



正在配置 **OnCommand Workflow Automation**

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

目录

- 正在配置 OnCommand Workflow Automation 1
 - 配置 AutoSupport 1
 - 配置身份验证设置 2
 - 添加 Active Directory 组 3
 - 配置电子邮件通知 3
 - 配置 SNMP 3
 - 配置系统日志 5
 - 配置用于连接到远程系统的协议 5

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。 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：
 - workflow规划已启动 / 失败 / 已完成
 - 已启动 workflow 执行
 - 已成功完成 workflow 执行
 - workflow 执行失败 / 部分成功
 - 正在执行 workflow，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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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 *。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。