

OnCommand® Workflow Automation 2.0

Installation and Setup Guide

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089 US
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: 215-07265_A0
December 2012

Contents

OnCommand Workflow Automation overview	5
OnCommand Workflow Automation deployment architecture	6
System requirements for OnCommand Workflow Automation	8
Hardware requirements for installing OnCommand Workflow Automation	8
Software requirements for installing OnCommand Workflow Automation	8
Ports required for OnCommand Workflow Automation	9
Installing and configuring OnCommand Workflow Automation	11
Prerequisites for installing Workflow Automation	12
Downloading the OnCommand Workflow Automation installer	13
Installing Workflow Automation	14
Setting up OnCommand Workflow Automation	16
Accessing OnCommand Workflow Automation	16
Starting the WFA Setup Wizard	17
Creating users	17
Setting up data sources	18
Setting up OnCommand Unified Manager as a data source	19
Setting up Performance Advisor as a data source	22
Configuring the credentials of a target system	23
Configuring OnCommand Workflow Automation	24
Configuring AutoSupport	24
Configuring LDAP	25
Configuring email notifications	25
Configuring SNMP	26
Configuring Syslog	26
Requirements for using Perl commands	27
Setting up a connection to VMware vCenter	28
Creating a read-only user using Microsoft SQL Server Management Studio	28
Creating a read-only user using the SQLCMD utility	29
Enabling remote access to the OnCommand Workflow Automation database	30
Restricting access rights of OnCommand Workflow Automation on the host	31

- Modifying the transaction timeout setting of OnCommand Workflow Automation 31
- Enabling HTTPS-only access to OnCommand Workflow Automation 32
- Upgrading OnCommand Workflow Automation 33**
 - Backing up OnCommand Workflow Automation database 33
 - Backing up the OnCommand Workflow Automation application database 34
 - Backing up the WFA database using PowerShell script 34
 - Restoring the OnCommand Workflow Automation database 35
- Importing OnCommand Workflow Automation content 36**
- Migrating the OnCommand Workflow Automation installation 37**
- Uninstalling OnCommand Workflow Automation 38**
- Troubleshooting installation and configuration issues 39**
 - Enabling remote access to the VC SQL server 39
 - Setting authentication mode of the VC SQL server to mixed mode 40
- Related documentation for OnCommand Workflow Automation 41**
- Copyright information 42**
- Trademark information 43**
- How to send your comments 44**
- Index 45**

OnCommand Workflow Automation overview

OnCommand Workflow Automation (WFA) is a software solution that provides you with “one-click” automation for key storage processes. You can automate storage management tasks such as storage provisioning, migration, decommissioning, and cloning. You can use WFA to build workflows that do exactly what your processes specify.

A workflow is a repetitive and procedural task that consists of sequential steps. A workflow can include the following 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

These workflows can be defined by storage architects to precisely follow their organization's requirements and best practices, such as the following:

- Naming conventions
- Setting unique options for storage objects
- Selecting resources
- Integration with internal configuration management database (CMDB) and ticketing applications

Defining workflows in WFA is a task that can be performed by your storage teams. WFA enables you to keep control on developing and maintaining automation and avoid costly custom software or scripting development.

Workflow Automation provides a history of all the executed workflows and their results enabling control of who executed what and when for audit and troubleshooting purposes.

Workflow Automation enables multiple execution options:

- Using the built-in portal
- Scheduling for a later date
- Using an orchestration tool or custom web page through web services

Workflow Automation can leverage information in multiple OnCommand Unified Manager deployments to assure that the automation process can be executed across environments and datacenters.

If WFA does not include the necessary "building blocks" (certified content that is developed and tested by NetApp or Product Services) that match your requirements as you develop workflows, you can add the required entities to the system on your own (by developing user-created content) or by collaborating with the WFA community (by sharing user-created content using the **Export** and **Import** features).

WFA integrates the following functional elements for creating, executing, and auditing workflows. Access to the capabilities available in each functional area is restricted based on the user's assigned role.

- **Built-in portal**

Using the Portal window, the storage operators are able to select any of the workflows that they are authorized to execute, enter the user input parameters, and let OnCommand Workflow Automation do the rest.

- **Audit feature**

Using the Monitoring window, the storage operator is able to audit (or track) the execution of a workflow and identify and troubleshoot any issues.

- **Designer section**

Available only to storage architects, this section of the application enables the construction and modification of workflows.

The architect selects the list of commands, which perform as the workflow steps, identifies the different execution options, and defines the resource selection options to complete the workflow. After defining the workflow, the architect can test the workflow and make it available to the storage operator.

- **Workflow Automation entities**

These entities, used as "building blocks" when developing your workflows, include various NetApp-related actions such as create volume, create vFiler unit, create Qtree, in addition to virtualization-related actions such as create datastore that are used to set up VLANs on Nexus switches and updating records in ticketing systems. These entities also aid in prioritizing the resources that have to be leveraged.

The included entities are as follows:

- **WFA**—developed and tested by NetApp
- **PS**—developed and supported by NetApp Professional Services data storage and management experts

Note: PS content is available through special service offerings arranged with NetApp Professional Services. For more information, contact your sales representative.

- **Samples**—developed by NetApp

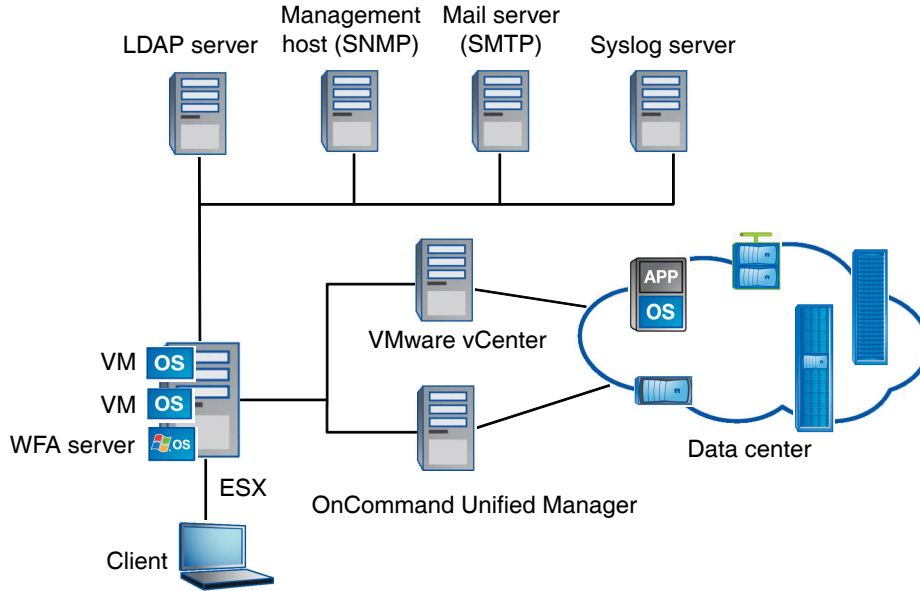
If there are no entities that meet your requirements, you can develop your own content that you can eventually export to others or you can import content created by others that meets your requirements.

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 (WFA) deployment

System requirements for OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) requires specific hardware and software configuration for installation.

Related references

[Hardware requirements for installing OnCommand Workflow Automation](#) on page 8

[Software requirements for installing OnCommand Workflow Automation](#) on page 8

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

Hardware requirements for installing OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) requires specific CPU, disk space, and memory to operate.

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 OnCommand Workflow Automation

OnCommand Workflow Automation runs on specific versions of Microsoft Windows and requires specific browsers and other software.

OnCommand Workflow Automation (WFA) runs only on 64-bit Windows operating system and should be installed on dedicated virtual machines (VMs).

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

Other required software

- One of the following supported browsers:

- Mozilla Firefox
- Microsoft Internet Explorer (IE)
- Google Chrome

Note: The fonts in WFA look distorted in some versions of the Google Chrome browser.

- The latest version of Adobe Flash player for your browser
- PowerShell 2.0
- .NET Framework 3.5
- VMware Power CLI version 5

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

- Perl, Perl modules, and NetApp Manageability SDK

Note: Perl, Perl modules, and NetApp Manageability SDK are required only if you want to enable Perl commands for WFA workflow operations.

For more details, see the NetApp Interoperability Matrix Tool.

Related information

[Interoperability Matrix: support.netapp.com/NOW/products/interoperability](http://support.netapp.com/NOW/products/interoperability)

Ports required for OnCommand Workflow Automation

If you are using a firewall, you must open certain ports for OnCommand Workflow Automation (WFA).

The following table lists the ports that are required for WFA:

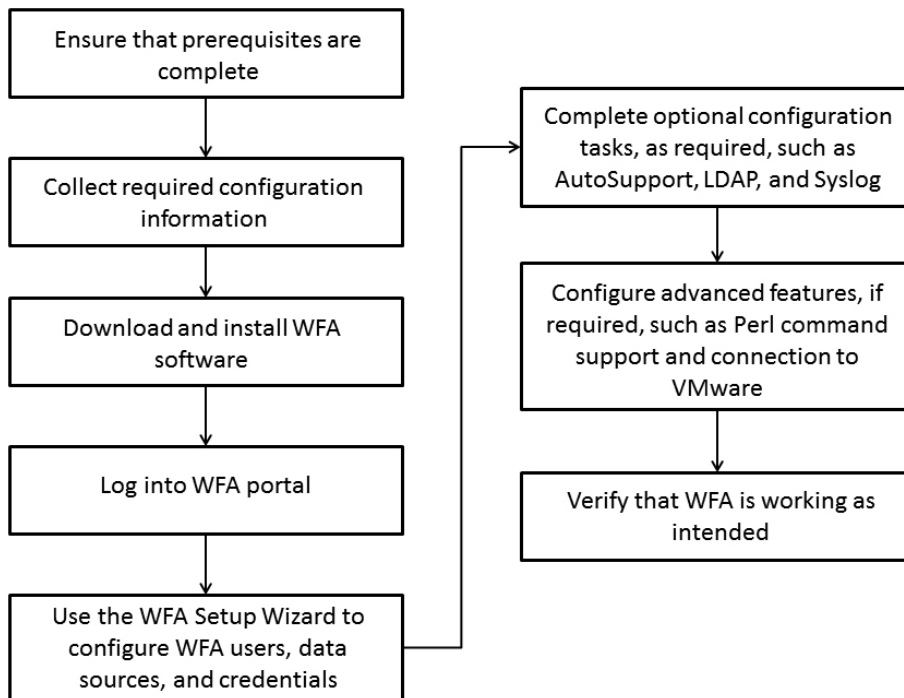
TCP port	Protocol	Direction	Purpose
80, 443	HTTP, HTTPS	Incoming	Opening WFA and logging in
80, 443, 22	HTTP, HTTPS, SSH	Outgoing	Command execution (ZAPI, PowerCLI)
1433	SQL	Outgoing	Caching VMware vCenter
2638	SQL	Outgoing	Caching Operations Manager console and OnCommand Unified Manager
445, 139	Microsoft-DS, NetBIOS-ssn	Outgoing	LDAP authentication

TCP port	Protocol	Direction	Purpose
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

Installing and configuring OnCommand Workflow Automation

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 describes the installation and configuration tasks:



Related tasks

[Downloading the OnCommand Workflow Automation installer](#) on page 13

[Installing Workflow Automation](#) on page 14

Related references

[Prerequisites for installing Workflow Automation](#) on page 12

Prerequisites for installing Workflow Automation

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

Before you begin installing WFA on a system, ensure that you complete the following tasks:

- Verify 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, ensure that SSH is enabled on the target controllers.
- Install all the .NET framework 3.5 run-time patches on the system.
 - Verify that PowerShell 2.0 is installed.
 - Ensure that port 80 is not used by any other software such as Internet Information Services (IIS).
 - Collect 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 NetApp storage (arrays).
vSphere	• IP address • User name and password of an administrator for the following: • vCenter • vCenter database	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 Note: 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	Receive WFA notifications through email.
AutoSupport server	Mail host	Send AutoSupport messages through SMTP. Note: If you do not have a mail host configured, you can use HTTP or HTTPS to send AutoSupport messages.
LDAP server	- IP address - User name and password - Group name	Authenticate and authorize using LDAP server.
SNMP management application	- IP address - Port	Receive WFA SNMP notifications.
Syslog server	IP address	Send log data.

Downloading the OnCommand Workflow Automation installer

Before you install OnCommand Workflow Automation (WFA), you must download the installer from the NetApp Support Site.

Before you begin

You must be a NetApp customer or partner and you must have valid credentials to log in to the NetApp Support Site at support.netapp.com. If you do not have valid credentials, contact NetApp technical support.

Steps

1. Download the WFA installation file from the NetApp Support Site at support.netapp.com.
2. Copy the WFA installation file to the server where you want to install WFA.

Installing Workflow Automation

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

Before you begin

- You must have reviewed all of the [installation prerequisites](#) on page 12.
- You must have downloaded the WFA installer.

About this task

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

Steps

1. Log in to Windows using an account with administrator privileges.
2. Open **Windows Explorer** and navigate to the directory where the installation files are located.
3. Right-click the WFA installer executable file and run the .exe as an administrator.
4. Click **Next**.
5. Accept the license agreement and click **Next**.

Note: If PowerShell is not found in your system, the installer prompts you to download and install PowerShell.

6. Click **Next** and enter a site name and your company name and click **Next**.
 7. Enter credentials for the administrator user and click **Next**.
- Note:** You must note the credentials of the administrator user.
8. Optional: If you want to change the default installation location, select the location where you want to install WFA and click **Next**.
 9. Click **Install** to continue the installation.

The installation should take only a few minutes to complete.

10. Review the information displayed by the setup wizard such as how to launch WFA and AutoSupport feature, and click **Next**.
11. Click **Finish** to complete the installation.

12. 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 is running.

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

[*Setting up data sources*](#) on page 18

[*Configuring OnCommand Workflow Automation*](#) on page 24

[*Setting up a connection to VMware vCenter*](#) on page 28

Related tasks

[*Accessing OnCommand Workflow Automation*](#) on page 16

[*Configuring the credentials of a target system*](#) on page 23

[*Starting the WFA Setup Wizard*](#) on page 17

[*Creating users*](#) on page 17

Related references

[*Requirements for using Perl commands*](#) on page 27

Accessing OnCommand Workflow Automation

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

Before you begin

You must have installed the 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 the following in the address bar: **`http://wfa_server_ip/wfa`**
wfa_server_ip is the IP address of the WFA server.

Alternatively, you can use **`http://localhost/wfa`**, if you are accessing WFA on the WFA server.

2. In the **Sign in** section, enter the credentials of the administrator user that you have entered during installation.

The WFA Setup Wizard opens at your first login, which enables you to set up credentials and a data source.

3. Optional: Bookmark the WFA page in the web browser for ease of access.

Starting the WFA Setup Wizard

You can use the WFA Setup Wizard to easily set up WFA by enabling access to OnCommand Unified Manager, and configuring a data source and credentials.

Before you begin

You must have installed OnCommand Workflow Automation (WFA).

About this task

If you have defined data sources and credentials, running the wizard deletes the existing data sources and credentials.

Steps

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

Note: If you had overridden the default credentials when running `ocsetup`, you must provide the credentials that you used for the override to configure the data sources.

Related tasks

[Accessing OnCommand Workflow Automation](#) on page 16

Creating users

OnCommand Workflow Automation (WFA) enables you to create and manage users with specific permissions for various roles.

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 only view the status of a workflow execution or 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 user is the only user who can remotely generate backups of the WFA server; however, they are restricted from all other access.

Steps

1. Click **Tools > Users**.
2. Create a new user by clicking **Actions > New**.
Alternatively, you can right-click the Users table and select **New**.
3. Enter the required information in the **New User** dialog box.
4. Click **Save**.

Setting up data sources

OnCommand Workflow Automation (WFA) operates on data acquired from data sources. You must set up data sources in WFA for data acquisition.

A data source is a read-only data structure that contains information about where the data in a specific database originates. For example, a data source can be either a OnCommand Unified Manager database that contains information about a storage environment or a VMware database with information about a data center.

To set up data sources in WFA, the WFA server must have access to the storage controllers, OnCommand Unified Manager, and the VMware vCenters to acquire data.

The following are the supported data source types:

- Operations Manager used with DataFabric Manager server 4.0.2
- OnCommand Unified Manager Core Package 5.0.2
- OnCommand Unified Manager Core Package 5.1
- Performance Advisor 4.0.2, 5.0.2, 5.1
- VMware vCenter Server 4.1

For more detailed and updated information about supported data sources, see the NetApp Interoperability Matrix.

Note: You should use the ocsetup tool to grant remote read-only access to WFA. The application does not actively install anything, but runs on the OnCommand Unified Manager machine to provide remote access to WFA.

You can set up data sources using the WFA Setup Wizard or through manual configuration.

Related tasks

[Setting up OnCommand Unified Manager as a data source](#) on page 19

[Setting up Performance Advisor as a data source](#) on page 22

Related information

[Interoperability Matrix: support.netapp.com/NOW/products/interoperability](http://support.netapp.com/NOW/products/interoperability)

Setting up OnCommand Unified Manager as a data source

You must set up connection with OnCommand Unified Manager and select the OnCommand Unified Manager as a data source in OnCommand Workflow Automation (WFA).

Before you begin

You must have run the ocsetup tool on the OnCommand Unified Manager server to get remote read-only access.

About this task

Alternatively, you can use the WFA Setup Wizard to set up OnCommand Unified Manager as a data source. However, you can set up only one data source using the wizard.

Steps

1. Access WFA using a web browser.
2. Click **Execution > Data Sources**.
3. Choose the appropriate action:

To...	Then...
Create a new data source	Perform one of the following actions: • Click Actions > New. • Right-click the Data Sources table and select New.
Edit a restored data source if you have upgraded WFA	Select the existing data source entry and click Actions > Edit .

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

Note: Based on the selected data source type, the port, user name, and password fields might be automatically populated with the default data, if available. If you had overridden the default credentials while running ocsetup, you must provide the credentials that you used when overriding the default credentials in the user name and password fields.

5. Click **Save**.
6. In the **Data Sources** table, select the data source and click **Actions > Acquire Now**.
Alternatively, you can right-click the source and select **Acquire Now**.
7. Verify the data acquisition status in the **History** table.

Related tasks

Running ocsetup on Windows on page 20

Running ocsetup on Linux on page 21

Running ocsetup on Windows

You can run the ocsetup file on the OnCommand Unified Manager server to create a read-only user account and provide remote read-only access to OnCommand Workflow Automation (WFA).

Before you begin

You must have Java Runtime Environment (JRE) version 6 or later installed on the OnCommand Unified Manager server.

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.

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 read-only user account is created to access the OnCommand Unified Manager.

Note: If you do not create a user account, the default credentials are used.

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

Running ocsetup on Linux

You can run the `ocsetup` file on the OnCommand Unified Manager server to create a read-only user account and provide remote read-only access to OnCommand Workflow Automation (WFA).

Before you begin

You must have Java Runtime Environment (JRE) version 6 or later installed on the OnCommand Unified Manager server.

Steps

1. Download the `wfa_ocsetup.sh` file to your home directory on the OnCommand Unified Manager server from the following location: `http://WFA_Server_IP/download/wfa_ocsetup.sh`.
WFA_Server_IP is the IP address of your WFA server.
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

```
/mnt/lun_iscsi_filer1_21/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 read-only user account is created to access OnCommand Unified Manager.

Note: If you do not create a user account, the default credentials are used.

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 Performance Advisor as a data source

You must set up connection with Performance Advisor and select the Performance Advisor as a data source in OnCommand Workflow Automation (WFA).

Steps

1. Access WFA using a web browser.
2. Click **Execution > Data Sources**.
3. Choose the appropriate action:

To...	Then...
Create a new data source	Perform one of the following actions: • Click Actions > New. • Right-click the Data Sources table and select New.
Edit a restored data source if you have upgraded WFA	Select the existing data source entry and click Actions > Edit .

4. In the **New Data Source** dialog box, select the required Performance Advisor version as the data source type, and enter the name, host name, port, user name, and password.

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

5. Enter a name and host name for the data source.
6. Enter the user name and password of an OnCommand Unified Manager user who has read permission on the arrays from which you want to acquire performance data.

You can also use the credentials of a user with GlobalRead permission.

Note: You must not provide the credentials of an OnCommand Unified Manager database user.

7. Click **Save**.
8. In the **Data Sources** table, select the data source and click **Actions > Acquire Now**.

Alternatively, you can right-click the source and select **Acquire Now**.

9. Verify the data acquisition status in the **History** table.

Configuring the credentials of a target system

You can configure 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 and then falls back to HTTP. You can also use LDAP authentication to connect to arrays without defining credentials in WFA. To use LDAP, you must configure the array to perform authentication with the same LDAP.
- 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 **Actions > New** or alternatively right-click the **Credentials** table and select **New**.
4. In the **New Credentials** dialog box, select one of the following from the **Match** list:
 - **Exact**: Credentials for a specific IP 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 Actions > Test Connectivity. • Right-click and select Test Connectivity.

8. Click **Save**.

Related tasks

[Accessing OnCommand Workflow Automation](#) on page 16

Configuring OnCommand Workflow Automation

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

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

- AutoSupport (ASUP) for sending ASUP messages to technical support
- Lightweight Directory Access Protocol (LDAP) server for LDAP authentication and authorization for WFA
- Mail for email notifications on workflow operations and sending ASUP messages
- Simple Network Management Protocol (SNMP) for notifications about workflow operations
- Syslog for data logging

Related tasks

[Configuring AutoSupport](#) on page 24

[Configuring LDAP](#) on page 25

[Configuring email notifications](#) on page 25

[Configuring SNMP](#) on page 26

[Configuring Syslog](#) on page 26

[Accessing OnCommand Workflow Automation](#) on page 16

Configuring AutoSupport

You can configure several attributes of AutoSupport such as schedule, content of AutoSupport messages, and proxy server. AutoSupport sends weekly logs of the content you select to NetApp to be archived and analyzed for issues.

Steps

1. Click **Tools > WFA Configuration**.
2. In the **AutoSupport** tab of the **WFA Configuration** dialog box, ensure that the **Enable AutoSupport** box is selected.
3. Enter the required information.
4. Optional: To test the downloading of an AutoSupport message, perform the following steps:
 - a) Click **Download**.
 - b) In the dialog box that opens, select the location to save the .7z file.
5. Optional: To test the sending of an AutoSupport message to the specified destination, click **Send Now**.

6. Click **Save**.

Configuring LDAP

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

Before you begin

You must have configured an LDAP server in your environment.

Steps

1. Log in to WFA through a web browser as an administrator.
2. Click **Tools > WFA Configuration**.
3. In the **WFA Configuration** dialog box, click the **LDAP** tab and 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, perform the following steps to 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 **Tools > 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.

Mail Host and **Sender** are required fields.

5. Optional: To test the mail settings, perform 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.

Steps

1. Access the WFA server through a web browser.
2. Click **Tools > WFA Configuration**.
3. In the **WFA Configuration** dialog box, click the **SNMP** tab and select **Enable SNMP** box.
4. 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.
5. In the **Notify On** section, select one or more of the following boxes, as required:
 - Workflow Execution Started
 - Workflow Execution Completed Successfully
 - Workflow Execution Failed
 - Workflow Execution Waiting For Approval
6. Click **Send Test Notifications** to verify the settings.
7. Click **Save**.

Configuring Syslog

You can configure OnCommand Workflow Automation (WFA) to send log data to a specific Syslog server.

Steps

1. Log in to WFA through a web browser as an administrator.
2. Click **Tools > 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**.

Requirements for using Perl commands

OnCommand Workflow Automation (WFA) supports Perl commands for workflow operations. WFA natively uses PowerShell, and you have to enable Perl commands only if you plan to use Perl commands for workflow operations.

You must install Perl and Perl modules on the WFA server to use Perl commands.

Supported Perl distributions

You should use one of the following Perl distributions that are tested to work with WFA:

- ActivePerl 5.14.2
- Strawberry Perl 5.14.2.1

Note: After installing Perl, you must ensure that the folder location of the Perl executable appears as part of your *Path* environment variable and then restart your NetApp WFA Server service.

Required Perl modules

Module	Instructions
NetApp Manageability SDK 4.1	You can download the SDK from the NetApp Support Site. You must copy all the .pm files from the SDK, excluding the test.pm file, to the lib folder under your Perl installation.
WFAUtil.pm	You must copy this module from <your_wfa_installation_folder>/perl folder to the lib folder under your Perl installation.

Related information

NetApp Support Site: support.netapp.com

ActivePerl 5.14.2: activestate.com/activeperl

Strawberry Perl 5.10.1.5: strawberryperl.com

Setting up a connection to VMware vCenter

OnCommand Workflow Automation (WFA) supports workflow operations on VMware vCenter. You can add a VMware vCenter as a data source to WFA.

WFA uses the MSSQL JDBC driver and the Oracle JDBC driver to acquire data from VMware vCenters. WFA connects to the VC SQL Server as a read-only user and acquires the relevant data. You must create a read-only user with public and db_datareader roles on the vCenter (VIM_VCDB) database.

Choices

- [Creating a read-only user using Microsoft SQL Server Management Studio](#) on page 28
- [Creating a read-only user using the SQLCMD utility](#) on page 29

Creating a read-only user using Microsoft SQL Server Management Studio

You should create a read-only user using the Microsoft SQL Server Management Studio in order to access the VC SQL server.

About this task

The user mapping should have public and db_datareader roles on the VIM_VCDB database.

Steps

1. Open **Microsoft SQL Server Management Studio** and connect to the SQL Server.
2. Right-click the **SQL Server** instance and select **Security > Logins > New Login**.
3. In the **Login-New** dialog box, select **General** in the left pane.
4. Select **SQL Server authentication** mode.
5. Type **wfa** in the **Login name** field and the **Password** field, which is the default defined in the WFA data source type.
6. Ensure that the following check boxes are not selected:
 - **User must change password in next login**
 - **Enforce password expiration**
 - **Enforce password policy**
7. Select **VIM_VCDB** from the **Default Database** list.
8. Select **English** from the **Default Language** list.
9. Select **Server Roles** in the left pane.
10. Ensure that the **public** check box is selected.

11. Select **User Mapping** in the left pane.
12. Map the **VIM_VCDB** database to the new user name (**wfa**) and the **dbo** schema:
 - a) Select the **Map** check box for the **VIM_VCDB** database.
 - b) Select **wfa** in the User column.
 - c) Select **dbo** in the Default Schema column.
13. Select **Status** in the left pane.
14. Select **Grant** as the **Settings** option.
15. Select **Enabled** as the **Login** option.
16. Click **OK** to save new user.
17. Select **SQL Server Instance > Databases > VIM_VCDB > Security > Users** and double-click the newly created user name (**wfa**) in the left pane.
18. In the **Database User – wfa** dialog box, click **General** in the left pane and select the **db_datareader** role check box.
19. Click **OK** to save the changes.

Creating a read-only user using the SQLCMD utility

You should create a read-only user using the SQLCMD utility in order to access the VC SQL server.

About this task

The user mapping should have public and db_datareader roles on the VIM_VCDB database.

Steps

1. Open a **cmd** session and enter the following command to connect to the SQL Server: **sqlcmd -S <HOME>\<SQL_server_name> -E**—for example **sqlcmd -S SRV-VC\SQLEXP_VIM -E**
 - *HOME* is the name of the server
 - *SQL_server_name* is the name of the SQL server
 - *-E* means using Windows authentication
2. To set VIM_VCDB as the current database:
 - a) Enter the following: **USE VIM_VCDB**
 - b) Enter the following: **GO**
3. To create a new server login name and password as defined by default in the WFA data source type:
 - a) Enter the following: **CREATE LOGIN wfa WITH PASSWORD = 'wfa',
DEFAULT_DATABASE=[VIM_VCDB], CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF**
 - b) Enter the following: **GO**
4. To create a new database user linked to the login name:

- a) Enter the following: **CREATE USER wfa FOR LOGIN wfa**
- b) Enter the following: **GO**
5. To grant database SELECT permission to the user:
 - a) Enter the following: **GRANT Select To wfa**
 - b) Enter the following: **GO**
6. To set the user role to db_datareader:
 - a) Enter the following: **EXEC sp_addrolemember 'db_datareader', wfa**
 - b) Enter the following: **GO**
7. Enter **Exit** to close the **cmd** session.

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.

About this task

The WFA database is accessed using the following read-only user credentials:

- Username: wfa
- Password: Wfa123

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 in the command prompt: **net start na_wfa_db**.
4. Enter the following in the command prompt: **net start na_wfa_srv**.

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 change this default setting if you want to increase or decrease the timeout duration.

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 `transaction-jboss-beans.xml` file:
 - a) Open the `transaction-jboss-beans.xml` file from the following location using an XML editor such as Notepad++: `c:\Program Files\NetApp\WFA\jboss\server\default\deploy`.
 - b) Locate the following element: `<property name="transactionTimeout">300</property>` in `transaction-jboss-beans.xml`.
 - c) Replace 300 with the value you want (in seconds).
 - d) Save the `transaction-jboss-beans.xml` file.
3. Restart the **NetApp WFA Server** service.

Enabling HTTPS-only access to OnCommand Workflow Automation

By default, OnCommand Workflow Automation (WFA) can be accessed 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.

Steps

1. Open the Windows services console by using `services.msc` and stop the **NetApp WFA Server** service.
2. Edit the `server.xml` file:
 - a) Open the `server.xml` file from the following location using an XML editor such as Notepad ++: `c:\Program Files\NetApp\WFA\jboss\server\default\deploy\jbossweb.sar`.
 - b) Locate the following element: `<Connector protocol="HTTP/1.1" port="{http.port}" address="{jboss.bind.address}" connectionTimeout="20000" redirectPort="{https.port}" maxSavePostSize="-1" restrictedUserAgents="^.*MS Web Services Client Protocol.*$" />`.
 - c) Replace `"{jboss.bind.address}"` with `"127.0.0.1"/`.
 - d) Save the `server.xml` file.
3. Restart 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.

Note: You can upgrade to WFA 2.0 from WFA 1.1.0.53.2 or later.

Upgrading your WFA installation includes the following tasks:

1. Backing up the OnCommand Workflow Automation database
2. Uninstalling the existing version of OnCommand Workflow Automation
3. Installing the latest version of Workflow Automation
4. Restoring the OnCommand Workflow Automation database

Related concepts

[*Backing up OnCommand Workflow Automation database*](#) on page 33

Related tasks

[*Backing up the WFA database using PowerShell script*](#) on page 34

[*Backing up the OnCommand Workflow Automation application database*](#) on page 34

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

[*Installing Workflow Automation*](#) on page 14

[*Restoring the OnCommand Workflow Automation database*](#) on page 35

Backing up OnCommand Workflow Automation database

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

When you back up the WFA database, the WFA configuration settings and cache information are saved as a GNU zip (.gz) file.

Choices

- [*Backing up the OnCommand Workflow Automation application database*](#) on page 34
- [*Backing up the WFA database using PowerShell script*](#) on page 34

Backing up the OnCommand Workflow Automation application database

You can back up the OnCommand Workflow Automation (WFA) database from the application itself.

Steps

1. Log in to WFA through a web browser as an administrator.
2. Click **Tools > Backup & Restore**.
3. Click **Backup**.
4. In the browser-specific dialog box that opens, select a location and save the file.
5. Optional: Click the **Return to WFA** link at the top right of the WFA interface to return to the main WFA window.

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 provide 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>\WFA\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.

For 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.

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.

About this task

Restoring a WFA database erases the currently used database.

Steps

1. Access WFA through a web browser.
2. Click **Tools > Backup & Restore**.
3. Optional: If you do not want to upgrade the certified definitions, clear the **Upgrade certified definitions** check box.
Note: You might not receive important updates and fixes if you do not upgrade the definitions. You should upgrade the definitions if no major changes were made to the definitions.
4. Click **Browse**.
5. In the browser-specific dialog box that opens, select the WFA backup file and click **Open**.
6. Click **Restore**.
7. Optional: Click the **Return to WFA** link at the top-right of the WFA interface to return to the main WFA window.

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 **Tools > 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

NetApp WFA community: https://communities.netapp.com/community/products_and_solutions/storage_management_software/workflow-automation

Migrating the OnCommand Workflow Automation installation

You can migrate an OnCommand Workflow Automation (WFA) installation from one system to another system.

Steps

1. Access WFA through a web browser as an administrator.
2. Back up the WFA database.
3. Open the command prompt on the WFA server and enter the following command to obtain the database key: **c:\Program Files\NetApp\WFA\bin wfa.cmd -key**

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

4. Note the database key that is displayed.
5. Uninstall WFA.
6. Install WFA on the required system.
7. Open the command prompt on the new WFA server and enter the following command to install the database key: **c:\Program Files\NetApp\WFA\bin wfa.cmd -key=<yourdatabasekey>**

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

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

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

Related concepts

[Backing up OnCommand Workflow Automation database](#) on page 33

Related tasks

[Backing up the OnCommand Workflow Automation application database](#) on page 34

[Backing up the WFA database using PowerShell script](#) on page 34

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

[Installing Workflow Automation](#) on page 14

[Restoring the OnCommand Workflow Automation database](#) on page 35

[Importing OnCommand Workflow Automation content](#) on page 36

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. Select **NetApp WFA** and click **Uninstall**.

Alternatively, you can 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.

Troubleshooting installation and configuration issues

You can troubleshoot issues related to the installation and configuration of OnCommand Workflow Automation (WFA).

Data acquisition from VMware vCenter fails

If the data acquisition process from VMware vCenter fails, you should perform the following procedures to ensure that the properties associated with connectivity are configured correctly:

- Enabling remote access to the VC SQL server.
- Setting the authentication mode of the VC SQL server to mixed mode.

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 that the IIS role is removed.

Related tasks

[Enabling remote access to the VC SQL server](#) on page 39

[Setting authentication mode of the VC SQL server to mixed mode](#) on page 40

Enabling remote access to the VC SQL server

You must enable remote access to the VC SQL server to acquire data from the vCenter.

Steps

1. Open the Microsoft SQL Server Configuration Manager from the Microsoft SQL Server Configuration Tools.
2. Expand **SQL Server Network Configuration** and select your SQL server instance.
3. Under **Protocol Name**, double-click **TCP/IP**.
4. In the **TCP/IP Properties** dialog box, perform the following:
 - a) In the **Protocol** tab, ensure that **Enabled** is set to **Yes**.
 - b) In the **IP Addresses** tab, expand **+ IPAll** and then enter the **TCP Port** value.

Note: By default, 1433 is defined as the port for the WFA data source type. If the SQL server uses another port, update the WFA data source type with that port number.

5. If the firewall is enabled, create an exception for the SQL server instance and port that is being used.
 - a) Open **Windows Firewall** from the **Control Panel**.
 - b) Click the **Exceptions** tab and add `sqlservr.exe`, which is typically located in `C:\Program Files (x86)\Microsoft SQL Server\MSSQL.x\MSSQL\Binn`, and the port used by the SQL server.
6. Restart the SQL server service and SQL server browser processes.
7. Verify connectivity to the SQL server:
 - a) Open the command prompt and enter the following at the prompt:

```
netstat -ano | findstr 1433
```



```
telnet IP 1433
```



```
ping -a IP
```

IP is the IP address of the SQL server.
 - b) Verify that the correct ports and IP addresses are displayed in the output.

Setting authentication mode of the VC SQL server to mixed mode

You must set the authentication mode of the VC SQL server to mixed mode for acquiring data from the vCenter.

About this task

OnCommand Workflow Automation (WFA) uses SQL server authentication to connect to the VC SQL server. To allow this type of connection, the authentication mode of the VC SQL server must be set to **Mixed Mode** (Windows Authentication and SQL Server Authentication).

Steps

1. Open Microsoft SQL Server Management Studio and connect to the SQL Server.
2. Right-click the SQL server instance and select **Properties**.
3. In the **Server Properties** dialog box, select **Security** in the left pane and then select **SQL Server and Windows Authentication mode**.
4. Click **OK** to save the changes.
5. Right-click the SQL server instance and select **Restart**.

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 Community page includes additional learning resources including the following:

WFA Web services primer	Describes the SOAP API provided by WFA and the methods to use them.
WFA Web services primer For REST API	Describes the REST API provided by WFA and the methods to use them.
WFA Sizing Guide	Provides sizing guidelines for the WFA deployment.
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.

You can access the WFA Community page at https://communities.netapp.com/community/products_and_solutions/storage_management_software/workflow-automation.

Tool references

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

You can access the IMT at support.netapp.com/NOW/products/interoperability

Copyright information

Copyright © 1994–2012 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, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, 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, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, 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 [31](#)
 - WFA, enabling HTTPS-only [32](#)
- accessing
 - WFA [16](#)
- authentication
 - VC SQL server, to mixed mode [40](#)
- AutoSupport
 - configuring [24](#)

B

- backing up
 - the WFA database [34](#)
 - using PowerShell script [34](#)
- backing up from WFA
 - database [34](#), [35](#)
- backup
 - of WFA database [33](#)

C

- configuring
 - AutoSupport [24](#)
 - credentials of target system [23](#)
 - email [25](#)
 - LDAP [25](#)
 - SNMP [26](#)
 - Syslog [26](#)
 - WFA [11](#), [24](#)
- connecting to
 - OnCommand Unified Manager [19](#)
 - Performance Advisor [22](#)
- creating
 - users [17](#)
- creating a VC user
 - Microsoft SQL Server Management Studio [28](#)
 - SQLCMD CLI [29](#)
- credentials
 - configuring in target system [23](#)
 - setting up [17](#)

D

- data
 - acquisition, troubleshooting [39](#)
- data source
 - VMware vCenter [28](#)
- data sources
 - setting up [17](#)
 - setting up OnCommand Unified Manager [19](#)
 - setting up Performance Advisor [22](#)
 - setup of [18](#)
 - supported [18](#)
- database
 - restoring the WFA [35](#)
- database transaction
 - modifying the timeout [31](#)
- deployment
 - of WFA, example [6](#)
- downloading
 - WFA [13](#)

E

- email
 - configuring notifications [25](#)
- enabling
 - remote access to VC SQL server [39](#)

H

- hardware requirements
 - WFA [8](#)
- host access
 - restricting WFA [31](#)
- HTTPS-only
 - enabling access, WFA [32](#)

I

- importing
 - WFA content [36](#)
- installation
 - prerequisites for WFA [12](#)
- installing
 - WFA [11](#), [14](#)

L

LDAP

- configuring [25](#)

M

Microsoft SQL Server Management Studio

- creating a VC user [28](#)

migrating

- WFA installation to a different system [37](#)

mixed mode

- setting authentication of VC SQL server to [40](#)

modifying

- transaction timeout, WFA database [31](#)

O

ocsetup

- on Linux [21](#)
- Windows [20](#)

OnCommand Unified Manager

- setting up as a data source [19](#)

overview

- Workflow Automation [5](#)

P

Performance Advisor

- setting up as a data source [22](#)

Perl commands

- requirements for [27](#)

Perl modules

- requirements [27](#)

ports

- required for WFA [9](#)

PowerShell script

- backing up WFA, using [34](#)

prerequisites

- for WFA installation [12](#)

R

remote access

- WFA database [30](#)

requirements

- hardware, WFA [8](#)
- software, WFA [8](#)

restoring

- the WFA database [35](#)

running ocsetup

- Linux [21](#)
- Windows [20](#)

S

setting up

- Performance Advisor as data source [22](#)
- Unified Manager as data source [19](#)
- WFA, tasks for [16](#)

SNMP

- configuring notifications [26](#)

software requirements

- WFA [8](#)

SQLCMD CLI

- creating a VC user [29](#)

Syslog

- configuring [26](#)

system requirements

- WFA [8](#)

T

TCP ports

- for WFA [9](#)

troubleshooting

- configuration issues [39](#)
- data acquisition [39](#)
- installation issues [39](#)
- VC SQL authentication mode, mixed mode [40](#)

U

Unified Manager

- setting up access [17](#)
- setting up as a data source [19](#)

uninstalling

- WFA [38](#)

upgrading

- WFA [33](#)

users

- creating [17](#)

V

VC SQL server

- enabling remote access [39](#)
- setting authentication to mixed mode [40](#)

VMware vCenter
 connection setup [28](#)

W

WFA

accessing [16](#)
 backing up the database [34](#)
 backing up with PowerShell script [34](#)
 configuring [24](#)
 configuring email notifications [25](#)
 configuring LDAP [25](#)
 configuring SNMP notifications [26](#)
 configuring Syslog [26](#)
 creating users [17](#)
 database, backup of [33](#)
 database, remote access [30](#)
 downloading [13](#)
 enabling access, HTTPS-only [32](#)
 hardware requirements [8](#)
 importing content [36](#)

installation and configuration tasks [11](#)
 installing [14](#)
 migrating the installation to a different system [37](#)
 modifying the timeout, database transaction [31](#)
 prerequisites for installation [12](#)
 restoring the database [35](#)
 restricting host access rights of [31](#)
 setting up access, data sources, and credentials [17](#)
 setup tasks [16](#)
 software requirements [8](#)
 system requirements [8](#)
 tasks for the upgrade of [33](#)
 troubleshooting [39](#)
 uninstalling [38](#)

WFA database
 remote access [30](#)

WFA deployment
 example [6](#)

Workflow Automation
 overview [5](#)