



設定 OnCommand Workflow Automation 功能

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

目錄

設定OnCommand Workflow Automation 功能	1
存取OnCommand Workflow Automation 功能	1
資料來源OnCommand Workflow Automation	1
建立本機使用者	6
設定目標系統的認證資料	7
設定OnCommand Workflow Automation 功能	8
停用預設密碼原則	14
修改Windows的預設密碼原則	14
可在OnCommand Workflow Automation Windows上遠端存取效能不整資料庫	15
限制OnCommand Workflow Automation 主機上的存取權限	15
修改OnCommand Workflow Automation 資訊的交易逾時設定	16
設定Workflow Automation的逾時值	16
啟用密碼並新增密碼	17

設定OnCommand Workflow Automation 功能

完成OnCommand Workflow Automation 安裝完整套功能（WFA）之後、您必須完成數項組態設定。您必須存取WFA、設定使用者、設定資料來源、設定認證、以及設定WFA。

存取OnCommand Workflow Automation 功能

您可以OnCommand Workflow Automation 從任何可存取WFA伺服器的系統、透過網頁瀏覽器存取功能。

您必須安裝適用於網頁瀏覽器的Adobe Flash Player。

步驟

1. 開啟網頁瀏覽器、然後在網址列中輸入下列其中一項：

- https://wfa_server_ip+

WFA_server_IP是WFA伺服器的IP位址（IPv4或IPv6位址）或完整網域名稱（FQDN）。

- 如果您正在WFA伺服器上存取WFA：`https://localhost/wfa`如果您已為WFA指定非預設連接埠、則必須包含下列連接埠號碼：

- https://wfa_server_ip:port+

- <https://localhost:port+> 連接埠是您在安裝期間用於WFA伺服器的TCP連接埠號碼。

2. 在「登入」區段中、輸入您在安裝期間輸入的管理員使用者認證。
3. 在*設定*>*設定*功能表中、設定認證資料和資料來源。
4. 將WFA Web GUI加入書籤、以方便存取。

資料來源OnCommand Workflow Automation

WFA（WFA）可針對從資料來源取得的資料運作。OnCommand Workflow Automation各種版本Active IQ Unified Manager 的VMware vCenter Server均以預先定義的WFA資料來源類型提供。在設定資料來源進行資料擷取之前、您必須先瞭解預先定義的資料來源類型。

資料來源是唯讀的資料結構、可作為特定資料來源類型之資料來源物件的連線。例如、資料來源可以是Active IQ Unified Manager 連接到Active IQ Unified Manager 某個含有還原6.3資料來源類型的還原資料庫。您可以在定義所需的資料來源類型之後、將自訂資料來源新增至WFA。

如需預先定義資料來源類型的詳細資訊、請參閱互通性對照表。

相關資訊

["NetApp 互通性對照表工具"](#)

在DataFabric Manager上設定資料庫使用者

您必須在DataFabric Manager 5.x上建立資料庫使用者、才能將DataFabric Manager 5.x資料庫的唯讀存取權設定為OnCommand Workflow Automation 僅供參考。

在Windows上執行ocsetup來設定資料庫使用者

您可以在DataFabric Manager 5.x伺服器上執行ocsetup檔案、將DataFabric Manager 5.x資料庫的唯讀存取設定為OnCommand Workflow Automation 還原。

步驟

1. 從下列位置將wfa_ocsetup.exe檔案下載至DataFabric Manager 5.x伺服器的目錄：
https://WFA_Server_ip/download/WFA_ocsetup.exe。

_WFA_Server_IP_是WFA伺服器的IP位址（IPv4或IPv6位址）。

如果您已為WFA指定非預設連接埠、則必須包含下列連接埠號碼：
https://WFA_server_ip:port/download/WFA_ocsetup.exe。

_port_是您在安裝期間用於WFA伺服器的TCP連接埠號碼。

如果要指定IPv6位址、則必須以方括弧括住。

2. 按兩下wfa_ocsetup.exe檔案。
3. 閱讀安裝精靈中的資訊、然後按「下一步」。
4. 瀏覽或鍵入OpenJDK*位置、然後按「下一步」。
5. 輸入使用者名稱和密碼以覆寫預設認證。

系統會建立新的資料庫使用者帳戶、以存取DataFabric Manager 5.x資料庫。



如果您未建立使用者帳戶、則會使用預設認證資料。為了安全起見、您必須建立使用者帳戶。

6. 單擊* Next*（下一步）並查看結果。
7. 按一下「下一步」、然後按一下「完成」以完成精靈。

在Linux上執行ocsetup來設定資料庫使用者

您可以在DataFabric Manager 5.x伺服器上執行ocsetup檔案、將DataFabric Manager 5.x資料庫的唯讀存取設定為OnCommand Workflow Automation 還原。

步驟

1. 使用終端機中的下列命令、將wfa_ocsetup.sh檔案下載到DataFabric Manager 5.x伺服器上的主目錄：

wGet https://WFA_Server_IP/download/wfa_ocsetup.sh+

WFA_Server_IP是WFA伺服器的IP位址（IPv4或IPv6位址）。

如果您已為WFA指定非預設連接埠、則必須包含下列連接埠號碼：

wGet https://wfa_server_ip:port/download/wfa_ocsetup.sh+

連接埠是您在安裝期間用於WFA伺服器的TCP連接埠號碼。

如果要指定IPv6位址、則必須以方括弧括住。

2. 在終端機中使用下列命令、將wfa_ocsetup.sh檔案變更為執行檔：「chmod+x wfa_ocsetup.sh」
3. 在終端機中輸入下列命令來執行指令碼：

```
wfa_ocsetup.sh OpenJDK_path'
```

OpenJDK_path是OpenJDK.

```
/opt/NTAPdfm/java
```

終端機中會顯示下列輸出、表示設定成功：

```
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. 輸入使用者名稱和密碼以覆寫預設認證。

系統會建立新的資料庫使用者帳戶、以存取DataFabric Manager 5.x資料庫。



如果您未建立使用者帳戶、則會使用預設認證資料。為了安全起見、您必須建立使用者帳戶。

終端機中會顯示下列輸出、表示設定成功：

```
***** 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 上設定資料庫使用者

您必須在Active IQ Unified Manager 還原上建立資料庫使用者、才能將Active IQ Unified Manager 僅讀取的功能設定為OnCommand Workflow Automation 僅供參考。

步驟

1. 使用系統管理員認證登入Active IQ Unified Manager 到解決方法。
2. 按一下「設定>*使用者*」。
3. 按一下「新增使用者」。
4. 選擇*資料庫使用者*作為使用者類型。

應在OnCommand Workflow Automation 使用相同使用者的情況下使用此功能、同時在Active IQ Unified Manager 功能上加入功能不一致的功能、作為OnCommand Workflow Automation 資料來源。

設定資料來源

您必須與OnCommand Workflow Automation 資料來源（WFA）建立連線、才能從資料來源取得資料。

- 若為Active IQ Unified Manager 更新版本的版本、您必須在Unified Manager伺服器上建立資料庫使用者帳戶。

如OnCommand 需詳細資訊、請參閱_《》統一化管理程式線上說明。

- Unified Manager伺服器上傳入連線的TCP連接埠必須開啟。

如需詳細資訊、請參閱防火牆上的文件。

以下是預設的TCP連接埠號碼：

TCP連接埠號碼	Unified Manager伺服器版本	說明
3306.	6.x	MySQL資料庫伺服器

- 對於Performance Advisor、您必須已建立Active IQ Unified Manager 一個角色最低為GlobalRead的不適用使用者帳戶。

如OnCommand 需詳細資訊、請參閱_《》統一化管理程式線上說明。

- 對於VMware vCenter Server、您必須在vCenter Server上建立使用者帳戶。

如需詳細資料、請參閱VMware vCenter Server文件。



您必須安裝VMware PowerCLI。如果您只想在vCenter Server資料來源上執行工作流程、則不需要將Unified Manager伺服器設定為資料來源。

- 必須開啟VMware vCenter Server上傳入連線的TCP連接埠。

預設的TCP連接埠號碼為443。如需詳細資訊、請參閱防火牆上的文件。

您可以使用此程序將多個Unified Manager伺服器資料來源新增至WFA。不過、如果您想要將Unified Manager 6.3及更新版本的伺服器與WFA配對、並使用Unified Manager伺服器中的保護功能、則不得使用此程序。



如需將WFA與Unified Manager伺服器6.x配對的詳細資訊、請參閱_《EWS Unified OnCommand Manager線上說明》_。



在使用WFA設定資料來源時、您必須注意Active IQ Unified Manager 到WFA 4.0版本中不支援使用的是NetApp 6.0、6.1和6.2資料來源類型、而且未來版本將不支援這些資料來源類型。

步驟

1. 使用網頁瀏覽器存取WFA。
2. 按一下「設定」、然後在「設定」下按一下「資料來源」。
3. 選擇適當的行動：

至...	執行此動作...
建立新的資料來源	按一下  在工具列上。
如果您已升級WFA、請編輯還原的資料來源	選取現有的資料來源項目、然後按一下  在工具列上。


如果您已將Unified Manager伺服器資料來源新增至WFA、然後升級Unified Manager伺服器版本、WFA將無法辨識Unified Manager伺服器的升級版本。您必須刪除舊版Unified Manager伺服器、然後將升級版Unified Manager伺服器新增至WFA。

4. 在「新增資料來源」對話方塊中、選取所需的資料來源類型、然後輸入資料來源名稱和主機名稱。

根據選取的資料來源類型、連接埠、使用者名稱、密碼和逾時欄位可能會自動填入預設資料（如果有）。您可以視需要編輯這些項目。

5. 選擇適當的行動：


適用於...	執行此動作...
不含更新版本Active IQ Unified Manager	<p>輸入您在Unified Manager伺服器上建立的資料庫使用者帳戶認證。如OnCommand 需建立資料庫使用者帳戶的詳細資訊、請參閱_《Unified Manager線上說明》_。</p> <div><p>您不得提供Active IQ Unified Manager 使用命令列介面或ocsetup 工具所建立之「現象資料庫使用者」帳戶的認證資料。</p></div>
VMware vCenter Server（僅適用於Windows）	（僅限Windows）輸入您在VMware vCenter伺服器上建立的使用者名稱和密碼。

6. 按一下「* 儲存 *」。
7. 在「資料來源」表格中、選取資料來源、然後按一下  在工具列上。
8. 驗證資料擷取程序的狀態。



新增升級的Unified Manager伺服器做為資料來源

如果Unified Manager伺服器（5.x或6.x）新增為WFA的資料來源、則Unified Manager伺服器會升級、您必須將升級後的Unified Manager伺服器新增為資料來源、因為除非手動新增為資料來源、否則與升級版本相關的資料不會填入WFA中。

步驟

1. 以管理員身分登入WFA Web GUI。
2. 按一下「設定」、然後在「設定」下、按一下「資料來源」。
3. 按一下  在工具列上。
4. 在「新增資料來源」對話方塊中、選取所需的資料來源類型、然後輸入資料來源名稱和主機名稱。

根據選取的資料來源類型、連接埠、使用者名稱、密碼和逾時欄位可能會自動填入預設資料（如果有）。您可以視需要編輯這些項目。

5. 按一下「* 儲存 *」。
6. 選取舊版Unified Manager伺服器、然後按一下  在工具列上。
7. 在刪除資料來源類型確認對話方塊中、按一下*是*。
8. 在「資料來源」表格中、選取資料來源、然後按一下  在工具列上。
9. 在History（歷史記錄）表中驗證資料擷取狀態。

建立本機使用者

利用NetApp（WFA）、您可以建立及管理具有各種角色特定權限的本機WFA使用者、例如來賓、營運者、核准者、架構設計師、OnCommand Workflow Automation 管理與備份：

您必須安裝WFA並以管理員身分登入。

WFA可讓您為下列角色建立使用者：

- 來賓

此使用者可檢視入口網站及工作流程執行狀態、並可收到工作流程執行狀態變更的通知。

- 營運者

此使用者可預覽及執行使用者有權存取的工作流程。

- 核准人

此使用者可預覽、執行、核准及拒絕使用者有權存取的工作流程。



建議提供核准者的電子郵件ID。如果有多位核准者、您可以在*電子郵件*欄位中提供群組電子郵件ID。

- 架構設計師

此使用者擁有建立工作流程的完整存取權、但受到限制、無法修改全域WFA伺服器設定。


- 管理

此使用者可完整存取WFA伺服器。

- 備份

這是唯一能夠遠端產生WFA伺服器備份的使用者。但是、使用者受到限制、無法存取所有其他存取。

步驟

1. 按一下「設定」、然後在「管理」下按一下「使用者」。
2. 按一下以建立新使用者  在工具列上。
3. 在「新使用者」對話方塊中輸入必要資訊。
4. 按一下「* 儲存 *」。

設定目標系統的認證資料

您可以在OnCommand Workflow Automation WFA (WFA) 中設定目標系統的認證、並使用認證來連線至該特定系統並執行命令。

在初次取得資料之後、您必須為執行命令的陣列設定認證資料。PowerShell WFA控制器連線可在兩種模式下運作：

- 憑證


WFA會先嘗試使用HTTPS建立連線、然後嘗試使用HTTP。您也可以使用Microsoft Active Directory LDAP驗證連線至陣列、而無需在WFA中定義認證。若要使用Active Directory LDAP、您必須將陣列設定為使用相同的Active Directory LDAP伺服器執行驗證。

- 無認證 (適用於以7-Mode運作的儲存系統)

WFA會嘗試使用網域驗證來建立連線。此模式使用遠端程序呼叫傳輸協定、此通訊協定是以NTLM傳輸協定來保護。

- WFA會檢查適用於ONTAP 各種系統的安全通訊端層 (SSL) 認證。如果SSL憑證不受信任、系統可能會提示使用者審查及接受/拒絕ONTAP 與該系統的連線。
- 還原備份或完成就地升級後、您必須重新輸入ONTAP 適用於NetApp Active IQ 的身分證明、NetApp的支援和輕量型目錄存取傳輸協定 (LDAP)。

步驟

1. 以管理員身分透過網頁瀏覽器登入WFA。
2. 按一下「設定」、然後在「設定」下按一下「認證」。
3. 按一下  在工具列上。
4. 在「新認證」對話方塊中、從* MATCH *清單中選取下列其中一個選項：

◦ 確切

特定IP位址或主機名稱的認證資料

◦ 模式

整個子網路或IP範圍的認證資料



此選項不支援使用規則運算式語法。

5. 從*類型*清單中選取遠端系統類型。
6. 輸入資源的主機名稱或IPv6位址、使用者名稱和密碼。



WFA 5.1會驗證加入WFA的所有資源的SSL憑證。由於憑證驗證可能會提示您接受憑證、因此不支援在認證中使用萬用字元。如果您有多個叢集使用相同的認證資料、則無法一次全部新增。

7. 執行下列動作來測試連線能力：

如果您選取下列相符類型...	然後...
確切	按一下* Test*。
模式	儲存認證資料、然後選擇下列其中一項： <ul style="list-style-type: none"> • 選取認證資料、然後按一下  在工具列上。 • 按一下滑鼠右鍵、然後選取*測試連線能力*。

8. 按一下「* 儲存 *」。

設定OnCommand Workflow Automation 功能

利用支援的支援功能、您可以設定各種設定、例如、功能性供您選擇的功能、例如：功能性供您選擇的功能和通知。OnCommand Workflow Automation AutoSupport

設定WFA時、您可以視需要設定下列一項或多項：

- 將不支援的訊息傳送給技術支援部門AutoSupport AutoSupport
- Microsoft Active Directory輕量型目錄存取傳輸協定（LDAP）伺服器、適用於WFA使用者的LDAP驗證與授權

- 電子郵件通知工作流程作業及傳送AutoSupport 功能不正常的訊息
- 簡單網路管理傳輸協定（SNMP）、以通知工作流程作業
- 用於遠端資料記錄的系統記錄

設定AutoSupport 功能

您可以設定數AutoSupport 種支援功能設定、例如排程、AutoSupport 支援各種資訊的內容、以及Proxy伺服器。針對您所選擇的內容、每週發送一次記錄給技術支援部門、以進行歸檔和問題分析。AutoSupport

步驟

1. 以管理員身分透過網頁瀏覽器登入WFA。
2. 按一下「設定」、然後在「設定」下按一下「* AutoSupport」。
3. 確認AutoSupport 已選取「啟用S16」方塊。
4. 輸入所需資訊。
5. 從*內容*清單中選取下列其中一項：

如果您想要包含...	然後選擇此選項...
只有組態詳細資料、例如WFA安裝的使用者、工作流程和命令	"僅結束組態資料"
WFA組態詳細資料和WFA快取表中的資料、例如配置	「End configuration and cache data」（結束組態與快取資料）（預設）
WFA組態詳細資料、WFA快取表中的資料、以及安裝目錄中的資料	「結束組態並快取延伸資料」



任何WFA使用者的密碼都不包含在AutoSupport 畫面資料中。

6. 測試您是否可以下載AutoSupport 一份資訊更新訊息：
 - a. 按一下*下載*。
 - b. 在開啟的對話方塊中、選取儲存.7z檔案的位置。
7. 按一下*立即傳送*、測試AutoSupport 將資訊傳送到指定目的地的過程。
8. 按一下「* 儲存 *」。

設定驗證設定

您可以設定OnCommand Workflow Automation 使用Microsoft Active Directory（AD）輕量型目錄存取傳輸協定（LDAP）伺服器進行驗證和授權。

您必須在環境中設定Microsoft AD LDAP伺服器。

WFA僅支援Microsoft AD LDAP驗證。您無法使用任何其他LDAP驗證方法、包括Microsoft AD輕量型目錄服務（AD LDS）或Microsoft通用目錄。



在通訊期間、LDAP會以純文字格式傳送使用者名稱和密碼。不過、LDAPS（LDAP安全）通訊是加密且安全的。

步驟

1. 以管理員身分透過網頁瀏覽器登入WFA。
2. 按一下「設定」、然後在「設定」下按一下「驗證」。
3. 選取*啟用Active Directory*核取方塊。
4. 在下列欄位中輸入必要資訊：
 - a. 如果您要使用網域使用者的user@domain格式、請在*使用者名稱屬性*欄位中、將sAMAccountName取代為userPrincipalName。
 - b. 如果您的環境需要唯一值、請編輯必填欄位。
 - c. 輸入AD伺服器URI、如下所示：「LDAP//active_directory_server_address[:port]」

LDAP：//NB-T01.example.com[:389]

如果您已啟用LDAP over SSL、則可使用下列URI格式：「LDAPS
：//active_directory_server_address[:port]」

- a. 新增所需角色的AD群組名稱清單。



您可以在Active Directory群組視窗中、將AD群組名稱清單新增至所需的角色。

5. 按一下「*儲存*」。
6. 如果需要LDAP連線至陣列、請將WFA服務設定為以所需的網域使用者身分登入：
 - a. 使用services.msc開啟Windows服務主控台。
 - b. 按兩下「*NetApp WFA Server*」服務。
 - c. 在NetApp WFA伺服器內容對話方塊中、按一下*登入*索引標籤、然後選取*此帳戶*。
 - d. 輸入網域使用者名稱和密碼、然後按一下「確定」。

新增Active Directory群組

您可以將Active Directory群組新增OnCommand Workflow Automation 至功能區（WFA）。

步驟

1. 以管理員身分透過網頁瀏覽器登入WFA。
2. 按一下*設定*、然後在*管理*下、按一下*Active Directory群組*。
3. 在Active Directory Groups（Active Directory組）窗口中，單擊*New*圖標。
4. 在「新Active Directory群組」對話方塊中、輸入所需的資訊。

如果您從*角色*下拉式清單中選取*核准者*、建議您提供核准者的電子郵件ID。如果有多位核准者、您可以在*電子郵件*欄位中提供群組電子郵件ID。選取要傳送通知至特定Active Directory群組的工作流程不同事件。

5. 按一下「* 儲存 *」。

設定電子郵件通知

您可以設定OnCommand Workflow Automation 將有關工作流程作業的電子郵件通知傳送給您（例如、工作流程已啟動或工作流程失敗）。

您必須在環境中設定郵件主機。

步驟

1. 以管理員身分透過網頁瀏覽器登入WFA。
2. 按一下「設定」、然後在「設定」下按一下「郵件」。
3. 在欄位中輸入必要資訊。
4. 請執行下列步驟來測試郵件設定：
 - a. 按一下*傳送測試郵件*。
 - b. 在「測試連線」對話方塊中、輸入您要傳送電子郵件的電子郵件地址。
 - c. 按一下* Test*。
5. 按一下「* 儲存 *」。

設定SNMP

您可以設定OnCommand Workflow Automation 功能區（WFA）、針對工作流程作業的狀態、傳送簡單網路管理傳輸協定（SNMP）陷阱。

WFA現在支援SNMP v1和SNMP v3傳輸協定。SNMP v3提供額外的安全功能。

WFA .mib檔案提供WFA伺服器所傳送之設陷的相關資訊。MIBA檔案位於WFA伺服器上的<WFA_install_location>\WFA\BIN\WFA.mib目錄中。



WFA伺服器會以一般物件識別碼（1.3.6.1.4.1.789.1.12.0）傳送所有陷阱通知。

您無法使用SNMP社群字串、例如commune_string@SNMP主機來進行SNMP組態。

設定SNMP版本1

步驟

1. 以管理使用者的身分透過網頁瀏覽器登入WFA、然後存取WFA伺服器。
2. 按一下「設定」、然後在「設定」下按一下「* SNMP *」。
3. 選中* Enable SNMP（啓用SNMP）*複選框。
4. 在「版本」下拉式清單中、選取「*版本1*」。

5. 輸入IPv4或IPv6位址或主機名稱、以及管理主機的連接埠號碼。

WFA會將SNMP設陷傳送至指定的連接埠號碼。預設連接埠號碼為162。

6. 在「通知時間」區段中、選取下列一或多個核取方塊：

- 工作流程執行已開始
- 工作流程執行成功完成
- 工作流程執行失敗/部分成功
- 工作流程執行等待核准
- 擷取失敗

7. 按一下*傳送測試通知*以驗證設定。

8. 按一下「* 儲存 *」。

設定SNMP版本3

您也可以設定OnCommand Workflow Automation S廳（WFA）、針對工作流程作業的狀態、傳送簡單網路管理傳輸協定（SNMP）版本3的陷阱。

第3版提供兩種額外的安全選項：

- 第3版含驗證

陷阱會以不加密的方式透過網路傳送。SNMP管理應用程式與SNMP設陷訊息的驗證參數相同、可接收設陷。

- 第3版：驗證與加密

陷阱會透過網路加密傳送。若要接收及解密這些陷阱、您必須使用與SNMP設陷相同的驗證參數和加密金鑰來設定SNMP管理應用程式。

步驟

1. 以管理使用者的身分透過網頁瀏覽器登入WFA、然後存取WFA伺服器。

2. 按一下「設定」、然後在「設定」下按一下「* SNMP *」。

3. 選中* Enable SNMP（啓用SNMP）*複選框。

4. 在*版本*下拉式清單中、選取下列其中一個選項：

- 版本3
- 第3版含驗證
- 第3版：驗證與加密

5. 選取對應於您在步驟4中選擇的特定SNMP版本3選項的SNMP組態選項。

6. 輸入IPv4或IPv6位址或主機名稱、以及管理主機的連接埠號碼。WFA會將SNMP設陷傳送至指定的連接埠號碼。預設連接埠號碼為162。

7. 在「通知時間」區段中、選取下列一或多個核取方塊：

- 工作流程規劃已開始/失敗/已完成
- 工作流程執行已開始
- 工作流程執行成功完成
- 工作流程執行失敗/部分成功
- 工作流程執行等待核准
- 擷取失敗

8. 按一下*傳送測試通知*以驗證設定。

9. 按一下「* 儲存 *」。

設定Syslog

您可以設定OnCommand Workflow Automation 將記錄資料傳送至特定的Syslog伺服器、以供事件記錄和記錄資訊分析等用途。

您必須設定Syslog伺服器、才能接受來自WFA伺服器的資料。

步驟

1. 以管理員身分透過網頁瀏覽器登入WFA。
2. 按一下「設定」、然後在「維護」下按一下「系統記錄」。
3. 選取*啟用Syslog*核取方塊。
4. 輸入Syslog主機名稱、然後選取Syslog記錄層級。
5. 按一下「* 儲存 *」。

設定連接遠端系統的傳輸協定

您可以設定OnCommand Workflow Automation 用來連接遠端系統的傳輸協定（WFA）。您可以根據組織的安全需求和遠端系統支援的傳輸協定來設定傳輸協定。

步驟

1. 以管理員身分透過網頁瀏覽器登入WFA。
2. 按一下*資料來源設計*>*遠端系統類型*。
3. 執行下列其中一項動作：

如果您想要...	執行此動作...
設定新遠端系統的傳輸協定	<ol style="list-style-type: none"> a. 按一下 。 b. 在「新增遠端系統類型」對話方塊中、指定名稱、說明和版本等詳細資料。
修改現有遠端系統的傳輸協定組態	<ol style="list-style-type: none"> a. 選取並按兩下您要修改的遠端系統。 b. 按一下 。

4. 從連線傳輸協定清單中、選取下列其中一項：
 - HTTPS搭配HTTP（預設）
 - 僅限HTTPS
 - 僅限HTTP
 - 自訂
5. 指定傳輸協定、預設連接埠和預設逾時的詳細資料。
6. 按一下「 * 儲存 * 」。

停用預設密碼原則

將WFA設定為強制本機使用者使用密碼原則。OnCommand Workflow Automation如果您不想使用密碼原則、可以停用該原則。

您必須以管理員身分登入WFA主機系統。

此程序使用預設的WFA安裝路徑。如果您在安裝期間變更預設位置、則必須使用變更的WFA安裝路徑。

步驟

1. 開啟Windows檔案總管、然後瀏覽至下列目錄：「WFA_install_LOUSE\WFA\BIN\。」
2. 按兩下ps。cmd檔案。

PowerShell命令列介面（CLI）提示字元隨即開啟、ONTAP 其中已載入畫面和WFA模組。

3. 出現提示時、輸入下列命令：

「et-WfaConfig -名稱密碼原則-啟用\$假」

4. 出現提示時、請重新啟動WFA服務。

修改Windows的預設密碼原則

針對本機使用者執行密碼原則（WFA） OnCommand Workflow Automation 。您可以修改預設密碼原則、根據需求設定密碼。

您必須以root使用者身分登入WFA主機系統。

- 此程序使用預設的WFA安裝路徑。

如果您在安裝期間變更了預設位置、則必須使用自訂的WFA安裝路徑。

- 修改預設密碼原則的命令是.\WFA --password-policy=Default。

預設設定為「minLength=true、8；specialChar=true、1；digitalChar=true、1；allercaseChar=true、1；uppercaseChar=true、1；whitespaceChar=假」。根據預設密碼原則的此設定、密碼長度必須至少為八個字元、必須包含至少一個特殊字元、一個數字、一個小寫字元和一個大寫字元、且不得包含空格。

步驟

1. 在命令提示字元中、瀏覽至WFA伺服器上的下列目錄：

WFA_install_LOUSE/WFA/BIN/

2. 修改預設密碼原則：

".\WFA --password-policy=PasswordPolicyStr"--eset=wfa"

可在OnCommand Workflow Automation Windows上遠端存取效能不整資料庫

根據預設、OnCommand Workflow Automation 只有在WFA主機系統上執行的用戶端、才能存取WFA（WFA）資料庫。若要從遠端系統存取WFA資料庫、您可以變更預設設定。

- 您必須以管理使用者的身分登入WFA主機系統。
- 如果WFA主機系統上安裝了防火牆、則您必須設定防火牆設定、以允許從遠端系統存取。

此程序使用預設的WFA安裝路徑。如果您在安裝期間變更了預設位置、則必須使用自訂的WFA安裝路徑。

步驟

1. 開啟Windows檔案總管、然後瀏覽至下列目錄：WFA_install_directory\WFA\bin
2. 執行下列其中一項動作：

至...	輸入下列命令...
啟用遠端存取	「.\WFA --db-access=public—restart」
停用遠端存取	「.\WFA --db-access=Default -重新啟動」

限制OnCommand Workflow Automation 主機上的存取權限

根據預設、OnCommand Workflow Automation 功能完善（WFA）會以主機系統管理員的身分執行工作流程。您可以變更預設設定、限制主機系統上的WFA權限。

您必須以管理員身分登入WFA主機系統。

步驟

1. 建立新的Windows使用者帳戶、並具有開啟套接字及寫入WFA主目錄的權限。
2. 使用services.msc開啟Windows服務主控台、然後按兩下「* NetApp WFA資料庫*」。
3. 按一下*登入*索引標籤。
4. 選取*此帳戶*並輸入您所建立之新使用者的認證資料、然後按一下*確定*。
5. 按兩下「* NetApp WFA Server*」。

6. 按一下*登入*索引標籤。
7. 選取*此帳戶*並輸入您所建立之新使用者的認證資料、然後按一下*確定*。
8. 重新啟動* NetApp WFA資料庫*和* NetApp WFA伺服器*服務。

修改OnCommand Workflow Automation 資訊的交易逾時設定

根據預設、還原（WFA）資料庫交易會在300秒內逾時。OnCommand Workflow Automation從備份還原大型WFA資料庫時、您可以延長預設的逾時時間、以避免資料庫還原可能發生故障。

您必須以管理員身分登入WFA主機系統。

此程序使用預設的WFA安裝路徑。如果您在安裝期間變更預設位置、則必須使用變更的WFA安裝路徑。

步驟

1. 開啟Windows檔案總管、然後瀏覽至下列目錄：

「wfa_install_location \wfa\bin」

2. 按兩下ps。cmd檔案。

PowerShell命令列介面（CLI）提示字元隨即開啟、ONTAP 其中已載入畫面和WFA模組。

3. 出現提示時、輸入下列命令：

「et-WfaConfig -名稱TransactionTimOut -秒數值」

「et-WfaConfig -Name TransactionTimOut -seconds 1000」

4. 出現提示時、請重新啟動WFA服務。

設定Workflow Automation的逾時值

您可以設定Workflow Automation（WFA）Web GUI的逾時值、而非使用預設的逾時值。

WFA Web GUI的預設逾時值為180分鐘。您可以透過CLI設定逾時值、以符合您的需求。您無法從WFA Web GUI設定逾時值。



您所設定的逾時值為絕對逾時、而非與閒置相關的逾時。例如、如果您將此值設為30分鐘、則即使您在此時間結束時處於作用中狀態、30分鐘後仍會登出。

步驟

1. 以管理員身分登入WFA主機機器。
2. 設定逾時值：

"install_dir bin/wFA -S=timeout value in Minutes"（安裝目錄BIM/WFA -S=timeout值（以分鐘

啟用密碼並新增密碼

支援許多現成密碼。OnCommand Workflow Automation此外、您也可以視需要新增其他密碼。

下列密碼可立即啟用：

```
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"
```

您可以在「獨立式-Full.xml」檔案中新增其他密碼到此組態。此檔案位於：「<installdir>/jboss/s獨立式/組態/獨立式-Full.xml」。

可修改檔案以支援其他密碼、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"/>
```

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。