國家發展委員會 ODF 文件 Web 應用元件伺服器佈署說明書

文件版本：1.6 版

中　華　民　國　109　年　12　月　2　日

目錄

壹、安裝基礎系統

本文件說明國家發展委員會【ODF 文件 Web 應用元件】伺服器端的佈署流程，並提供所需 Linux 系統的下載及安裝方式。

一、下載 CentOS 作業系統 ISO 連結

國家發展委員會【ODF 文件 Web 應用元件】伺服器端的作業系統可採用開源的【CentOS】，該系統與商用 Linux 系統公司 Redhat 所提供的商用級伺服器來自於相同的原始碼版本，同樣可運用在各種網路伺服器環境，CentOS ISO 在國內的下載連結如下，目前採用的最新版本號碼為 7.x：

- 元智大學載點

  http://ftp.yzu.edu.tw/Linux/CentOS/7/isos/x86_64/

- 國家高速網路中心載點

  http://free.nchc.org.tw/centos/7/isos/x86_64/

- 崑山科技大學載點

  http://ftp.ksu.edu.tw/pub/CentOS/7/isos/x86_64/

- 國家實驗研究院載點

  http://ftp.twaren.net/Linux/CentOS/7/isos/x86_64/

- 樹德科技大學載點

  http://ftp.stu.edu.tw/Linux/CentOS/7/isos/x86_64/

- 交通大學載點

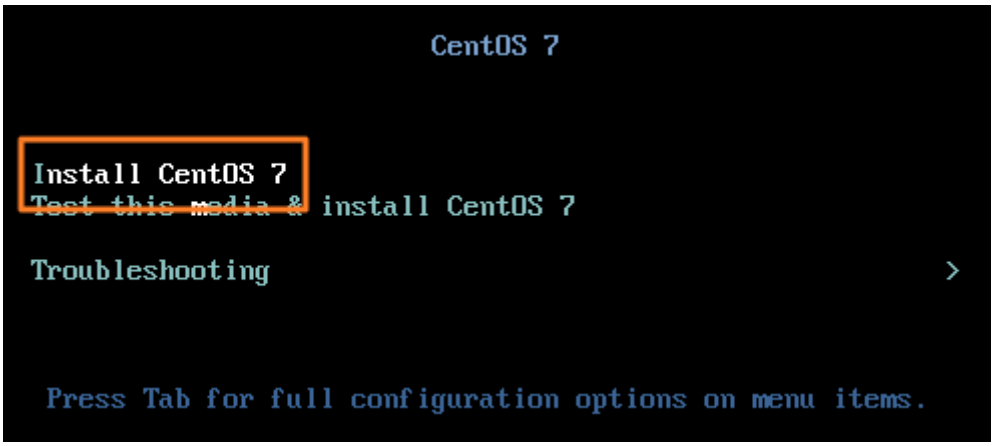
  http://centos.cs.nctu.edu.tw/7/isos/x86_64/

下載檔名為：【CentOS-7-x86_64-Minimal-2003.iso】，若是要佈署在實體主機上的話，請將 ISO 檔燒錄至光碟上，若是安裝於虛擬主機環境的話，請將此 ISO 檔掛載至虛擬主機的光碟裝置中，以下說明安裝過程。

二、 系統安裝過程

(1)光碟片開機

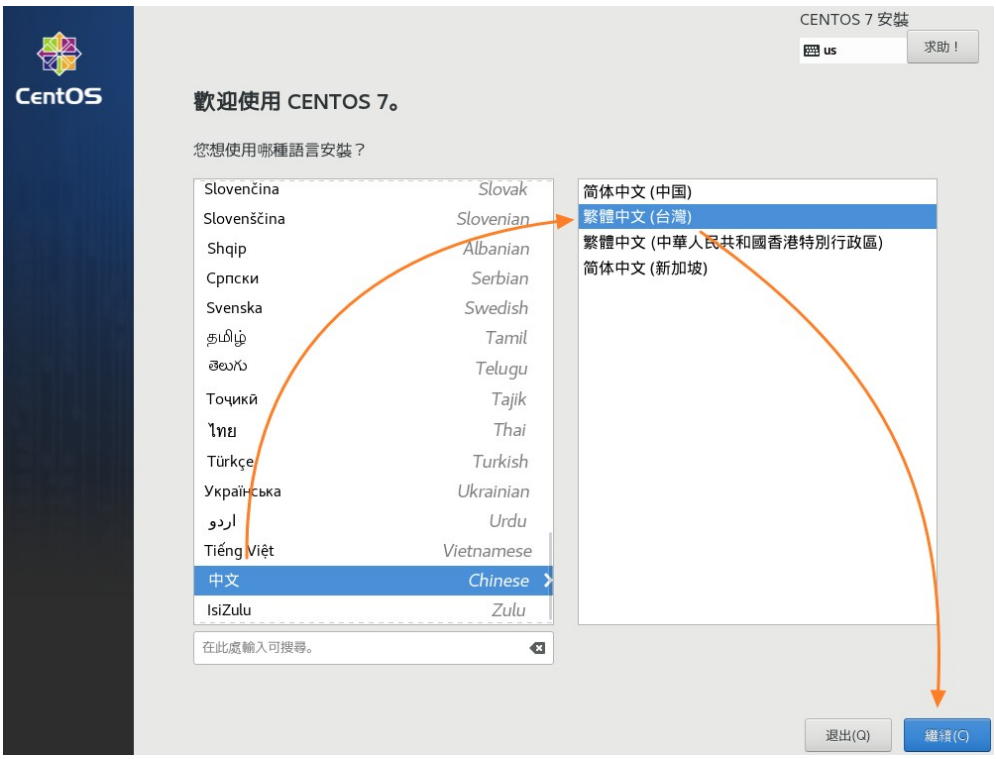
開機後會先出現以下畫面，請利用方向鍵往上切換至【Install CentOS 7】，並按下 Enter 鍵繼續安裝流程。



畫面如果又出現一次請您按「Enter」鍵時，請等待或是直接再按一次「Enter」鍵即可。

(2)選擇系統語系

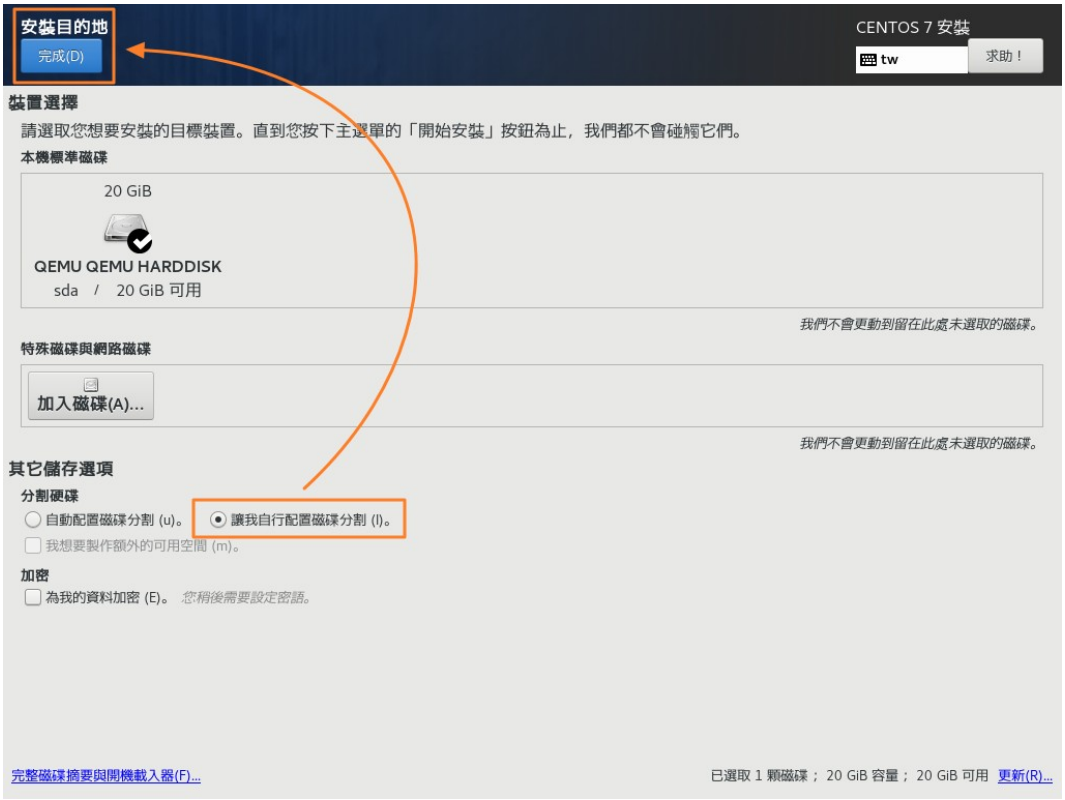
安裝程式會經過一連串偵測硬體的過程，完成後會進入選擇語系的畫面，畫面左方請下拉並選擇【中文】，畫面右方請選擇【繁體中文(台灣)】，如下圖所示，完成後按下「繼續」鍵。



(3)分割硬碟

請先進行硬碟分割的設定，點選畫面中的【安裝目的地】。

接下來的畫面中，請先點選【讓我自行配置磁碟分割】，再往上點選【完成】。



先將分割格式指定為【標準分割區】再按下【+】繼續新增分割區。

安裝過程【基本】需新增 2 個分割區(也可參考下方進階分割建議)，說明如下：

- SWAP

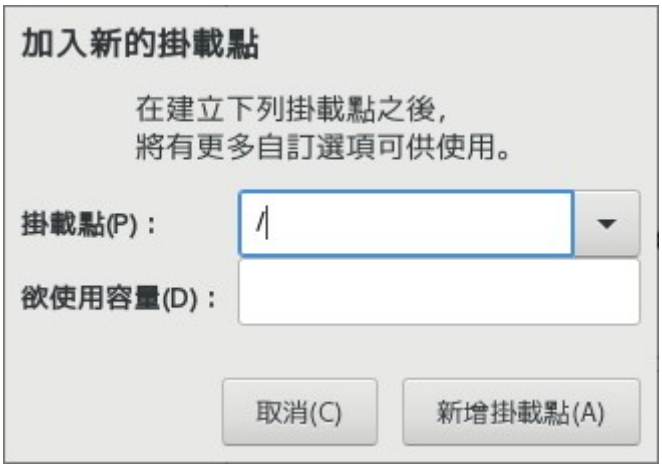
Linux 系統需要的記憶體暫存區，建議可以新增 4096MB 供系統使用。

- /

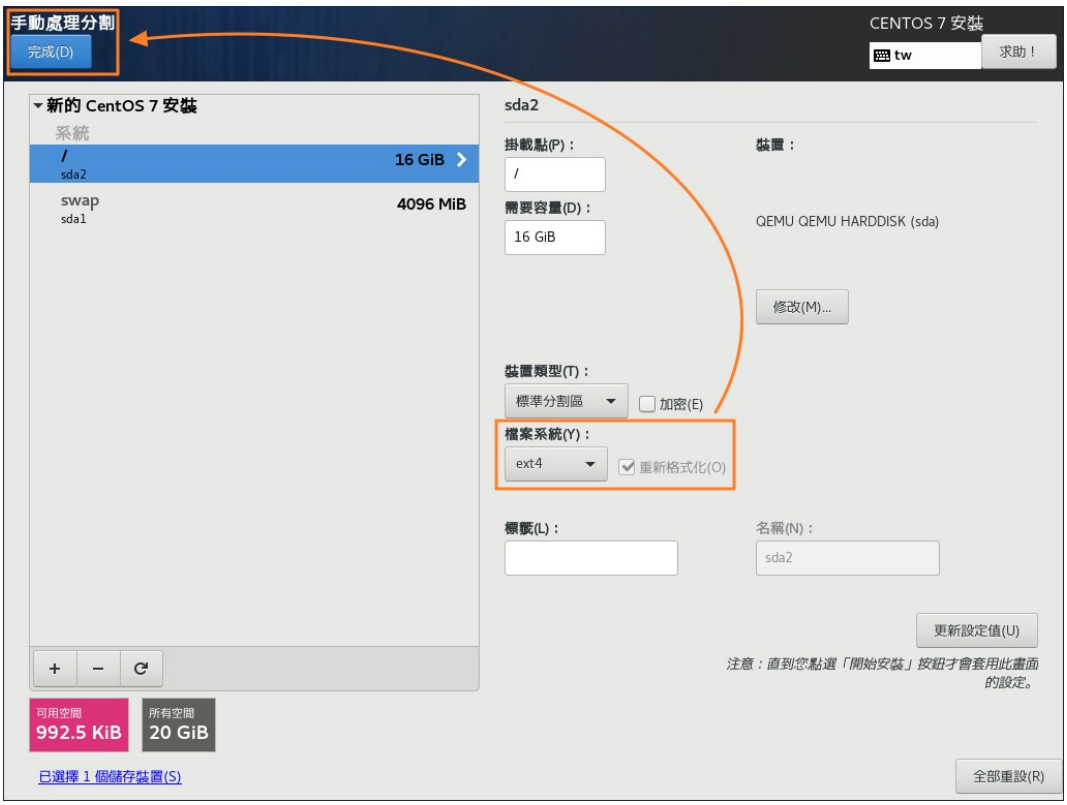
系統主要分割區，剩下來的空間都全部分配到此處。

點擊【+】號後，系統會出現分割區設定的畫面，以 SWAP 為例，設定畫面如下所示，請指定【掛載點】為 swap，【容量】建議指定為 4096(或自行規劃)。

若是【/】分割區的話，由於剩下的空間都要分配給它，所以在【欲使用容量】的部份保持空白即可，畫面如下。



按下【新增掛載點】後，畫面會出現此分割區的詳細設定畫面，SWAP 的部份不需要特別設定，但是在【/】的部份，需額外指定【檔案系統】的部份為【ext4】(系統預設會為 xfs)，如下圖所示，指定完成後按下畫面左上方的【完成】鍵。



系統會再次確認分割區的資訊，確認後請按下【接受變更】繼續。

以下有二組建議的進階硬碟分割區列表提供參考：

1. 50GB 空間

- SWAP - 4GB
- / - 10GB
- /tmp - 8GB
- /var/log - 10GB
- /opt - 8GB
- /home - 10GB

2. 100GB 空間

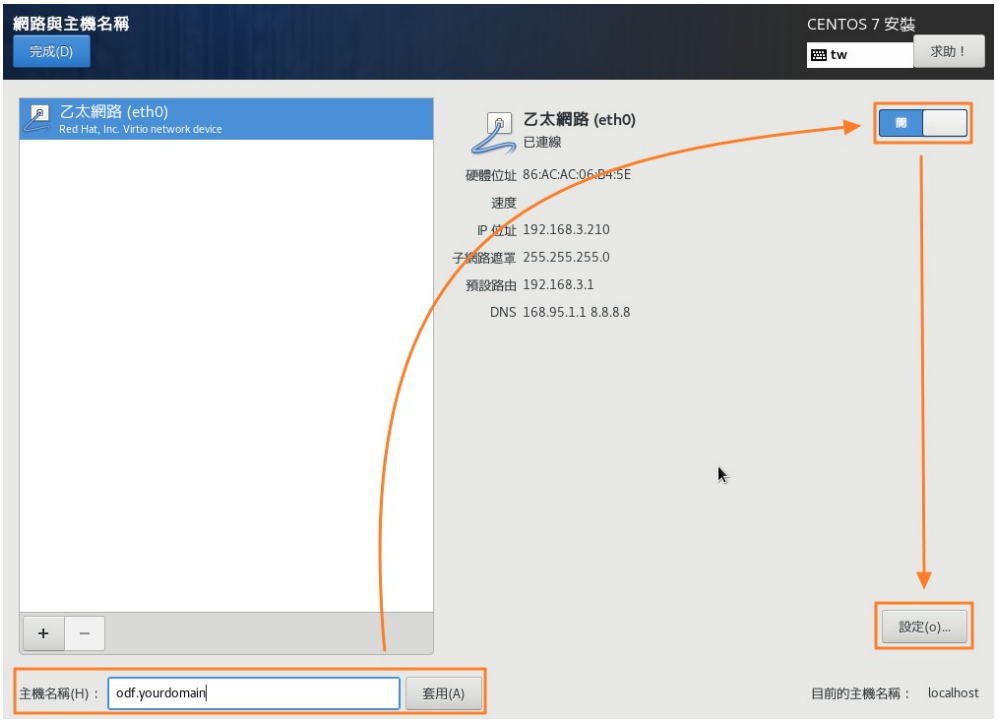
- SWAP - 4GB
- / - 16GB
- /tmp - 10GB
- /var/log - 10GB
- /opt - 10GB
- /home - 50GB

備註：用戶的空間可以透過掛載其它儲存裝置的方式來擴充。

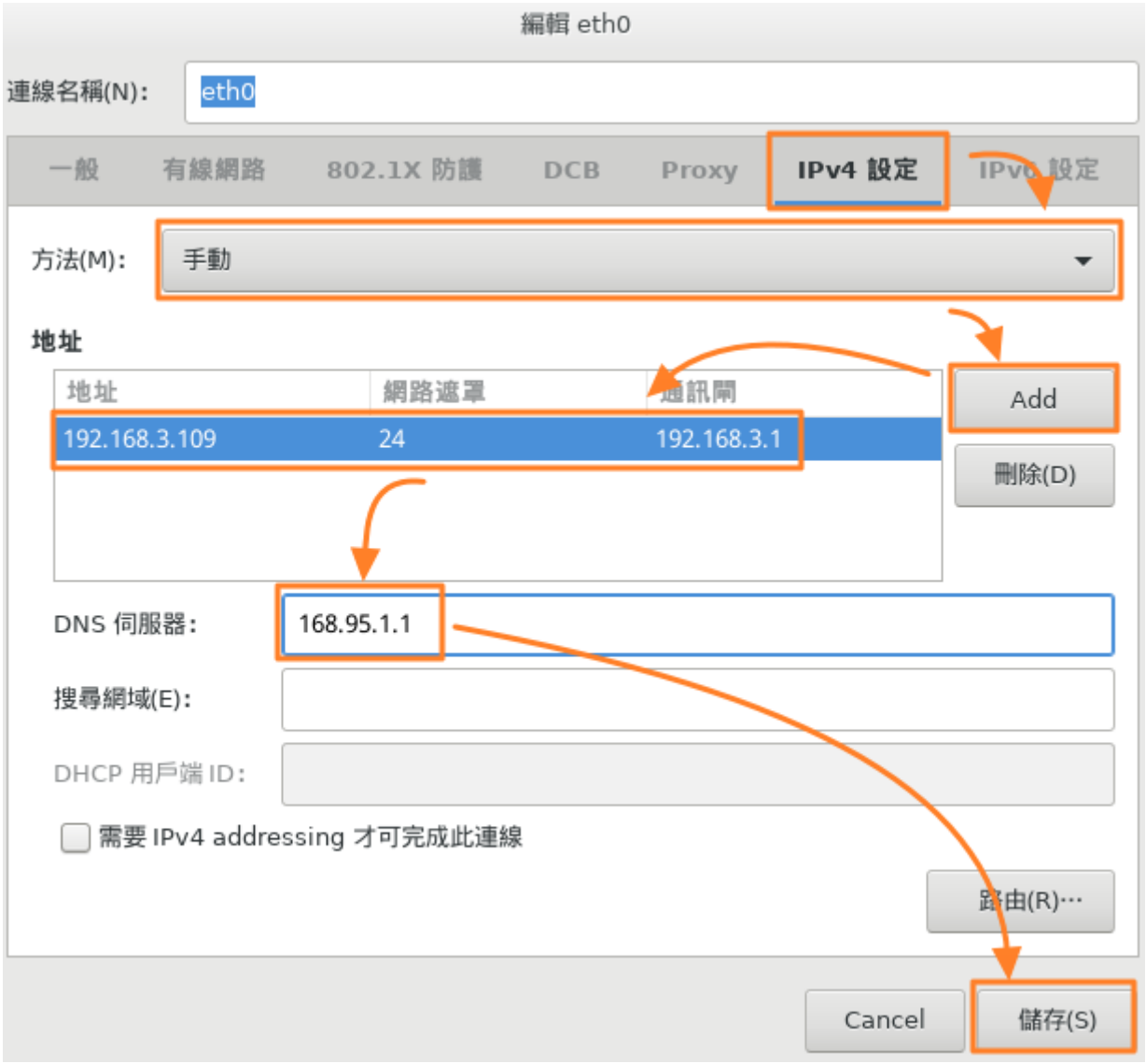
(4)設定網路

接下來畫面會回到原本的頁面，請點選畫面中的【網路與主機名稱】。

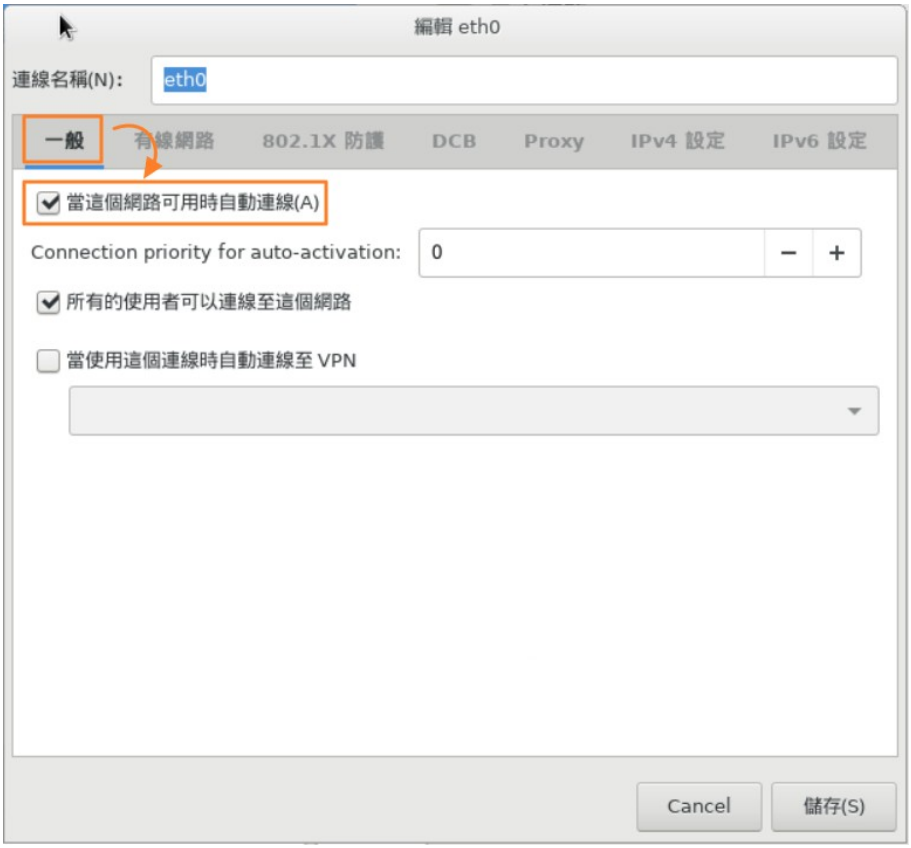
分別設定【主機名稱】(完成後按下「套用」)、開啟乙太網路，最後按下【設定】鍵進行詳細的網路設定。



詳細的網路設定畫面如下，因為是伺服器環境，故建議使用固定 IP，請先點選畫面中的【IPV4 設定】，方法選擇【手動】，並按下畫面中的【Add】鍵後輸入固定的 IP 資訊，在輸入【DNS 伺服器】資訊後點選【儲存】即完成網路設定。

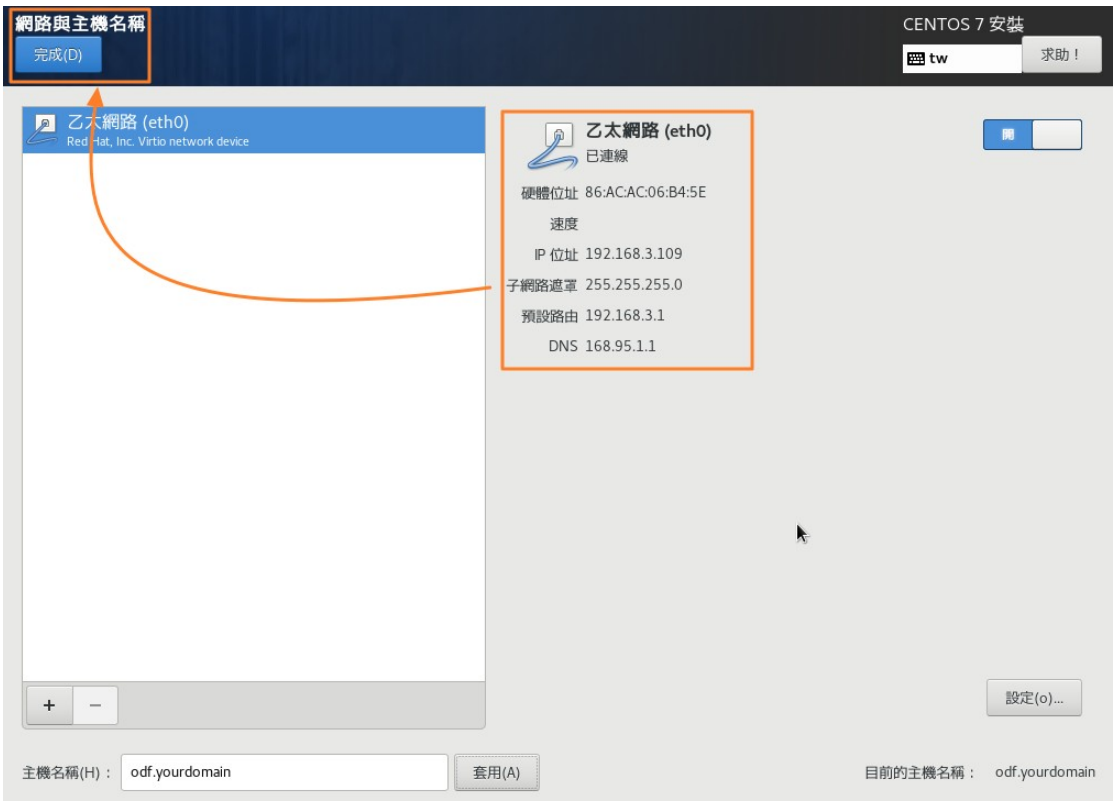


再按一下「設定」，請點選「一般」並勾選「當這個網路可用時自動連線」如下圖所示：



點選【儲存】即完成網路設定。

設定完成後會回到上一個畫面，請確認相關的設定是否正確，確認後按下畫面左上方的【完成】鍵再回到安裝主畫面。

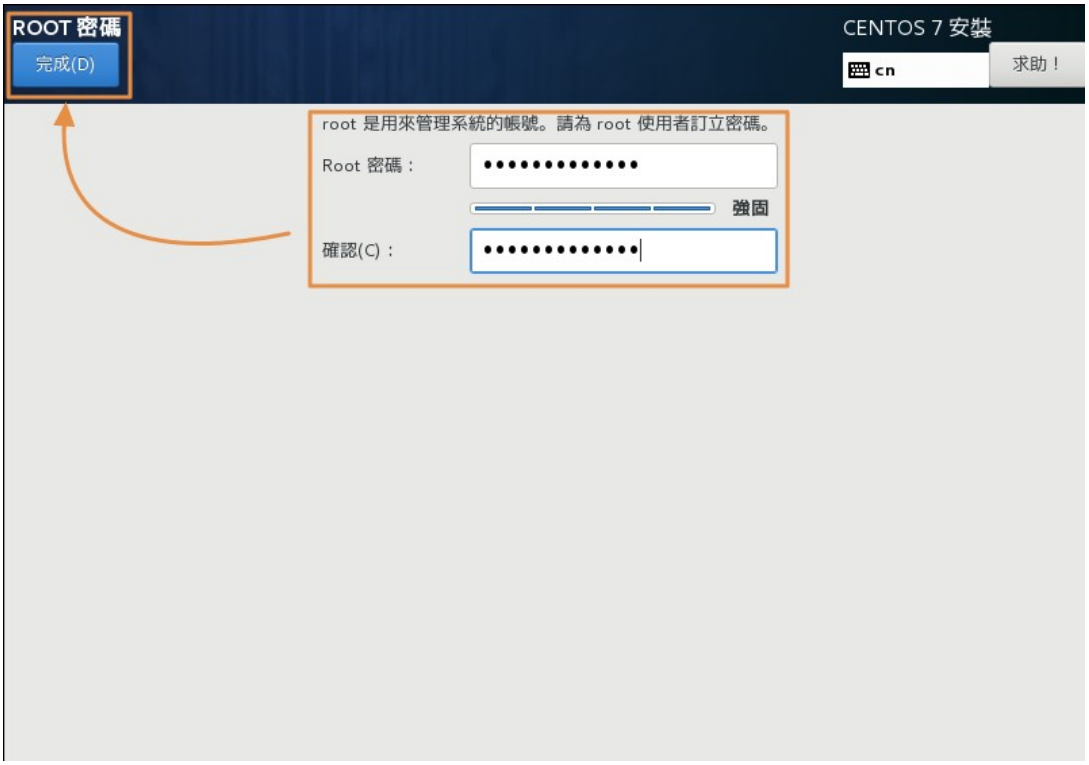


請按下【開始安裝】，系統就會開始正式進行安裝。

(5)設定 ROOT 密碼

安裝過程中會跳出以下畫面，請按下【ROOT 密碼】進入設定畫面。

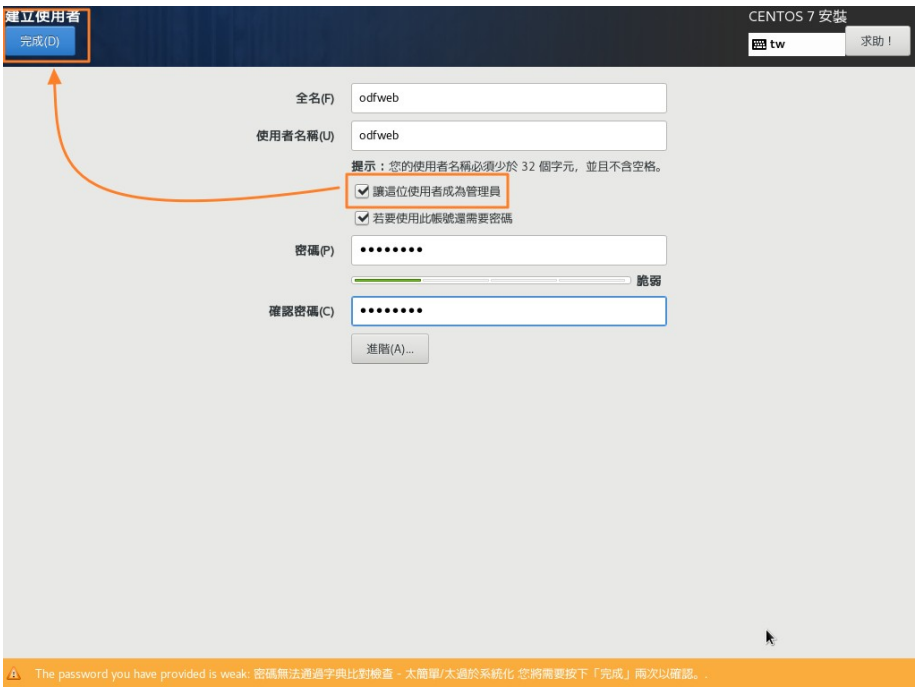
設定畫面如下，請輸入二次 ROOT 密碼，並按下【完成】鍵完成設定。


ROOT 密碼
完成(D)
CENTOS 7 安裝
cn
求助！
root 是用來管理系統的帳號。請為 root 使用者訂立密碼。
Root 密碼：
強固
確認(C)：

(6)用戶建立

設定完ROOT 密碼後會回到安裝程式主畫面，如果需要建立一般用戶的帳號，請點選【用戶建立】鍵。

進到用戶建立的畫面後，如圖請填入使用者姓名及密碼，重點是若要使用一般使用者管理系統，請記得勾選【讓這位使用者成為管理員】，如下圖。



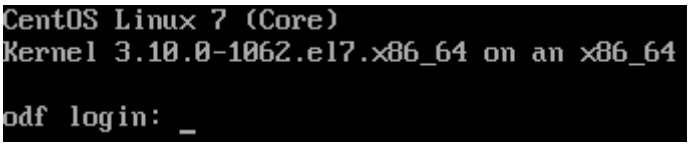
同時要點選【完成】，才會跳回系統安裝主畫面，當安裝完成後，畫面右下角會出現【完成設定】的按鍵，按下後系統就會開始設定開機等系統參數。


CentOS
配置
CENTOS 7 安裝
tw
求助！
用戶設定
ROOT 密碼
Root 密碼已設定
用戶建立(U)
將建立管理員 odfweb
已完成！
CentOS 已成功安裝，但還需要做一些設定。
請在完成後按下「完成設定」按鈕。
完成設定(F)

(7)重新開機

當完成所有設定時，畫面右下角會出現【重新開機】的按鍵，即代表已完成安裝作業，重新開機就可以啟動基本的系統了。

重新開機後的畫面如下所示。



三、 系統環境設定

在安裝完基礎系統後，需進行基本的調校及安裝【ODF 文件 Web 應用元件】所需之基礎套件。

(1)系統升級

請先以 root 身份登入後，執行以下指令進行系統升級工作。

```
# yum update -y
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
.....(升級過程訊息略)
Complete!
```

完成基礎系統套件的升級工作。

(2)調整防火牆

由於多數機關都有建置專屬的防火牆，故建議先設定本機上的基本防火牆設定即可符合多數機關環境安裝設置需求，指令如下：

```
# firewall-cmd --zone=public --add-service=http
# firewall-cmd --zone=public --permanent --add-service=http
# firewall-cmd --zone=public --add-service=https
# firewall-cmd --zone=public --permanent --add-service=https
```

firewall-cmd --zone=public --add-port=9980/tcp

firewall-cmd --zone=public --permanent --add-port=9980/tcp

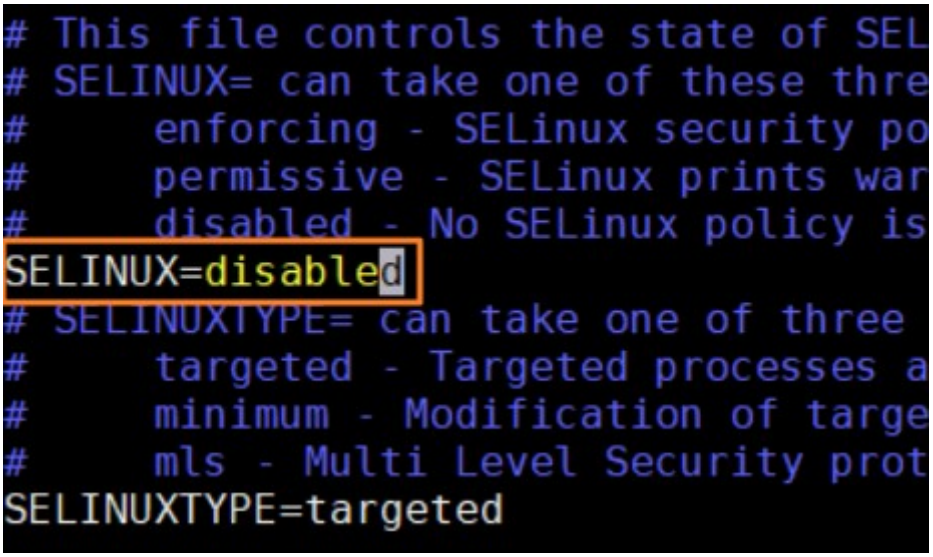
(3)關閉 selinux

預設請關閉 selinux 機制，建議先安裝 vim 編輯器及基本網路工具後，再進行編輯：

yum install vim net-tools unzip -y

vim /etc/selinux/config

出現編輯畫面後，請用方向鍵移動到第 7 行 enforcing 的部份，將內容改為【disabled】，如下畫面，編輯完成後存檔離開，**並重新開機**。



(4)vim 編輯器的基本使用方式如下：

「x」鍵：在【瀏覽模式】時，直接刪除游標所在字元。

「i」鍵：進入【編輯模式】，可以插入及刪除(透過 backspace 鍵)字元。

「u」鍵：回復上一步的動作。

按下 2 次「y」鍵：複製一整行。

「p」鍵：插入並貼上剛剛複製的整行內容。

「ESC」鍵：回到【瀏覽模式】。

(5)vim 編輯器的存檔方式：

在按下「ESC」鍵回到【瀏覽模式】後，直接輸入【wq!】三個字元，並按下【Enter】鍵後完成編輯作業。其中 w 代表寫入，q 代表跳出，!代表強制執行，如果輸入【w】代表寫入，但留在 vim 編輯器畫中，輸入【q】代表離開 vim 編輯器畫面，【q!】代表即便檔案有變更，也要直接退出不儲存變更。

編輯完成後，建議先行重新開機讓部份設定生效，指令如下：

reboot

(6)安裝 WinSCP 檔案上傳工具

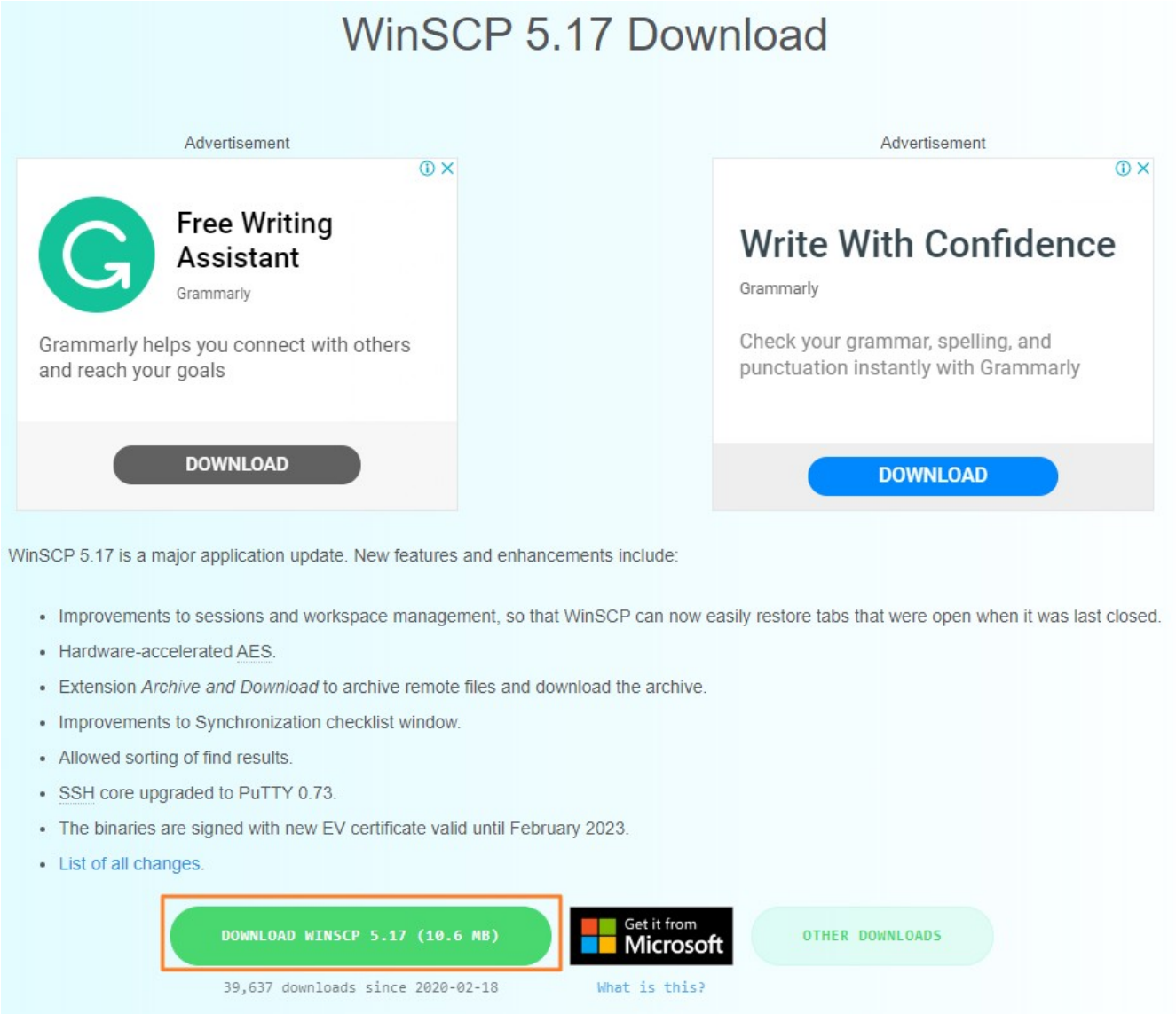
基本系統安裝完成並重新開機後，開始先安裝【ODF 文件 Web 應用元件】相關套件，請先到國發會的網站下載相關檔案，下載點說明如下：

請至國發會網站 http://www.ndc.gov.tw > 主要業務 > 基礎服務 > 開放文件格式(Open Document Format, ODF) > 支援 ODF 文件格式軟體工具 > **雲端編輯工具**

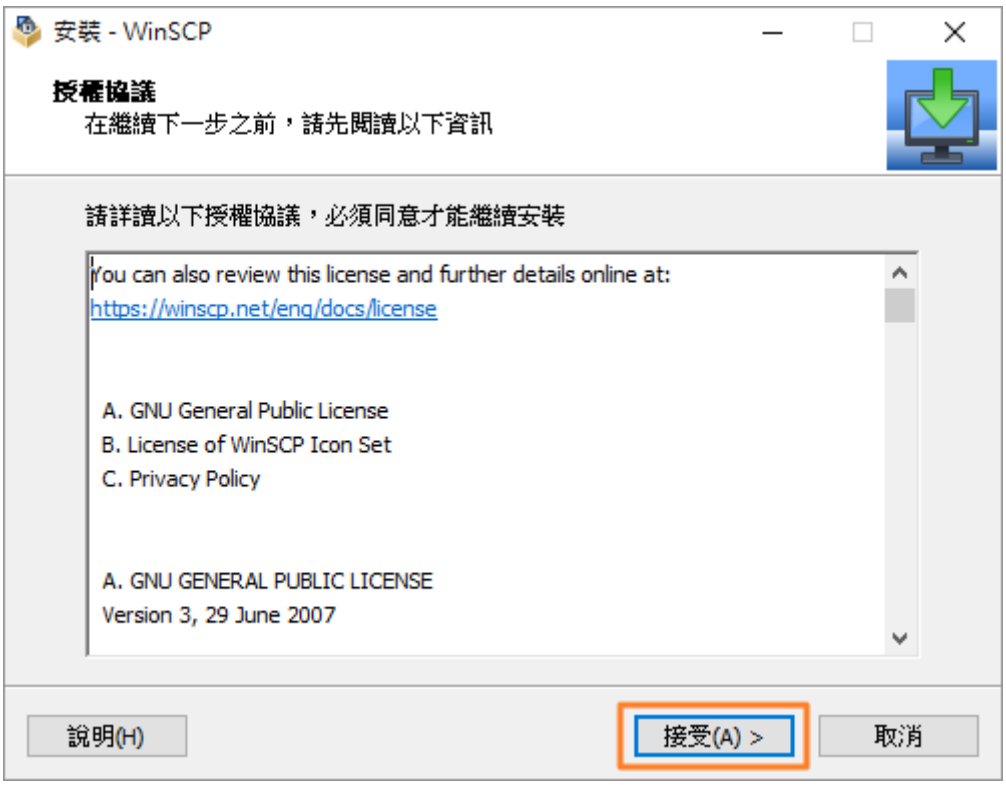
下載成功後，需先把檔案上傳到先前安裝的 Linux 主機上，在 Windows 平台上可使用「WinSCP」這套工具進行，下載網頁的連結如下：

https://winscp.net/eng/download.php

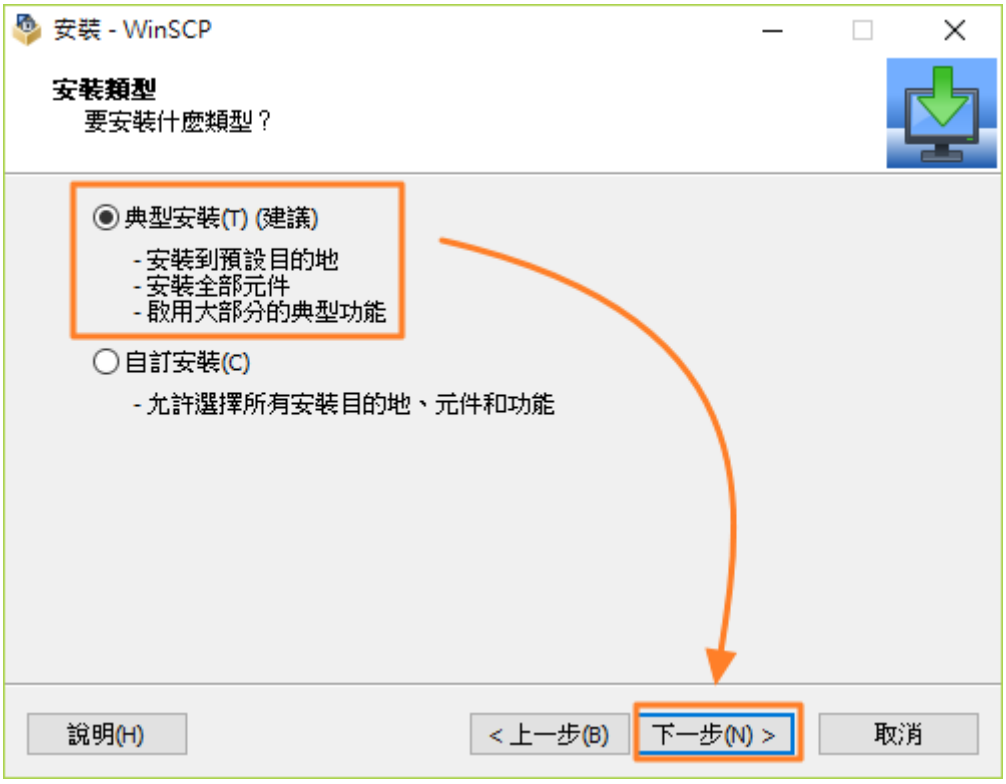
目前最新的版本為 5.17，請直接點選畫面下方的下載連結圖示。



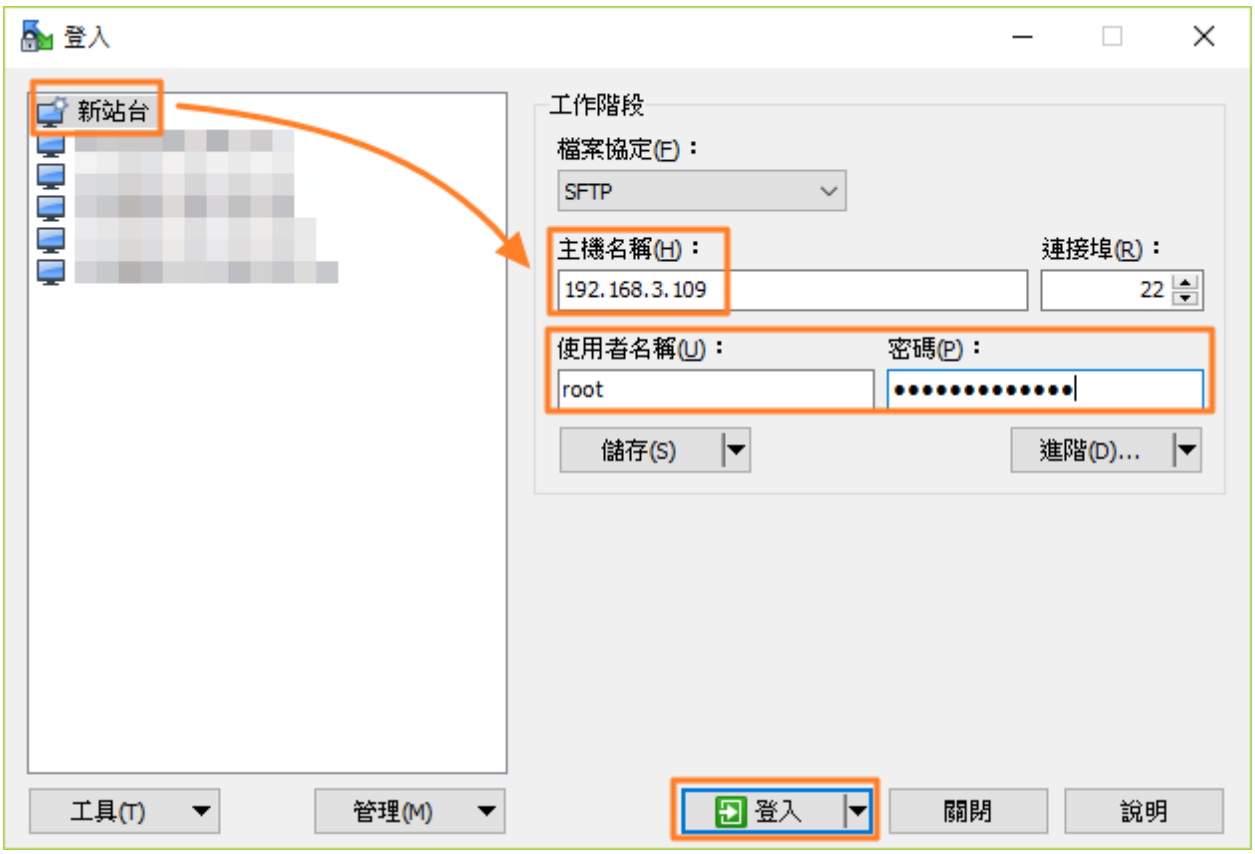
下載完成請直接執行安裝動作，Windows 會先詢問是否允許 WinSCP 變更您的系統，請點選「是」繼續，接下來出現【授權協議】的畫面：



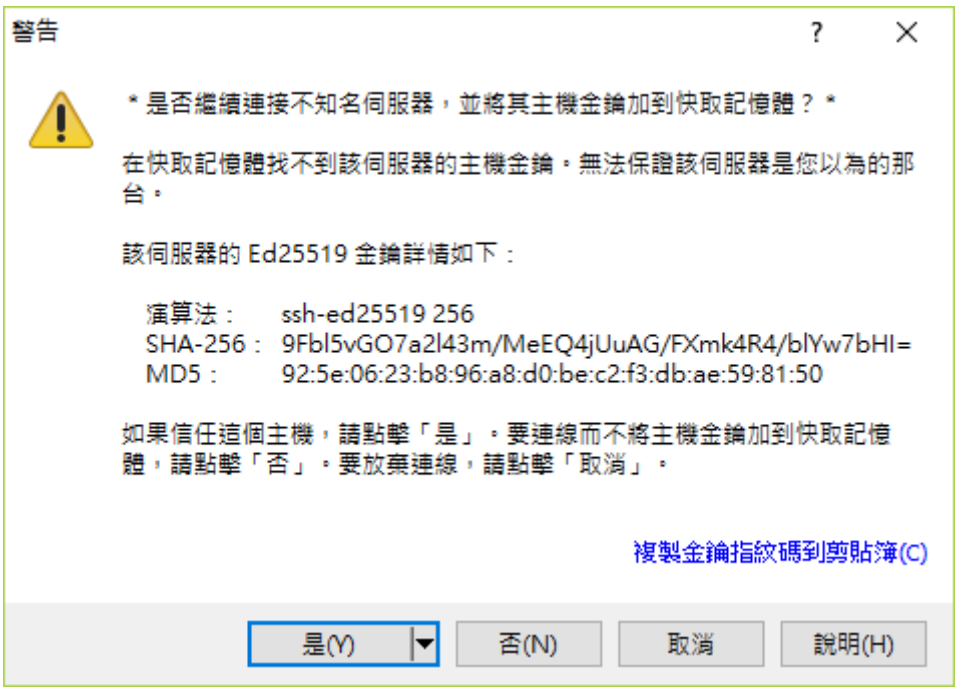
請按下【接受】鍵，繼續下一步畫面，請選擇【典型安裝】即可，接下來的畫面只要不斷按【下一步】直接到完成安裝作業的畫面，按下【完成】。



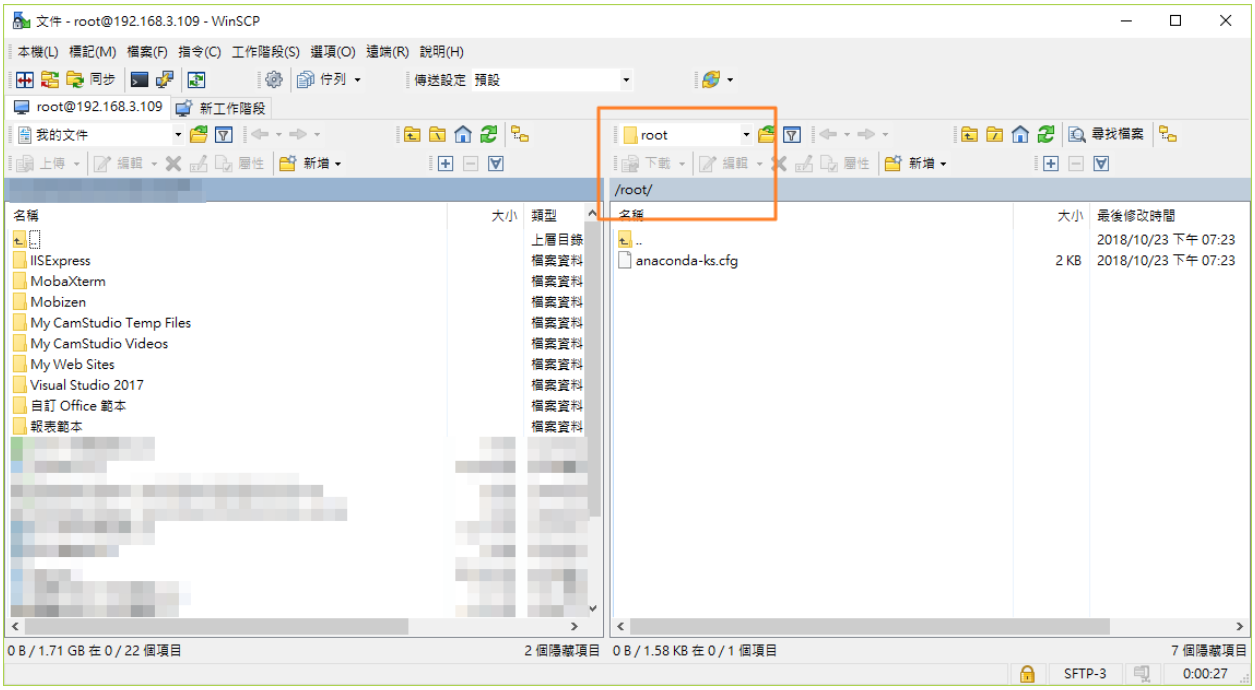
安裝完成後，會直接進入 WinSCP 的設定畫面，請直接點選【新站台】並輸入主機名稱、使用者名稱及密碼等資訊(剛剛安裝完的 ODF 文件 Web 應用元件 Server)，完成後按下【登入】鍵就可以登入主機了。



登入後第一個畫面會看到憑證的訊息，請按下【是(Y)】鍵略過，接下來可以看到類似於檔案總管的介面，此時就可以利用 WinSCP 將檔案上傳到主機上，後續進行 ODF 文件 Web 應用元件的安裝說明。



左方為 Windows 的檔案目錄區，右方為 Server 端的目錄路徑及檔案列表。



貳、安裝 ODF 文件 Web 應用元件套件

請利用 WinSCP 將【ODF 文件 Web 應用元件】相關安裝套件上傳至 Linux 主機後，執行以下安裝指令：

一、 安裝系統主程式

```
# cd /root

# unzip NDCODFWEB-V1.6.zip

# cd NDCODFWEB-V1.6/ndcodfsys

# yum localinstall gumbo* -y

# yum localinstall ndcodfsys* -y
```

二、 安裝函式庫

```
# cd /root/NDCODFWEB-V1.6/poco

# yum localinstall poco* -y
```

三、 安裝 ODF 文件 Web 應用元件主程式

```
# cd /root/NDCODFWEB-V1.5/ndcodfweb

# yum localinstall ndcodfweb* -y
```

四、啟動 ODF 文件 Web 應用元件主程式並確認狀態

systemctl enable ndcodfweb

systemctl restart ndcodfweb

使用以下指令就可以確認初始化服務是否已正常啟動，指令如下：

netstat -tlnp

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	748/sshd
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN	902/master
tcp	0	0	127.0.0.1:9981	0.0.0.0:*	LISTEN	26766/ndcodfweb
tcp6	0	0	:::80	:::*	LISTEN	744/httpd
tcp6	0	0	:::22	:::*	LISTEN	748/sshd
tcp6	0	0	::1:25	:::*	LISTEN	902/master
tcp6	0	0	:::9980	:::*	LISTEN	26766/ndcodfweb

如果出現 9980 那行，代表【ODF 文件 Web 應用元件】服務已啟動，您可以重新啟動系統，再測試服務是否可正常啟動。

五、 進階設定

(1)設定使用對外服務位置

本文件前面所描述之使用情境，皆預設在「**內網 IP 環境**」，若機關佈署的環境開放以下二種情境者，需額外進行進階的設定，二種情境如下：

1. 使用真實 IP 對外開放服務(例如：117.56.68.133)
2. 使用 FQDN 做為服務主機名稱(例如：odf.nat.gov.tw)

請進入 ndcodfweb 主機上，修改 /etc/ndcodfweb/ndcodfweb.xml 的內容，找到以下這段：

<wopi desc="Allow/deny wopi storage. Mutually exclusive with webdav." allow="true">

<host desc="Regex pattern of hostname to allow or deny." allow="true">localhost</host>

<host desc="Regex pattern of hostname to allow or deny." allow="true">10\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}</host>

<host desc="Regex pattern of hostname to allow or deny." allow="true">172\.1[6789]\.[0-9]{1,3}\.[0-9]{1,3}</host>

<host desc="Regex pattern of hostname to allow or deny." allow="true">172\.2[0-9]\.[0-9]{1,3}\.[0-9]{1,3}</host>

<host desc="Regex pattern of hostname to allow or deny." allow="true">172\.3[01]\.[0-9]{1,3}\.[0-9]{1,3}</host>

<host desc="Regex pattern of hostname to allow or deny." allow="true">192\.168\.[0-9]{1,3}\.[0-9]{1,3}</host>

<host desc="Regex pattern of hostname to allow or deny." allow="true">117\.56\.68\.133</host>

<host desc="Regex pattern of hostname to allow or deny." allow="true">odf\.nat\.gov\.tw</host>

<host desc="Regex pattern of hostname to allow or deny." allow="false">192\.168\.1\.1</host>

<max_file_size desc="Maximum document size in bytes to load. 0 for unlimited."

type="uint">0</max_file_size>

</wopi>

請加入上述紅色那二段的範例內容，儲存後跳出，重新啟動 ndcodfweb 的服務即可。

systemc restart ndcodfweb

另外開放對外可連到這台主機以下的 port 號：80、9980

就可正常使用 ODF 雲端編輯器。

(2)設定啟用 SSL 憑證

若服務的主機運作在 SSL 協定上時，則可透過以下設定方式啟動 SSL，憑證申請的流程可參考 GCA 資證申請作業流程。

https://gca.nat.gov.tw/web2/apply01.html

申請好了之後，請將相關的憑證上傳至 ndcodfweb 主機上，建議可將憑證檔案放在 /etc/httpd/ssl 目錄下。

- Apache Web Server 的設定

先安裝 ssl 套件

yum install -y mod_ssl

vim /etc/httpd/conf.d/ssl.conf

修改以下 3 行(請依照實際的路徑設定)

SSLCertificateFile /etc/httpd/ssl/certificate.crt

SSLCertificateKeyFile /etc/httpd/ssl/private.key

SSLCACertificateFile /etc/httpd/ssl/ca_bundle.crt

存檔後，重啟服務。

systemctl restart httpd

- ODF 文件 Web 應用元件主程式

請進入 ndcodfweb 主機上，修改 /etc/ndcodfweb/ndcodfweb.xml 的內容，找到以下這段：

<enable type="bool" desc="Controls whether SSL encryption is enable (do not disable for production deployment). If default is false, must first be compiled with SSL support to enable." default="true">**true**</enable>

請將上述紅色的部份，由原來的 false 改為 true。

另外再指定以下 3 個憑證位置(路徑可與上述 httpd 的 SSL 憑證相同)，例子如下：

<cert_file_path desc="Path to the cert file" relative="false">**/etc/httpd/ssl/certificate.crt**</cert_file_path>

<key_file_path desc="Path to the key file" relative="false">**/etc/httpd/ssl/private.key**</key_file_path>

<ca_file_path desc="Path to the ca file"

relative="false">**/etc/httpd/ssl/ca_bundle.crt**</ca_file_path>

儲存後跳出，重新啟動 ndcodfweb 的服務即可。

systemc restart ndcodfweb

依照上述設定，正常就可以使用以下的連結使用服務：

https://yourhostname:9980 → 為【ODF 文件 Web 應用元件主程式(一般安裝說明如第貳章所示)】測試服務位置，出現 OK 字樣，並且瀏覽器端會顯示為合法憑證。

https://yourhostname/odfweb → 為預設【ODF 文件 Web 應用元件網路儲存空間軟體(一般安裝說明如第參章所示)】進入點，此時可成為加密型態。

參、安裝 ODF 文件 Web 應用元件網路儲存空間軟體

一、 安裝基本架構

(1)PHP 安裝

請安裝基本的 AMP(Apache、MariaDB 及 PHP)架構，因為 CentOS 預設的 PHP 版本過舊，建議直接升級至最新的 7 版本，相關指令如下：

rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

rpm -ivh http://rpms.remirepo.net/enterprise/remi-release-7.rpm

(注意)以上二個指令需按照順序執行。

啟動新版 PHP 的套件庫，利用 vim 修改設定檔：

vim /etc/yum.repos.d/remi-php72.repo

把第 9 行的 enabled=0 改為【enabled=1】並存檔離開。

```
[remi-php72]
name=Remi's PHP 7.2 RPM repository for Enterprise Linux 7 - $basearch
#baseurl=http://rpms.remirepo.net/enterprise/7/php72/$basearch/
#mirrorlist=https://rpms.remirepo.net/enterprise/7/php72/httpsmirror
mirrorlist=http://cdn.remirepo.net/enterprise/7/php72/mirror
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-remi
```

yum update -y

yum install php php-mysql php-gd php-ldap php-odbc php-pear php-xml php-xmlrpc php-mbstring php-snmp php-soap php-intl curl -y

設定啟動 httpd 服務，指令如下：

systemctl enable httpd

systemctl restart httpd

(2)MariaDB 資料庫安裝

接下來安裝資料庫 MariaDB，指令如下：

yum install mariadb mariadb-server -y

設定啟動 MariaDB 服務，指令如下：

systemctl enable mariadb

systemctl restart mariadb

接下來請初始化 MariaDB 的環境，指令如下：

mysql_secure_installation

會出現以下訊息：

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB

SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current

password for the root user. If you've just installed MariaDB, and

you haven't set the root password yet, the password will be blank,

so you should just press enter here.

Enter current password for root (enter for none):(**按 enter 鍵繼續**)

OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB

root user without the proper authorisation.

Set root password? [Y/n] **Y + Enter 鍵**

New password:**輸入第一次資料庫管理員(root)密碼 + Enter 鍵**

Re-enter new password:**輸入第二次資料庫管理員(root)密碼 + Enter 鍵**

Password updated successfully!

Reloading privilege tables..

... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone

to log into MariaDB without having to have a user account created for

them. This is intended only for testing, and to make the installation

go a bit smoother. You should remove them before moving into a

production environment.

Remove anonymous users? [Y/n] **Y + Enter 鍵**

... Success!

Normally, root should only be allowed to connect from 'localhost'. This

ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] **Y + Enter 鍵**

... Success!

By default, MariaDB comes with a database named 'test' that anyone can

access. This is also intended only for testing, and should be removed

before moving into a production environment.

Remove test database and access to it? [Y/n] **Y + Enter 鍵**

- Dropping test database...

... Success!

- Removing privileges on test database...

... Success!

Reloading the privilege tables will ensure that all changes made so far

will take effect immediately.

Reload privilege tables now? [Y/n]] **Y + Enter 鍵**

... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB

installation should now be secure.

Thanks for using MariaDB!

完成資料庫安裝作業。

(注意)請記得您剛剛設定的資料庫 root 密碼，等一下會需要使用到。

(3)安裝資料庫管理介面 phpMyAdmin

為了可以設定資料庫的權限，及便於未來可管理(備份或是修改資料)資料庫，建議可安裝 phpMyAdmin 這套網頁介面的 MariaDB 管理工具，安裝指令如下：

```
# yum install phpMyAdmin -y
```

利用 vim 編輯/etc/httpd/conf.d/phpMyAdmin.conf 內容，並註解以下的內容(大約從第 11 行至第 28 行)，允許從其他的網段登入 phpMyAdmin：

```
[...]

Alias /phpMyAdmin /usr/share/phpMyAdmin

Alias /phpmyadmin /usr/share/phpMyAdmin

#<Directory /usr/share/phpMyAdmin/>

#   <IfModule mod_authz_core.c>

#     # Apache 2.4

#     <RequireAny>

#       Require ip 127.0.0.1

#       Require ip ::1

#     </RequireAny>

#   </IfModule>

#   <IfModule !mod_authz_core.c>

#     # Apache 2.2

#     Order Deny,Allow

#     Deny from All

#     Allow from 127.0.0.1

#     Allow from ::1

#   </IfModule>

#</Directory>
```

並在該段下面加入以下內容：

```
<Directory /usr/share/phpMyAdmin/>

        Options none

        AllowOverride Limit
```

```
        Require all granted
</Directory>
[...]
```

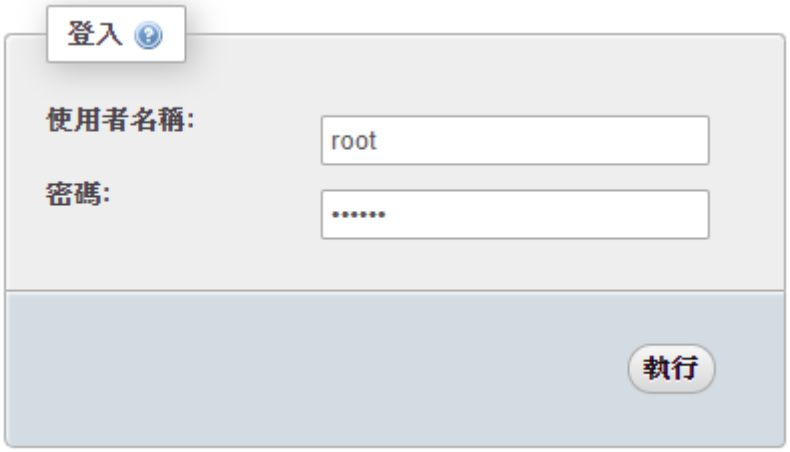
存檔離開後，再重新啟動網頁伺服器的服務。

```
# systemctl restart httpd
```

(4)設定一般的資料庫使用者帳號及權限

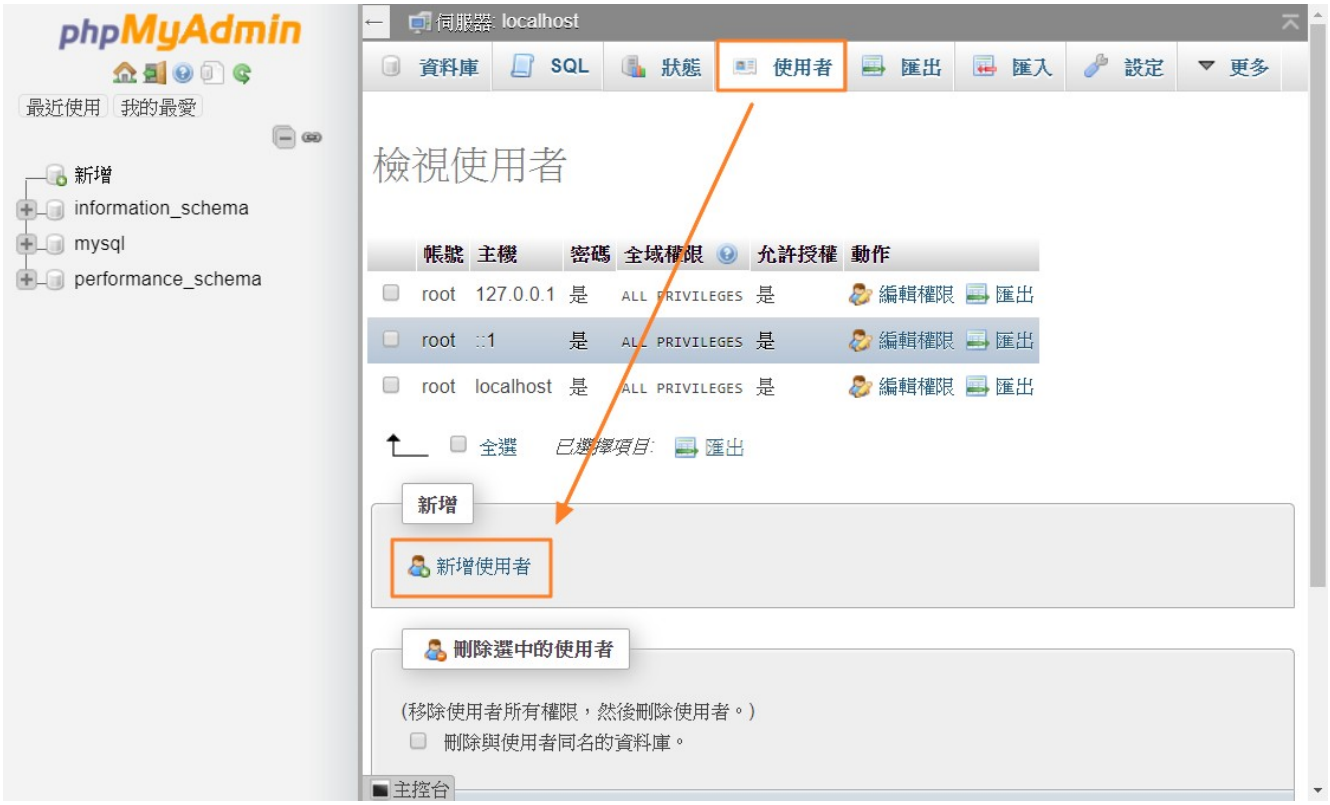
為了資安問題，建議資料庫的 root 使用者帳號儘量不要在開放的網站上使用，可透過 phpMyAdmin 新增一組權限較少的一般用戶帳號給網站專案使用，請登入 phpMyAdmin 的網頁，以本文件為例，登入頁面如下：

http://yourserverip/phpMyAdmin

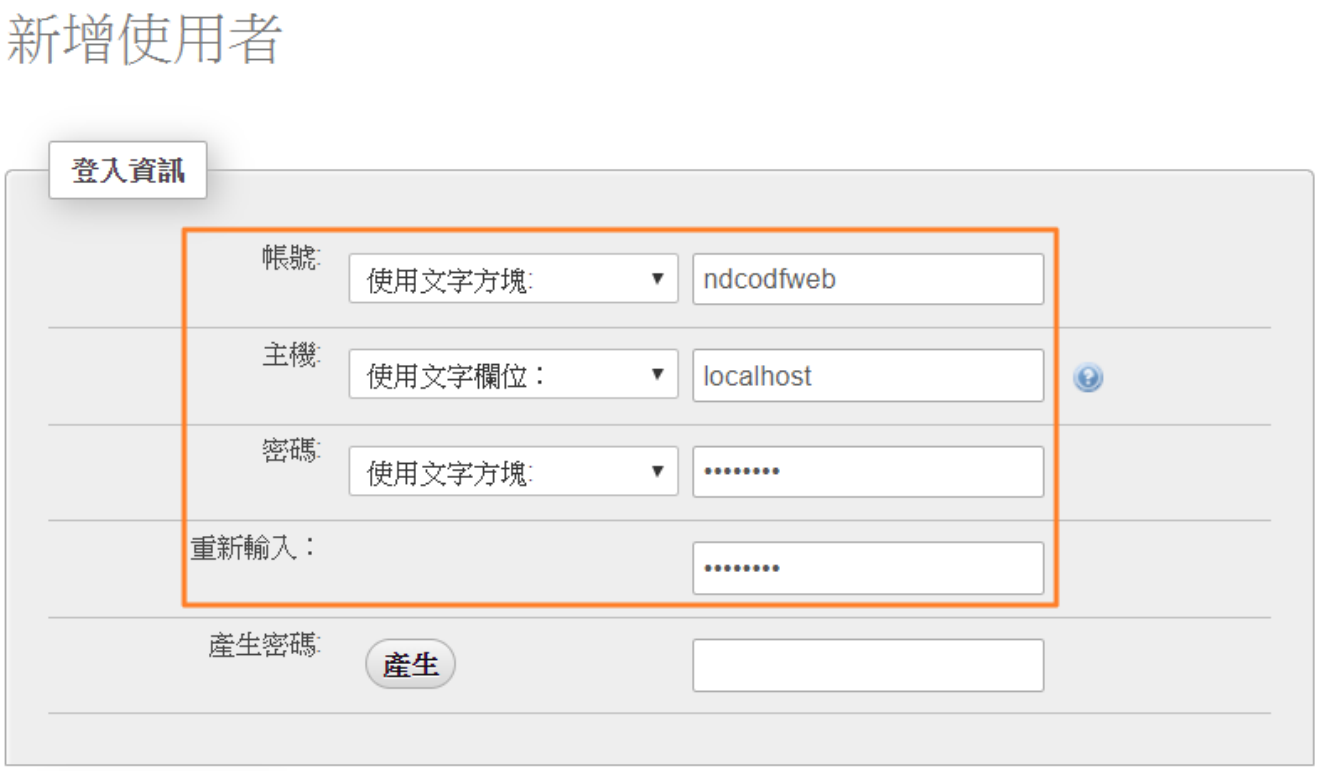


輸入剛剛的 root 帳號及密碼，登入 phpMyAdmin 主畫面，如下所示：

點擊畫面上的【使用者】及【新增使用者】連結。

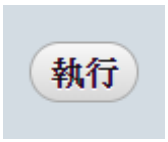


輸入資料庫「使用者帳號」、「主機」及二次密碼，其中建議主機的部份填入「localhost」。

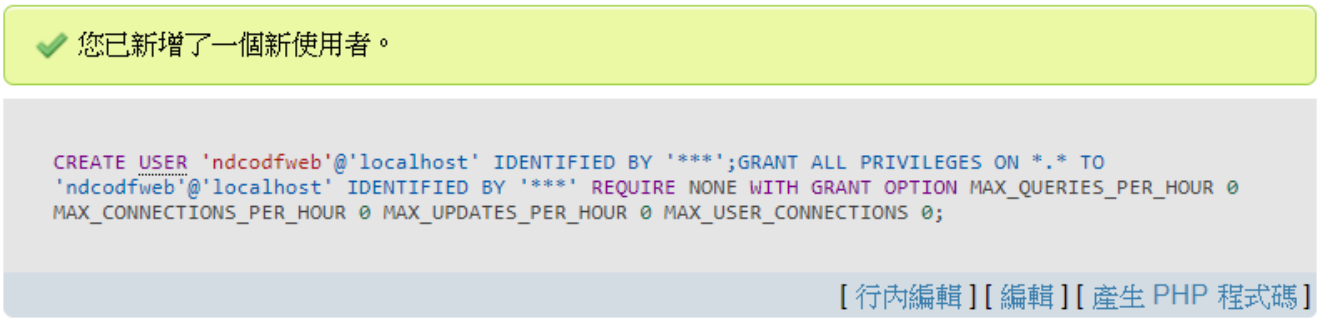


再把畫面往下拖曳，選擇權限相關的設定，這裡我們將暫時為此使用者開放所有的指令權限。

最後畫面拉到最下方，按下【執行】鍵完成用戶新增的作業。



成功的畫面如下所示，完成後就可以登出這個管理介面，請記得這個使用者的名稱及密碼。



(5)初始化資料庫

請登入剛剛建立的 phpMyAdmin 管理者畫面，點選畫面最上方的【資料庫】，並在【建立新資料庫】的名稱部份填入【ndcodfweb】、【編碼與規則】的部份選擇【utf8mb4_unicode_ci】，最後請按下【建立】鍵完成。

完成畫面如下：


phpMyAdmin
最近使用
我的最愛
新增
information_schema
mysql
ndcodfweb
performance_schema

二、 安裝 ODF 文件 Web 元件應用儲存空間軟體工具

(1)上傳安裝檔案

剛剛已上傳整個「NDCODFWEB-V1.6.zip」檔案，解壓縮之後會有以下檔案。

cd /root/NDCODFWEB-V1.6

ls -la

- odfweb-1.6.zip

(2)解壓縮並設定目錄權限

操作指令如下：

cd /root/NDCODFWEB-V1.6/

unzip odfweb-1.6.zip

mv odfweb /var/www/html

rm odfweb-1.6.zip

rm：是否移除普通檔案 ‘odfweb-1.6.zip’? **Y + Enter 鍵**

cd /var/www/html

chown apache.apache -R odfweb

(3)進入安裝網頁

本系統的預設安裝網址連結如下，實際登入畫面請依據各機關網路設定為準。

http://192.168.3.109/odfweb，登入畫面如下圖。

請先自行初始化管理者的【使用者名稱】及【密碼】，如上圖所示，並且點擊畫面上的【儲存空間和資料庫】選擇【MySQL/MariaDB】的部份，以下欄位請填寫對應的值：

資料庫使用者：填入第參章第一節第(四)點所設定的資料庫使用者名稱。

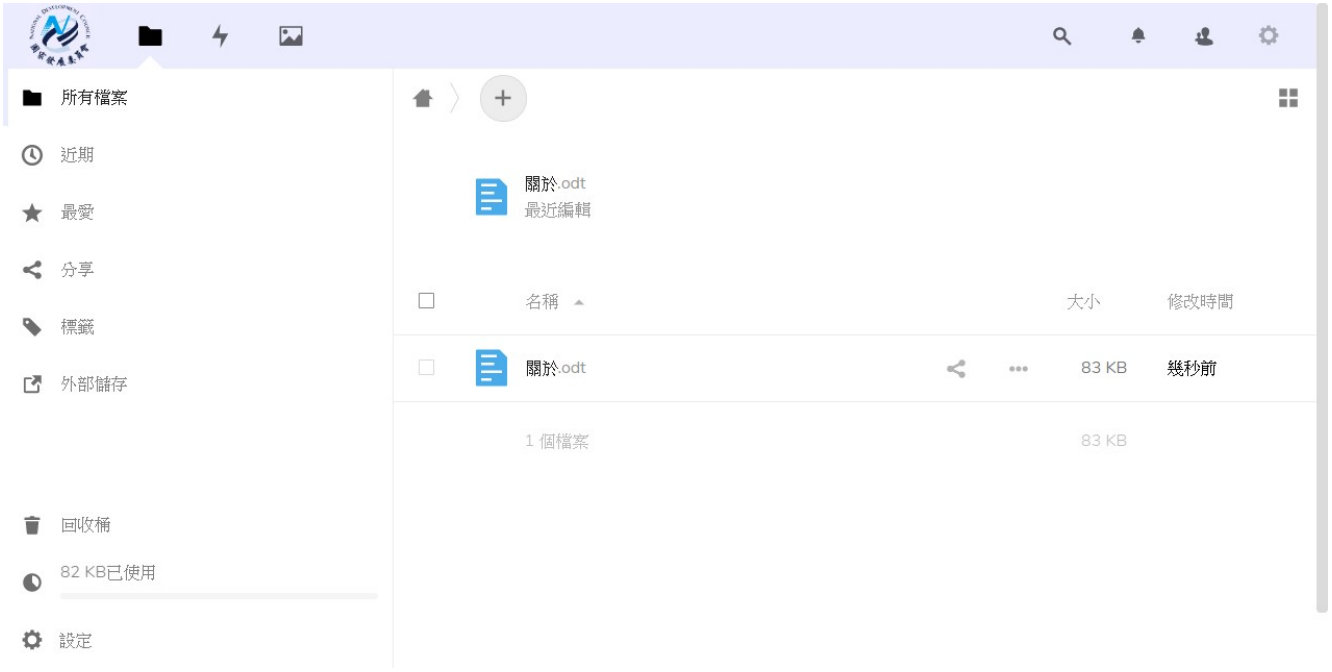
資料庫密碼：填入第參章第一節第(四)點所設定的資料庫使用者密碼。

資料庫名稱：填入第參章第一節第(五)點所設定的資料庫名稱。


儲存空間和資料庫
資料儲存位置
/var/www/html/odfweb/data
設定資料庫
SQLite
MySQL/MariaDB
ndcodfweb
ndcodfweb
localhost
請將具體指定連接埠號與主機名稱。(例如：
localhost:5432)
完成設定
需要協助嗎？ 閱讀 odfweb 安裝說明書 ↗

(4)進入安裝網頁

完成設定後按下【完成設定】，系統就會進行安裝的作業流程，完成後系統會自動入管理員的帳號，會出現以下的畫面。



至此已完成【ODF 文件 WEB 應用元件】系統的基本安裝作業。

(5)調整資料庫帳號權限

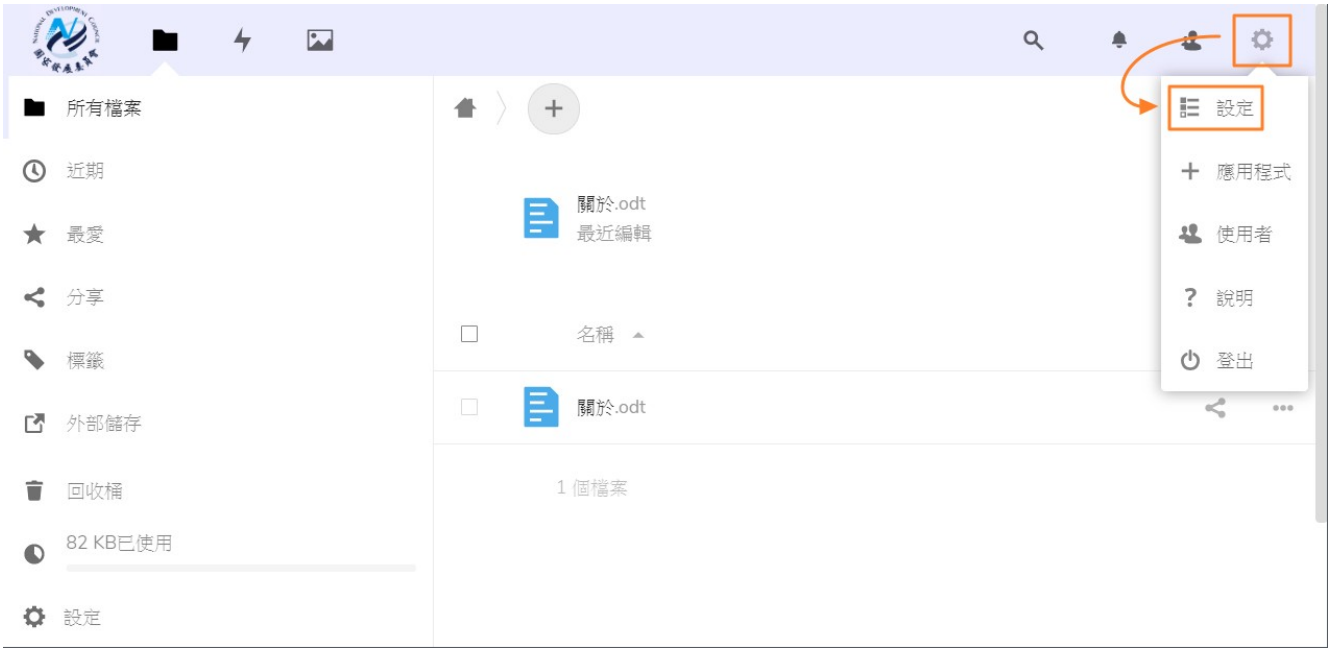
安裝完成後，需要將原有的資料庫帳號的權限調回一般的設定，請依照第參章第一節第(四)點的說明，修改使用者的權限，請參考以下的畫面：

完成後把畫面往下拖曳，按下「執行」鍵即完成設定。

三、 網站基本參數設定（重要）

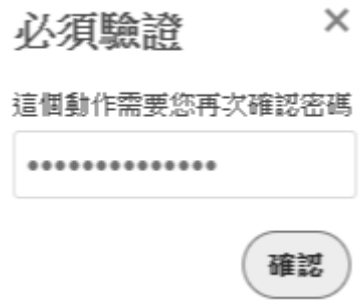
(1)設定基本資料、語言與時區

以 admin 登入後的畫面如下：



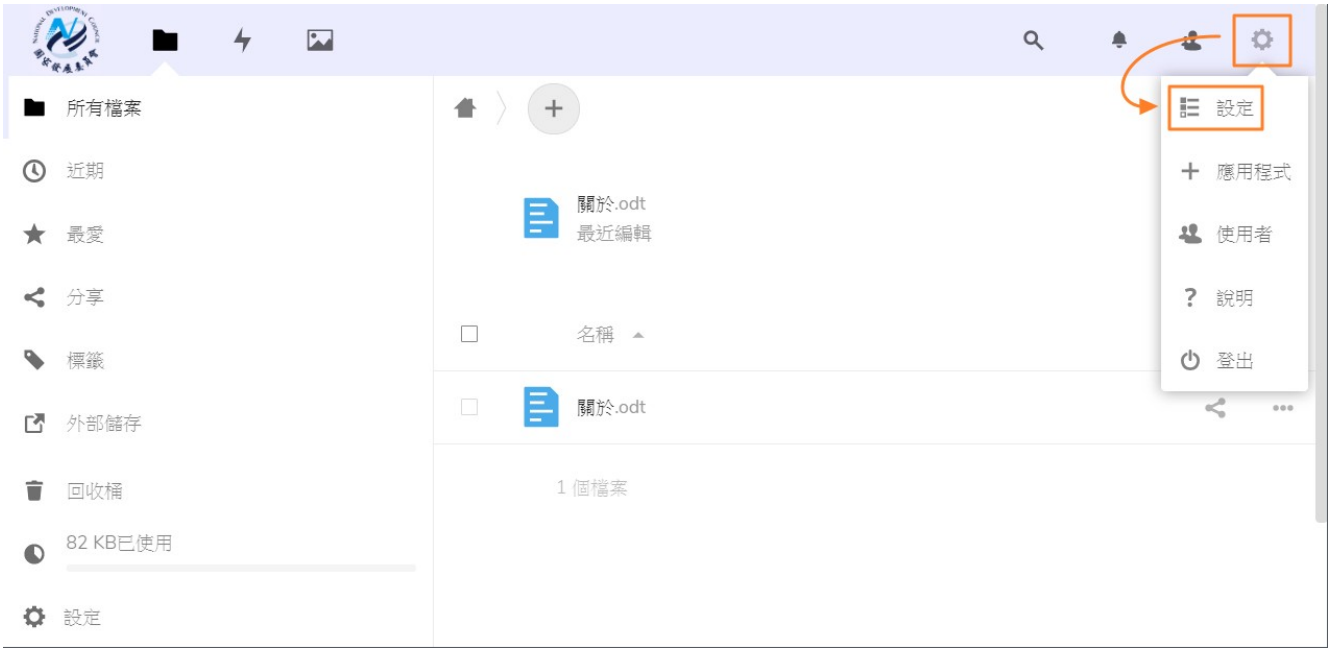
請點選右上角的「齒輪」圖示，在下拉式選單點選「設定」，會出現以下的設定畫面。

在此畫面可以設定此帳號的基本資料、語系及所在地，完成後系統會詢問一次密碼，輸入正確密碼後即完成變更動作。



(2)設定系統 Logo

以 admin 登入後的畫面如下：

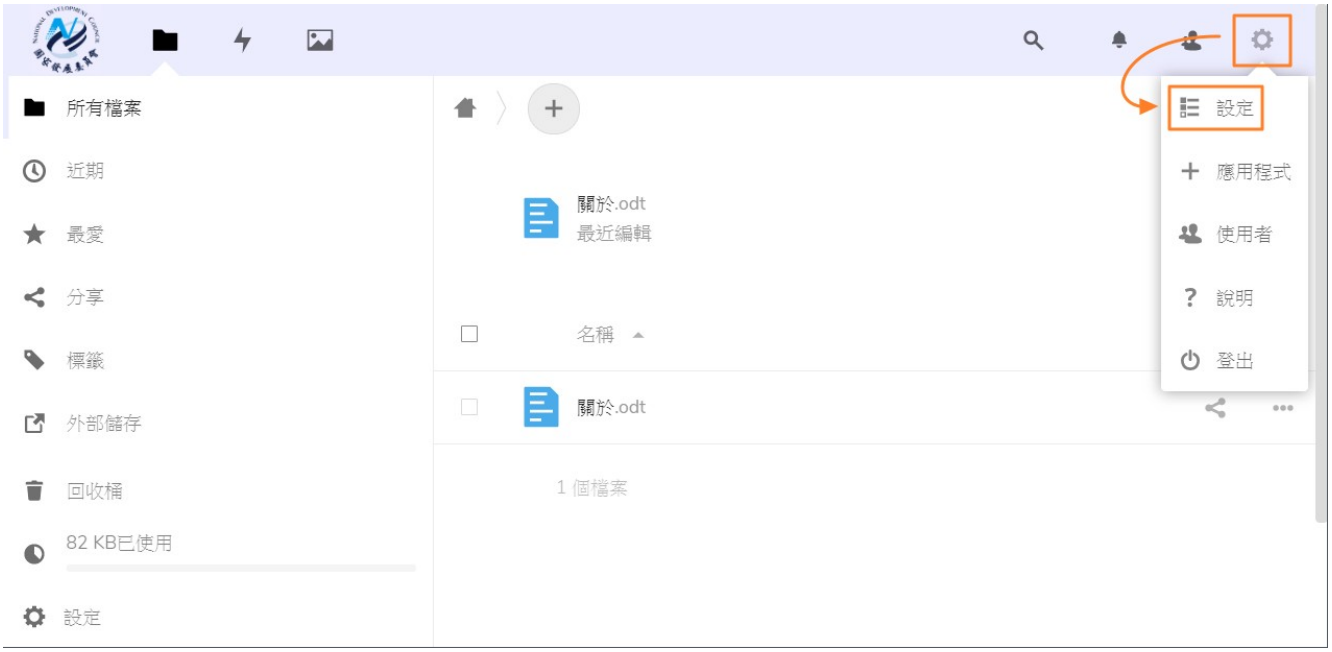


請按下右上角的「齒輪」圖示，在下拉式選單點選「設定」，進入到設定畫面後，在左方選單往下捲動後，按下左方的【佈景主題】，會出現右方的畫面，如下圖所示。

請點選【Logo】右方的上傳圖示，並選擇要設定的 logo 檔案即可生效，畫面如下。

(3)設定 ODF 文件 Web 應用元件模組

以 admin 登入後的畫面如下：



請按下右上角的「齒輪」圖示，在下拉式選單點選「設定」，進入到設定畫面後，在左方選單往下捲動後，按下左方的【ODF 文件 Web 應用元件】，會出現右方的畫面，如下圖所示。

請在【ODF 文件 WEB 應用元件伺服器的 URL(及服務 port 號)】的欄位輸入第貳章第四節的 IP 及埠號，本文件的例子為：【 http://192.168.3.109:9980】

完成後按下【套用】鍵後，即完成【ODF 文件 Web 應用元件】模組的設定工作，接下來按下畫面上方的資料匣圖示，接著點擊其中一個文件。

如果有開啟編輯文件的畫面，就代表設定成功了，如下圖所示。

四、 設定掛載外部網路芳鄰空間

(1)請先安裝 smbclient 套件

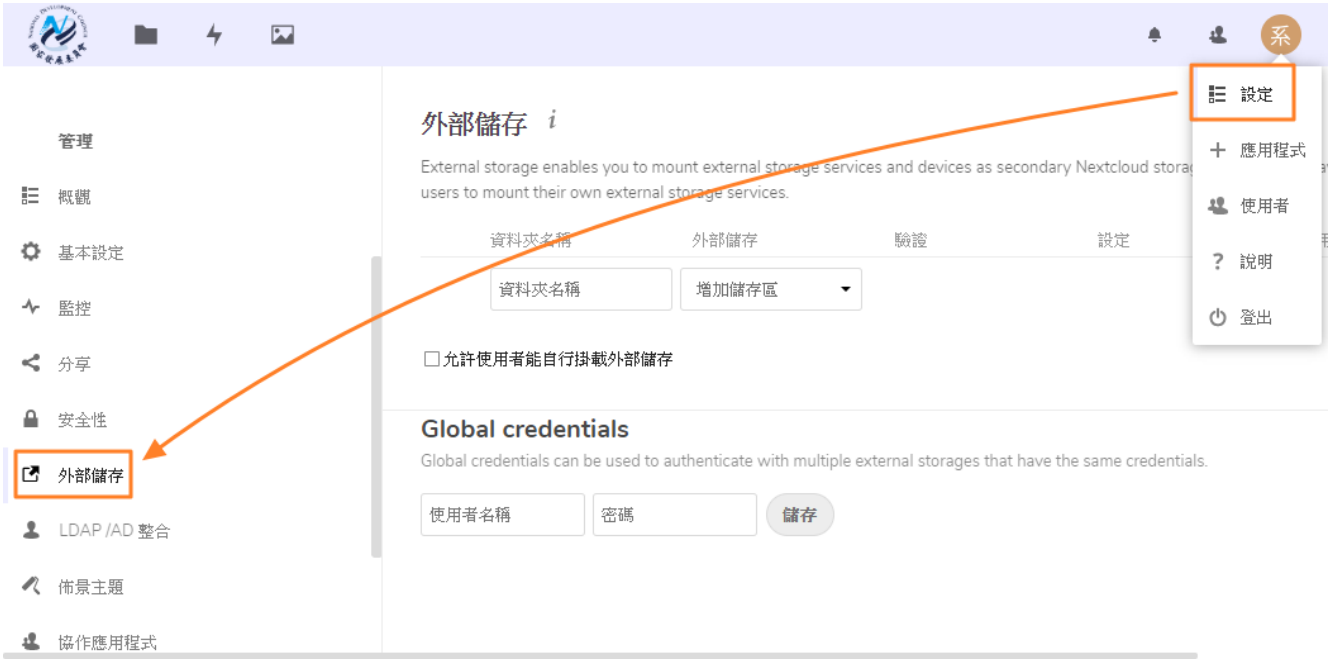
操作指令如下：

yum install -y php-smbclient

systemctl restart httpd

(2)設定 ODF 文件 Web 應用元件模組

以 admin 登入後的畫面如下：



請按下右上角的「齒輪」圖示，在下拉式選單點選「設定」，進入到設定畫面後，在左方選單往下捲動後，按下左方的【外部儲存】，會出現右方的畫面，如下圖所示。

資料夾名稱：可自訂一個顯示在使用者目錄列表的名稱。

主機：設定 SMB(NAS)的主機位置

分享：設定要掛載的 SMB 目錄名稱

網域名稱：NAS 所在的網域名稱

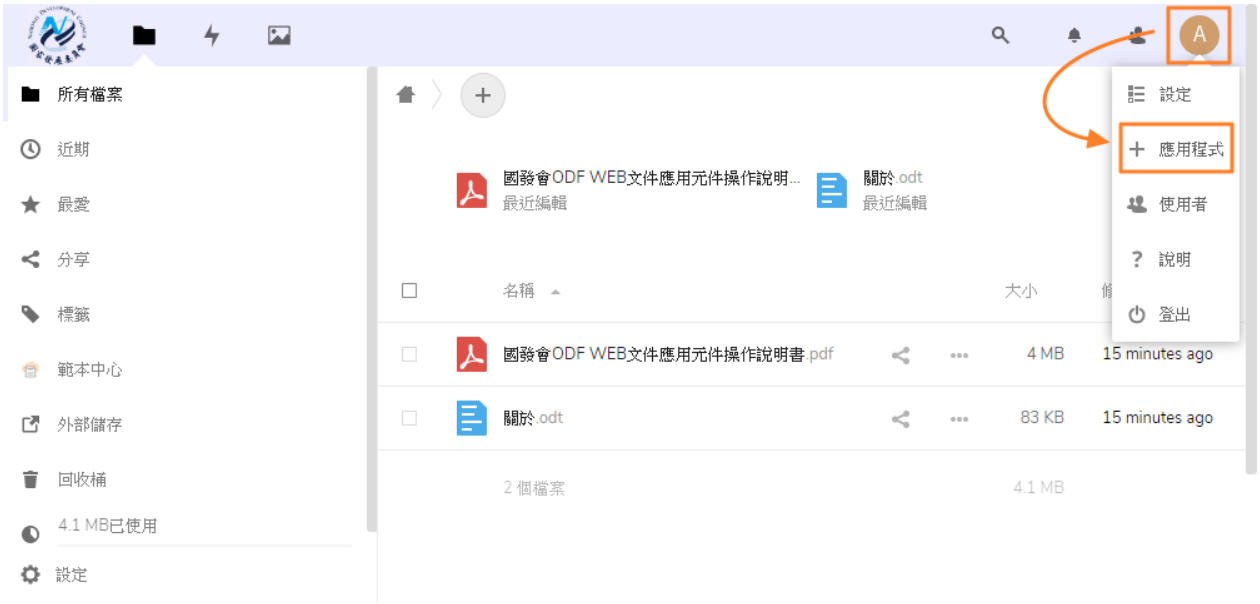
使用者名稱、密碼：提供登入此 SMB 位置的使用者資訊，建議使用公共帳號。

可用的：預設為所有 ODF 文件 Web 應用元件模組的帳號都能用，可設定特定帳號才可存取此目錄。

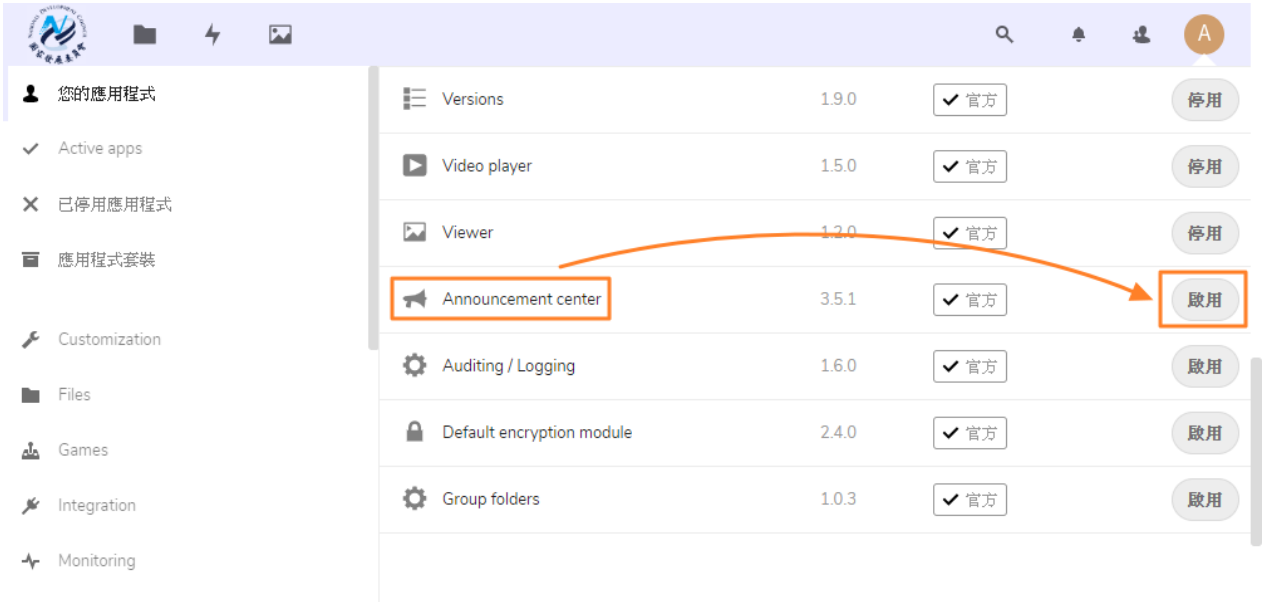
完成後按下右方的勾勾，即可掛載 SMB(NAS)目錄。

五、 啟動訊息公告模組

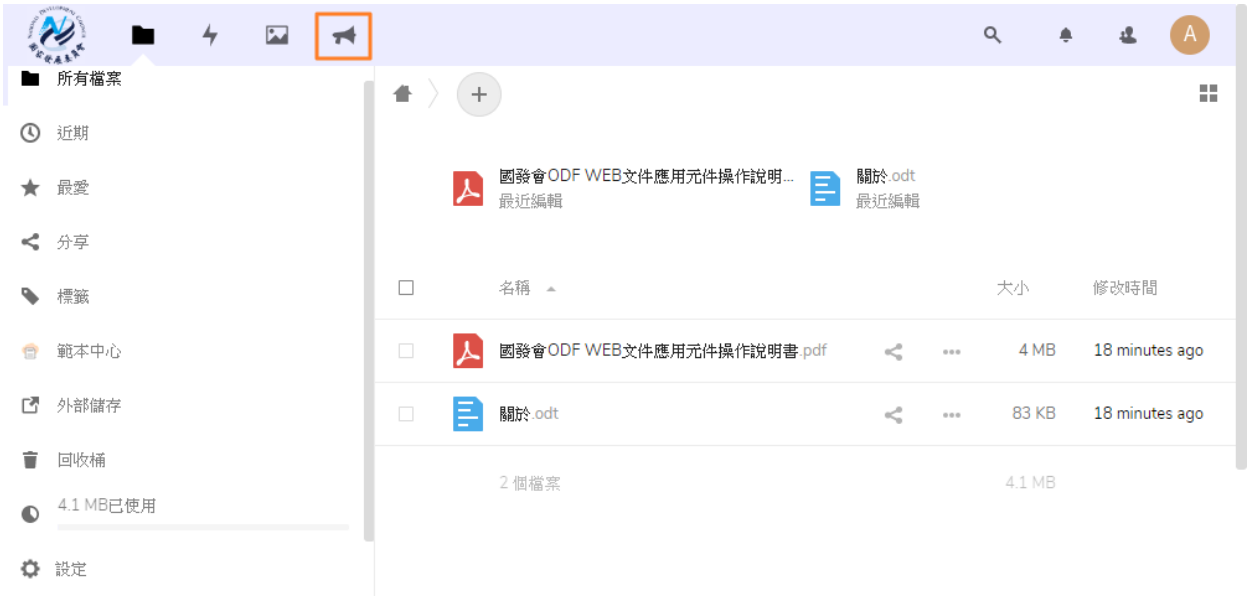
以 admin 登入後的畫面如下：



接下來會看到目前可使用的模組清單，點選【Announcement center】右方的「啟用」鍵啟用此功能。

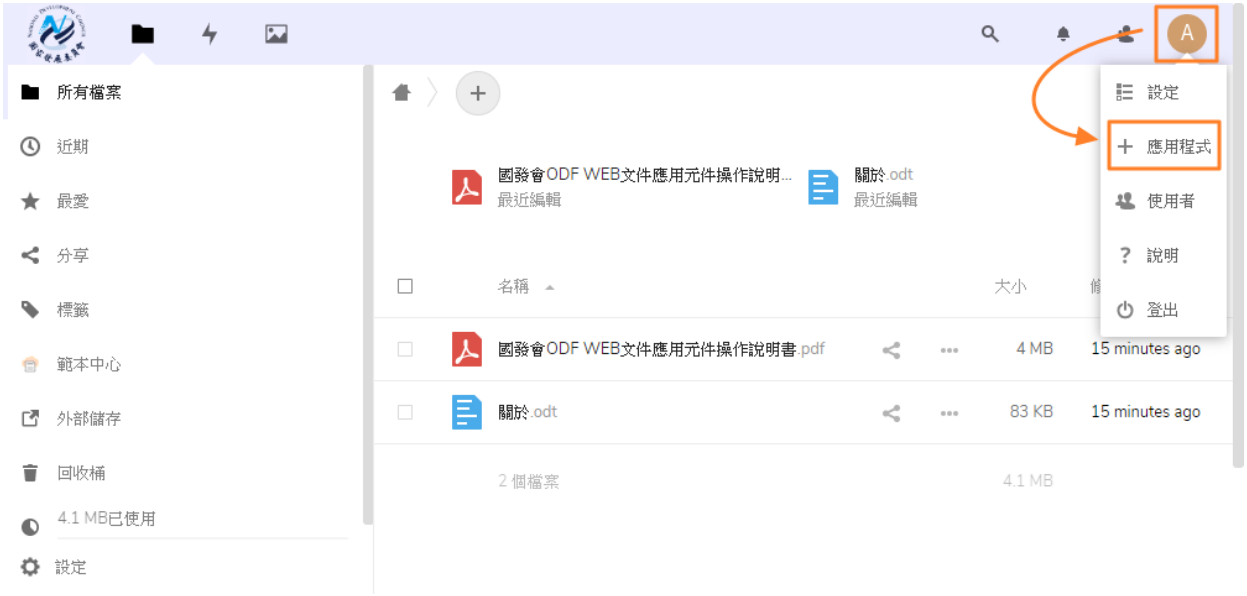


第一次啟用請輸入這個登入管理者的密碼，輸入完成後就成功啟動功能，回到首頁就可以看到功能圖示。

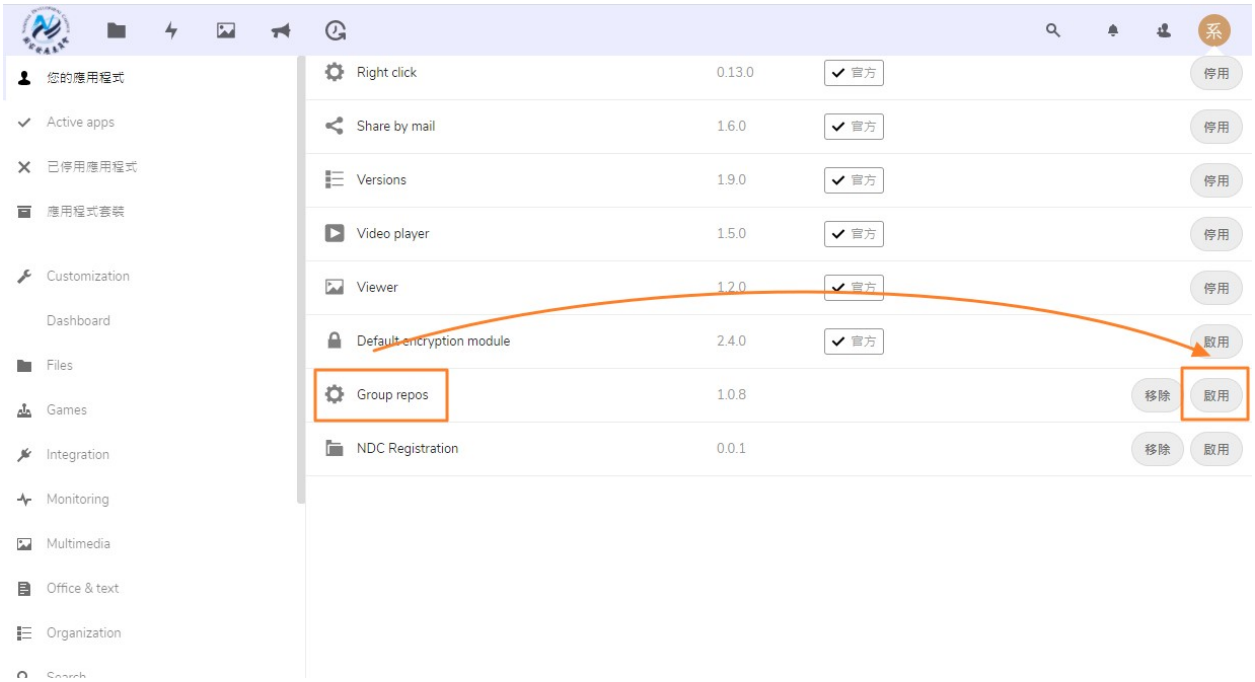


六、 啟動群組共享目錄模組

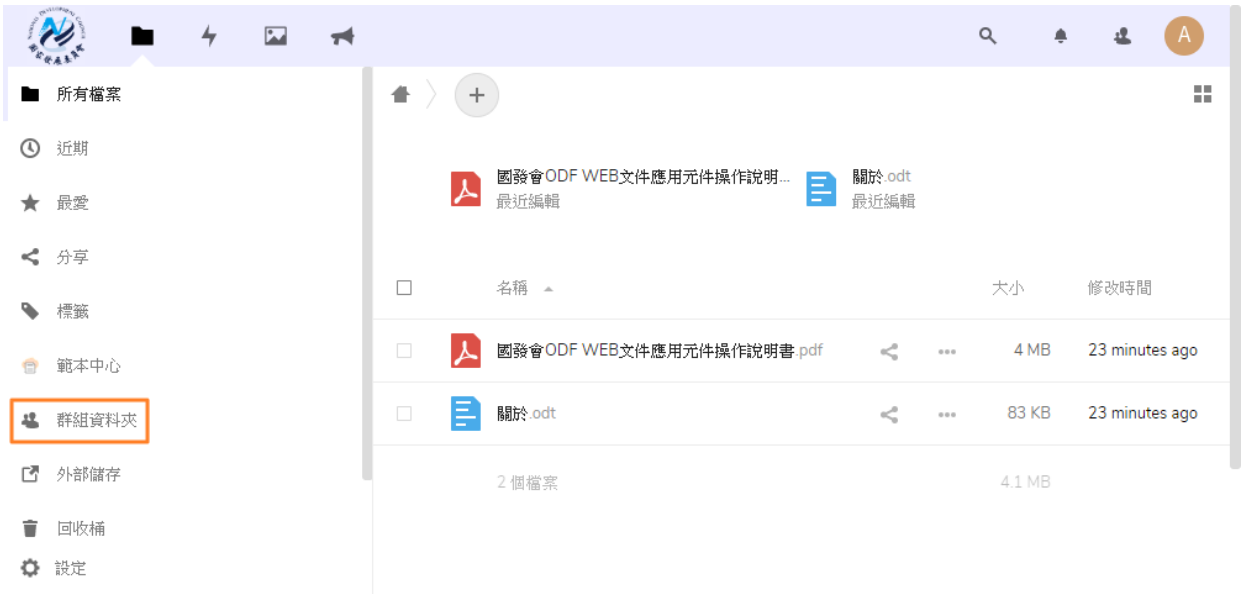
以 admin 登入後的畫面如下：



接下來會看到目前可使用的模組清單，點選【Group repos】右方的「啟用」鍵啟用此功能。

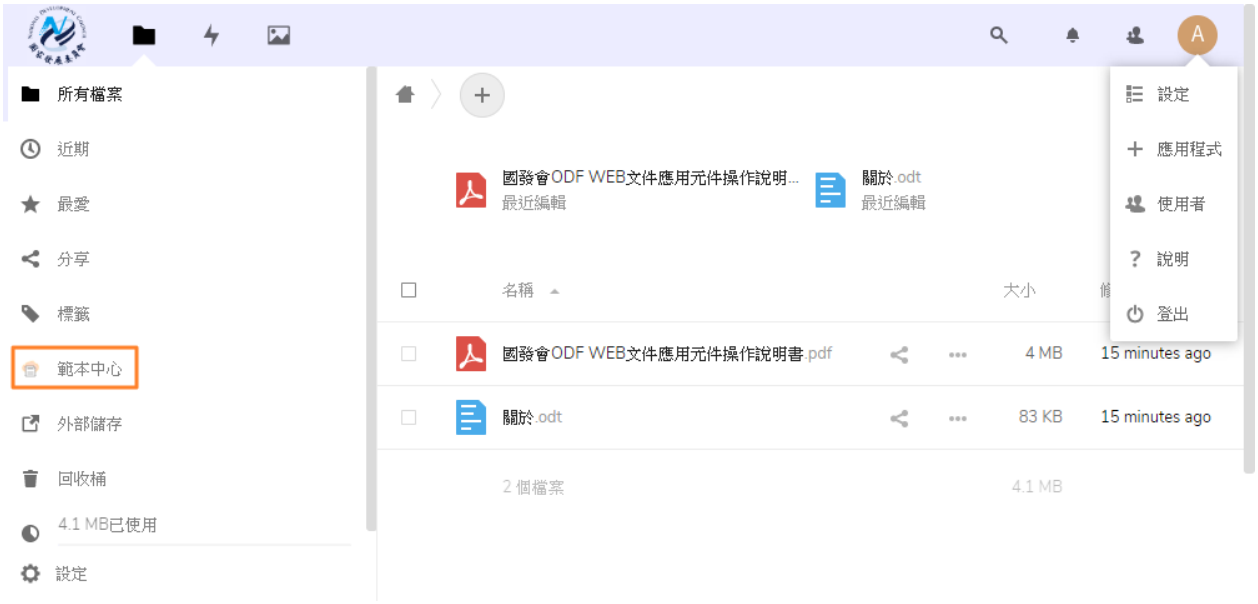


第一次啟用請輸入這個登入管理者的密碼，輸入完成後就成功啟動功能，回到首頁就可以看到畫面左方有新增功能圖示。



七、 啟動機關範本中心模組

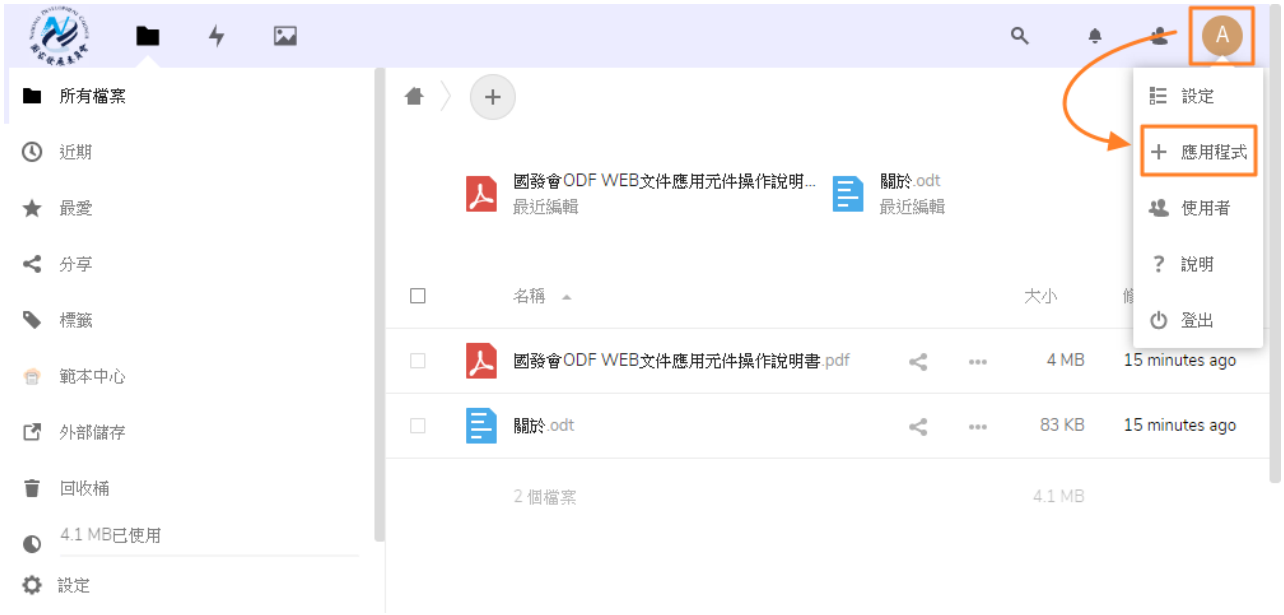
以 admin 登入後的畫面如下：



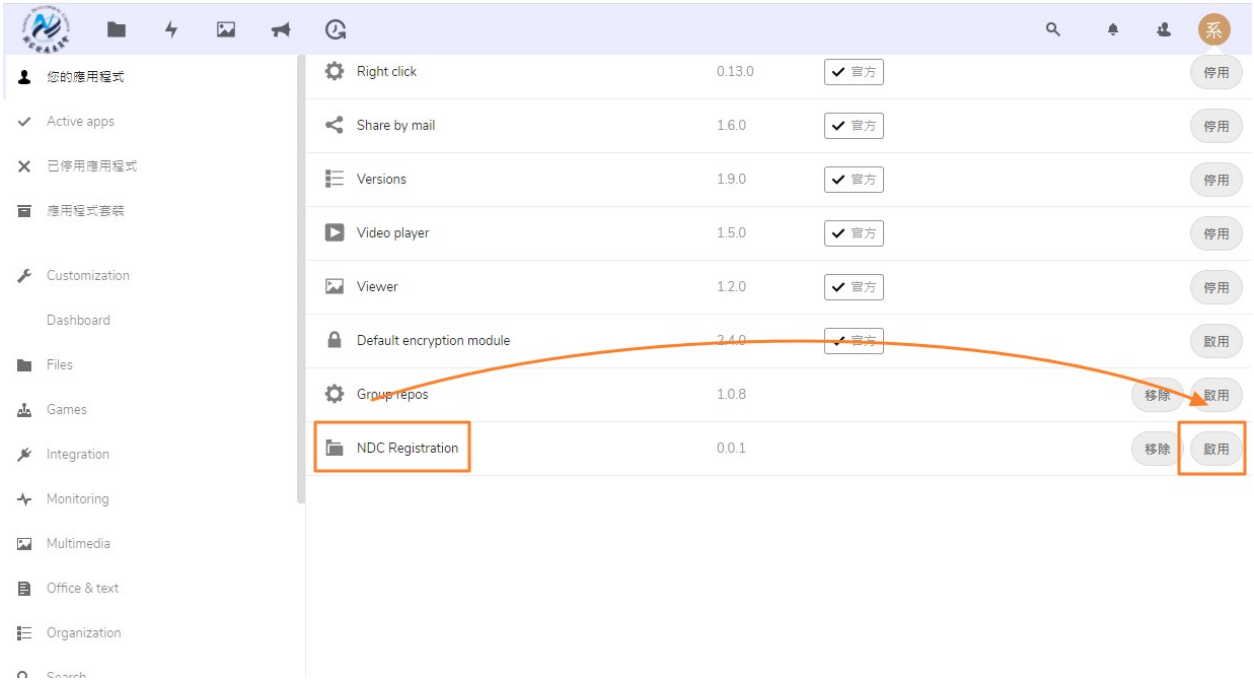
機關範本中心模組預設會自動啟用，看到此圖示就代表已可使用此功能。

八、 啟動自助註冊模組

以 admin 登入後的畫面如下：



接下來會看到目前可使用的模組清單，點選【NDC Registration】右方的「啟用」鍵啟用此功能。

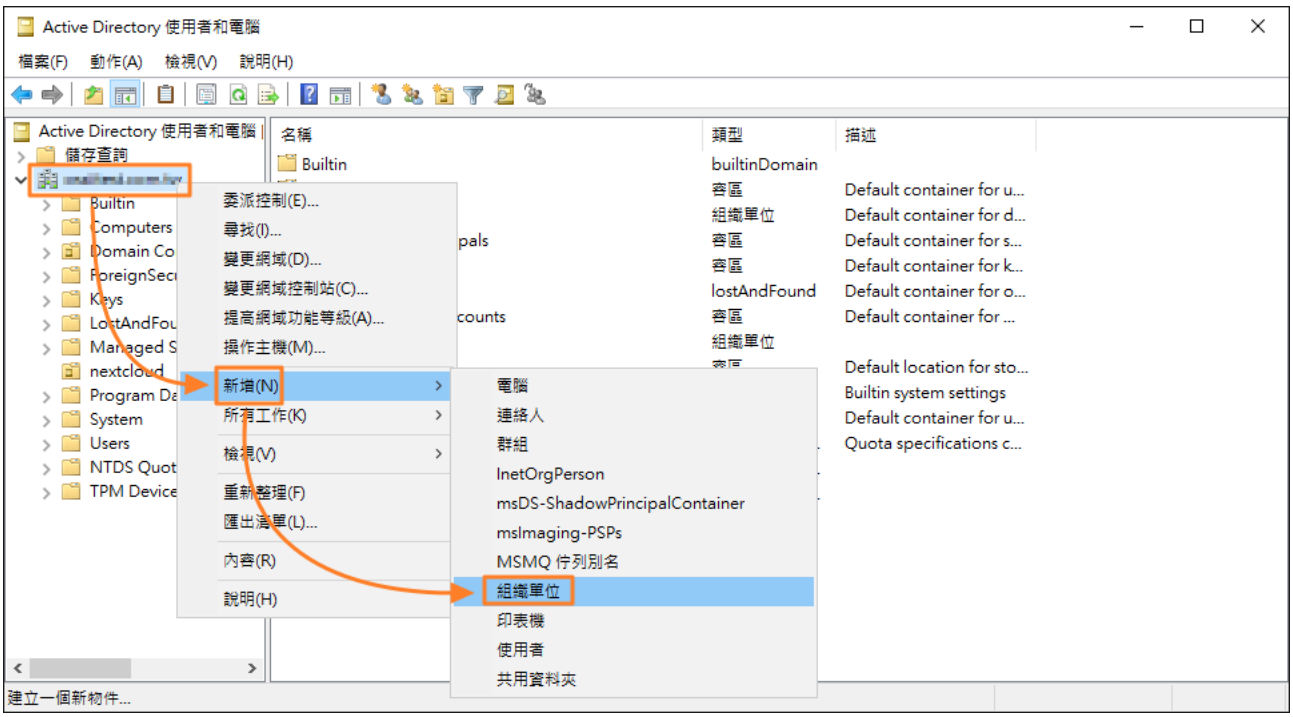


九、AD 整合設定範例

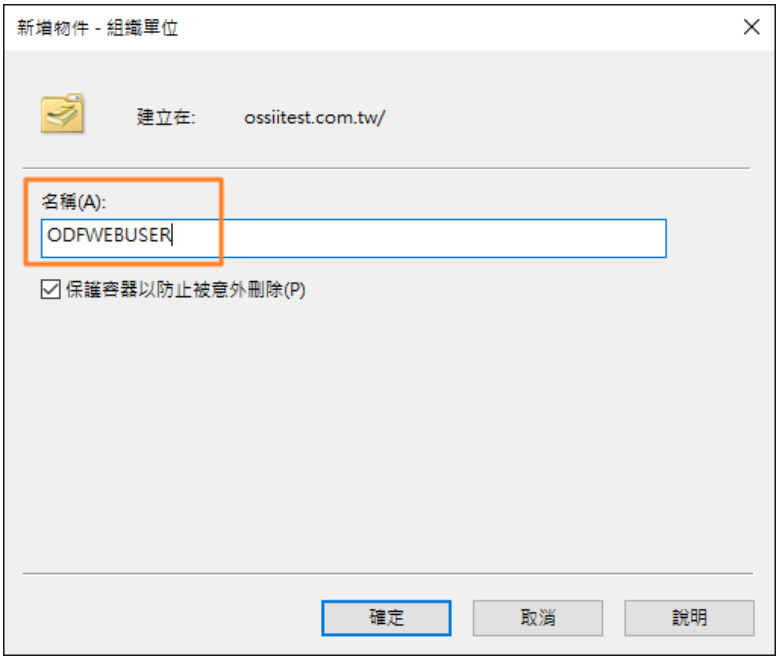
(1)AD 端設定

首先建議需先在 AD 端建立一個提供給 Web 端具備查詢 AD 帳號功能的帳號，請使用機關內 AD 的「伺服器管理員」並點選「工具」選擇「Active Directory」。

接下來在網域的根目錄下按下「滑鼠右鍵」並選擇「新增」-「組織單位」。

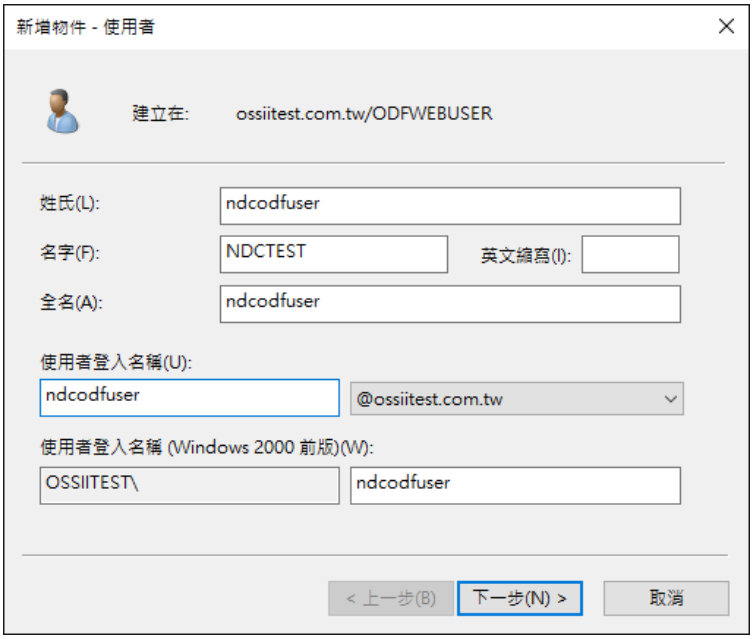


輸入組織單位(後簡稱 OU)的名稱(此處為示範內容，一般會使用現有的 OU 內容，通常不需另行新增)。

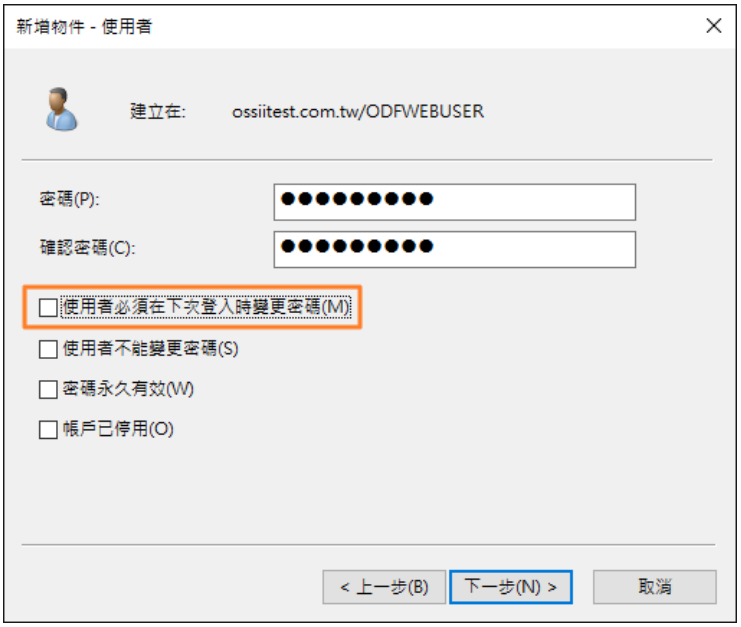


在此 OU 下，建立一個使用者帳號(該使用者也可以不建立於相同的 OU 中，在此只單純示範設定方式)，用以賦予查詢帳號資訊的權限，以供 ODF 文件

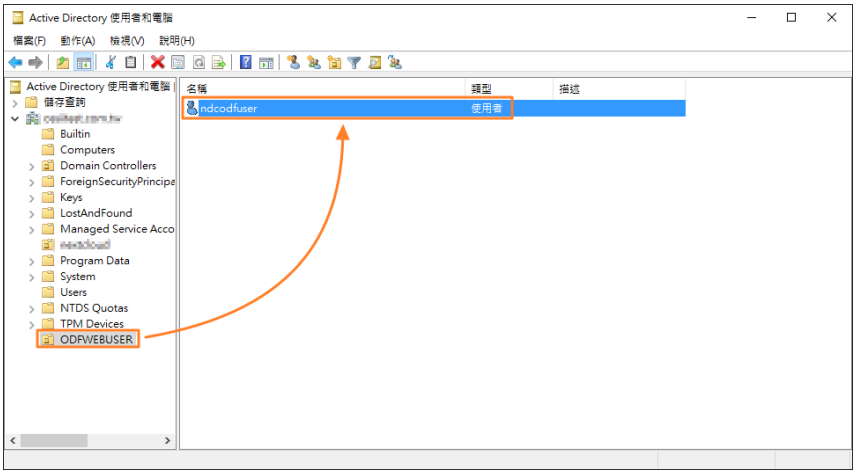
Web 應用元件網路儲存空間軟體使用，一樣利用滑鼠右鍵點擊剛剛建立的 OU(範例為 ODFWEBUSER)，選擇「新增」-「使用者」，輸入使用者的相關資訊。



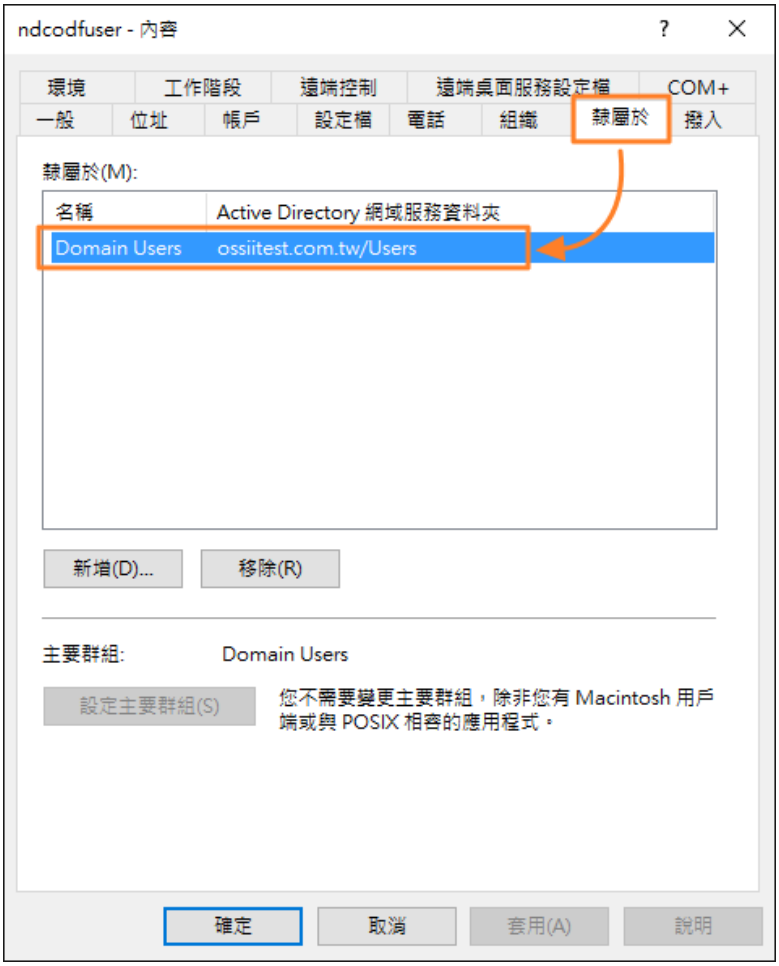
輸入密碼並完成設定，請注意，基於資安因素，通常只限於在 AD 端變更密碼，故此帳號會取消第一次登入變更密碼的功能，才能正常查詢資訊。



完成的畫面如下所示：

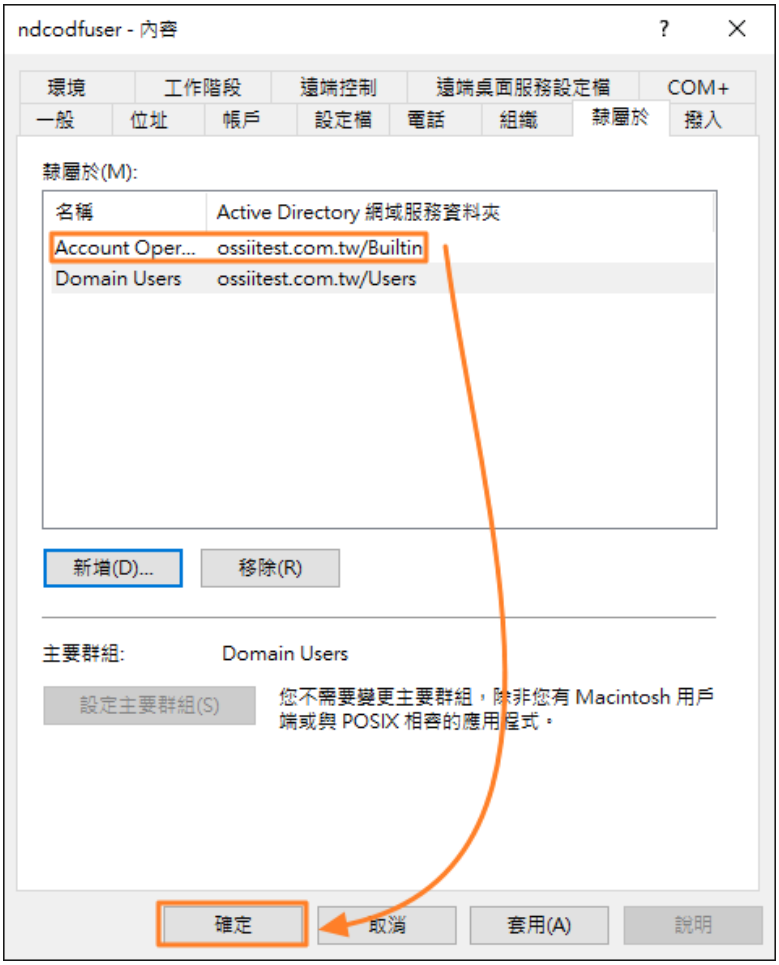


接下來請利用滑鼠右點選這個新增的使用者並選擇「內容」，並點選視窗的「隸屬於」選項，預設畫面如下：

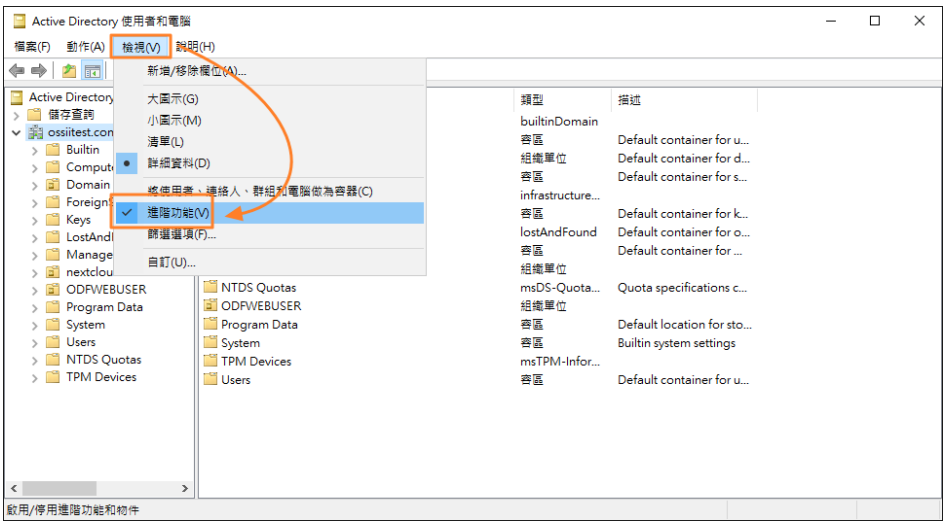


點選畫面的「新增」並加入「Account Operators」，檢查名稱後按下確定完成。

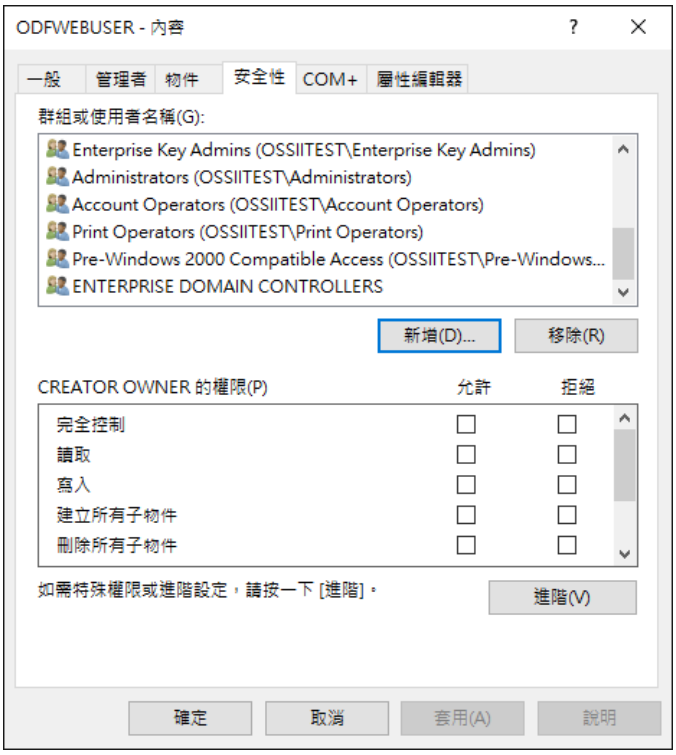
按下「確定」鍵後會出現以下畫面，確認新增完成後再按下「確定」離開。



接下來要設定剛剛這個新增的使用者，具備查詢 NDCWEBUSER 這個 OU 資訊的權限，請先在「Active Directory 使用者和電腦」的畫面點選「檢視」-「進階」，畫面如下：

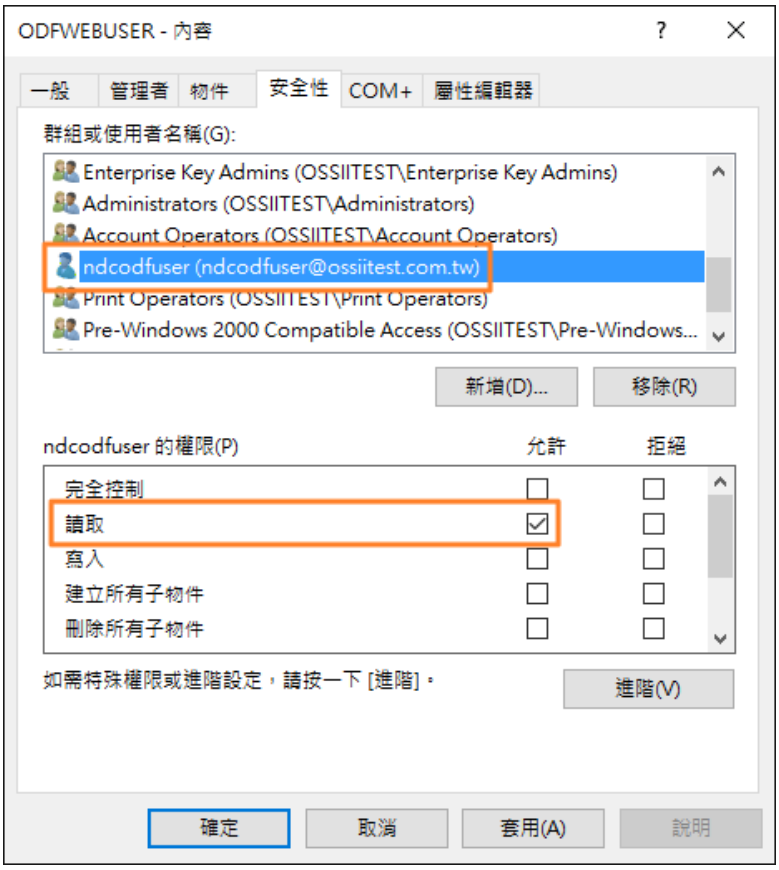


接下來，利用滑鼠右鍵點選剛剛的範例 OU，點選「內容」並在視窗中選擇「安全性」，如下圖所示。

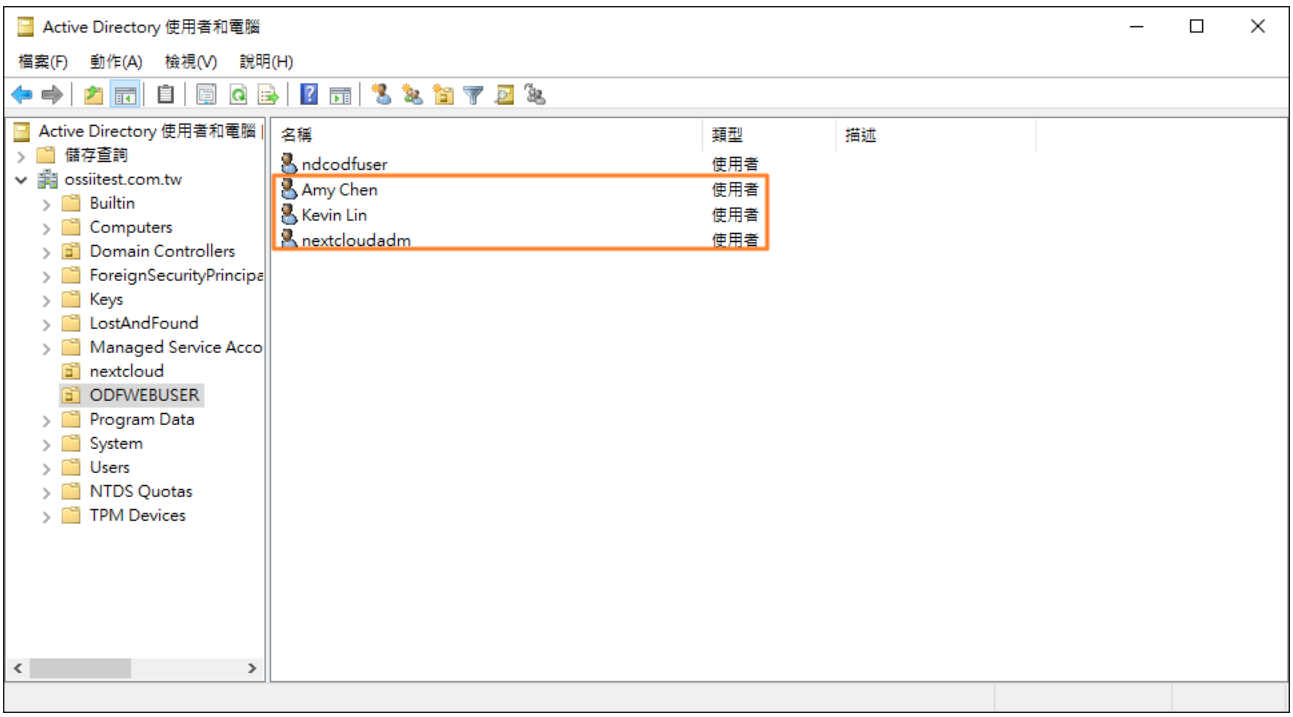


點選畫面中的「新增」來新增一個使用者，在「輸入物件名稱來選取」的區域中，輸入剛剛建立的 user 名稱(範例為：ndcodfuser)，並按下「檢查名稱」-「確定」如下圖所示：

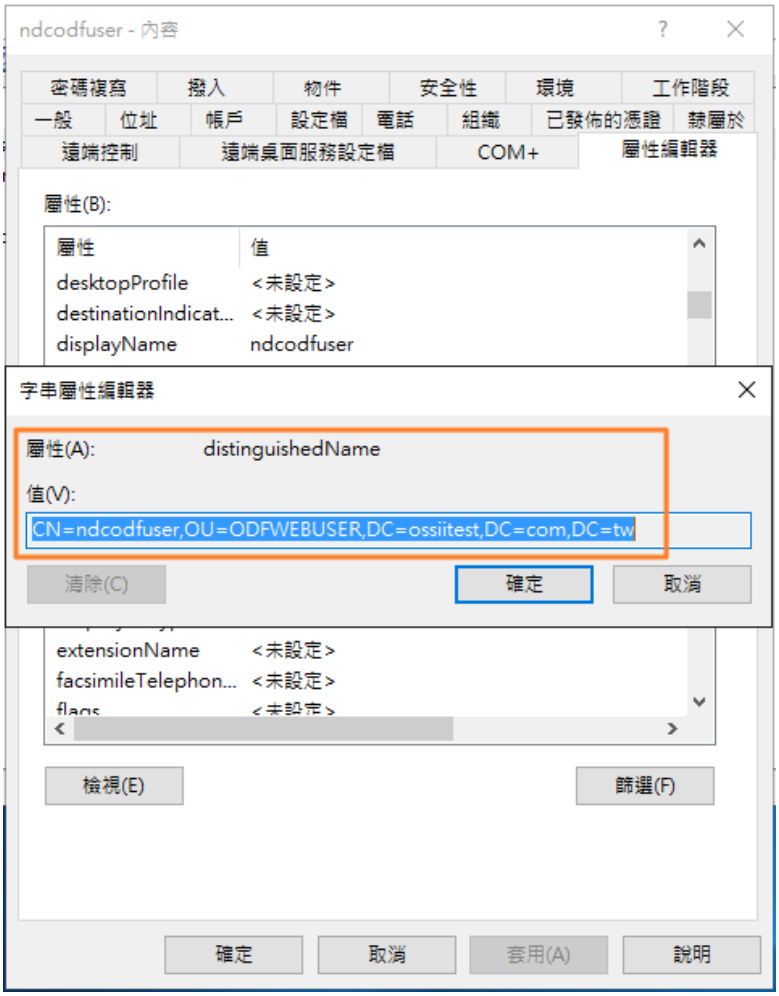
完成後，如下圖所示，請確認該使用者具備「允許讀取」的權限。



在本文件的測試 OU 中，可以多新增幾個使用者帳號，如下圖所示：



再回頭看一下剛剛建立的 OU 查詢權限的帳號資訊(本文件案例為：ndcodfuser)，利用滑鼠右鍵點選 ndcodfuser，並選擇「內容」在畫面上點選「屬性編輯器」並下拉到「distinguisheName」這個值，並點擊二下看詳細的值，等一下在設定 ODF 文件 Web 應用元件網路儲存空間軟體時會用到。



查詢完後，按下「確定」鍵離開。

(2)ODF 文件 Web 應用元件網路儲存空間軟體端設定

以 admin 登入後的畫面如下，點選右上角的圖示， 在下拉式選單點選選「設定」接下來在左邊點選「LDAP/AD 整合」會出現主要的設定畫面，如下圖所示，設定參數說明如下。

主機：請輸入 AD 的位置，例如：ldap://192.168.3.62，若是有 SSL，則請輸入：ldaps://192.168.3.62。

連接埠：預設為 389，或是在輸入「主機」後，按下右方的「偵測連接埠」自動偵測。

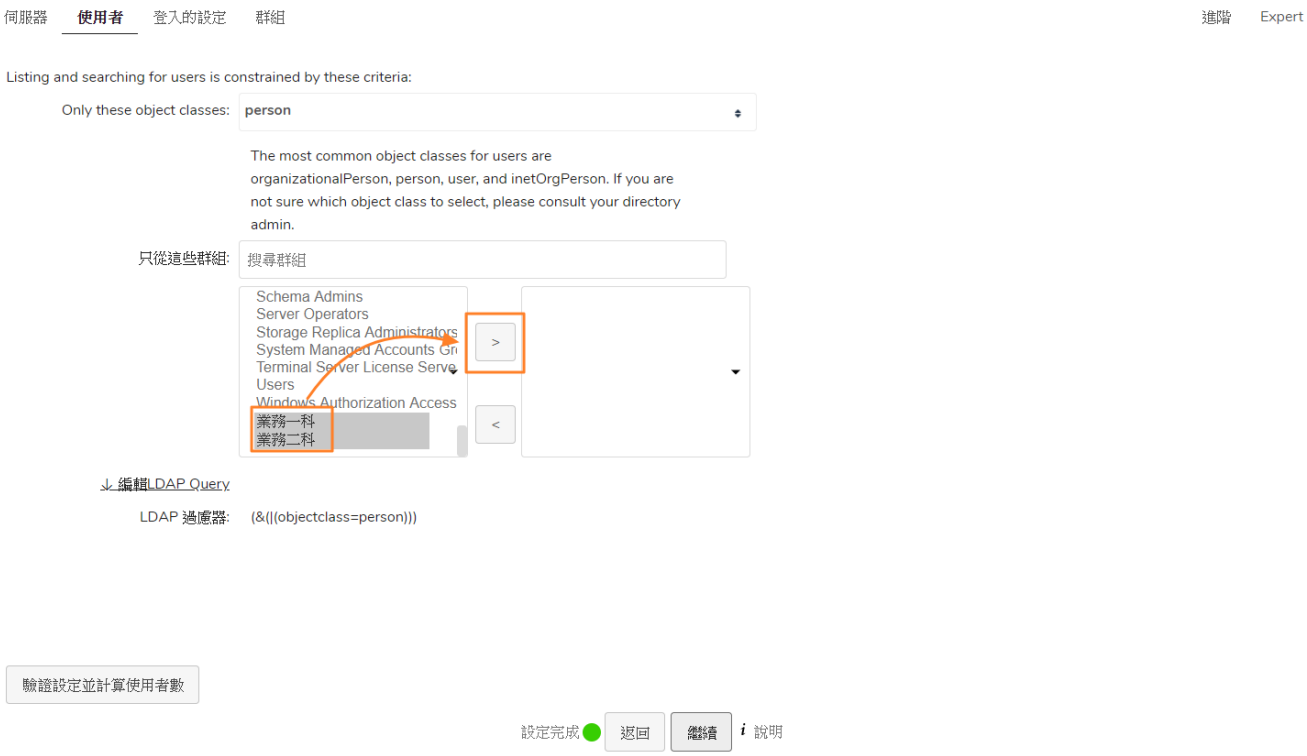
User DN：請輸入在上一節所查詢到的「distinguisheName」值，本文件示範值 CN=Wu.Mary,OU=業務部,DC=ossiitest,DC=com,DC=tw。

密碼：請填入 User DN 對應的密碼，完成後按下「儲存憑證 or Save Credentials」。

一行一個 Base DN：請按下右方的「偵測 Base DN」鍵，正常來說會自動填入，若不正確，請回頭檢視 AD 的設定內容是否正確。

完成後的畫面如下：

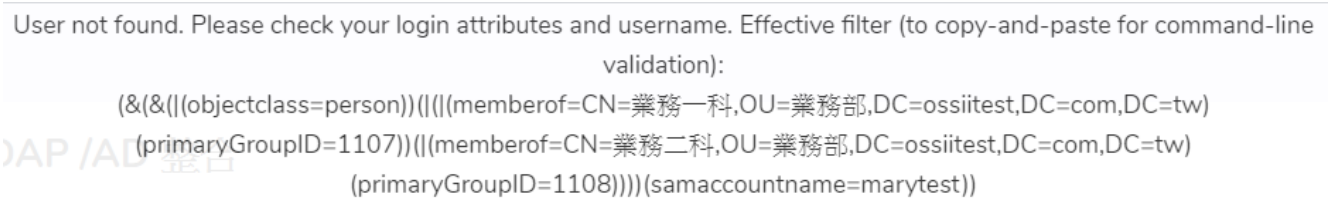
接下來按下「繼續」往下一個設定畫面進行。



在群組的列表上選擇相關要開放的群組後，按下往右的箭頭，接下來會像下圖，並可按下「驗證設定並計算使用者數」，若成功則會回傳數字，成功後按下「繼續」鍵。

接下來的畫面，可在畫面下方輸入一個實際存在的帳號，並按下「驗證設定」若使用者存在，系統會回應設定正確的訊息。

若隨便輸入一個使用者，系統會回應失敗訊息。



按下「繼續」鍵前往下一頁，請直接點選「編輯 LDAP Query」，並輸入「(|(ou=業務部))」，並按下「Verify settings and count the groups」如下畫面。

完成後，就完成 AD 目錄服務的帳號整合工作，只需要使用一般帳號的登入入方式即可，**不需在登入帳號名稱前加入「網域名稱\」。**

肆、以虛擬伺服器映像檔方式佈署

一、下載【ODF 文件 Web 應用元件】虛擬伺服器映像檔連結

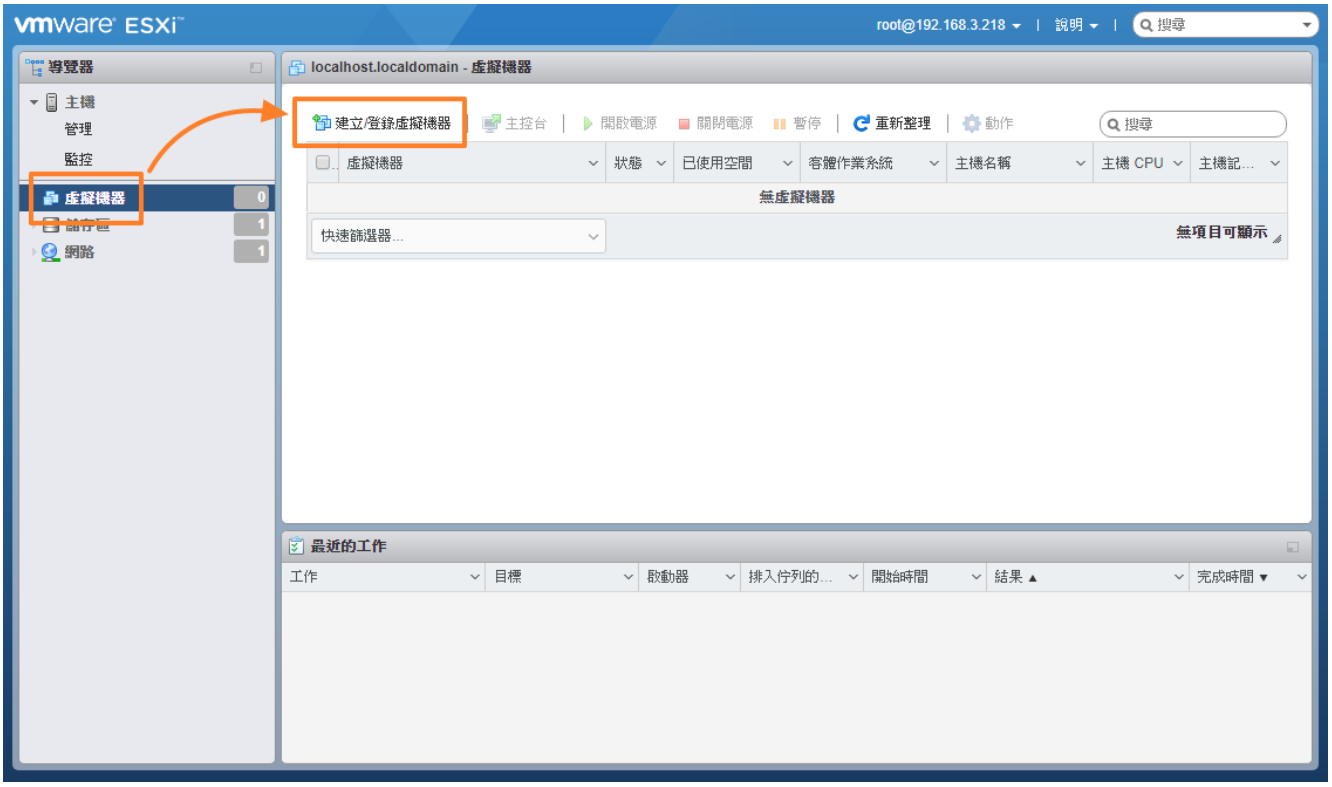
本章說明國家發展委員會【ODF 文件 Web 應用元件】虛擬伺服器映像檔的設定流程，並提供所需 Linux 系統的系統設定參數說明。

國家發展委員會【ODF 文件 Web 應用元件】虛擬伺服器映像檔請至國家發展委員會網站首頁點選【主要業務】>【數位發展規劃】>【基礎服務】>【開放文件格式(ODF)】>【支援 ODF 文件格式軟體工具】>【ODF 雲端編輯工具】頁面下載，下載檔名為：【NDCODFWEB-1.5.ova】目前採用的最新版本號碼為 1.5。

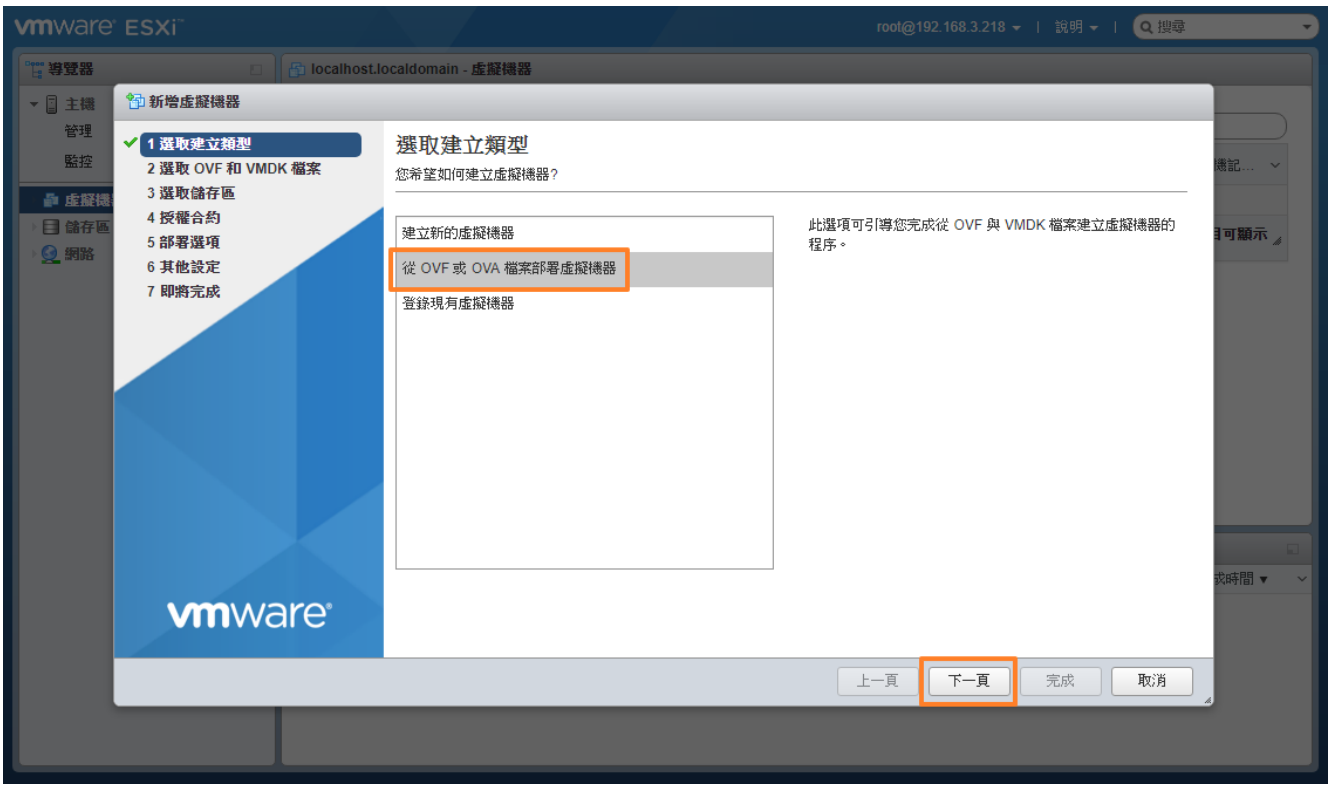
二、 映像檔匯入方式

(1)VMware EXSi

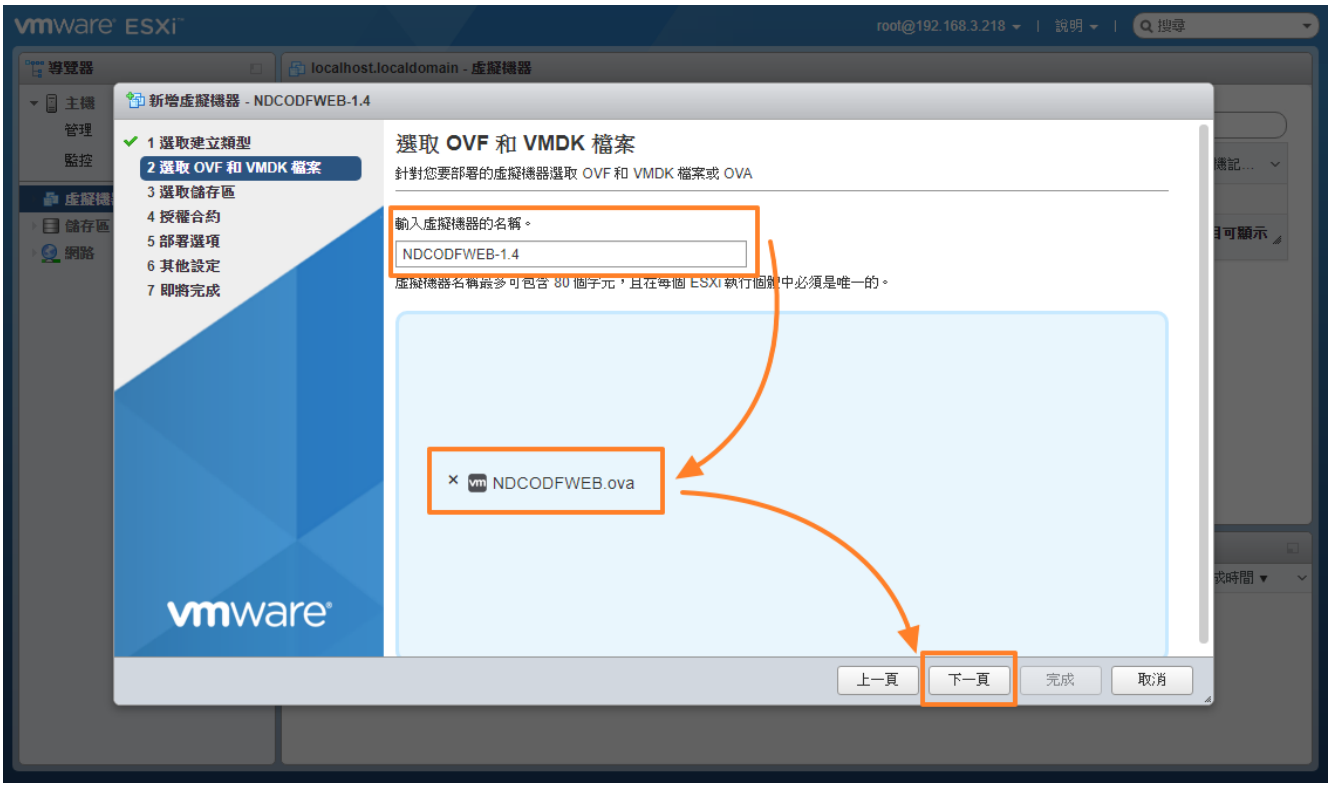
測試的環境為【VMWare ESXi 7.0】，請登入系統主頁，點選「虛擬機器」→「建立/登錄虛擬機器」，如下圖所示。



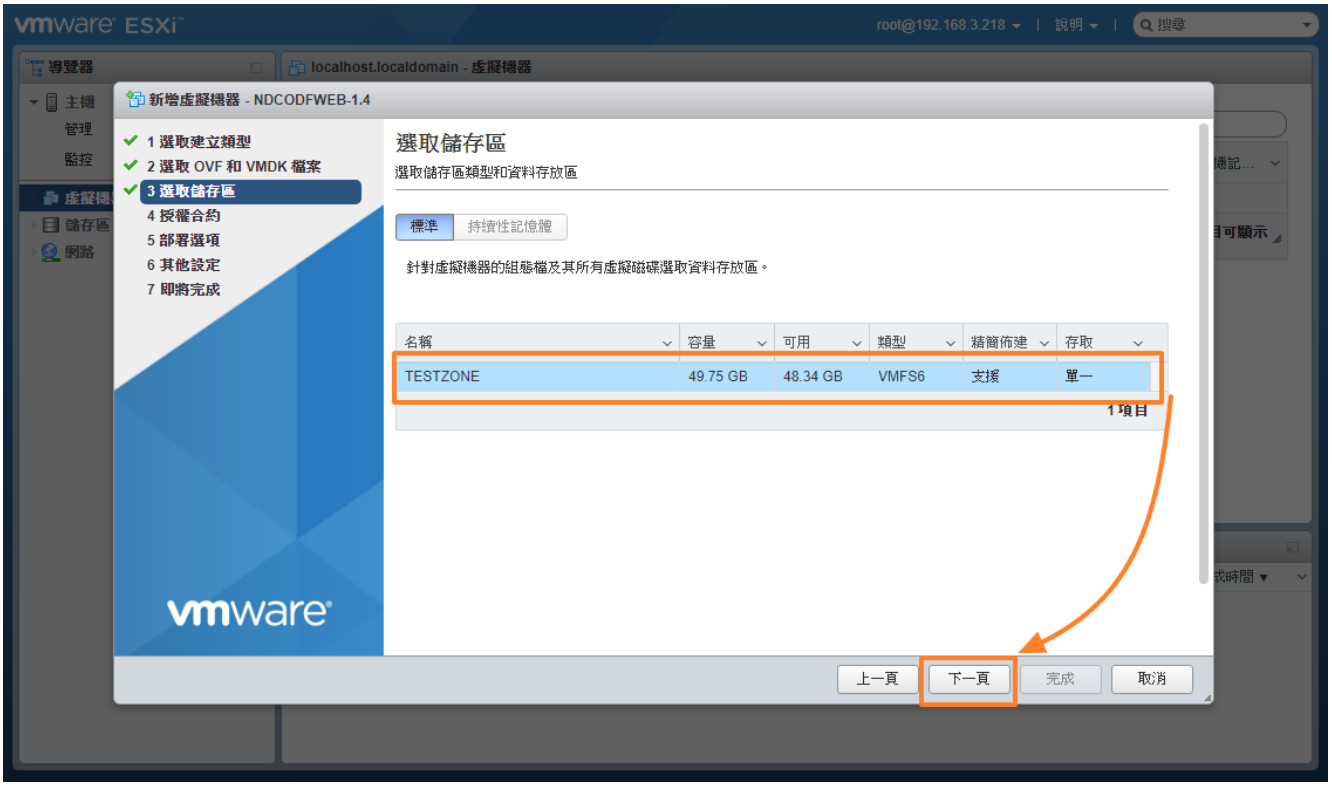
選擇「從 OVF 或 OVA 檔案部署虛擬機器」，並按「下一頁」繼續。



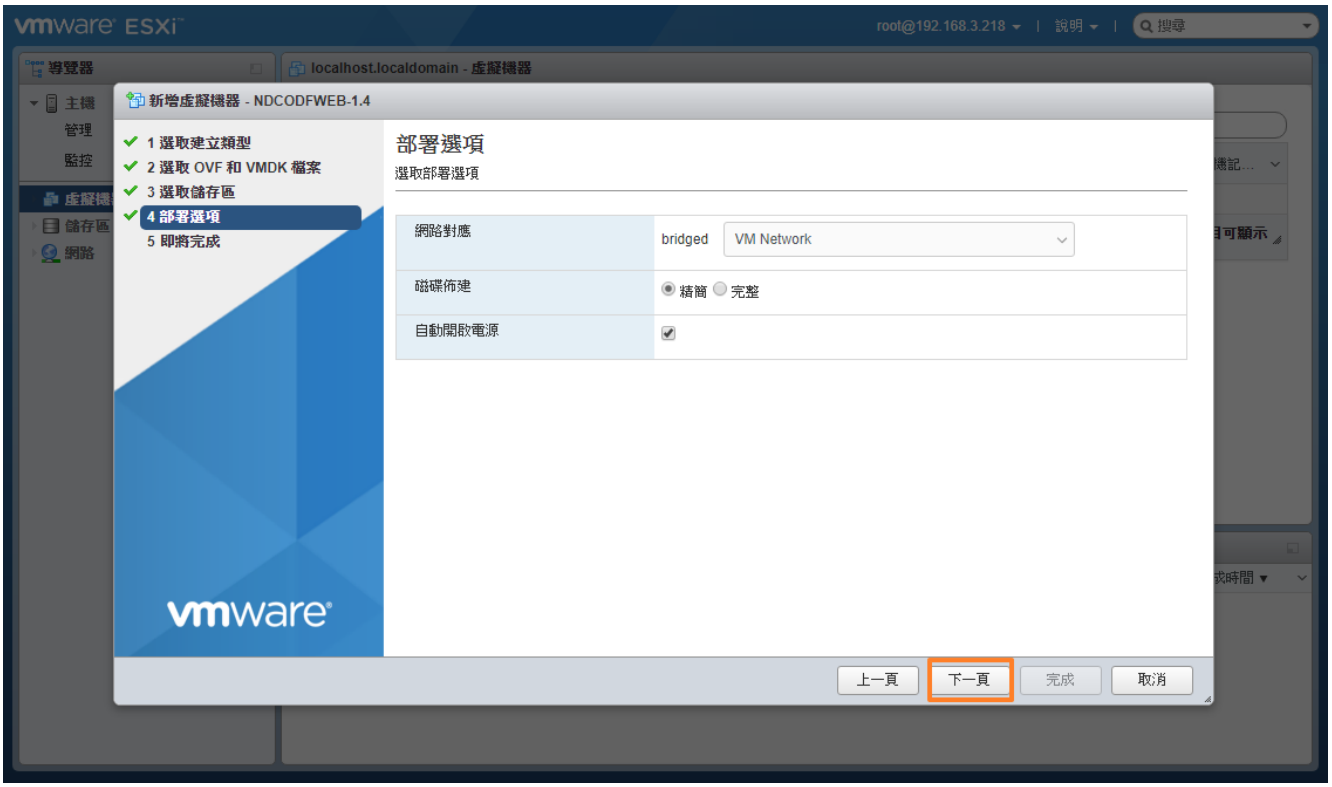
輸入虛擬機器名稱，並選取剛剛下載的 OVA 檔案，並按「下一頁」繼續，如下圖所示。



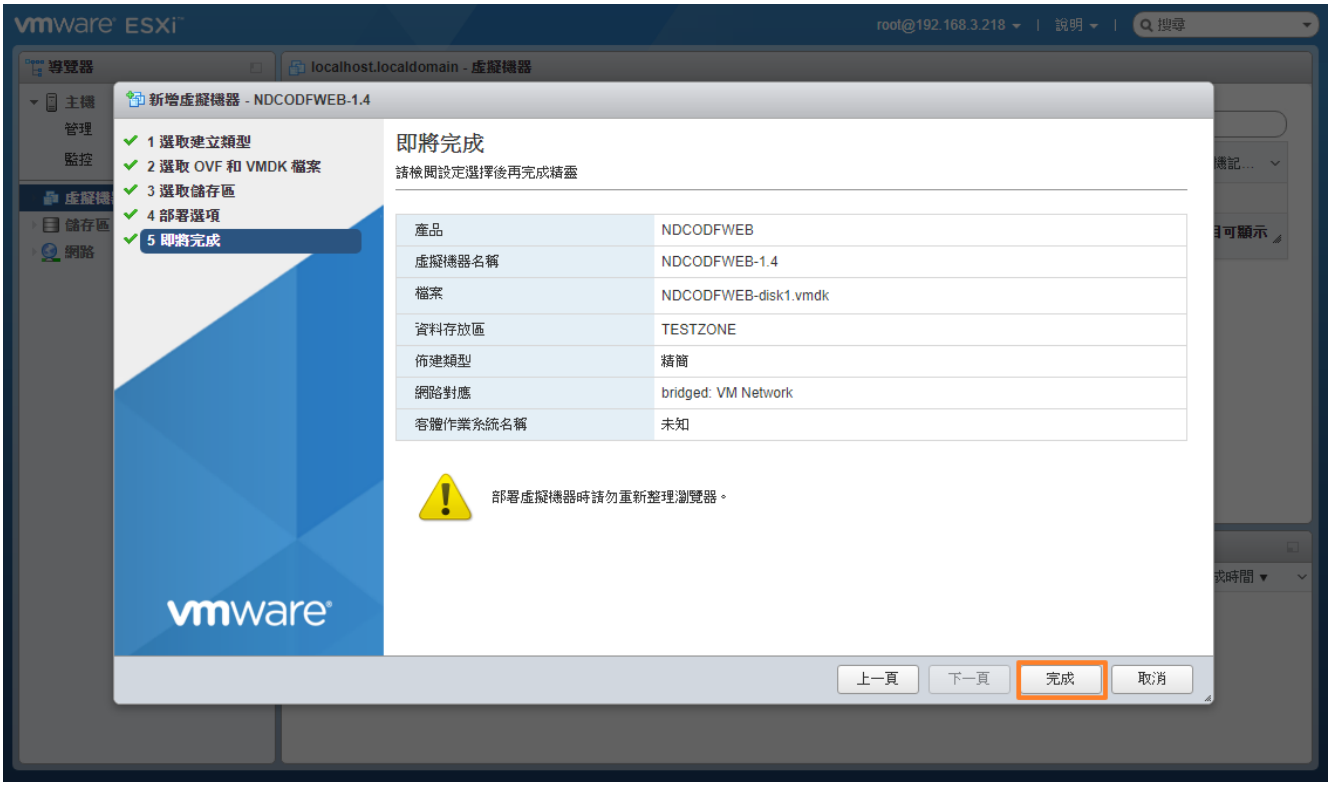
選擇虛擬主機所在的儲存區，並按「下一頁」繼續。



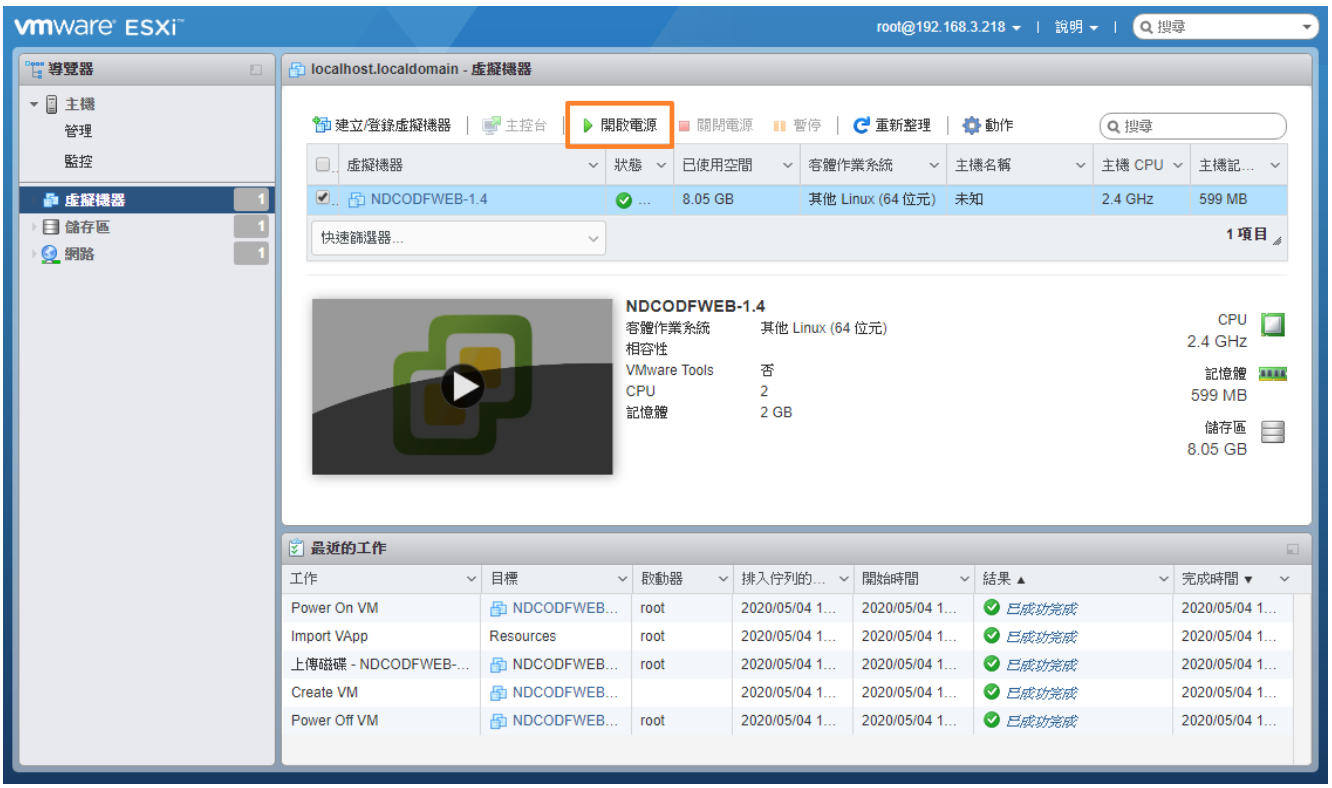
使用預設的部署選項，並按「下一頁」即可繼續部署。



確認資訊無誤後，按下「完成」鍵開始匯入虛擬機器的內容。

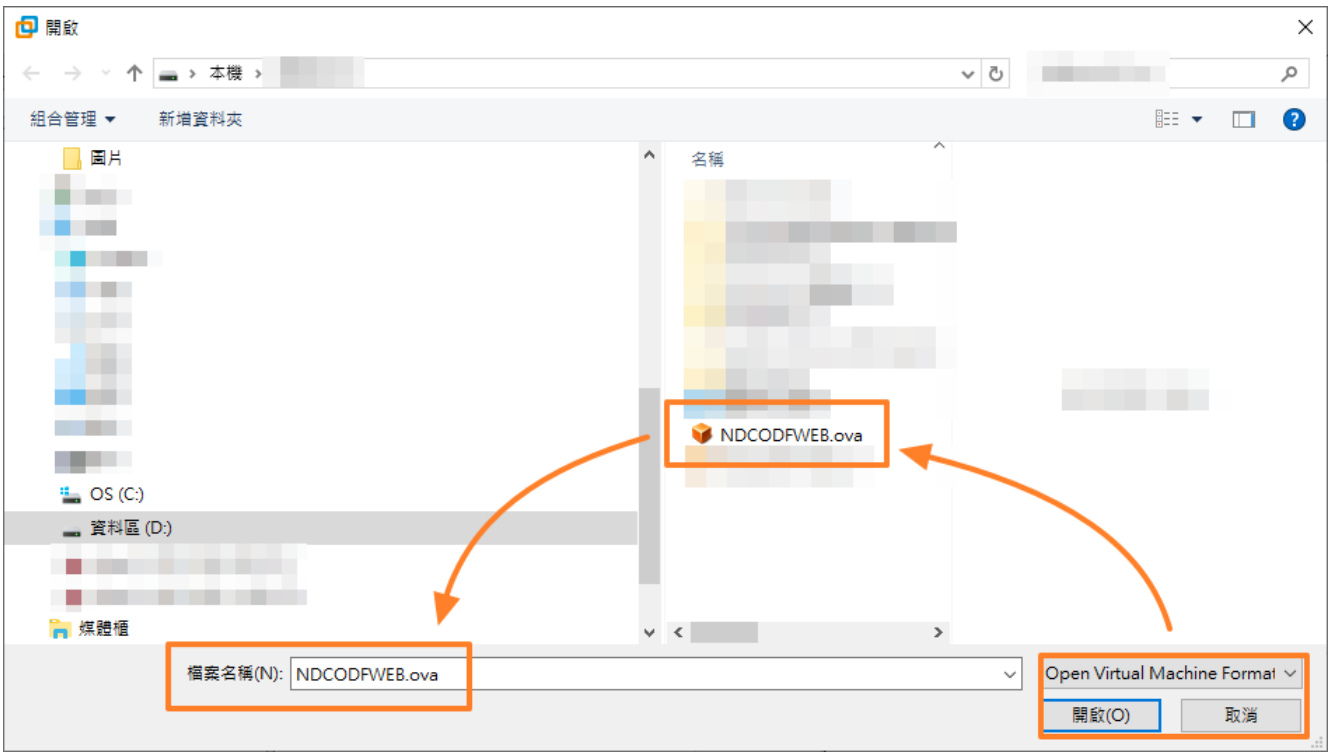


匯入成功後的畫面如下所示，可以點選「開啟電源」來啟動主機。

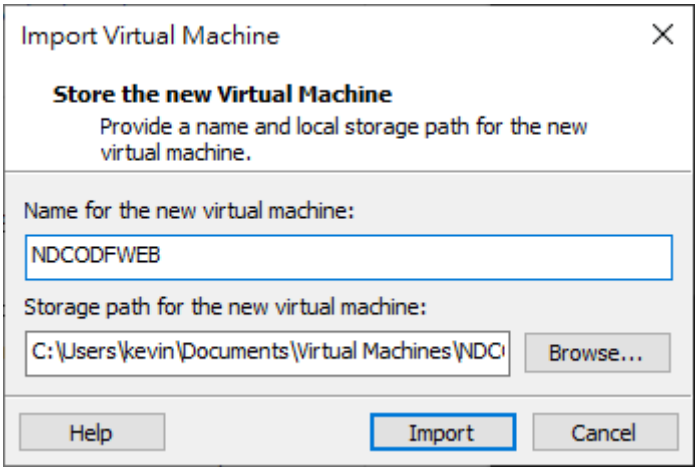


(2)VMware Workstation

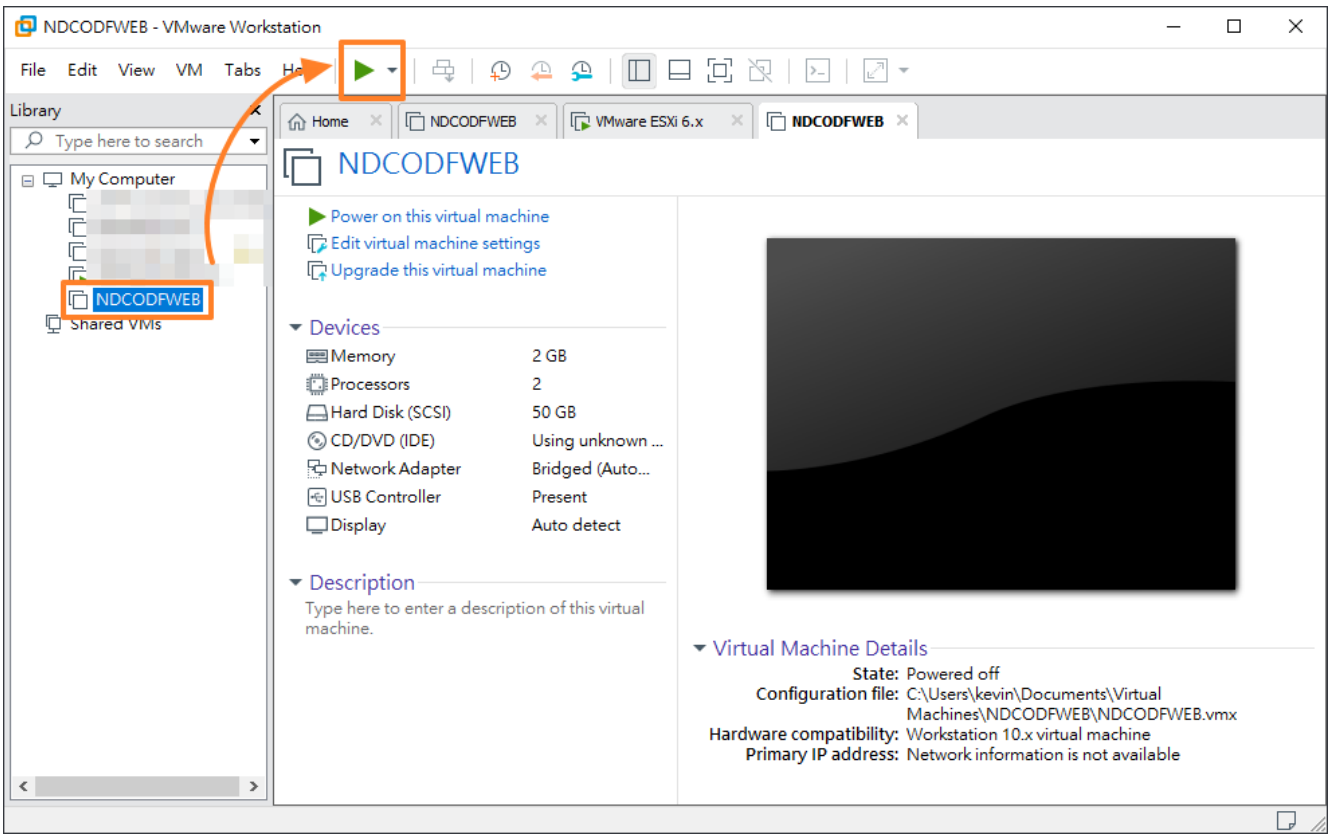
測試的環境為【VMWare Workstation 15】，請開啟程式主畫面，點選選單上的「File」→「Open」，選擇剛剛下載的 OVA 檔案，並按下「開啟」，如下圖所示。



設定匯入的虛擬主機名稱，並選擇要儲放的位置，確認後按下「Import」，如下圖所示。

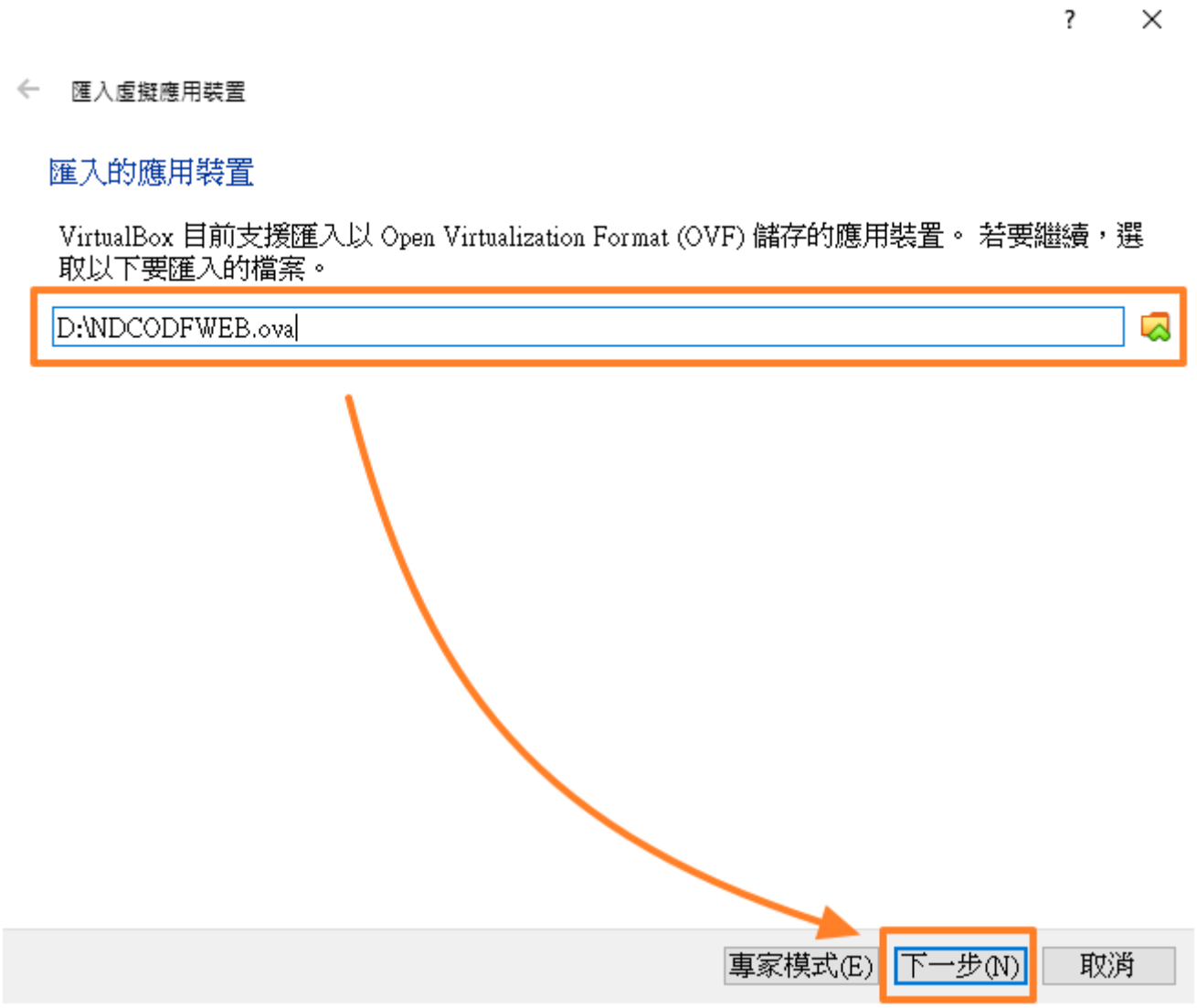


匯入成功後，畫面如下所示，按下啟動鍵即可啟動虛擬主機。


NDCODFWEB - VMware Workstation
File Edit View VM Tabs
Library
Type here to search
My Computer
NDCODFWEB
Shared VMs
Home
NDCODFWEB
VMware ESXi 6.x
NDCODFWEB
NDCODFWEB
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 2 GB
Processors 2
Hard Disk (SCSI) 50 GB
CD/DVD (IDE) Using unknown ...
Network Adapter Bridged (Auto...
USB Controller Present
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\kevin\Documents\Virtual Machines\NDCODFWEB\NDCODFWEB.vmx
Hardware compatibility: Workstation 10.x virtual machine
Primary IP address: Network information is not available

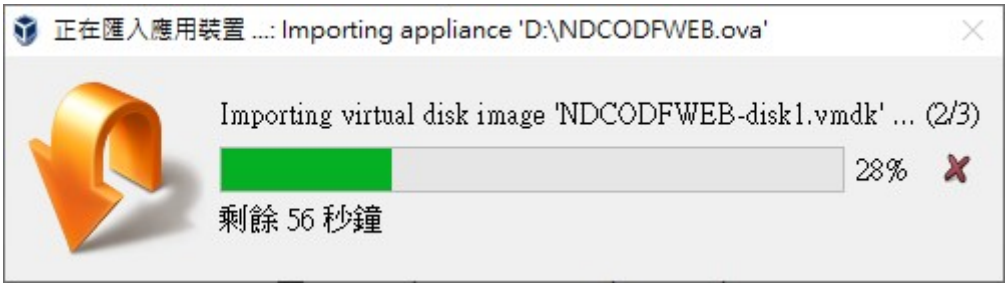
(3)Oracle VM VirtualBox

測試的環境為【Oracle VM VirtualBox 6.0】，請開啟程式主畫面，點選選單上的「檔案」→「匯入應用裝置」，選擇剛剛下載的 OVA 檔案，並按下「下一步」，如下圖所示。



接下來會出現系統設定值畫面，名稱預設為「vm」，直接按下「匯入」即可。

匯入的畫面如下。



匯入成功後，畫面如下所示，按下啟動鍵即可啟動虛擬主機。

三、 系統環境設定

在匯入虛擬主機系統後，需進行基本的調校才能登入【ODF 文件 Web 應用元件】的畫面。

(1)各種預設密碼

1. 初始 root 密碼

   初始密碼為：ndcodfweb2020

2. 初始 odfweb 管理者登入帳號/密碼

   初始管理者帳號為：admin

   初始管理者密碼為：ndcodfweb2020

3. 初始資料庫登入帳號/密碼

   初始管理者帳號為：root

   初始管理者密碼為：ndcodfweb2020

(2)變更系統網路設定

初始化的系統網路資訊如下：

- IP：192.168.3.199
- GATEWAY：192.168.3.1
- DNS：8.8.8.8

若需調整網路的設定，請先以 root 身份登入後，執行以下指令進行變更工作。

vim /etc/sysconfig/network-scripts/ifcfg-ens33 (ifcfg-ens33 要依實際檔名為準，也有可能是 ifcfg-eth0)

修改該檔案的資訊：

IPADDR=192.168.3.199 → 改成貴單位的 IP 位置

PREFIX=24 → 改為實際的網路設定(目前為 Class C)

GATEWAY=192.168.3.1 → 改成貴單位實際的網路閘導位置

DNS1=8.8.8.8 → 改成貴單位實際的 DNS 位置

存檔後，執行以下指令重新啟動網路。

systemctl restart network

(3)變更 odfweb 網路設定

1. 變更 odfweb 的連線 IP

當系統 IP 變更後，若與 odfweb 連線 IP 不同時，會出現以下畫面。

此時請執行以下指令進行變更工作。

vim /var/www/html/odfweb/config/config.php

修改以下二行：

…

array (

0 => '192.168.3.199', → 改為貴單位的 IP(與系統 IP 相同)

),

…

'overwrite.cli.url' => 'http://192.168.3.199/odfweb', → 改為貴單位的 IP(與系統 IP 相同)

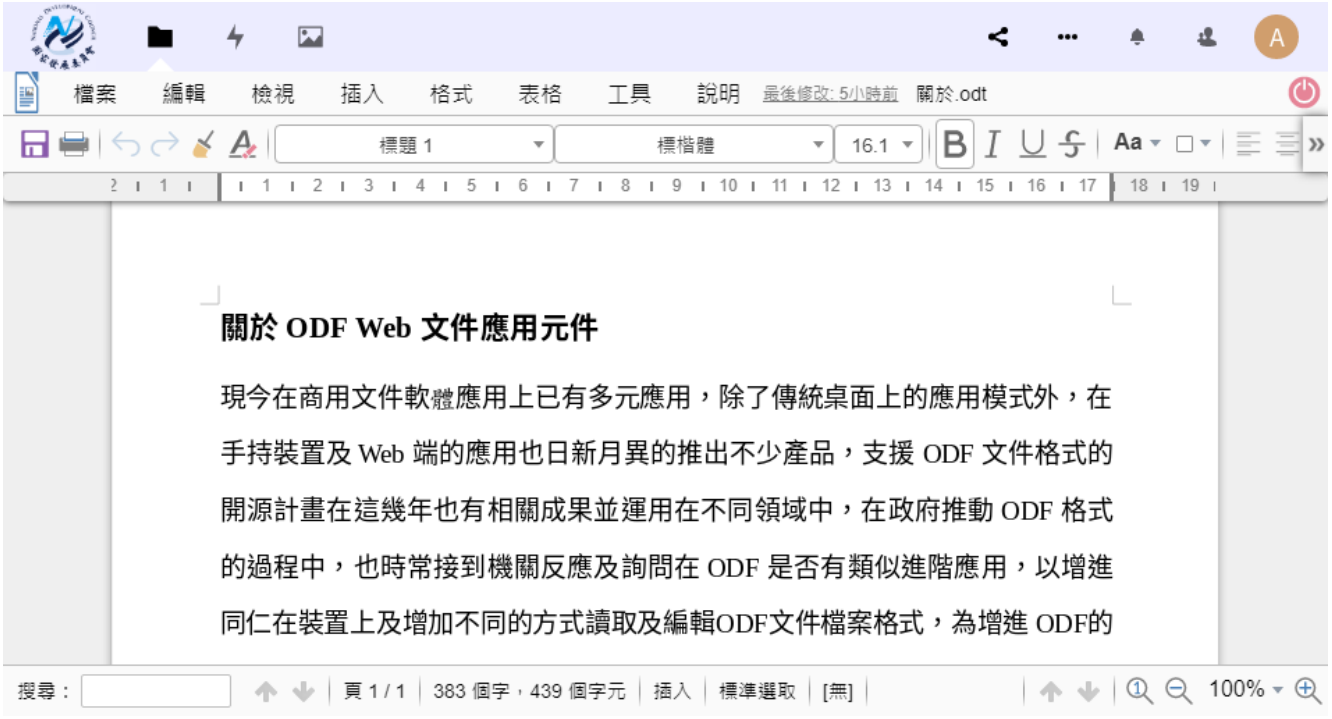
儲存後重新登入，即可看到以下正常畫面。

2. 變更 ndcodfweb 的服務位置

請透過 http://yourip/odfweb，輸入系統管理者的帳號(預設為 admin)及密碼(預設為 ndcodfweb2020)登入後，點擊畫面右上角的圓形圖示後選單中的「設定」，並選擇左方的【ODF Web 文件應用元件】。

接下來請將「ODF 文件 WEB 應用元件伺服器的 URL(及服務 port 號)」改為 http://yourip:9980，並按下「套用」即可。

完成後，就可以開始使用 NDCODFWEB 的相關功能了。



(4)變更各式密碼

1. root 密碼變更

   指令如下：

   # passwd

   更改使用者 root 的密碼。

   新 密碼：輸入第一次

   再次輸入新的 密碼：輸入第二次

   passwd：所有驗證 token 都已成功更新。

2. 資料庫 root 密碼變更

   請先以 root 登入系統，並以以下指令修改資料庫預設密碼：

   # mysqladmin -uroot -pndcodfweb2020 password 您的新密碼

   連線測試位置：

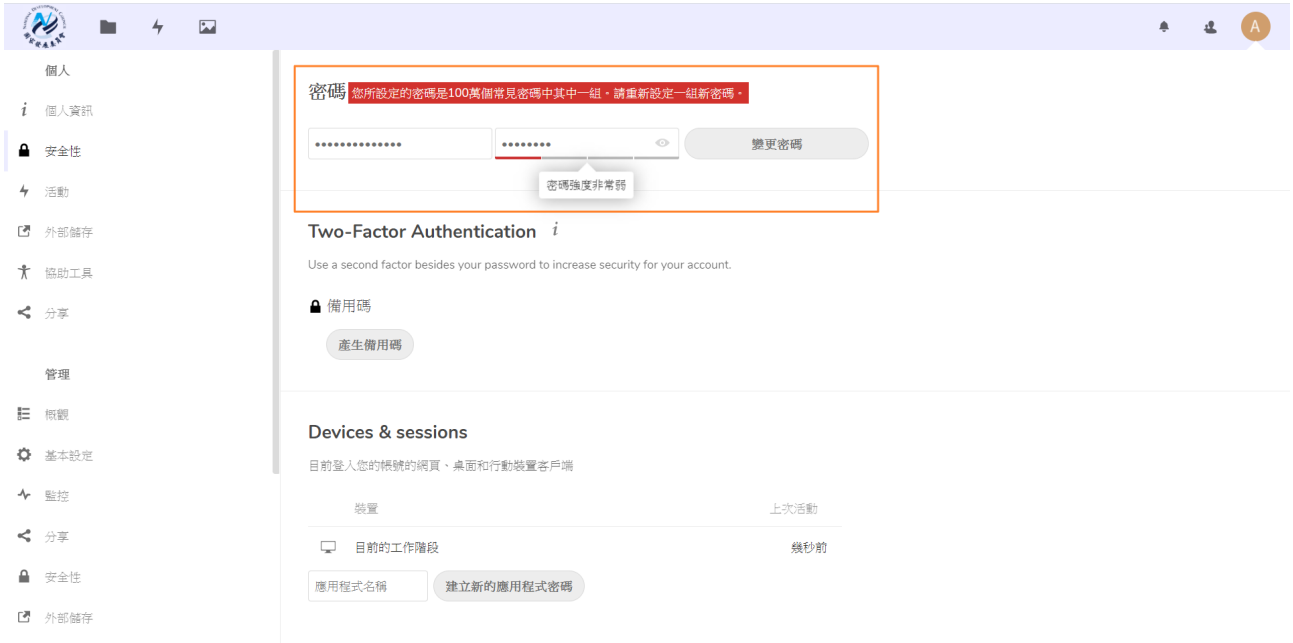
   http://yourip/phpMyAdmin (大小寫有別)

   帳號為 root，密碼為您設定的新密碼，完成後就可登入。

3. odfweb 管理者密碼變更

請在設定的畫面點選左方「安全性」頁面，並在右方「密碼」區域設定目前密碼及新密碼，完成後按下「變更密碼」即可完成變更。

如果密碼設定的太簡單，系統會提出警告並要求重新指定一組密碼。



設定成功後會出現「已儲存」的訊息，代表已設定成功。

(5)其他重要設定

設定使用對外服務位置、網站 SSL 設定、機關 LOGO 設定、網路磁碟機設定及整合機關 AD 設定，請參閱第 33 頁、第 34 頁、第 56 頁、第 61 頁及第 68 頁。

伍、更新方式

請下載更新的 NDCODFWEB-V1.x.zip 的壓縮檔，並上傳至主機目錄(本例還是使用/root 說明，可依實際目錄進行之)進行解壓縮。

cd *root*

unzip NDCODFWEB-V1.x.zip

cd /root/NDCODFWEB-V1.x/ndcodfsys

請先先確認套件與更新檔的版本是否一致，若更新檔的版本更新才需要下更新指令。

rpm -qa | grep gumbo-parser → 如果下載的 gumbo-parser 版本更新則需要升級。

rpm -qa | grep ndcodfsys → 如果下載的 ndcodfsys 版本更新則需要升級。

升級指令如下：

rpm -Uvh gumbo*.rpm

rpm -Uvh ndcodfsys*.rpm

cd /root/NDCODFWEB-V1.x/poco

一樣請先確認版號，有更新的才需要升級，升級指令如下。

rpm -Uvh poco*.rpm

cd /root/NDCODFWEB-V1.x/ndcodfweb

rpm -Uvh ndcodfweb*.rpm

重新啟動服務。

systemctl restart ndcodfweb

接下來更新 odfweb 主程式，流程如下：

首先請先備份/var/www/html/odfweb 目錄，方式如下：

cd /var/www/html

tar cvzf odfweb-backup.tar.gz odfweb

手動備份一下資料庫，或是透過 phpMyAdmin 匯出，手動的指令如下：

cd /var/www/html

tar cvzf odfweb-db-backup.tar.gz /var/lib/mysql

cd /var/www/html/odfweb

進入維護模式。

sudo -u apache php occ maintenance:mode --on

開始進行升級，先將更新檔 copy 至主目錄，指令如下：

cd /root/NDCODFWEB-V1.x

unzip odfweb-1.x.zip

cd odfweb

\cp * -a /var/www/html/odfweb

chown apache.apache /var/www/html/odfweb -R

cd /var/www/html/odfweb

sudo -u apache php occ upgrade

最後若顯示了【Update Successful】代表升級成功。

關閉維護模式：

sudo -u apache php occ maintenance:mode –off

升級成功，重新進入網頁即完成。

陸、政府組態基準(GCB)參考文件

以下設定是參考政府組態基準(GCB)內所建議之設定，詳細內容可參考以下連結：

https://www.nccst.nat.gov.tw/GCBDownloadDetail?lang=zh&seq=1014

一、 調整密碼原則

修改 /etc/login.defs 以下幾個參數：

- PASS_MAX_DAYS 90 密碼最長過期天數，GCB 規定為 3 個月
- PASS_MIN_DAYS 0 密碼最小過期天數，設定後幾天內不得變更
- PASS_WARN_AGE 7 密碼過期之前幾天會開始警告

修改 /etc/security/pwquality.conf

- minlen = 8 密碼最小長度
- maxrepeat = 0 密碼中連續相同字元的最大數量
- maxclassrepeat = 0 密碼中連結相同類型字元的最大數量
- lcredit = -1 密碼中至少需要 1 個小寫字元
- ucredit = -1 密碼中至少需要 1 個大寫字元
- dcredit = 0 密碼中至少需要 0 個數字
- ocredit = 0 密碼中至少需要 0 個其它字元

二、 建立 sudo 帳號

- 建立一個管理者帳號

  # adduser 管理者帳號

  # password 管理者帳號，並輸入二次密碼

- 設定 sudo 帳號

  # echo "要開放的帳號名稱　　ALL=(ALL)　　ALL" >> /etc/sudoers

三、 設定 YUM 套件庫來源

把 /etc/yum.repos.d/ 目錄內的 CentOS-Base.repo 設定檔內容做以下修正：

原本是：

mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra

#baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/

改為是：

#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra

baseurl=http://free.nchc.org.tw/centos/$releasever/os/$basearch/

並且使用指令增加以下來源：

```
# cd /etc/pki/rpm-gpg
# wget http://free.nchc.org.tw/fedora-epel/RPM-GPG-KEY-EPEL-7
# wget https://rpms.remirepo.net/RPM-GPG-KEY-remi
# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-remi
# cat << EOF > /etc/yum.repos.d/epel.repo
[epel]
name=Extra Packages for Enterprise Linux 7 - \$basearch
baseurl=http://free.nchc.org.tw/fedora-epel/7/\$basearch
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
EOF
# cat << EOF > /etc/yum.repos.d/remi.repo
[remi]
name=Remi's RPM repository for Enterprise Linux 7 - \$basearch
baseurl=http://rpms.remirepo.net/enterprise/7/remi/\$basearch/
enabled=1
```

gpgcheck=1

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-remi

[remi-php74]

name=Remi's PHP 7.4 RPM repository for Enterprise Linux 7 - \$basearch

baseurl=http://rpms.remirepo.net/enterprise/7/php74/\$basearch/

enabled=1

gpgcheck=1

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-remi

EOF

四、 設定 SSH Root 登入限制，限制服務的演算法

執行以下指令：

sed -i 's/#PermitRootLogin yes/PermitRootLogin no/g' /etc/ssh/sshd_config

修改 /etc/ssh/sshd_config，加入以下 2 行內容

Ciphers aes128-ctr

MACS hmac-sha1

重新啟動 SSH 服務：

systemctl restart sshd