OnCommand Workflow Automation 설정

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

목차

OnCommand Workflow Automation 설정

WFA(OnCommand Workflow Automation) 설치를 완료한 후에는 몇 가지 구성 설정을 완료해야 합니다. WFA에 액세스하고, 사용자를 구성하고, 데이터 소스를 설정하고, 자격 증명을 구성하고, WFA를 구성해야 합니다.

OnCommand Workflow Automation에 액세스합니다

WFA 서버에 액세스할 수 있는 모든 시스템에서 웹 브라우저를 통해 OnCommand Workflow Automation(WFA)에 액세스할 수 있습니다.

웹 브라우저에 Adobe Flash Player를 설치해야 합니다.

단계

1. 웹 브라우저를 열고 주소 표시줄에 다음 중 하나를 입력합니다.
   - (https://wfa_server_ip`)

     WFA_SERVER_IP는 WFA 서버의 IP 주소(IPv4 또는 IPv6 주소) 또는 FQDN(정규화된 도메인 이름)입니다.

   - WFA 서버에 대해 WFA를 액세스하는 경우: 'https://localhost/wfa` WFA에 대해 기본값이 아닌 포트를 지정한 경우 다음과 같이 포트 번호를 포함해야 합니다.
   - (https://wfa_server_ip:port`)
   - 'https://localhost:port` 포트는 설치 중에 WFA 서버에 사용한 TCP 포트 번호입니다.
2. 로그인 섹션에서 설치 중에 입력한 admin 사용자의 자격 증명을 입력합니다.
3. 설정 * > * 설정 * 메뉴에서 자격 증명과 데이터 소스를 설정합니다.
4. 쉽게 액세스할 수 있도록 WFA 웹 GUI를 북마크하십시오.

OnCommand Workflow Automation 데이터 소스

WFA(OnCommand Workflow Automation)는 데이터 소스에서 가져온 데이터에 대해 작동합니다. 다양한 버전의 Active IQ Unified Manager 및 VMware vCenter Server가 사전 정의된 WFA 데이터 소스 유형으로 제공됩니다. 데이터 획득을 위해 데이터 소스를 설정하기 전에 미리 정의된 데이터 소스 유형을 알고 있어야 합니다.

데이터 소스는 특정 데이터 소스 형식의 데이터 소스 개체에 대한 연결 역할을 하는 읽기 전용 데이터 구조입니다. 예를 들어, 데이터 소스는 Active IQ Unified Manager 6.3 데이터 소스 유형의 Active IQ Unified Manager 데이터베이스에 대한 연결이 될 수 있습니다. 필요한 데이터 소스 유형을 정의한 후 WFA에 사용자 지정 데이터 소스를 추가할 수 있습니다.

사전 정의된 데이터 소스 유형에 대한 자세한 내용은 상호 운용성 매트릭스 를 참조하십시오.

- 관련 정보 *

"NetApp 상호 운용성 매트릭스 툴"

DataFabric Manager에서 데이터베이스 사용자 구성

OnCommand Workflow Automation에 대한 DataFabric Manager 5.x 데이터베이스의 읽기 전용 액세스를 구성하려면 DataFabric Manager 5.x에서 데이터베이스 사용자를 만들어야 합니다.

Windows에서 **ocsetup**을 실행하여 데이터베이스 사용자를 구성합니다

DataFabric Manager 5.x 서버에서 ocsetup 파일을 실행하여 OnCommand Workflow Automation에 대한 DataFabric Manager 5.x 데이터베이스의 읽기 전용 액세스를 구성할 수 있습니다.

단계

1. wfa_ocsetup.exe 파일을 다음 위치에서 DataFabric Manager 5.x 서버의 디렉토리에 다운로드합니다. *https*://WFA_Server_IP/download/WFA_ocsetup.exe.

   _WFA_Server_IP_는 WFA 서버의 IP 주소(IPv4 또는 IPv6 주소)입니다.

   WFA에 대해 기본값이 아닌 포트를 지정한 경우 다음과 같이 포트 번호를 입력해야 합니다. *https*://WFA_server_IP: port/download/WFA_ocsetup.exe.

   _port_는 설치 중에 WFA 서버에 사용한 TCP 포트 번호입니다.

   IPv6 주소를 지정하는 경우 대괄호로 묶어야 합니다.

2. wfa_ocsetup.exe 파일을 두 번 클릭합니다.
3. 설정 마법사의 정보를 읽고 * 다음 * 을 클릭합니다.
4. OpenJDK 위치를 찾거나 입력하고 * 다음 * 을 클릭합니다.
5. 사용자 이름과 암호를 입력하여 기본 자격 증명을 재정의합니다.

   DataFabric Manager 5.x 데이터베이스에 대한 액세스 권한을 사용하여 새 데이터베이스 사용자 계정이 생성됩니다.

   > 사용자 계정을 만들지 않으면 기본 자격 증명이 사용됩니다. 보안을 위해 사용자 계정을 만들어야 합니다.

6. 다음 * 을 클릭하고 결과를 검토합니다.
7. 다음 * 을 클릭한 다음 * 마침 * 을 클릭하여 마법사를 완료합니다.

Linux에서 **ocsetup**을 실행하여 데이터베이스 사용자를 구성합니다

DataFabric Manager 5.x 서버에서 ocsetup 파일을 실행하여 OnCommand Workflow Automation에 대한 DataFabric Manager 5.x 데이터베이스의 읽기 전용 액세스를 구성할 수 있습니다.

단계

1. 터미널에서 다음 명령을 사용하여 DataFabric Manager 5.x 서버의 홈 디렉토리에 wfa_ocsetup.sh 파일을

다운로드합니다.

"와우와 https://WFA_Server_IP/download/wfa_ocsetup.sh`[]

WFA_Server_IP는 WFA 서버의 IP 주소(IPv4 또는 IPv6 주소)입니다.

WFA에 대해 기본값이 아닌 포트를 지정한 경우 다음과 같이 포트 번호를 포함해야 합니다.

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

port는 설치 중에 WFA 서버에 사용한 TCP 포트 번호입니다.

IPv6 주소를 지정하는 경우 대괄호로 묶어야 합니다.

2. 터미널에서 다음 명령을 사용하여 wfa_ocsetup.sh 파일을 실행 파일('chmod + x WFA_ocsetup.sh'로 변경합니다
3. 터미널에 다음을 입력하여 스크립트를 실행합니다.

   './wfa_ocsetup.sh OpenJDK_PATH'

   OpenJDK_PATH는 OpenJDK의 경로입니다.

   /opt/NTAPdfm/java

   다음 출력이 단말기에 표시되어 설치가 성공적으로 완료되었음을 나타냅니다.

```
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. 사용자 이름과 암호를 입력하여 기본 자격 증명을 재정의합니다.

   DataFabric Manager 5.x 데이터베이스에 대한 액세스 권한을 사용하여 새 데이터베이스 사용자 계정이 생성됩니다.

   > 사용자 계정을 만들지 않으면 기본 자격 증명이 사용됩니다. 보안을 위해 사용자 계정을 만들어야 합니다.

   다음 출력이 단말기에 표시되어 설치가 성공적으로 완료되었음을 나타냅니다.

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

Active IQ Unified Manager에서 데이터베이스 사용자를 구성합니다

OnCommand Workflow Automation에 대한 Active IQ Unified Manager 데이터베이스의 읽기 전용 액세스를 구성하려면 Active IQ Unified Manager에서 데이터베이스 사용자를 만들어야 합니다.

단계

1. 관리자 자격 증명을 사용하여 Active IQ Unified Manager에 로그인합니다.
2. 설정 * > * 사용자 * 를 클릭합니다.
3. 새 사용자 추가 * 를 클릭합니다.
4. 사용자 유형으로 * 데이터베이스 사용자 * 를 선택합니다.

   OnCommand Workflow Automation에서 Active IQ Unified Manager를 데이터 소스로 추가하는 동안 OnCommand Workflow Automation에서 동일한 사용자를 사용해야 합니다.

데이터 원본을 설정합니다

데이터 소스에서 데이터를 가져오려면 WFA(OnCommand Workflow Automation)에서 데이터 소스와의 연결을 설정해야 합니다.

- Active IQ Unified Manager 6.0 이상에서는 Unified Manager 서버에 데이터베이스 사용자 계정을 만들어야 합니다.

  자세한 내용은 _OnCommand Unified Manager 온라인 도움말_을 참조하십시오.

- Unified Manager 서버에서 들어오는 연결의 TCP 포트가 열려 있어야 합니다.

  자세한 내용은 방화벽 설명서를 참조하십시오.

  다음은 기본 TCP 포트 번호입니다.

TCP 포트 번호입니다	**Unified Manager** 서버 버전입니다	설명
3306	6.x	MySQL 데이터베이스 서버

- Performance Advisor의 경우 GlobalRead 이상의 역할을 가진 Active IQ Unified Manager 사용자 계정을 만들어야 합니다.

  자세한 내용은 _OnCommand Unified Manager 온라인 도움말_을 참조하십시오.

- VMware vCenter Server의 경우 vCenter Server에서 사용자 계정을 생성해야 합니다.

  자세한 내용은 VMware vCenter Server 설명서를 참조하십시오.

  > VMware PowerCLI를 설치해야 합니다. vCenter Server 데이터 소스에서만 워크플로우를 실행하려면 Unified Manager 서버를 데이터 소스로 설정하지 않아도 됩니다.

- VMware vCenter Server에서 들어오는 연결의 TCP 포트가 열려 있어야 합니다.

  기본 TCP 포트 번호는 443입니다. 자세한 내용은 방화벽 설명서를 참조하십시오.

이 절차를 사용하여 여러 Unified Manager 서버 데이터 소스를 WFA에 추가할 수 있습니다. 하지만 Unified Manager Server 6.3 이상을 WFA와 페어링하고 Unified Manager 서버에서 보호 기능을 사용하려는 경우에는 이 절차를 사용하지 않아야 합니다.

WFA를 Unified Manager Server 6.x와 페어링하는 방법에 대한 자세한 내용은 _OnCommand Unified Manager 온라인 도움말_을 참조하십시오.

> WFA를 사용하여 데이터 소스를 설정하는 동안에는 Active IQ Unified Manager 6.0, 6.1 및 6.2 데이터 소스 유형이 WFA 4.0 릴리즈에서 사용되지 않으며, 이러한 데이터 소스 유형은 이후 릴리즈에서 지원되지 않습니다.

단계

1. 웹 브라우저를 사용하여 WFA에 액세스합니다.
2. 설정 * 을 클릭하고 * 설정 * 에서 * 데이터 소스 * 를 클릭합니다.
3. 적절한 작업을 선택합니다.

대상...	수행할 작업...
새 데이터 원본을 만듭니다	을 클릭합니다 를 클릭합니다.
WFA를 업그레이드한 경우 복원된 데이터 소스를 편집합니다	기존 데이터 원본 항목을 선택하고 을 클릭합니다 를 클릭합니다.

   WFA에 Unified Manager 서버 데이터 소스를 추가한 다음 Unified Manager 서버 버전을 업그레이드한 경우, WFA에서 Unified Manager 서버의 업그레이드된 버전을 인식하지 못합니다. 이전 버전의 Unified Manager 서버를 삭제한 다음, 업그레이드된 버전의 Unified Manager 서버를 WFA에 추가해야 합니다.

4. 새 데이터 원본 대화 상자에서 필요한 데이터 원본 유형을 선택하고 데이터 원본 이름과 호스트 이름을 입력합니다.

   선택한 데이터 소스 유형에 따라 포트, 사용자 이름, 암호 및 시간 제한 필드가 가능한 경우 기본 데이터로 자동으로 채워질 수 있습니다. 필요에 따라 이러한 항목을 편집할 수 있습니다.

5. 적절한 작업 선택:

대상...	수행할 작업...
Active IQ Unified Manager 6.3 이상	Unified Manager 서버에서 생성한 데이터베이스 사용자 계정의 자격 증명을 입력합니다. 데이터베이스 사용자 계정 만들기에 대한 자세한 내용은 _OnCommand Unified Manager 온라인 도움말_을 참조하십시오. 명령줄 인터페이스 또는 ocsetup 도구를 사용하여 만든 Active IQ Unified Manager 데이터베이스 사용자 계정의 자격 증명을 제공해서는 안 됩니다.
VMware vCenter Server(Windows 전용)	(Windows만 해당) VMware vCenter Server에서 생성한 사용자의 사용자 이름과 암호를 입력합니다.

6. 저장 * 을 클릭합니다.
7. 데이터 원본 테이블에서 데이터 원본을 선택하고 을 클릭합니다 를 클릭합니다.
8. 데이터 획득 프로세스의 상태를 확인합니다.

업그레이드된 **Unified Manager** 서버를 데이터 소스로 추가합니다

Unified Manager 서버(5.x 또는 6.x)가 WFA에 데이터 소스로 추가된 경우 Unified Manager 서버가 업그레이드됩니다. 업그레이드된 버전과 연결된 데이터가 WFA에 채워지지 않기 때문에 데이터 소스로 수동으로 추가하지 않은 경우 업그레이드된 Unified Manager 서버를 데이터 소스로 추가해야 합니다.

단계

1. WFA 웹 GUI에 admin으로 로그인합니다.
2. 설정 * 을 클릭하고 * 설정 * 에서 * 데이터 소스 * 를 클릭합니다.
3. 을 클릭합니다 를 클릭합니다.
4. 새 데이터 원본 대화 상자에서 필요한 데이터 원본 형식을 선택한 다음 데이터 원본의 이름과 호스트 이름을 입력합니다.

   선택한 데이터 소스 유형에 따라 포트, 사용자 이름, 암호 및 시간 제한 필드가 가능한 경우 기본 데이터로 자동으로 채워질 수 있습니다. 필요에 따라 이러한 항목을 편집할 수 있습니다.

5. 저장 * 을 클릭합니다.
6. Unified Manager 서버의 이전 버전을 선택하고 을 클릭합니다 를 클릭합니다.
7. 데이터 원본 유형 삭제 확인 대화 상자에서 * 예 * 를 클릭합니다.
8. 데이터 원본 테이블에서 데이터 원본을 선택한 다음 을 클릭합니다 를 클릭합니다.
9. History(이력) 표에서 데이터 획득 상태를 확인합니다.

로컬 사용자를 생성합니다

OnCommand Workflow Automation(WFA)를 사용하여 게스트, 운영자, 승인자, 설계자, 권한 등 다양한 역할에 대한 특정 권한을 가진 로컬 WFA 사용자를 생성하고 관리할 수 관리, 백업.

WFA를 설치하고 관리자로 로그인해야 합니다.

WFA를 사용하여 다음 역할에 맞는 사용자를 생성할 수 있습니다.

- * 게스트 *

  이 사용자는 포털과 워크플로 실행 상태를 볼 수 있으며 워크플로 실행 상태의 변경 사항을 알릴 수 있습니다.

- * 연산자 *

  이 사용자는 사용자에게 액세스 권한이 부여된 워크플로우를 미리 보고 실행할 수 있습니다.

- * 승인자 *

  이 사용자는 사용자에게 액세스 권한이 부여된 워크플로우를 미리 보고, 실행, 승인 및 거부할 수 있습니다.

  > 승인자의 이메일 ID를 제공하는 것이 좋습니다. 승인자가 여러 개인 경우 * 이메일 * 필드에 그룹 이메일 ID를 제공할 수 있습니다.

- * 설계자 *

  이 사용자는 워크플로우를 생성할 수 있는 모든 액세스 권한을 가지고 있지만, 글로벌 WFA 서버 설정을 수정할 수 없습니다.

- * 관리자 *

  이 사용자는 WFA 서버에 완전히 액세스할 수 있습니다.

- * 백업 *

  WFA 서버의 백업을 원격으로 생성할 수 있는 유일한 사용자입니다. 그러나 사용자는 다른 모든 액세스로부터 제한됩니다.

단계

1. 설정 * 을 클릭하고 * 관리 * 에서 * 사용자 * 를 클릭합니다.
2. 를 클릭하여 새 사용자를 생성합니다 를 클릭합니다.
3. New User(새 사용자) 대화 상자에 필요한 정보를 입력합니다.
4. 저장 * 을 클릭합니다.

대상 시스템의 자격 증명을 구성합니다

WFA(OnCommand Workflow Automation)에서 타겟 시스템의 자격 증명을 구성하고 자격 증명을 사용하여 특정 시스템에 연결하고 명령을 실행할 수 있습니다.

초기 데이터 획득 후에는 명령을 실행할 어레이에 대한 자격 증명을 구성해야 합니다. PowerShell WFA 컨트롤러 연결은 다음 두 가지 모드에서 작동합니다.

- 자격 증명을 사용합니다

  WFA는 먼저 HTTPS를 사용하여 연결을 설정한 다음 HTTP를 사용하려고 합니다. 또한 Microsoft Active Directory LDAP 인증을 사용하여 WFA에 자격 증명을 정의하지 않고 어레이에 연결할 수 있습니다. Active Directory LDAP를 사용하려면 동일한 Active Directory LDAP 서버에서 인증을 수행하도록 어레이를 구성해야 합니다.

- 자격 증명 없음(7-Mode로 운영되는 스토리지 시스템의 경우)

  WFA는 도메인 인증을 사용하여 연결을 시도합니다. 이 모드는 NTLM 프로토콜을 사용하여 보호되는 원격 프로시저 호출 프로토콜을 사용합니다.

- WFA는 ONTAP 시스템용 SSL(Secure Sockets Layer) 인증서를 확인합니다. SSL 인증서를 신뢰할 수 없는 경우 ONTAP 시스템에 대한 연결을 검토 및 수락/거부하라는 메시지가 사용자에게 표시될 수 있습니다.
- 백업을 복원하거나 전체 업그레이드를 완료한 후 ONTAP, NetApp Active IQ 및 LDAP(Lightweight Directory Access Protocol)에 대한 자격 증명을 다시 입력해야 합니다.

단계

1. 웹 브라우저를 통해 admin으로 WFA에 로그인합니다.
2. 설정 * 을 클릭하고 * 설정 * 에서 * 자격 증명 * 을 클릭합니다.
3. 을 클릭합니다 를 클릭합니다.
4. 새 자격 증명 대화 상자의 * 일치 * 목록에서 다음 옵션 중 하나를 선택합니다.

   - * 정확히 일치 *

     특정 IP 주소 또는 호스트 이름에 대한 자격 증명

   - * 패턴 *

     전체 서브넷 또는 IP 범위에 대한 자격 증명

     이 옵션에서는 정규식 구문 사용이 지원되지 않습니다.

5. Type * 목록에서 원격 시스템 유형을 선택합니다.
6. 리소스의 호스트 이름 또는 IPv4 또는 IPv6 주소, 사용자 이름 및 암호를 입력합니다.

   WFA 5.1은 WFA에 추가된 모든 리소스의 SSL 인증서를 검증합니다. 인증서 확인 시 인증서를 수락하라는 메시지가 표시될 수 있으므로 자격 증명에서 와일드카드를 사용하는 것은 지원되지 않습니다. 동일한 자격 증명을 사용하는 클러스터가 여러 개인 경우 한 번에 모두 추가할 수 없습니다.

7. 다음 작업을 수행하여 연결을 테스트합니다.

다음 일치 유형을 선택한 경우...	그러면...
• 정확히 일치 *	Test * 를 클릭합니다.
• 패턴 *	자격 증명을 저장하고 다음 중 하나를 선택합니다. • 자격 증명을 선택하고 을 클릭합니다 를 클릭합니다. • 마우스 오른쪽 버튼을 클릭하고 * Test Connectivity * 를 선택합니다.

8. 저장 * 을 클릭합니다.

OnCommand Workflow Automation 구성

OnCommand Workflow Automation(WFA)를 사용하여 AutoSupport, 알림 등의 다양한 설정을 구성할 수 있습니다.

WFA를 구성할 때 필요에 따라 다음 중 하나 이상을 설정할 수 있습니다.

- AutoSupport - 기술 지원 부서에 AutoSupport 메시지를 보냅니다
- WFA 사용자에 대한 LDAP 인증 및 인증을 위한 Microsoft Active Directory LDAP(Lightweight Directory Access Protocol) 서버
- 워크플로 작업 및 AutoSupport 메시지 전송에 대한 이메일 알림을 위한 메일입니다
- 워크플로우 작업에 대한 알림을 위한 SNMP(Simple Network Management Protocol
- 원격 데이터 로깅을 위한 syslog

AutoSupport를 구성합니다

일정, AutoSupport 메시지 내용 및 프록시 서버와 같은 여러 AutoSupport 설정을 구성할 수 있습니다. AutoSupport는 사용자가 선택한 콘텐츠의 주간 로그를 기술 지원 부서에 전송하여 보관 및 문제 분석을 수행합니다.

단계

1. 웹 브라우저를 통해 admin으로 WFA에 로그인합니다.
2. 설정 * 을 클릭하고 * 설정 * 에서 * AutoSupport * 를 클릭합니다.
3. AutoSupport 사용 * 상자가 선택되어 있는지 확인합니다.
4. 필요한 정보를 입력합니다.
5. 컨텐츠 * 목록에서 다음 중 하나를 선택합니다.

포함하려는 경우...	그런 다음 이 옵션을 선택하십시오...
WFA 설치의 사용자, 워크플로우, 명령과 같은 구성 세부 정보만 제공됩니다	'설정 데이터 종료
WFA 구성 세부 정보 및 데이터를 스키마와 같은 WFA 캐시 테이블에 저장	'설정 및 캐시 데이터 종료'(기본값)
WFA 구성 세부 정보, WFA 캐시 표의 데이터 및 설치 디렉터리의 데이터	'최종 구성 및 캐시 확장 데이터

WFA 사용자의 암호는 AutoSupport 데이터에 _NOT_포함되어 있습니다.

6. AutoSupport 메시지를 다운로드할 수 있는지 테스트합니다.
   a. 다운로드 * 를 클릭합니다.
   b. 대화 상자가 열리면 .7z 파일을 저장할 위치를 선택합니다.
7. 지금 보내기 * 를 클릭하여 지정된 대상으로 AutoSupport 메시지 전송을 테스트합니다.
8. 저장 * 을 클릭합니다.

인증 설정을 구성합니다

인증 및 승인을 위해 Microsoft Active Directory(AD) LDAP(Lightweight Directory Access Protocol) 서버를 사용하도록 WFA(OnCommand Workflow Automation)를 구성할 수 있습니다.

사용자 환경에서 Microsoft AD LDAP 서버를 구성해야 합니다.

WFA에는 Microsoft AD LDAP 인증만 지원됩니다. Microsoft AD LDS(Lightweight Directory Services) 또는 Microsoft Global Catalog를 비롯한 다른 LDAP 인증 방법은 사용할 수 없습니다.

통신 중에 LDAP는 사용자 이름과 암호를 일반 텍스트로 보냅니다. 그러나 LDAPS(LDAP 보안) 통신은 암호화되어 안전하게 보호됩니다.

단계

1. 웹 브라우저를 통해 admin으로 WFA에 로그인합니다.
2. 설정 * 을 클릭하고 * 설정 * 에서 * 인증 * 을 클릭합니다.
3. Active Directory* 활성화 확인란을 선택합니다.
4. 필드에 필수 정보를 입력합니다.
   a. 도메인 사용자에 대해 user@domain 형식을 사용하려면 sAMAccountName을 * 사용자 이름 특성 * 필드의 userPrincipalName으로 바꿉니다.
   b. 환경에 고유한 값이 필요한 경우 필수 필드를 편집합니다.
   c. AD 서버 URI를 'LDAP://active_directory_server_address\[:port\]'와 같이 입력한다

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

SSL을 통해 LDAP를 활성화한 경우 'LDAPS://active_directory_server_address\[:port\]'라는 URI 형식을 사용할 수 있습니다

a. 필요한 역할에 필요한 AD 그룹 이름 목록을 추가합니다.

> Active Directory 그룹 창에서 필요한 역할에 AD 그룹 이름 목록을 추가할 수 있습니다.

5. 저장 * 을 클릭합니다.
6. 어레이에 대한 LDAP 연결이 필요한 경우 WFA 서비스를 필요한 도메인 사용자로 로그온하도록 구성합니다.
   a. services.msc를 사용하여 Windows 서비스 콘솔을 엽니다.
   b. NetApp WFA Server * 서비스를 두 번 클릭합니다.
   c. NetApp WFA Server 속성 대화 상자에서 * 로그온 * 탭을 클릭한 다음 * 이 계정 * 을 선택합니다.
   d. 도메인 사용자 이름과 암호를 입력한 다음 * 확인 * 을 클릭합니다.

Active Directory 그룹을 추가합니다

WFA(OnCommand Workflow Automation)에서 Active Directory 그룹을 추가할 수 있습니다.

단계

1. 웹 브라우저를 통해 admin으로 WFA에 로그인합니다.
2. 설정 * 을 클릭하고 * 관리 * 에서 * Active Directory 그룹 * 을 클릭합니다.
3. Active Directory 그룹 창에서 * 새 * 아이콘을 클릭합니다.
4. 새 Active Directory 그룹 대화 상자에서 필요한 정보를 입력합니다.

   역할 * 드롭다운 목록에서 * 승인자 * 를 선택한 경우 승인자의 이메일 ID를 제공하는 것이 좋습니다. 승인자가 여러 개인 경우 * 이메일 * 필드에 그룹 이메일 ID를 제공할 수 있습니다. 알림을 특정 Active Directory 그룹으로 보낼 워크플로의 다른 이벤트를 선택합니다.

5. 저장 * 을 클릭합니다.

이메일 알림을 구성합니다

WFA(OnCommand Workflow Automation)를 구성하여 워크플로우 작업(예: 워크플로우 시작 또는 워크플로우 실패)에 대한 이메일 알림을 보낼 수 있습니다.

사용자 환경에서 메일 호스트를 구성해야 합니다.

단계

1. 웹 브라우저를 통해 admin으로 WFA에 로그인합니다.
2. 설정 * 을 클릭하고 * 설정 * 에서 * 메일 * 을 클릭합니다.
3. 필드에 필수 정보를 입력합니다.
4. 다음 단계를 수행하여 메일 설정을 테스트합니다.

a. 테스트 메일 보내기 * 를 클릭합니다.
b. 연결 테스트 대화 상자에서 전자 메일을 보낼 전자 메일 주소를 입력합니다.
c. Test * 를 클릭합니다.

5. 저장 * 을 클릭합니다.

SNMP를 구성합니다

WFA(OnCommand Workflow Automation)를 구성하여 워크플로우 작업의 상태에 대한 SNMP(Simple Network Management Protocol) 트랩을 보낼 수 있습니다.

WFA는 이제 SNMP v1 및 SNMP v3 프로토콜을 지원합니다. SNMP v3은 추가 보안 기능을 제공합니다.

WFA.MIB 파일에는 WFA 서버에서 보낸 트랩에 대한 정보가 들어 있습니다. MIB 파일은 WFA 서버의 <WFA_install_location>\WFA\bin\WFA.mib 디렉토리에 있습니다.

> WFA 서버는 범용 개체 식별자(1.3.6.1.4.1.789.1.1.12.0)가 있는 모든 트랩 알림을 보냅니다.

SNMP 구성에 community_string@snmp_host와 같은 SNMP 커뮤니티 문자열을 사용할 수 없습니다.

SNMP 버전 1을 구성합니다

단계

1. 웹 브라우저를 통해 WFA에 admin 사용자로 로그인한 다음 WFA 서버에 액세스합니다.
2. 설정 * 을 클릭하고 * 설정 * 에서 * SNMP * 를 클릭합니다.
3. SNMP 사용 * 확인란을 선택합니다.
4. 버전 드롭다운 목록에서 * 버전 1*을 선택합니다.
5. IPv4 또는 IPv6 주소 또는 호스트 이름 및 관리 호스트의 포트 번호를 입력합니다.

   WFA는 SNMP 트랩을 지정된 포트 번호로 보냅니다. 기본 포트 번호는 162입니다.

6. 알림 설정 섹션에서 다음 확인란 중 하나 이상을 선택합니다.
   - 워크플로 실행이 시작되었습니다
   - 워크플로 실행이 성공적으로 완료되었습니다
   - 워크플로 실행에 실패했거나 부분적으로 성공했습니다
   - 승인을 기다리는 워크플로 실행
   - 획득 실패
7. 테스트 알림 전송 * 을 클릭하여 설정을 확인합니다.
8. 저장 * 을 클릭합니다.

SNMP 버전 3을 구성합니다

WFA(OnCommand Workflow Automation)를 구성하여 워크플로우 작업의 상태에 대한 SNMP(Simple Network Management Protocol) 버전 3 트랩을 보낼 수도 있습니다.

버전 3은 두 가지 추가 보안 옵션을 제공합니다.

- 버전 3(인증 포함)

  트랩은 네트워크를 통해 암호화되지 않은 상태로 전송됩니다. SNMP 트랩 메시지와 동일한 인증 매개 변수로 구성된 SNMP 관리 애플리케이션은 트랩을 수신할 수 있습니다.

- 버전 3(인증 및 암호화 포함)

  트랩은 네트워크를 통해 암호화됩니다. 이러한 트랩을 수신하고 해독하려면 SNMP 트랩과 동일한 인증 매개 변수와 암호화 키를 사용하여 SNMP 관리 애플리케이션을 구성해야 합니다.

단계

1. 웹 브라우저를 통해 WFA에 admin 사용자로 로그인한 다음 WFA 서버에 액세스합니다.
2. 설정 * 을 클릭하고 * 설정 * 에서 * SNMP * 를 클릭합니다.
3. SNMP 사용 * 확인란을 선택합니다.
4. 버전 * 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
   - 버전 3
   - 버전 3(인증 포함)
   - 버전 3(인증 및 암호화 포함)
5. 4단계에서 선택한 특정 SNMP 버전 3 옵션에 해당하는 SNMP 구성 옵션을 선택합니다.
6. IPv4 또는 IPv6 주소 또는 호스트 이름 및 관리 호스트의 포트 번호를 입력합니다. WFA는 SNMP 트랩을 지정된 포트 번호로 보냅니다. 기본 포트 번호는 162입니다.
7. 알림 설정 섹션에서 다음 확인란 중 하나 이상을 선택합니다.
   - 워크플로 계획이 시작/실패/완료되었습니다
   - 워크플로 실행이 시작되었습니다
   - 워크플로 실행이 성공적으로 완료되었습니다
   - 워크플로 실행에 실패했거나 부분적으로 성공했습니다
   - 승인을 기다리는 워크플로 실행
   - 획득 실패
8. 테스트 알림 전송 * 을 클릭하여 설정을 확인합니다.
9. 저장 * 을 클릭합니다.

Syslog를 구성합니다

이벤트 로깅 및 로그 정보 분석과 같은 목적으로 특정 Syslog 서버로 로그 데이터를 보내도록 OnCommand Workflow Automation(WFA)를 구성할 수 있습니다.

Syslog 서버가 WFA 서버의 데이터를 수락하도록 구성해야 합니다.

단계

1. 웹 브라우저를 통해 admin으로 WFA에 로그인합니다.
2. 설정 * 을 클릭하고 * 유지 관리 * 에서 * Syslog * 를 클릭합니다.
3. Syslog * 활성화 확인란을 선택합니다.
4. Syslog 호스트 이름을 입력하고 Syslog 로그 수준을 선택합니다.
5. 저장 * 을 클릭합니다.

원격 시스템에 연결하기 위한 프로토콜을 구성합니다

WFA(OnCommand Workflow Automation)에서 원격 시스템에 연결하는 데 사용하는 프로토콜을 구성할 수 있습니다. 조직의 보안 요구 사항 및 원격 시스템에서 지원하는 프로토콜을 기반으로 프로토콜을 구성할 수 있습니다.

단계

1. 웹 브라우저를 통해 admin으로 WFA에 로그인합니다.
2. 데이터 소스 디자인 * > * 원격 시스템 유형 * 을 클릭합니다.
3. 다음 작업 중 하나를 수행합니다.

원하는 작업	수행할 작업...
새 원격 시스템에 대한 프로토콜을 구성합니다	a. 을 클릭합니다 . b. 새 원격 시스템 유형 대화 상자에서 이름, 설명 및 버전과 같은 세부 정보를 지정합니다.
기존 원격 시스템의 프로토콜 구성을 수정합니다	a. 수정할 원격 시스템을 선택하고 두 번 클릭합니다. b. 을 클릭합니다 .

4. 연결 프로토콜 목록에서 다음 중 하나를 선택합니다.
   - HTTP(기본값)로 폴백하는 HTTPS
   - HTTPS만 해당
   - HTTP만 해당
   - 맞춤형
5. 프로토콜, 기본 포트 및 기본 시간 제한에 대한 세부 정보를 지정합니다.
6. 저장 * 을 클릭합니다.

기본 암호 정책을 사용하지 않도록 설정합니다

WFA(OnCommand Workflow Automation)는 로컬 사용자에 대해 암호 정책을 적용하도록 구성되어 있습니다. 암호 정책을 사용하지 않으려면 사용하지 않도록 설정할 수 있습니다.

WFA 호스트 시스템에 admin으로 로그인해야 합니다.

기본 WFA 설치 경로가 이 절차에 사용됩니다. 설치 중에 기본 위치를 변경한 경우 변경된 WFA 설치 경로를 사용해야 합니다.

단계

1. Windows 탐색기를 열고 'WFA_INSTALL_LOCATION\WFA\BIN\.'으로 이동합니다
2. PS.cmd 파일을 두 번 클릭합니다.

   ONTAP 및 WFA 모듈이 로드되면 PowerShell CLI(Command-Line Interface) 프롬프트가 열립니다.

3. 프롬프트에서 다음을 입력합니다.

   Set-WfaConfig-Name PasswordPolicy - Enable $false

4. 메시지가 표시되면 WFA 서비스를 다시 시작합니다.

Windows의 기본 암호 정책을 수정합니다

OnCommand Workflow Automation(WFA)에서는 로컬 사용자에 대한 암호 정책을 적용합니다. 기본 암호 정책을 수정하여 요구 사항에 따라 암호를 설정할 수 있습니다.

WFA 호스트 시스템에 루트 사용자로 로그인해야 합니다.

- 기본 WFA 설치 경로가 이 절차에 사용됩니다.

  설치 중에 기본 위치를 변경한 경우 사용자 지정 WFA 설치 경로를 사용해야 합니다.

- 기본 암호 정책을 수정하기 위한 명령은.\WFA—password-policy=default입니다.

  기본 설정은 " minLength=true,8; specialChar=true,1; digitalChar=true,1; lowercaseChar=true,1; uppercaseChar=true,1; white espaceChar=false" 입니다. 기본 암호 정책에 대한 이 설정에 따라 암호는 최소 8자의 길이여야 하며, 특수 문자, 숫자, 소문자 및 대문자를 하나 이상 포함해야 하며 공백을 포함할 수 없습니다.

단계

1. 명령 프롬프트에서 WFA 서버의 다음 디렉토리로 이동합니다.

   'WFA_INSTALL_LOCATION/WFA/BIN/

2. 기본 암호 정책을 수정합니다.

   '.\WFA—password-policy=PasswordPolicyString—restart=WFA'입니다

Windows에서 OnCommand Workflow Automation 데이터베이스에 대한 원격 액세스를 설정합니다

기본적으로 WFA(OnCommand Workflow Automation) 데이터베이스는 WFA 호스트 시스템에서 실행 중인 클라이언트에서만 액세스할 수 있습니다. 원격 시스템에서 WFA 데이터베이스에 액세스하려는 경우 기본 설정을 변경할 수 있습니다.

- WFA 호스트 시스템에 admin 사용자로 로그인해야 합니다.
- WFA 호스트 시스템에 방화벽이 설치되어 있는 경우, 원격 시스템에서 액세스할 수 있도록 방화벽 설정을 구성해야 합니다.

기본 WFA 설치 경로가 이 절차에 사용됩니다. 설치 중에 기본 위치를 변경한 경우 사용자 지정 WFA 설치 경로를 사용해야 합니다.

단계

1. Windows 탐색기를 열고 WFA_INSTALL_LOCATION\WFA\BIN 디렉터리로 이동합니다
2. 다음 작업 중 하나를 수행합니다.

대상...	다음 명령을 입력합니다...
원격 액세스를 설정합니다	'.\WFA—db-access=public—restart'를 선택합니다
원격 액세스를 해제합니다	'.\WFA—db-access=default—restart'를 선택합니다

호스트에서 **OnCommand Workflow Automation**의 액세스 권한을 제한합니다

기본적으로 WFA(OnCommand Workflow Automation)는 호스트 시스템의 관리자로 워크플로우를 실행합니다. 기본 설정을 변경하여 호스트 시스템에 대한 WFA 권한을 제한할 수 있습니다.

WFA 호스트 시스템에 admin으로 로그인해야 합니다.

단계

1. 소켓을 열고 WFA 홈 디렉토리에 쓸 수 있는 권한이 있는 새 Windows 사용자 계정을 생성합니다.
2. services.msc를 사용하여 Windows 서비스 콘솔을 열고 * NetApp WFA Database * 를 두 번 클릭합니다.
3. Log On * 탭을 클릭합니다.
4. 이 계정 * 을 선택하고 생성한 새 사용자의 자격 증명을 입력한 다음 * 확인 * 을 클릭합니다.
5. NetApp WFA Server * 를 두 번 클릭합니다.
6. Log On * 탭을 클릭합니다.
7. 이 계정 * 을 선택하고 생성한 새 사용자의 자격 증명을 입력한 다음 * 확인 * 을 클릭합니다.
8. NetApp WFA 데이터베이스 * 및 * NetApp WFA Server * 서비스를 다시 시작합니다.

OnCommand Workflow Automation의 트랜잭션 제한 시간 설정을 수정합니다

WFA(OnCommand Workflow Automation) 데이터베이스 트랜잭션 시간이 기본적으로 300초 후에 로그아웃됩니다. 대용량 WFA 데이터베이스를 백업에서 복원할 때 기본 시간 초과 기간을

늘려 데이터베이스 복원의 잠재적 오류를 방지할 수 있습니다.

WFA 호스트 시스템에 admin으로 로그인해야 합니다.

기본 WFA 설치 경로가 이 절차에 사용됩니다. 설치 중에 기본 위치를 변경한 경우 변경된 WFA 설치 경로를 사용해야 합니다.

단계

1. Windows 탐색기를 열고 다음 디렉토리로 이동합니다.

   'WFA_INSTALL_LOCATION\WFA\BIN'

2. PS.cmd 파일을 두 번 클릭합니다.

   ONTAP 및 WFA 모듈이 로드되면 PowerShell CLI(Command-Line Interface) 프롬프트가 열립니다.

3. 프롬프트에서 다음을 입력합니다.

   'Set-WfaConfig-Name TransactionTimeOut-Seconds NumericValue'

   세트 WfaConfig-이름 TransactionTimeOut-Seconds 1000

4. 메시지가 표시되면 WFA 서비스를 다시 시작합니다.

Workflow Automation의 시간 초과 값을 구성합니다

기본 시간 초과 값을 사용하지 않고 WFA(Workflow Automation) 웹 GUI에 대한 시간 초과 값을 구성할 수 있습니다.

WFA 웹 GUI의 기본 시간 초과 값은 180분입니다. CLI를 통해 요구 사항에 맞게 시간 초과 값을 구성할 수 있습니다. WFA 웹 GUI에서 시간 초과 값을 설정할 수 없습니다.

> 설정한 시간 초과 값은 비활성 관련 시간 초과가 아니라 절대 시간 초과입니다. 예를 들어 이 값을 30분으로 설정하면 이 시간이 끝날 때 활성 상태인 경우에도 30분 후에 로그아웃됩니다.

단계

1. WFA 호스트 시스템에 관리자로 로그인합니다.
2. 시간 초과 값을 설정합니다.

   'installdir bin/WFA-S = 시간 초과 값(분)'

암호화 활성화 및 새 암호 추가

OnCommand Workflow Automation 5.1은 여러 가지 암호를 즉시 지원합니다. 또한 필요에 따라 추가 암호를 추가할 수도 있습니다.

다음 사이퍼를 즉시 활성화할 수 있습니다.

```
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"
```

이 설정에 'tandalone-full.xml' 파일에서 추가 cipherer를 추가할 수 있다. 이 파일은 '<installdir>/jboss/standalone/configuration/standalone-full.xml'에 있습니다.

다음과 같이 추가 암호를 지원하도록 파일을 수정할 수 있습니다.

```
<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"/>
```