设置 OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

目录

设置 OnCommand Workflow Automation . . . 1
访问 OnCommand Workflow Automation . . . 1
OnCommand Workflow Automation 数据源 . . . 1
创建本地用户 . . . 6
配置目标系统的凭据 . . . 7
正在配置 OnCommand Workflow Automation . . . 8
禁用默认密码策略 . . . 14
修改 Windows 的默认密码策略 . . . 14
在 Windows 上启用对 OnCommand Workflow Automation 数据库的远程访问 . . . 15
限制主机上 OnCommand Workflow Automation 的访问权限 . . . 15
修改 OnCommand Workflow Automation 的事务超时设置 . . . 16
配置 Workflow Automation 的超时值 . . . 16
启用密码并添加新密码 . . . 17

设置 OnCommand Workflow Automation

安装完 OnCommand Workflow Automation （ WFA ）后，必须完成多项配置设置。您必须访问 WFA ，配置用户，设置数据源，配置凭据以及配置 WFA 。

访问 OnCommand Workflow Automation

您可以从有权访问 WFA 服务器的任何系统通过 Web 浏览器访问 OnCommand Workflow Automation （ WFA ）。

您必须已为 Web 浏览器安装 Adobe Flash Player 。

步骤

1. 打开 Web 浏览器，然后在地址栏中输入以下内容之一：
   - ` + https://wfa_server_ip+`

     wfa_server_ip 是 WFA 服务器的 IP 地址（ IPv4 或 IPv6 地址）或完全限定域名（ FQDN ）。

   - 如果要在 WFA 服务器上访问 WFA： ` https://localhost/wfa` 如果已为 WFA 指定非默认端口，则必须包括端口号，如下所示：
   - ` + https://wfa_server_ip:port+`
   - ` https://localhost:port` port 是您在安装期间用于 WFA 服务器的 TCP 端口号。
2. 在登录部分中，输入您在安装期间输入的管理员用户凭据。
3. 在 * 设置 * > * 设置 * 菜单中，设置凭据和数据源。
4. 将 WFA Web 图形用户界面添加到书签以方便访问。

OnCommand Workflow Automation 数据源

OnCommand Workflow Automation （ WFA ）对从数据源获取的数据进行操作。提供了各种版本的 Active IQ Unified Manager 和 VMware vCenter Server 作为预定义的 WFA 数据源类型。在设置数据源以进行数据采集之前，您必须了解预定义的数据源类型。

数据源是一种只读数据结构，用作与特定数据源类型的数据源对象的连接。例如，数据源可以是与 Active IQ Unified Manager 6.3 数据源类型的 Active IQ Unified Manager 数据库的连接。定义所需的数据源类型后，您可以将自定义数据源添加到 WFA 中。

有关预定义的数据源类型的详细信息，请参见互操作性表。

- 相关信息 *

"NetApp 互操作性表工具"

在 DataFabric Manager 上配置数据库用户

您必须在 DataFabric Manager 5.x 上创建一个数据库用户，才能配置对 OnCommand

Workflow Automation 的 DataFabric Manager 5.x 数据库的只读访问权限。

通过在 **Windows** 上运行 **ocsetup** 来配置数据库用户

您可以在 DataFabric Manager 5.x 服务器上运行 ocsetup 文件，以配置对 OnCommand Workflow Automation 的 DataFabric Manager 5.x 数据库的只读访问权限。

步骤

1. 从以下位置将 wfa_ocsetup.exe 文件下载到 DataFabric Manager 5.x 服务器中的目录： *https*： //wfa_Server_IP/download/wfa_ocsetup.exe 。

   WFA_SERVER_IP 是 WFA 服务器的 IP 地址（ IPv4 或 IPv6 地址）。

   如果为 WFA 指定了非默认端口，则必须包括端口号，如下所示： *https*： //wfa_server_ip：port/download/wfa_ocsetup.exe 。

   port 是您在安装期间用于 WFA 服务器的 TCP 端口号。

   如果要指定 IPv6 地址，则必须将其用方括号括起来。

2. 双击 wfa_ocsetup.exe 文件。
3. 阅读设置向导中的信息，然后单击 * 下一步 * 。
4. 浏览或键入 OpenJDK 位置，然后单击 * 下一步 * 。
5. 输入用户名和密码以覆盖默认凭据。

   此时将创建一个可访问 DataFabric Manager 5.x 数据库的新数据库用户帐户。

   > 如果不创建用户帐户，则会使用默认凭据。出于安全考虑，您必须创建一个用户帐户。

6. 单击 * 下一步 * 并查看结果。
7. 单击 * 下一步 * ，然后单击 * 完成 * 完成向导。

通过在 **Linux** 上运行 **ocsetup** 来配置数据库用户

您可以在 DataFabric Manager 5.x 服务器上运行 ocsetup 文件，以配置对 OnCommand Workflow Automation 的 DataFabric Manager 5.x 数据库的只读访问权限。

步骤

1. 在终端中使用以下命令将 wfa_ocsetup.sh 文件下载到 DataFabric Manager 5.x 服务器上的主目录：

   ` wget https://WFA_Server_IP/download/wfa_ocsetup.sh`[]

   WFA_SERVER_IP 是 WFA 服务器的 IP 地址（ IPv4 或 IPv6 地址）。

   如果为 WFA 指定了非默认端口，则必须包括以下端口号：

   ` wget https://wfa_server_ip:port/download/wfa_ocsetup.sh`[]

port 是安装期间 WFA 服务器使用的 TCP 端口号。

如果要指定 IPv6 地址，则必须将其用方括号括起来。

2. 在终端中使用以下命令将 wfa_ocsetup.sh 文件更改为可执行文件： `chmod +x WFA_ocsetup.sh`
3. 在终端中输入以下命令以运行此脚本：

   `。 /wfa_ocsetup.sh OpenJDK_path`

   OpenJDK_path 是 OpenJDK 的路径。

   /opt/NTAPdfm/java

   终端中将显示以下输出，表示设置成功：

   ```
   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. 输入用户名和密码以覆盖默认凭据。

   此时将创建一个可访问 DataFabric Manager 5.x 数据库的新数据库用户帐户。

   > 如果不创建用户帐户，则会使用默认凭据。出于安全考虑，您必须创建一个用户帐户。

   终端中将显示以下输出，表示设置成功：

   ```
   ***** 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 *****
   ```

在 **Active IQ Unified Manager** 上配置数据库用户

您必须在 Active IQ Unified Manager 上创建一个数据库用户，才能配置对 OnCommand Workflow Automation 的 Active IQ Unified Manager 数据库的只读访问权限。

步骤

1. 使用管理员凭据登录到 Active IQ Unified Manager 。
2. 单击 * 设置 * > * 用户 * 。
3. 单击 * 添加新用户 * 。
4. 选择 * 数据库用户 * 作为用户类型。

   在 OnCommand Workflow Automation 中将 Active IQ Unified Manager 添加为数据源时，应在 OnCommand Workflow Automation 中使用同一用户。

设置数据源

您必须在 OnCommand Workflow Automation （ WFA ）中设置与数据源的连接，才能从数据源获取数据。

- 对于Active IQ Unified Manager 6.0及更高版本、您必须已在Unified Manager服务器上创建数据库用户帐户。

  有关 OnCommand 详细信息，请参见 _Unified Manager 联机帮助。

- Unified Manager 服务器上用于传入连接的 TCP 端口必须处于打开状态。

  有关详细信息，请参见防火墙上的文档。

  以下是默认 TCP 端口号：

TCP 端口号	**Unified Manager** 服务器版本	**Description**
3306	6.x	MySQL 数据库服务器

- 对于 Performance Advisor ，您必须已创建一个至少具有 GlobalRead 角色的 Active IQ Unified Manager 用户帐户。

  有关 OnCommand 详细信息，请参见 _Unified Manager 联机帮助。

- 对于 VMware vCenter Server ，您必须已在 vCenter Server 上创建用户帐户。

  有关详细信息，请参见 VMware vCenter Server 文档。

  > 您必须已安装 VMware PowerCLI 。如果只想在 vCenter Server 数据源上执行工作流，则不需要将 Unified Manager 服务器设置为数据源。

- VMware vCenter Server 上用于传入连接的 TCP 端口必须处于打开状态。

  默认 TCP 端口号为 443 。有关详细信息，请参见防火墙上的文档。

您可以使用此操作步骤 向 WFA 添加多个 Unified Manager 服务器数据源。但是，如果要将操作步骤 服务器 6.3 及更高版本与 WFA 配对并使用 Unified Manager 服务器中的保护功能，则不能使用此 Unified Manager 。

有关将 WFA 与 OnCommand 服务器 6.x 配对的详细信息，请参见 _Unified Manager 联机帮助。

> 在使用 WFA 设置数据源时，您必须注意， WFA 4.0 版已弃用 Active IQ Unified Manager 6.0 ，6.1 和 6.2 数据源类型，未来版本将不支持这些数据源类型。

步骤

1. 使用 Web 浏览器访问 WFA 。
2. 单击 * 设置 * ，然后在 * 设置 * 下单击 * 数据源 * 。
3. 选择相应的操作：

至 ...	执行此操作 ...
创建新数据源	单击 在工具栏上。
如果已升级 WFA ，请编辑已还原的数据源	选择现有数据源条目，然后单击 在工具栏上。

如果已将 Unified Manager 服务器数据源添加到 WFA 中，然后升级了 Unified Manager 服务器的版本，则 WFA 将无法识别升级后的 Unified Manager 服务器版本。您必须删除 Unified Manager 服务器的先前版本，然后将 Unified Manager 服务器的升级版本添加到 WFA 。

4. 在新建数据源对话框中，选择所需的数据源类型，然后输入数据源的名称和主机名。

   根据选定的数据源类型，端口，用户名，密码和超时字段可能会自动填充默认数据（如果有）。您可以根据需要编辑这些条目。

5. 选择适当的操作：

针对 ...	执行此操作 ...
Active IQ Unified Manager 6.3 及更高版本	输入您在 Unified Manager 服务器上创建的数据库用户帐户的凭据。有关创建数据库用户帐户的详细信息，请参见 _Unified OnCommand Manager 联机帮助。 您不能提供使用命令行界面或 ocsetup 工具创建的 Active IQ Unified Manager 数据库用户帐户的凭据。
VMware vCenter Server （仅适用于 Windows ）	（仅适用于 Windows ）输入您在 VMware vCenter 服务器上创建的用户的用户名和密码。

6. 单击 * 保存 * 。
7. 在数据源表中，选择数据源，然后单击 在工具栏上。
8. 验证数据采集过程的状态。

将升级后的 **Unified Manager** 服务器添加为数据源

如果将 Unified Manager 服务器（ 5.x 或 6.x ）作为数据源添加到 WFA 中，然后升级 Unified Manager 服务器， 您必须将升级后的 Unified Manager 服务器添加为数据源，因为与升级后的版本关联的数据不会填充到 WFA 中，除非手动将其添加为数据源。

步骤

1. 以管理员身份登录到 WFA Web 图形用户界面。
2. 单击 * 设置 * ，然后在 * 设置 * 下，单击 * 数据源 * 。
3. 单击 在工具栏上。
4. 在新建数据源对话框中，选择所需的数据源类型，然后输入数据源的名称和主机名。

   根据选定的数据源类型，端口，用户名，密码和超时字段可能会自动填充默认数据（如果有）。您可以根据需要编辑这些条目。

5. 单击 * 保存 * 。
6. 选择 Unified Manager 服务器的先前版本，然后单击 在工具栏上。
7. 在删除数据源类型确认对话框中，单击 * 是 * 。
8. 在数据源表中，选择数据源，然后单击 在工具栏上。
9. 在历史记录表中验证数据采集状态。

创建本地用户

通过 OnCommand Workflow Automation （ WFA ），您可以创建和管理具有各种角色的特定权限的本地 WFA 用户，例如来宾，操作员，审批者，架构师， 管理和备份。

您必须已安装 WFA 并以管理员身份登录。

使用 WFA 可以为以下角色创建用户：

- * 来宾 *

  此用户可以查看门户和工作流执行状态，并可收到工作流执行状态更改的通知。

- * 运算符 *

  允许此用户预览和执行为其授予访问权限的工作流。

- * 审批者 *

  允许此用户预览，执行，批准和拒绝授予用户访问权限的工作流。

  > 建议提供审批者的电子邮件 ID 。如果有多个审批者，您可以在 * 电子邮件 * 字段中提供组电子邮件 ID 。

- * 架构师 *

此用户具有创建工作流的完全访问权限，但无法修改全局 WFA 服务器设置。

- * 管理员 *

  此用户可以完全访问 WFA 服务器。

- * 备份 *

  这是唯一能够远程生成 WFA 服务器备份的用户。但是，用户不能进行所有其他访问。

步骤

1. 单击 * 设置 * ，然后在 * 管理 * 下单击 * 用户 * 。
2. 单击以创建新用户 在工具栏上。
3. 在新建用户对话框中输入所需信息。
4. 单击 * 保存 * 。

配置目标系统的凭据

您可以在 OnCommand Workflow Automation （ WFA ）中配置目标系统的凭据，并使用这些凭据连接到该特定系统并执行命令。

首次数据采集后，您必须为运行命令的阵列配置凭据。PowerShell WFA 控制器连接在两种模式下工作：

- 凭据

  WFA 首先尝试使用 HTTPS 建立连接，然后尝试使用 HTTP 。您还可以使用 Microsoft Active Directory LDAP 身份验证连接到阵列，而无需在 WFA 中定义凭据。要使用 Active Directory LDAP ，必须将阵列配置为使用同一 Active Directory LDAP 服务器执行身份验证。

- 无凭据（适用于在 7- 模式下运行的存储系统）

  WFA 尝试使用域身份验证建立连接。此模式使用远程操作步骤 调用协议，该协议使用 NTLM 协议进行保护。

- WFA 检查 ONTAP 系统的安全套接字层（ SSL ）证书。如果 SSL 证书不可信，则可能会提示用户检查并接受 / 拒绝与 ONTAP 系统的连接。
- 还原备份或完成原位升级后，您必须重新输入 ONTAP ， NetApp Active IQ 和轻型目录访问协议（ LDAP ）的凭据。

步骤

1. 以管理员身份通过 Web 浏览器登录到 WFA 。
2. 单击 * 设置 * ，然后在 * 设置 * 下单击 * 凭据 * 。
3. 单击 在工具栏上。
4. 在新建凭据对话框中，从 * 匹配 * 列表中选择以下选项之一：

   - * 精确 *

特定 IP 地址或主机名的凭据

- * 模式 *

  整个子网或 IP 范围的凭据

> 此选项不支持使用正则表达式语法。

5. 从 * 类型 * 列表中选择远程系统类型。
6. 输入资源的主机名或 IPv4 或 IPv6 地址，用户名和密码。

> WFA 5.1 验证添加到 WFA 中的所有资源的 SSL 证书。由于证书验证可能会提示您接受证书，因此不支持在凭据中使用通配符。如果多个集群使用相同的凭据，则不能一次性全部添加。

7. 执行以下操作以测试连接：

如果选择了以下匹配类型 ...	那么 ...
• 精确 *	单击 * 测试 * 。
• 模式 *	保存凭据并选择以下选项之一： • 选择凭据，然后单击 在工具栏上。 • 右键单击并选择 * 测试连接 * 。

8. 单击 * 保存 * 。

正在配置 OnCommand Workflow Automation

使用 OnCommand Workflow Automation （ WFA ）可以配置各种设置，例如 AutoSupport 和通知。

配置 WFA 时，您可以根据需要设置以下一项或多项：

- AutoSupport ，用于向技术支持发送 AutoSupport 消息
- Microsoft Active Directory 轻型目录访问协议（ Lightweight Directory Access Protocol ， LDAP ）服务器，用于对 WFA 用户进行 LDAP 身份验证和授权
- 有关工作流操作和发送 AutoSupport 消息的电子邮件通知
- 简单网络管理协议（ Simple Network Management Protocol ， SNMP ），用于发送有关工作流操作的通知
- 用于远程数据日志记录的系统日志

配置 AutoSupport

您可以配置多个 AutoSupport 设置，例如计划， AutoSupport 消息内容和代理服务

器。AutoSupport 会将您选择的内容的每周日志发送给技术支持，以便进行归档和问题描述 分析。

步骤

1. 以管理员身份通过 Web 浏览器登录到 WFA 。
2. 单击 * 设置 * ，然后在 * 设置 * 下单击 * AutoSupport * 。
3. 确保已选中 * 启用 AutoSupport * 框。
4. 输入所需信息。
5. 从 * 内容 * 列表中选择以下选项之一：

如果要包括 ...	然后选择此选项 ...
仅配置详细信息，例如 WFA 安装的用户，工作流和命令	s仅限最终配置数据
WFA 配置详细信息以及方案等 WFA 缓存表中的数据	sEnd configuration and cache data （结束配置和缓存数据）（默认）
WFA 配置详细信息， WFA 缓存表中的数据以及安装目录中的数据	s结束配置并缓存扩展数据

> AutoSupport 数据中包含任何 WFA 用户的密码 *not* 。

6. 测试您是否可以下载 AutoSupport 消息：
   a. 单击 * 下载 * 。
   b. 在打开的对话框中，选择要保存 .7z 文件的位置。
7. 单击 * 立即发送 * ，测试向指定目标发送 AutoSupport 消息的情况。
8. 单击 * 保存 * 。

配置身份验证设置

您可以将 OnCommand Workflow Automation （ WFA ）配置为使用 Microsoft Active Directory （ AD ）轻型目录访问协议（ LDAP ）服务器进行身份验证和授权。

您必须已在环境中配置 Microsoft AD LDAP 服务器。

WFA 仅支持 Microsoft AD LDAP 身份验证。您不能使用任何其他 LDAP 身份验证方法，包括 Microsoft AD 轻型目录服务（ AD LDS ）或 Microsoft 全局目录。

> 在通信期间， LDAP 会以纯文本格式发送用户名和密码。但是， LDAPS （ LDAP 安全）通信已加密且安全。

步骤

1. 以管理员身份通过 Web 浏览器登录到 WFA 。

2. 单击 * 设置 * ，然后在 * 设置 * 下单击 * 身份验证 * 。
3. 选中 * 启用 Active Directory* 复选框。
4. 在以下字段中输入所需信息：

   a. 如果要对域用户使用用户@域格式，请在 * 用户名属性 * 字段中将 sAMAccountName 替换为 userPrincipalName 。
   b. 如果您的环境需要唯一值，请编辑所需字段。
   c. 按如下所示输入 AD 服务器 URI： `ldap ： //active_directory_server_address\[ ： port\]`

      LDAP： //NB-T01.example.com[:389]

   如果已启用基于 SSL 的 LDAP ，则可以使用以下 URI 格式： `ldaps ： //active_directory_server_address\[ ： port\]`

   a. 添加所需角色的 AD 组名称列表。

      > 您可以在 Active Directory 组窗口中为所需角色添加 AD 组名称列表。

5. 单击 * 保存 * 。
6. 如果需要使用 LDAP 连接到阵列，请配置 WFA 服务以所需域用户身份登录：
   a. 使用 services.msc 打开 Windows 服务控制台。
   b. 双击 * NetApp WFA Server* 服务。
   c. 在 NetApp WFA 服务器属性对话框中，单击 * 登录 * 选项卡，然后选择 * 此帐户 * 。
   d. 输入域用户名和密码，然后单击 * 确定 * 。

添加 **Active Directory** 组

您可以在 OnCommand Workflow Automation （ WFA ）中添加 Active Directory 组。

步骤

1. 以管理员身份通过 Web 浏览器登录到 WFA 。
2. 单击 * 设置 * ，然后在 * 管理 * 下，单击 * Active Directory 组 * 。
3. 在 Active Directory 组窗口中，单击 * 新建 * 图标。
4. 在新建 Active Directory 组对话框中，输入所需信息。

   如果从 * 角色 * 下拉列表中选择 * 审批者 * ，建议提供审批者的电子邮件 ID 。如果有多个审批者，您可以在 * 电子邮件 * 字段中提供组电子邮件 ID 。选择要将通知发送到特定 Active Directory 组的工作流的不同事件。

5. 单击 * 保存 * 。

配置电子邮件通知

您可以将 OnCommand Workflow Automation （ WFA ）配置为向您发送有关工作流操作的电子邮件通知，例如，工作流已启动或工作流失败。

您必须已在环境中配置邮件主机。

步骤

1. 以管理员身份通过 Web 浏览器登录到 WFA 。
2. 单击 * 设置 * ，然后在 * 设置 * 下单击 * 邮件 * 。
3. 在字段中输入所需信息。
4. 执行以下步骤以测试邮件设置：
   a. 单击 * 发送测试邮件 * 。
   b. 在测试连接对话框中，输入要将电子邮件发送到的电子邮件地址。
   c. 单击 * 测试 * 。
5. 单击 * 保存 * 。

配置 **SNMP**

您可以将 OnCommand Workflow Automation （ WFA ）配置为发送有关工作流操作状态的简单网络管理协议（ Simple Network Management Protocol ， SNMP ）陷阱。

WFA 现在支持 SNMP v1 和 SNMP v3 协议。SNMP v3 可提供其他安全功能。

WFA .mib 文件提供了有关 WFA 服务器发送的陷阱的信息。MIB 文件位于 WFA 服务器上的 <wfa_install_location>\wfa\bin\wfa.mib 目录中。

> WFA 服务器会使用通用对象标识符（ 1.3.6.1.4.1.789.1.1.12.0 ）发送所有陷阱通知。

您不能对 SNMP 配置使用 SNMP 社区字符串，例如 community_string@snmp_host 。

配置 **SNMP** 版本 **1**

步骤

1. 以管理员用户身份通过 Web 浏览器登录到 WFA ，然后访问 WFA 服务器。
2. 单击 * 设置 * ，然后在 * 设置 * 下单击 * SNMP * 。
3. 选中 * 启用 SNMP* 复选框。
4. 在 "* 版本 1* " 下拉列表中，选择 * 版本 1* 。
5. 输入 IPv4 或 IPv6 地址或主机名以及管理主机的端口号。

   WFA 将 SNMP 陷阱发送到指定端口号。默认端口号为 162 。
6. 在通知位置部分中，选中以下一个或多个复选框：

- 已启动工作流执行
- 已成功完成工作流执行
- 工作流执行失败 / 部分成功
- 正在执行工作流，等待批准
- 采集失败

7. 单击 * 发送测试通知 * 以验证设置。
8. 单击 * 保存 * 。

配置 **SNMP** 版本 **3**

您还可以配置 OnCommand Workflow Automation （ WFA ），以发送有关工作流操作状态的简单网络管理协议（ SNMP ）版本 3 陷阱。

版本 3 提供了两个额外的安全选项：

- 使用身份验证的版本 3

  陷阱会通过网络以未加密方式发送。SNMP 管理应用程序使用与 SNMP 陷阱消息相同的身份验证参数进行配置，可以接收陷阱。

- 具有身份验证和加密功能的版本 3

  陷阱会通过网络进行加密发送。要接收和解密这些陷阱，您必须为 SNMP 管理应用程序配置与 SNMP 陷阱相同的身份验证参数和加密密钥。

步骤

1. 以管理员用户身份通过 Web 浏览器登录到 WFA ，然后访问 WFA 服务器。
2. 单击 * 设置 * ，然后在 * 设置 * 下单击 * SNMP * 。
3. 选中 * 启用 SNMP* 复选框。
4. 在 * 版本 * 下拉列表中，选择以下选项之一：
   - 版本 3
   - 使用身份验证的版本 3
   - 具有身份验证和加密功能的版本 3
5. 选择与您在步骤 4 中选择的特定 SNMP 版本 3 选项对应的 SNMP 配置选项。
6. 输入 IPv4 或 IPv6 地址或主机名以及管理主机的端口号。WFA 将 SNMP 陷阱发送到指定端口号。默认端口号为 162 。
7. 在通知位置部分中，选中以下一个或多个复选框：
   - 工作流规划已启动 / 失败 / 已完成
   - 已启动工作流执行
   - 已成功完成工作流执行
   - 工作流执行失败 / 部分成功

- 正在执行工作流，等待批准
- 采集失败

8. 单击 * 发送测试通知 * 以验证设置。
9. 单击 * 保存 * 。

配置系统日志

您可以将 OnCommand Workflow Automation （ WFA ）配置为将日志数据发送到特定的系统日志服务器，以用于事件日志记录和日志信息分析等目的。

您必须已将系统日志服务器配置为接受来自 WFA 服务器的数据。

步骤

1. 以管理员身份通过 Web 浏览器登录到 WFA 。
2. 单击 * 设置 * ，然后在 * 维护 * 下单击 * 系统日志 * 。
3. 选中 * 启用系统日志 * 复选框。
4. 输入系统日志主机名并选择系统日志日志日志级别。
5. 单击 * 保存 * 。

配置用于连接到远程系统的协议

您可以配置 OnCommand Workflow Automation （ WFA ）用来连接到远程系统的协议。您可以根据组织的安全要求以及远程系统支持的协议来配置协议。

步骤

1. 以管理员身份通过 Web 浏览器登录到 WFA 。
2. 单击 * 数据源设计 * > * 远程系统类型 * 。
3. 执行以下操作之一：

如果您要 ...	执行此操作 ...
为新的远程系统配置协议	a. 单击 。 b. 在新建远程系统类型对话框中，指定名称，问题描述 和版本等详细信息。
修改现有远程系统的协议配置	a. 选择并双击要修改的远程系统。 b. 单击 。

4. 从连接协议列表中，选择以下选项之一：
   - HTTPS 与回退到 HTTP （默认）
   - 仅限 HTTPS

- 仅限 HTTP
- 自定义

5. 指定协议，默认端口和默认超时的详细信息。
6. 单击 * 保存 * 。

禁用默认密码策略

OnCommand Workflow Automation （ WFA ）已配置为对本地用户强制实施密码策略。如果不想使用密码策略，可以将其禁用。

您必须以管理员身份登录到 WFA 主机系统。

此操作步骤 将使用默认 WFA 安装路径。如果您在安装期间更改了默认位置，则必须使用更改后的 WFA 安装路径。

步骤

1. 打开 Windows 资源管理器并导航到以下目录： `WFA_INSTALL_location\WFA\bin\` 。
2. 双击 ps.cmd 文件。

   此时将打开 PowerShell 命令行界面（ CLI ）提示符，其中已加载 ONTAP 和 WFA 模块。

3. 在提示符处，输入以下内容：

   ```
   sET-WfaConfig -Name PasswordPolicy -Enable $false
   ```

4. 出现提示时，重新启动 WFA 服务。

修改 **Windows** 的默认密码策略

OnCommand Workflow Automation （ WFA ）为本地用户强制实施密码策略。您可以根据需要修改默认密码策略以设置密码。

您必须以 root 用户身份登录到 WFA 主机系统。

- 此操作步骤 将使用默认 WFA 安装路径。

  如果您在安装期间更改了默认位置，则必须使用自定义 WFA 安装路径。

- 用于修改默认密码策略的命令为 .\WFA -password-policy=default 。

  默认设置为 `minLperf=true ， 8 ； specialChar=true ， 1 ； DigitalChar=true ， 1 ； lowercaseChar=true ， 1 ； uppercaseChar=true ， 1 ； whiteespaceChar=false` 。根据默认密码策略的此设置，密码必须至少包含八个字符，并且必须至少包含一个特殊字符，一个数字，一个小写字符和一个大写字符，并且不能包含空格。

步骤

1. 在命令提示符处，导航到 WFA 服务器上的以下目录：

```
wfa_install_location/wfa/bin/
```

2. 修改默认密码策略：

   ` .\WFA -password-policy=PasswordPolicyString -restart=WFA`

在 Windows 上启用对 OnCommand Workflow Automation 数据库的远程访问

默认情况下， OnCommand Workflow Automation （ WFA ）数据库只能由 WFA 主机系统上运行的客户端访问。如果要从远程系统访问 WFA 数据库，可以更改默认设置。

- 您必须以管理员用户身份登录到 WFA 主机系统。
- 如果 WFA 主机系统上安装了防火墙，则必须已将防火墙设置配置为允许从远程系统进行访问。

此操作步骤 将使用默认 WFA 安装路径。如果您在安装期间更改了默认位置，则必须使用自定义 WFA 安装路径。

步骤

1. 打开 Windows 资源管理器，然后导航到以下目录： wfa_install_location\wfA\bin
2. 执行以下操作之一：

至 ...	输入以下命令 ...
启用远程访问	` .\WFA -db-access=public -restart`
禁用远程访问	` .\wFA -db-access=default -restart`

限制主机上 OnCommand Workflow Automation 的访问权限

默认情况下， OnCommand Workflow Automation （ WFA ）以主机系统的管理员身份执行工作流。您可以通过更改默认设置来限制主机系统上的 WFA 权限。

您必须以管理员身份登录到 WFA 主机系统。

步骤

1. 创建一个新的 Windows 用户帐户，该帐户有权打开套接字并写入 WFA 主目录。
2. 使用 services.msc 打开 Windows 服务控制台，然后双击 * NetApp WFA Database* 。
3. 单击 * 登录 * 选项卡。
4. 选择 * 此帐户 * 并输入您创建的新用户的凭据，然后单击 * 确定 * 。
5. 双击 * NetApp WFA Server* 。
6. 单击 * 登录 * 选项卡。
7. 选择 * 此帐户 * 并输入您创建的新用户的凭据，然后单击 * 确定 * 。

8. 重新启动 * NetApp WFA 数据库 * 和 * NetApp WFA Server* 服务。

修改 OnCommand Workflow Automation 的事务超时设置

默认情况下， OnCommand Workflow Automation （ WFA ）数据库事务在 300 秒内超时。在从备份还原大型 WFA 数据库时，您可以增加默认超时持续时间，以避免数据库还原可能失败。

您必须以管理员身份登录到 WFA 主机系统。

此操作步骤 将使用默认 WFA 安装路径。如果您在安装期间更改了默认位置，则必须使用更改后的 WFA 安装路径。

步骤

1. 打开 Windows 资源管理器并导航到以下目录：

   ```
   wfa_install_location\wfA\bin
   ```

2. 双击 ps.cmd 文件。

   此时将打开 PowerShell 命令行界面（ CLI ）提示符，其中已加载 ONTAP 和 WFA 模块。

3. 在提示符处，输入以下内容：

   ```
   sET-WfaConfig -Name TransactionTimeOut -seconds NumbericValue
   ```

   ```
   sET-WfaConfig -Name TransactionTimeOut -seconds 1000
   ```

4. 出现提示时，重新启动 WFA 服务。

配置 Workflow Automation 的超时值

您可以为 Workflow Automation （ WFA） Web 图形用户界面配置超时值，而不是使用默认超时值。

WFA Web 图形用户界面的默认超时值为 180 分钟。您可以通过命令行界面配置超时值以满足您的要求。您不能从 WFA Web 图形用户界面设置超时值。

> 您设置的超时值为绝对超时，而不是与非活动相关的超时。例如，如果将此值设置为 30 分钟，则即使您在此时间结束时处于活动状态，您也会在 30 分钟后注销。

步骤

1. 以管理员身份登录到 WFA 主机。
2. 设置超时值：

   ```
   installdir bin/wFA -s=timeout value in minutes
   ```

启用密码并添加新密码

OnCommand Workflow Automation 5.1 支持多个即装即用的密码。此外，您还可以根据需要添加其他密码。

以下密码可以即装即用：

```
enabled-cipher-suites=
"TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,T
LS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA25
6,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA38
4,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA25
6,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384"
```

可以在 `standalis-full.xml` 文件中将其他密码添加到此配置中。此文件位于：` <installdir>/jboss/standalone 或 configuration/standstandstandalone Full.xml` 。

可以对该文件进行修改，以支持其他密码，如下所示：

```
<https-listener name="https" socket-binding="https" max-post-
size="1073741824" security-realm="SSLRealm"
enabled-cipher-suites="**< --- add additional ciphers here ---\>**
enabled-protocols="TLSv1.1,TLSv1.2"/>
```