
- **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 **Administration > 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 22

[Configuring LDAP](#) on page 24

OnCommand Workflow Automation data sources

OnCommand Workflow Automation (WFA) operates on data acquired from data sources. Various versions of OnCommand 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 OnCommand Unified Manager database of OnCommand Unified Manager 5.1 data source type. You can add a custom data source to WFA after defining the required data source type.

The following are the predefined WFA data source types:

- OnCommand Unified Manager 5.0.x, 5.1.x, 5.2, 6.0, and 6.1
- Performance Advisor with OnCommand Unified Manager 5.0.x, 5.1.x, and 5.2
- VMware vCenter Server 4.x, 5.0.x, 5.1, and 5.5

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

Related information

[Interoperability Matrix: support.netapp.com/matrix](http://support.netapp.com/matrix)

Configuring a database user on OnCommand Unified Manager

You must create a database user on OnCommand Unified Manager versions earlier than 6.0 to configure read-only access of the OnCommand Unified Manager database to OnCommand Workflow Automation.

Configuring a database user by running ocsetup on Windows

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

Steps

1. Download the `wfa_ocsetup.exe` file to a directory on the OnCommand Unified Manager server from the following location: `http://WFA_Server_IP/download/wfa_ocsetup.exe`.

WFA_Server_IP is the IP address of your WFA server.

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

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

2. Double-click the `wfa_ocsetup.exe` file.
3. Read the information in the setup wizard and click **Next**.
4. Browse or type the JRE 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 OnCommand Unified Manager 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 OnCommand Unified Manager server to configure read-only access of the OnCommand Unified Manager database to OnCommand Workflow Automation.

Steps

1. Download the `wfa_ocsetup.sh` file to your home directory on the OnCommand Unified Manager server using the following command in the terminal: **`wget http://WFA_Server_IP/download/wfa_ocsetup.sh`**.

WFA_Server_IP is the IP address of your WFA server.

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

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

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

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 JRE_path`

JRE_path is the path to the JRE.

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 OnCommand Unified Manager 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 connection with a data source in OnCommand Workflow Automation (WFA) to acquire data from the data source.

Before you begin

- For OnCommand 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 OnCommand 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.
The default TCP port number is 2638. See the documentation on your firewall for details.
- For Performance Advisor, you must have created an OnCommand Unified Manager user account with a minimum role of GlobalRead.
See the *OnCommand Unified Manager Online Help* for details.
- For VMware vCenter Server, you must have created a user account on the vCenter Server.
See the VMware vCenter Server documentation for details.

Note: If you want to set up only vCenter Server data sources, setting up Unified Manager server as a data source is not required.

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

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

About this task

If you are integrating WFA with the Unified Manager server 6.1 for workflow execution, you must set up WFA in that Unified Manager server. However, you can add multiple Unified Manager server data sources to WFA using this procedure.

For more information about integrating WFA with the Unified Manager server 6.1, see the *OnCommand Unified Manager Online Help*.

Steps

1. Access WFA using a web browser.
2. Click **Execution > 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.

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.

Note: 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 the appropriate action:

For...	Do this...
OnCommand Unified Manager versions earlier than 6.0	Enter the credentials that you used for overriding the default credentials while running ocsetup, in the user name and password fields.
OnCommand Unified Manager 6.0 and later	Enter the credentials of the Database User account that you created on the Unified Manager server.
Performance Advisor	Enter the credentials of an OnCommand Unified Manager user with a minimum role of GlobalRead. Note: You must not provide the credentials of an OnCommand Unified Manager Database User account that was created using the command-line interface or the ocsetup tool.

For...	Do this...
VMware vCenter Server	Enter the user name and password of the user that you created on the VMware vCenter server.

6. Click **Save**.
7. Optional: In the Data Sources table, select the data source and click  on the toolbar.
8. Verify the data acquisition status in the History table.

Related tasks

[Configuring a database user by running ocsetup on Windows](#) on page 18

[Configuring a database user by running ocsetup on Linux](#) on page 19

[Setting up WFA using the Setup Wizard](#) on page 16

Configuring the credentials of a target system

You can configure the credentials of a target system in 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 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
WFA tries to establish a connection using domain authentication. This mode uses RPC protocol, which is secured using NTLM protocol.

Steps

1. Log in to WFA through a web browser as an administrator.
2. Click **Execution > Credentials**.
3. Click  on the toolbar.
4. In the **New Credentials** dialog box, select one of the following 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.

Note: If you choose pattern match, you must enter only the IP address in the **Name/IP** field.

5. Select the resource type from the **Type** list.
6. Enter either the host name or IP 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 .
Pattern	Save the credential 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 15

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 (ASUP) for sending ASUP 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 ASUP messages
- Simple Network Management Protocol (SNMP) for notifications about workflow operations
- Syslog for remote data logging

Related tasks

[Configuring AutoSupport](#) on page 24

[Configuring LDAP](#) on page 24

[Configuring email notifications](#) on page 25

[Configuring SNMP](#) on page 25

[Configuring Syslog](#) on page 26

[Accessing OnCommand Workflow Automation](#) on page 15

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 administrator.
2. Click **Administration > WFA Configuration**.
3. In the **AutoSupport** tab of the **WFA Configuration** dialog box, ensure that the **Enable AutoSupport** box is selected.
4. Enter the required information.
5. Optional: Test that you can download an AutoSupport message by performing the following steps:
 - a) Click **Download**.
 - b) In the dialog box that opens, select the location to save the .7z file.
6. Optional: Test the sending of an AutoSupport message to the specified destination by clicking **Send Now**.
7. Click **Save**.

Configuring LDAP

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

You cannot configure WFA to use other LDAP servers such as OpenLDAP.

Steps

1. Log in to WFA through a web browser as an administrator.
2. Click **Administration > WFA Configuration**.
3. In the **WFA Configuration** dialog box, click the **LDAP** tab, and then select the **Enable LDAP** check box.

4. Enter the required information in the fields.
5. Click **Save**.
6. Optional: If LDAP connectivity to an array is required, configure the WFA service to log on as the required domain user:
 - a) Open Windows services console by using `services.msc`.
 - b) Double-click the **NetApp WFA Server** service.
 - c) In the **NetApp WFA Server Properties** dialog box, click the **Log On** tab and select the **This account** option.
 - d) Enter the domain user name and password and click **OK**.

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 administrator.
2. Click **Administration > WFA Configuration**.
3. In the **WFA Configuration** dialog box, click the **Mail** tab, and select the **Enable Email Notifications** check box.
4. Enter the required information in the fields.
5. 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**.
6. Click **Save**.

Configuring SNMP

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

About this task

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

Steps

1. Log in to WFA through a web browser as an administrator.
2. Access the WFA server through a web browser.
3. Click **Administration > WFA Configuration**.
4. In the **WFA Configuration** dialog box, click the **SNMP** tab and select the **Enable SNMP** check box.
5. Enter the IP address or name and the port number of the management host.
WFA sends SNMP notifications to this port number, and the default port number is 162.
6. In the Notify On section, select one or more of the following check boxes, as required:
 - Workflow execution started
 - Workflow execution completed successfully
 - Workflow execution failed
 - Workflow execution waiting for approval
 - Acquisition failure
7. Click **Send Test Notification** to verify the settings.
8. Click **Save**.

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.

Steps

1. Log in to WFA through a web browser as an administrator.
2. Click **Administration > WFA Configuration**.
3. In the **WFA Configuration** dialog box, click the **Syslog** tab, and select the **Enable Syslog** check box.
4. Enter the Syslog host name and select the Syslog log level.
5. Click **Save**.

Enabling 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 access the WFA database from a remote system.

Before you begin

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

Steps

1. Open the command prompt and enter the following: **net stop /y na_wfa_db**.
2. Edit the `my.ini` file:
 - a) Open the `my.ini` file from the following location using a text editor such as Notepad: `c:\Program Files\NetApp\wfa\mysql`.
 - b) Delete the following entry from the file: `bind-address=localhost`.
 - c) Save the `my.ini` file.
3. Enter the following at the command prompt: **net start na_wfa_db**.
4. Enter the following at the command prompt: **net start na_wfa_srv**.

Related references

[Ports required for Workflow Automation](#) on page 9

Restricting access rights of OnCommand Workflow Automation on the host

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

Before you begin

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

Steps

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

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 an administrator.

Steps

1. Open the Windows services console by using `services.msc` and stop the **NetApp WFA Server** service.
2. Edit the `standalone-full.xml` file:
 - a) Open the `standalone-full.xml` file from the following location using an XML editor: `c:\Program Files\NetApp\WFA\jboss\standalone\configuration`.
 - b) Locate the following element: `<coordinator-environment default-timeout="300"/>`.
 - c) Replace 300 with the value you want (in seconds).
3. Save the `standalone-full.xml` file.
4. Restart the **NetApp WFA Server** service.

Enabling HTTPS-only access to OnCommand Workflow Automation

By default, OnCommand Workflow Automation (WFA) can be accessed by using both HTTP and HTTPS. You can enable HTTPS-only access if you want to secure the access to WFA.

Before you begin

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

About this task

- Enabling HTTPS-only access does not automatically redirect HTTP to HTTPS. You must type **https://<wfa_host_ip>/wfa** in the address bar to access WFA.
- The default WFA installation path is used in this procedure. If you changed the default location during installation, you must use the changed WFA installation path.

Steps

1. Open the Windows services console by using `services.msc` and stop the **NetApp WFA Server** service.
2. Edit the `standalone-full.xml` file:
 - a) Open the `standalone-full.xml` file from the following location using an XML editor: `c:\Program Files\NetApp\WFA\jboss\standalone\configuration`.
 - b) Locate the following element: `<connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http" executor="http-executor"/>`.
 - c) Comment out or delete the line.
 - d) Save the `standalone-full.xml` file.
3. Start the **NetApp WFA Server** service.

Upgrading OnCommand Workflow Automation

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

About this task

You can upgrade to Workflow Automation 2.2 from Workflow Automation 2.0 or later.

Note: If you want to upgrade from Workflow Automation 1.1.x, you must first upgrade to Workflow Automation 2.0 or later before upgrading to Workflow Automation 2.2.

Steps

1. Back up the OnCommand Workflow Automation database using one of the following options:
 - WFA web portal
 - PowerShell script
2. Uninstall the existing version of WFA.
3. Install the latest version of WFA.
4. Restore the WFA database.

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 31

Related tasks

[*Backing up the WFA database using PowerShell script*](#) on page 32

[*Backing up the WFA database from the web portal*](#) on page 32

[*Uninstalling OnCommand Workflow Automation*](#) on page 38

[*Installing OnCommand Workflow Automation*](#) on page 13

[*Restoring the OnCommand Workflow Automation database*](#) on page 34

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.

Starting from WFA 2.1, WFA creates a backup of the database on a daily basis and saves it as a GNU zip (.gz) file in the following location: *wfa_install_location\WFA-Backups*.

Automatic backups are created at 2 a.m., by default. WFA saves up to two 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 automatic backup for restoration if you have not created a backup of the WFA database when 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 you have made before the automatic backup occurs.

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 (ASUP) data; however, the password of any WFA user is not included in the ASUP data.

When a WFA database is restored from a backup, the following occurs:

- Only the administrator credentials created during the current WFA installation are preserved.
- If a user with administrator privileges other than the default administrator restores the database, credentials of both the administrators are preserved.
- 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 32
- [Backing up the WFA database using PowerShell script](#) on page 32

Related tasks

[Upgrading OnCommand Workflow Automation](#) on page 30

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.

Before you begin

You must have administrator privileges 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. WFA users with backup role can only perform remote or scripted backups.

Steps

1. Log in to WFA through a web browser.
2. Click **Administration > Backup & Restore**.
3. Click **Backup**.
4. In the dialog box that opens, select a location and save the file.
5. Optional: Click the **Return to WFA** link at the upper-left corner of the WFA interface to return to the main WFA window.

Related tasks

[Upgrading OnCommand Workflow Automation](#) on page 30

Backing up the WFA database using PowerShell script

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

Before you begin

You must have created a user for the backup role.

Steps

1. Open Windows PowerShell as an administrator and at the prompt enter the following:
&'wfa_install_location\bin\Backup.ps1' -User user_name -Password password -Filename backup_file_name
 - *wfa_install_location* is the WFA installation directory.

- *user_name* is the user name of the backup user.
- *password* is the password of the backup user.
- *backup_file_name* is the complete directory path for the backup file.

Example

C:\WFA_backups\backup_10_08_12

After the backup is complete, the following output is displayed at the prompt:
backup_file_name.sql.gz

Note: The file name you have provided is appended with *.sql.gz*—for example,
backup_10_08_12.sql.gz.

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

Related tasks

Upgrading OnCommand Workflow Automation on page 30

Restoring the OnCommand Workflow Automation 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 administrator privileges or architect credentials to perform this task.
- If you are restoring the database as part of the migration procedure, ensure that you have completed the other migration steps.

About this task

Restoring a WFA database erases the currently used database.

Steps

1. Log in to WFA through a web browser.
2. Click **Administration > Backup & Restore**.
3. Click **Browse**.
4. In the dialog box that opens, select the WFA backup file and click **Open**.
5. Click **Restore**.
6. Optional: Click the **Return to WFA** link at the top right of the WFA interface to return to the main WFA window.

Related concepts

[Backing up the OnCommand Workflow Automation database](#) on page 31

Related tasks

[Upgrading OnCommand Workflow Automation](#) on page 30

[Migrating the OnCommand Workflow Automation installation](#) on page 36

Importing OnCommand Workflow Automation content

You can import OnCommand Workflow Automation (WFA) content that you have created or downloaded from the WFA community.

Before you begin

You must have access to the WFA content that you want to import.

About this task

- WFA content is saved as a .dar file, and it might include items such as workflows, finders, and commands.
- Questions and support request for any content downloaded from the NetApp WFA community must be directed to the WFA community.

Steps

1. Access WFA through a web browser.
2. Click **Administration > Import**.
3. In the dialog box that opens, select the .dar file you want to import and click **Open**.
4. In the **Import DAR File** dialog box, verify the content you want to import and click **Import**.
5. In the **Import Success** dialog box, click **OK**.

Related information

[Workflow Automation space within the OnCommand Community: netapp.com/oncommand_community](http://netapp.com/oncommand_community)

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. For example, you can migrate the WFA installation when you want to move the installation from one WFA server to another.

About this task

- A WFA database restore does not migrate the WFA key.
- You must perform this procedure only when you want to migrate a WFA installation including the WFA database key.
- Migrating a WFA installation does not migrate the SSL certificates.

Steps

1. Access WFA through a web browser as an administrator.
2. Back up the WFA database.
3. Open a command prompt on the WFA server and change directories to the following location: **c:\Program Files\NetApp\WFA\bin**
Note: If you changed the default location, you must specify the changed WFA installation path.
4. Enter the following at the command prompt to obtain the database key: **wfa.cmd -key**
5. Note the database key that is displayed.
6. Uninstall WFA.
7. Install WFA on the required system.
8. Open the command prompt on the new WFA server and change directories to the following location: **c:\Program Files\NetApp\WFA\bin**
Note: If you changed the default location, you must specify the changed WFA installation path.
9. Enter the following at the command prompt to install the database key: **wfa.cmd -key=yourdatabasekey**
yourdatabasekey is the key that you noted from the previous WFA installation.
10. Restore the WFA database from the backup that you created.

Related concepts

[*Backing up the OnCommand Workflow Automation database*](#) on page 31

Related tasks

[*Backing up the WFA database from the web portal*](#) on page 32

[*Backing up the WFA database using PowerShell script*](#) on page 32

[*Uninstalling OnCommand Workflow Automation*](#) on page 38

[*Installing OnCommand Workflow Automation*](#) on page 13

[*Restoring the OnCommand Workflow Automation database*](#) on page 34

[*Importing OnCommand Workflow Automation content*](#) on page 35

Uninstalling OnCommand Workflow Automation

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

Steps

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

Related tasks

[Upgrading OnCommand Workflow Automation](#) on page 30

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 Windows administrator privileges on the WFA server.

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. Log in as the administrator on the WFA host machine.
2. Use the Windows Services console and stop the following WFA services:
 - NetApp WFA Database
 - NetApp WFA Server
3. Delete the `wfa.keystore` file from the following location: `C:\Program Files\NetApp\WFA\jboss\standalone\configuration`.
4. Open a command prompt on the WFA server and change directories to the following location: `C:\Program Files\NetApp\WFA\jre\bin`.
5. Enter the following at the command prompt to obtain the database key: **keytool -keysize 2048 -genkey -alias "ssl keystore" -keyalg RSA -keystore "C:\Program Files\NetApp\WFA\jboss\standalone\configuration\wfa.keystore" -validity xxxx**

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

6. Specify the password when prompted for the password and new password.
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: C:\Program Files\NetApp\WFA\jboss\standalone\configuration\.

Example

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

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

Related tasks

[Creating a certificate signing request for Workflow Automation](#) on page 40

Creating a certificate signing request for Workflow Automation

You can create a certificate signing request (CSR) such that you can use the SSL certificate signed by a Certificate Authority (CA) instead of the default SSL certificate.

Before you begin

- You must have Windows administrator privileges on the WFA server.
- You must have replaced the default SSL certificate provided by Workflow Automation (WFA).

Steps

1. Log in as administrator on the WFA host machine.
2. Open a command prompt on the WFA server and change directories to the following location: C:\Program Files\NetApp\WFA\jre\bin.
3. Enter the following at the command prompt to create a CSR:

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

file_name is the name of the CSR file.

Note: If you have changed the default location, you must specify the changed WFA installation path.

4. Specify the password when prompted for the password and new password.

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: C:\Program Files\NetApp\WFA\jboss\standalone\configuration\.

Example

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

After you finish

1. Send the `file_name.csr` to the CA to obtain a signed certificate.
See the CA's web site for details.
2. Download a chain certificate from the CA and import the chain certificate in to your keystore using the following command:

```
keytool -import -alias "ssl keystore" -keystore "C:\Program Files\NetApp\WFA\jboss\standalone\configuration\wfa.keystore" -trustcacerts -file C:\chain_cert.p7b
```

3. Import the signed certificate that you have received from the CA using the following command:

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

4. Restart the following WFA services:

- NetApp WFA Database
- NetApp WFA Server

Related tasks

[Replacing the default Workflow Automation SSL certificate](#) on page 39

Managing Perl and Perl modules

OnCommand Workflow Automation (WFA) supports Perl commands for workflow operations. ActivePerl 5.16 is installed and configured on the WFA server when you install WFA. You can install and configure your preferred Perl distribution and Perl modules.

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

Configuring your preferred Perl distribution

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

Before you begin

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

About this task

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

Steps

1. Open the Windows services console by using `services.msc` and stop the **NetApp WFA Server** service.
2. Edit the `standalone-full.xml` file:
 - a) Open the `standalone-full.xml` file from the following location using an XML editor: `c:\Program Files\NetApp\WFA\jboss\standalone\configuration`.
 - b) Add the following XML element between the extensions and the management elements:


```
<system-properties> <property name="perl.path"
value="perl_interpreter_path"/> <property name="perl.pathtype"
value="absolute"/> </system-properties>
```

perl_interpreter_path is the absolute path to the `Perl.exe` file of your preferred Perl installation.

Example

```
<system-properties>
  <property name="perl.path" value="c:\perl\bin\perl.exe"/>
```

```
<property name="perl.pathtype" value="absolute"/>
</system-properties>
```

3. Save the standalone-full.xml file.
4. Copy the required components listed in the following table to the Perl module library of the Perl interpreter you want to use:

Module	Location of the module
WFAUtil.pm	<WFA_Install_Location>/WFA/perl/
WFAWrapper.pl	<WFA_Install_Location>/WFA/perl/
NetApp Manageability SDK modules	<WFA_Install_Location>/WFA/perl/ nmsdk

<WFA_Install_Location> is the WFA installation directory.

5. Make sure that the following Perl modules are available to the Perl interpreter you want to use:
 - Getopt-Long
 - libwww-perl
 - HTTP-Message
 - XML-Parser
 - XML-Simple
 - XML-DOM
 - URI
6. Start the **NetApp WFA Server** service.

Managing site-specific Perl modules

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

About this task

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

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

Steps

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

Example

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

```
c:\Perl
```

2. Optional: Verify that the Perl module area is not initialized by using **ppm area list**.

Example

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

name	pkgs	lib
(user)	n/a	C:/Perl
site*	0	C:/Program Files/NetApp/WFA/Perl64/site/lib
perl	229	C:/Program Files/NetAPP/WFA/Perl64/lib

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

Example

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

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

4. Optional: Verify that the Perl module area is initialized by using **ppm area list**.

Example

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

name	pkgs	lib
user	0	C:/Perl
site*	0	C:/Program Files/NetApp/WFA/Perl64/site/lib
perl	229	C:/Program Files/NetAPP/WFA/Perl64/lib

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

Example

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

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

- b) Optional: Verify that the required repository is added by using **ppm repo list**.

Example

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

id	pkgs	name
1	17180	ppmr.activestate.com

(1 enabled repository)

- c) Install the required Perl module by using **ppm install**.

Example

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

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

- d) Optional: Verify that the required Perl module is installed by using **ppm area list**.

Example

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

name	pkgs	lib
user	1	C:/Perl
site*	0	C:/Program Files/NetApp/WFA/Perl64/site/lib
perl	229	C:/Program Files/NetAPP/WFA/Perl64/lib

Repairing the ActivePerl installation

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

Steps

1. Back up the WFA database using one of the following options:
 - WFA web portal
 - PowerShell script
2. Uninstall WFA.
3. Install the version of WFA that you uninstalled.
ActivePerl is installed when you install WFA.
4. Restore the WFA database.

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 31

Related tasks

[*Backing up the WFA database from the web portal*](#) on page 32

[*Backing up the WFA database using PowerShell script*](#) on page 32

[*Uninstalling OnCommand Workflow Automation*](#) on page 38

[*Installing OnCommand Workflow Automation*](#) on page 13

[*Restoring the OnCommand Workflow Automation database*](#) on page 34

Troubleshooting installation and configuration issues

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

Cannot open the OnCommand Workflow Automation (WFA) login page

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

Ensure that either IIS is turned off or the IIS role is removed.

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 the following:

- Ensure that you have specified the credentials of an OnCommand Unified Manager user with a minimum of GlobalRead role 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, OnCommand Unified Manager uses port 8088 for an HTTP connection and port 8488 for an HTTPS connection.
- Ensure that performance data is collected by the OnCommand Unified Manager server.

Related documentation for OnCommand Workflow Automation

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

Other references

The WFA space within the OnCommand community provides additional learning resources, including the following:

WFA Web services primer for REST API

Describes the REST API provided by WFA and the methods to use them.

Custom dictionary entries and custom cache tables use cases and upgrade procedure

Describes how to upgrade the cache tables used in WFA versions earlier than 2.0.

Tool references

Interoperability Matrix Tool (IMT) Lists supported combinations of hardware components and software versions.

Related information

[Workflow Automation space within the OnCommand community: netapp.com/oncommand_community](https://netapp.com/oncommand_community)

[Interoperability Matrix: support.netapp.com/matrix](https://support.netapp.com/matrix)

Copyright information

Copyright © 1994–2014 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to 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.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

- access
 - restricting WFA rights on the host [27](#)
 - WFA, enabling HTTPS-only [29](#)
- accessing
 - WFA [15](#)
- ActiveState ActivePerl
 - repairing the installation [46](#)
- ASUP
 - See* AutoSupport
- AutoSupport
 - configuring [24](#)

B

- backing up
 - the WFA database [32](#)
 - using PowerShell script [32](#)
- backup
 - of the WFA database [32](#)
 - of the WFA database, how it works [31](#)
- browsers
 - accessing WFA using [15](#)

C

- capabilities
 - of WFA [5](#)
- certificates
 - creating a CSR [40](#)
 - management of [39](#)
 - replacing the default SSL certificate [39](#)
- configuration
 - where to find information about advanced [48](#)
- configuring
 - AutoSupport messages [24](#)
 - credentials of a target system [22](#)
 - email [25](#)
 - LDAP [24](#)
 - preferred Perl distribution [42](#)
 - SNMP [25](#)
 - Syslog [26](#)
 - WFA [23](#)
- connecting
 - Performance Advisor [20](#)

- to OnCommand Unified Manager [20](#)
 - VMware vCenter [20](#)
- creating
 - CSR [40](#)
 - database user on Linux [19](#)
 - database user on Windows [18](#)
 - users [17](#)
- credentials
 - backup of [31](#)
 - configuring in the target system [22](#)
 - restore of [31](#)
 - setting up [16](#)
- CSR
 - creating [40](#)

D

- data sources
 - setting up [16](#)
 - setting up OnCommand Unified Manager, Performance Advisor, VMware vCenter [20](#)
 - supported [18](#)
- database transactions
 - modifying the timeout [28](#)
- databases
 - backing up from WFA [32](#)
 - restoring the WFA [34](#)
- deployment
 - of WFA, example [5](#)

E

- email
 - configuring notifications [25](#)

H

- hardware requirements
 - WFA [8](#)
- host access
 - restricting WFA [27](#)
- HTTPS-only
 - enabling access, WFA [29](#)

I

- importing
 - WFA content [35](#)
- installation
 - prerequisites for WFA [11](#)
- installing
 - repairing ActivePerl installation [46](#)
 - WFA [13](#)

L

- LDAP settings
 - configuring [24](#)
- Linux
 - creating a database user on [19](#)

M

- managing
 - Perl [43](#)
 - Perl and Perl modules [42](#)
 - Perl modules [43](#)
- migrating
 - WFA installation to a different system [36](#)
- modifying
 - path to Perl interpreter [42](#)
 - transaction timeout, WFA database [28](#)

N

- notifications
 - configuring email [25](#)
 - configuring SNMP [25](#)

O

- ocsetup
 - running on Linux [19](#)
 - running on Windows [18](#)
- OnCommand Unified Manager
 - supported data sources [18](#)

P

- Performance Advisor
 - setting up access [16](#)
 - supported data sources [18](#)
- Perl
 - configuring preferred distribution [42](#)
 - managing site-specific modules [43](#)
 - repairing or reinstalling ActivePerl [46](#)

- Perl interpreter
 - specifying the path [42](#)
- Perl modules
 - managing [43](#)
- ports
 - required for WFA [9](#)
- PowerShell script
 - backing up WFA, using [32](#)
- prerequisites
 - for WFA installation [11](#)

R

- read-only access
 - to OnCommand Unified Manager, providing (Linux) [19](#)
 - to OnCommand Unified Manager, providing (Windows) [18](#)
- reinstalling
 - ActivePerl [46](#)
- related documentation
 - for advanced configuration [48](#)
- remote access
 - to WFA database [27](#)
- repairing
 - ActivePerl [46](#)
- requirements
 - for WFA installation [11](#)
 - hardware, WFA [8](#)
 - software, WFA [8](#)
- restoring
 - the WFA database [34](#)
- restricting
 - WFA access rights on the host [27](#)
- running
 - ocsetup on Linux [19](#)

S

- setting up
 - Performance Advisor as data source [20](#)
 - Unified Manager as data source [20](#)
 - VMware vCenter as data source [20](#)
 - WFA, tasks for [15](#)
- SNMP
 - configuring notifications [25](#)
- software requirements

- WFA [8](#)
- SSL
 - creating a CSR [40](#)
 - replacing the default certificate [39](#)
- SSL certificates
 - management of [39](#)
- Syslog
 - configuring [26](#)
- system requirements
 - WFA [8](#)

T

- target systems
 - configuring credentials for [22](#)
- TCP ports
 - for WFA [9](#)
- timeout
 - for database transaction, modifying [28](#)
- troubleshooting
 - configuration issues [47](#)
 - installation issues [47](#)

U

- Unified Manager
 - setting up access [16](#)
- uninstalling
 - WFA [38](#)
- upgrading
 - WFA [30](#)
- user accounts
 - creating database, Linux [19](#)
 - creating database, Windows [18](#)
- users
 - creating [17](#)

V

- VMware vCenter Server
 - supported data sources [18](#)

W

- WFA

- accessing [15](#)
- backing up the database [32](#)
- backing up with PowerShell script [32](#)
- certificate management [39](#)
- configuring [23](#)
- configuring email notifications [25](#)
- configuring LDAP [24](#)
- configuring SNMP notifications [25](#)
- configuring Syslog [26](#)
- creating a CSR [40](#)
- creating users [17](#)
- database, how backup works [31](#)
- database, remote access to [27](#)
- enabling access, HTTPS-only [29](#)
- hardware requirements [8](#)
- importing content [35](#)
- installation and setup tasks overview [6](#)
- installing [13](#)
- migrating the installation to a different system [36](#)
- modifying the timeout, database transaction [28](#)
- overview [5](#)
- prerequisites for installation [11](#)
- replacing SSL certificates [39](#)
- restoring the database [34](#)
- restricting host access rights of [27](#)
- setting up access, data sources, and credentials [16](#)
- setup tasks [15](#)
- software requirements [8](#)
- system requirements [8](#)
- tasks for the upgrade of [30](#)
- troubleshooting [47](#)
- uninstalling [38](#)
- WFA database
 - remote access to [27](#)
- WFA deployment
 - example [5](#)
- Windows
 - creating a database user on [18](#)
- workflow automation
 - overview of [5](#)
- workflows
 - configuring email notifications [25](#)
 - configuring SNMP notification about [25](#)