



คู่มือการติดตั้งและใช้งาน VPN, Cloud Portal
สำหรับบริการ Enterprise Cloud

คู่มือการติดตั้งและใช้งาน VPN ผ่าน Windows/Mac OS ผ่านโปรแกรม SoftEther VPN Client

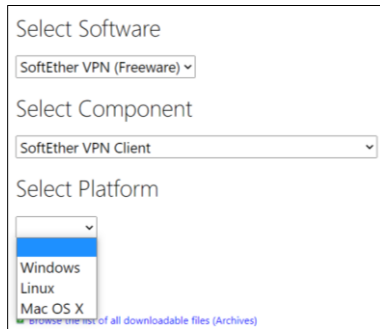
1. เจ้าหน้าที่จะจัดส่งข้อมูลสำหรับติดตั้ง VPN Client ผ่านทางอีเมล

1.1 ตัวอย่าง ข้อมูลสำหรับการใช้งาน VPN Client และเข้าสู่ระบบ Cloud

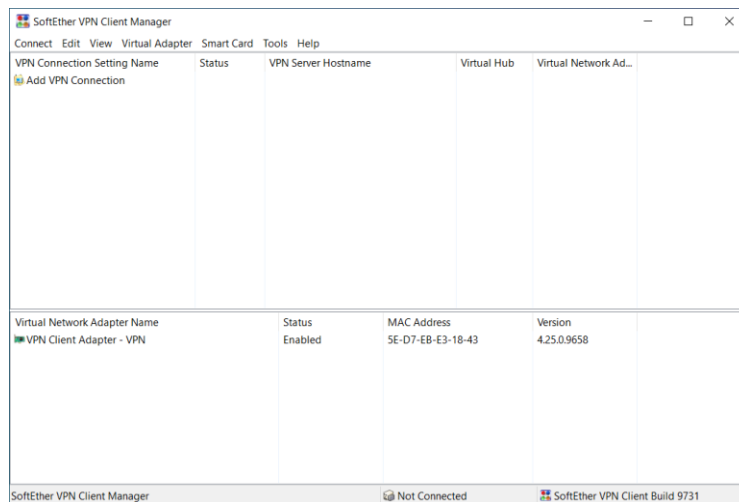
Host IP	222.222.XXX.XXX		
Username	Admin-XXXX	Password	*****
Username	Admin-XXXY	Password	*****

2. ดาวน์โหลดและติดตั้งโปรแกรม SoftEther VPN Client

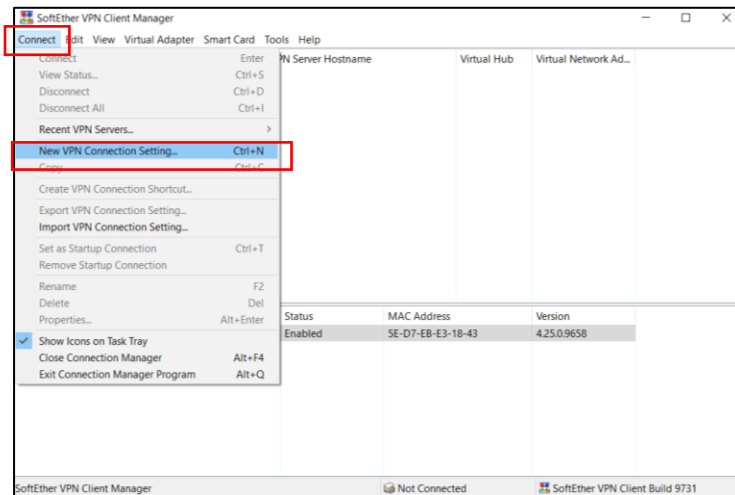
URL: <https://www.softether-download.com/en.aspx?product=softether>



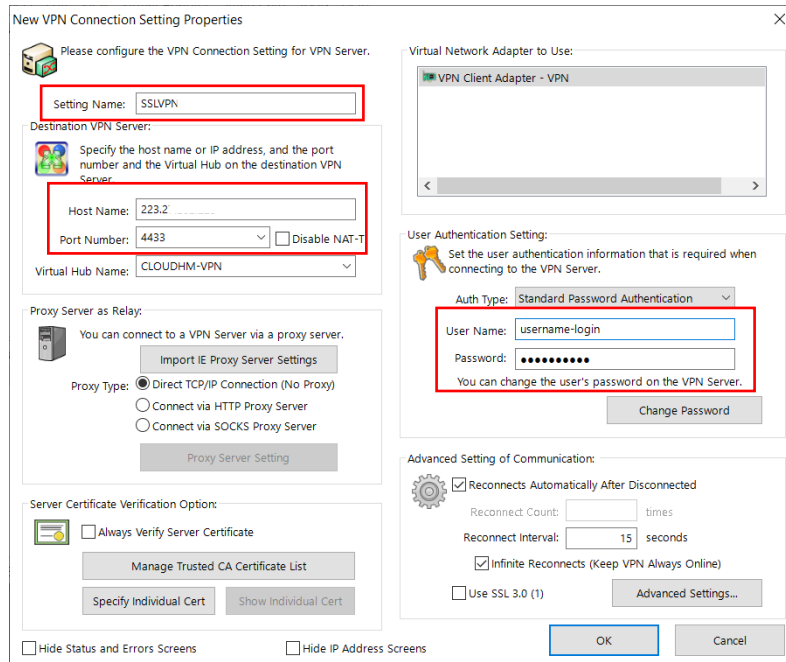
3. เปิดโปรแกรม



4. ไปที่ Connect > New VPN Connection Setting



5. ระบุข้อมูลสำหรับเข้าใช้งาน SSLVPN และกด OK



Setting Name: ตั้งชื่อ SSLVPN

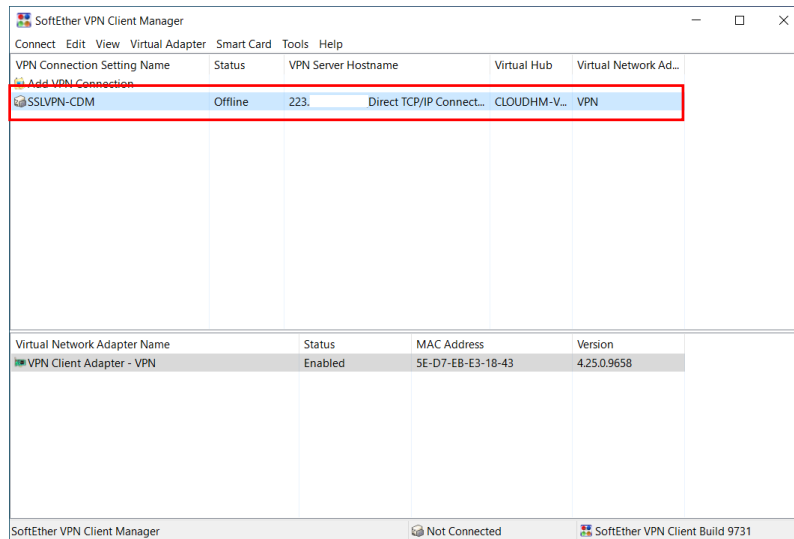
Hostname: ระบุ Server IP ที่ทาง Cloud HM ส่งให้

Port Number: 4433

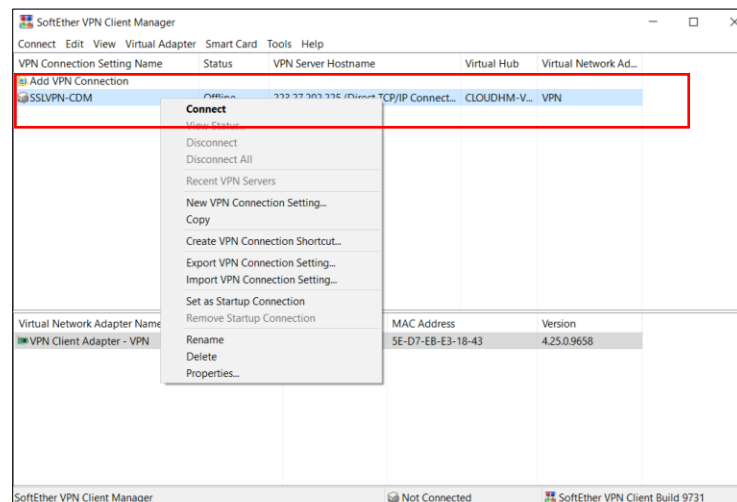
Username: ระบุ Username (ที่ถูกสร้างสำหรับใช้ Log in VPN)

Password: ระบุ Password (ที่ถูกสร้างสำหรับใช้ Log in VPN)

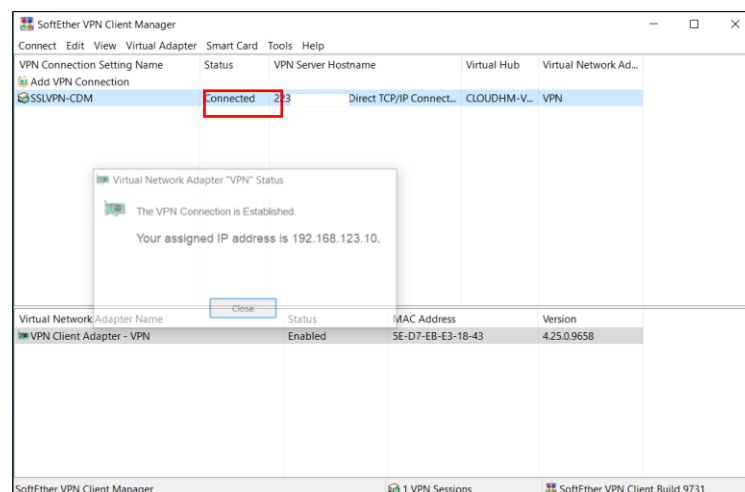
6. โปรแกรมจะแสดง SSLVPN Connection ที่เราได้ระบุไว้



7. คลิกขวา กด Connect เพื่อเชื่อมต่อ VPN



8. เมื่อเชื่อมต่อสำเร็จ ระบบจะแสดงสถานะ Connected และ VPN จะ Assign IP Private ให้สำหรับใช้งาน



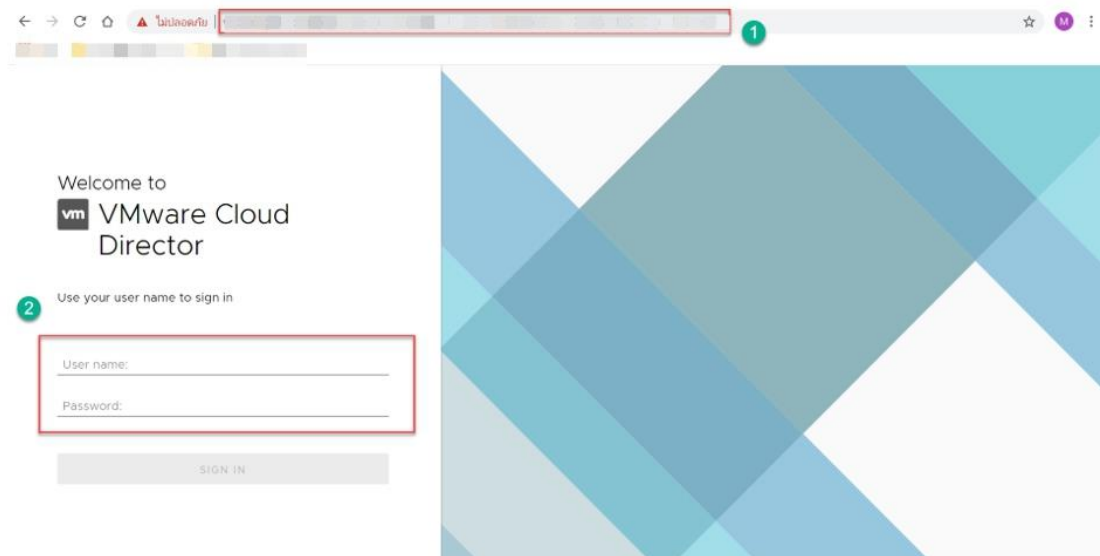
คู่มือการใช้งาน Cloud Portal สำหรับจัดการ Virtual Machine

1. เจ้าหน้าที่จะจัดส่งข้อมูลสำหรับเข้า Cloud Portal ผ่านทางอีเมล
2. Login เข้าระบบ VMware Cloud Director (HTML) ผ่าน URL:

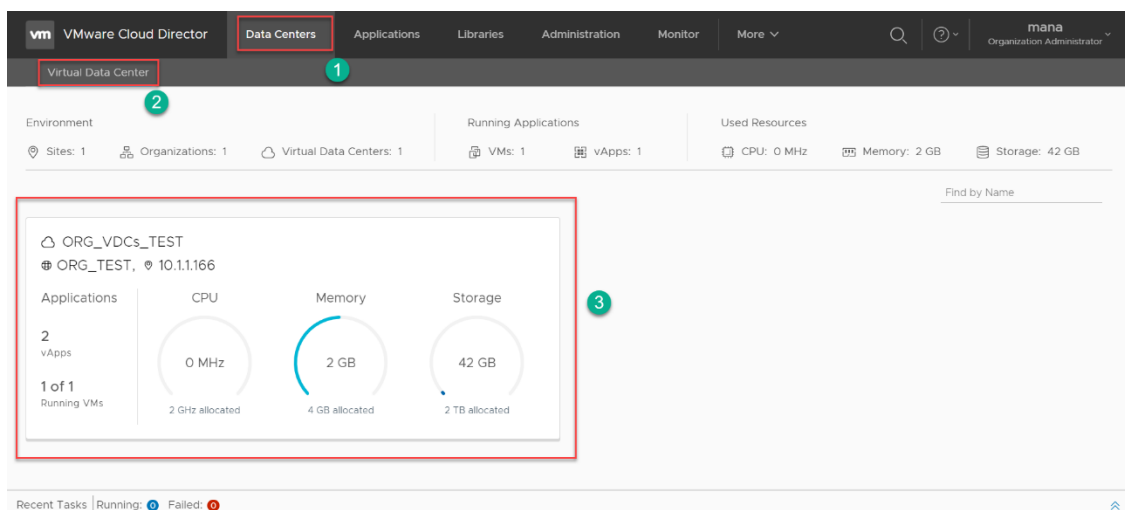
Example : <https://cloud.example.com/tenant/MyOrg>

URL	https://snap-vcd.cloudhm.io/tenant/ORG
Username	ORG-Admin
Password	98T59:pT

3. กรอก Username และ Password สำหรับการใช้งาน



4. เลือก Virtual Data Center ที่ผู้ให้บริการต้องการเข้าใช้งาน
5. รายละเอียดข้อมูลทั้งหมดใน Virtual Data Center ที่ผู้ให้บริการใช้งานอยู่



VMware Cloud Director

Data Centers Applications Libraries Administration Monitor More ▾

Site: 10.11.106 Organization: ORG_TEST Data center: ORG_VDCS_TEST administrator System Administrator

Virtual Machines

Find by: Name ADVANCED FILTERING

Sort by: Creation Date

1 Virtual Machines Expired false Clear all filters

NEW VM

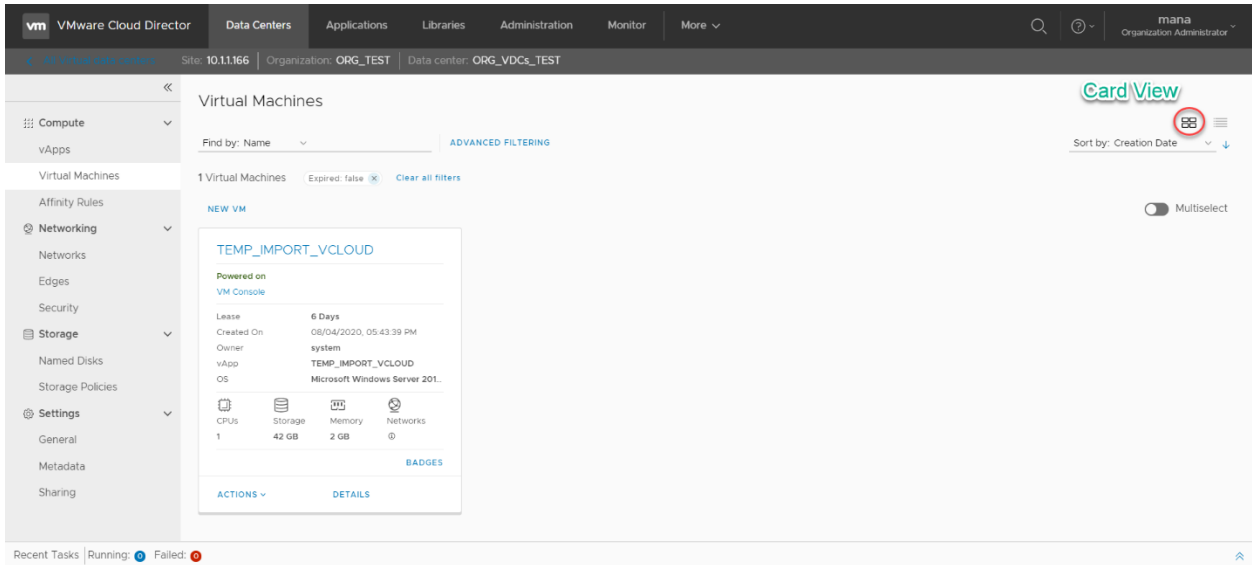
TEMP_IMPORT__VCILOUD	
Powered off	
VM Console	
Lease 29 Days	
Created On	09/24/2020, 10:41:26 AM
Owner	system
vApp	TEMP_IMPORT__VOICLOUD
OS	Microsoft Windows Server 201.
CPU's	Storage Memory Networks
1	42 GB 2 GB Ⓢ
BADGES	
ACTIONS ▾	DETAILS

Recent Tasks Running: 0 Failed: 0

ขั้นตอนการใช้งาน Virtual Machine

1. View Virtual Machines

1.1 View Virtual Machines ผ่าน card view



Virtual Machines

Find by: Name [ADVANCED FILTERING](#)

1 Virtual Machines Expired: false [Clear all filters](#)

[NEW VM](#)

TEMP_IMPORT_VCLOUD

Powered on
[VM Console](#)

Lease: 6 Days
Created On: 08/04/2020, 05:43:39 PM
Owner: system
vApp: TEMP_IMPORT_VCLOUD
OS: Microsoft Windows Server 201...

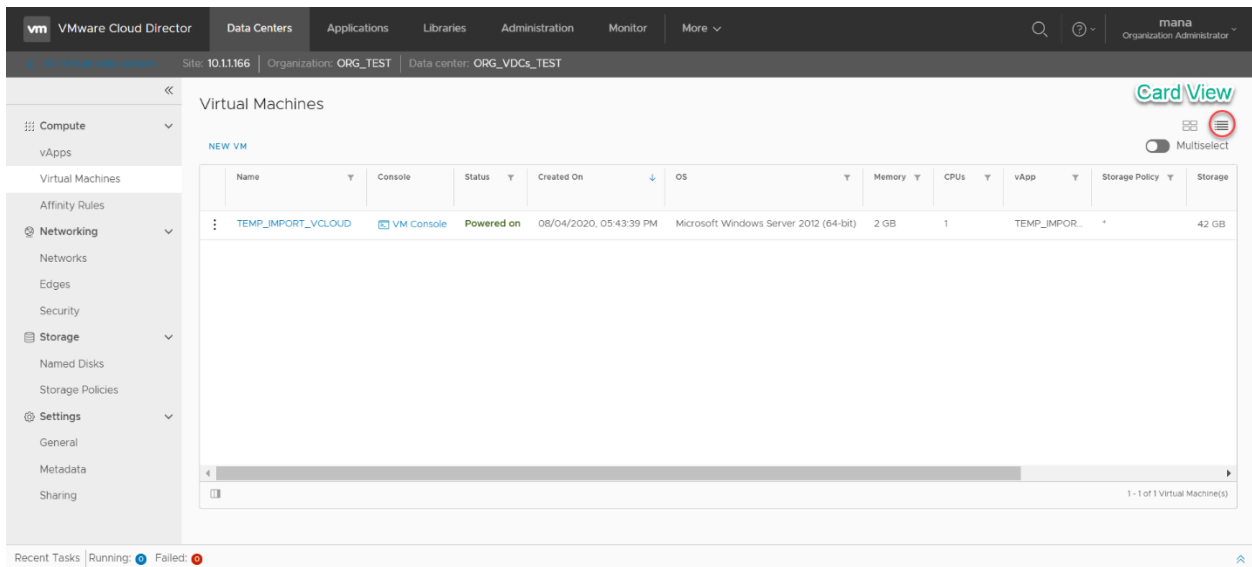
CPU: 1 Storage: 42 GB Memory: 2 GB Networks: 0

[BADGES](#)

[ACTIONS](#) [DETAILS](#)

Recent Tasks | Running: 0 Failed: 0

1.2 View Virtual Machine ผ่าน grid view



Virtual Machines

[NEW VM](#)

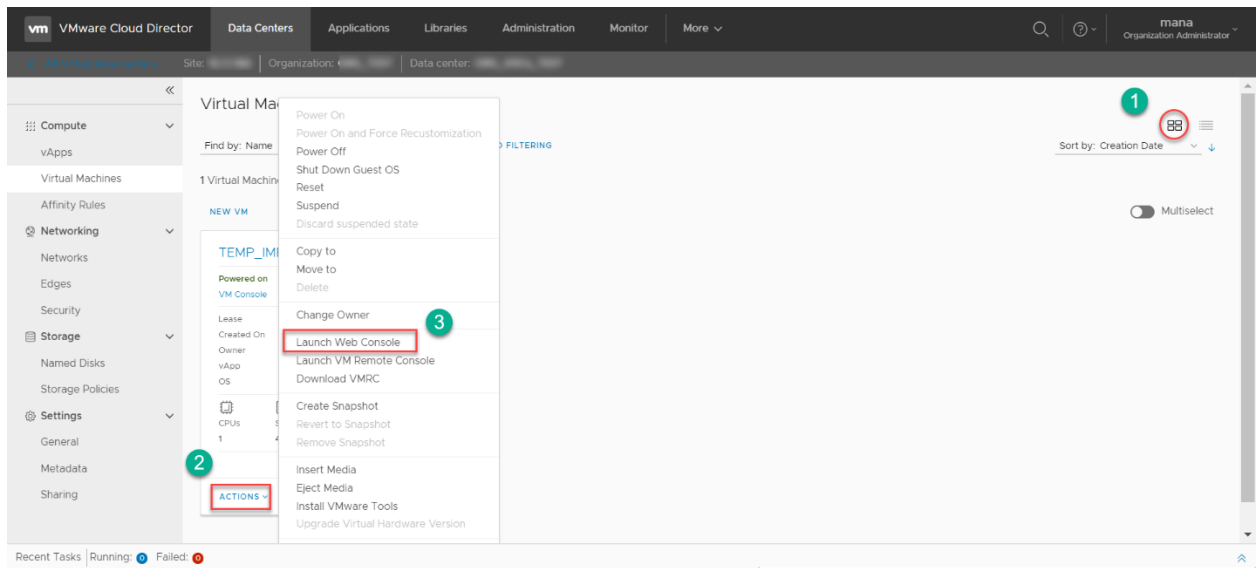
Name	Console	Status	Created On	OS	Memory	CPUs	vApp	Storage Policy	Storage
TEMP_IMPORT_VCLOUD	VM Console	Powered on	08/04/2020, 05:43:39 PM	Microsoft Windows Server 2012 (64-bit)	2 GB	1	TEMP_IMPORT...	*	42 GB

1 - 1 of 1 Virtual Machine(s)

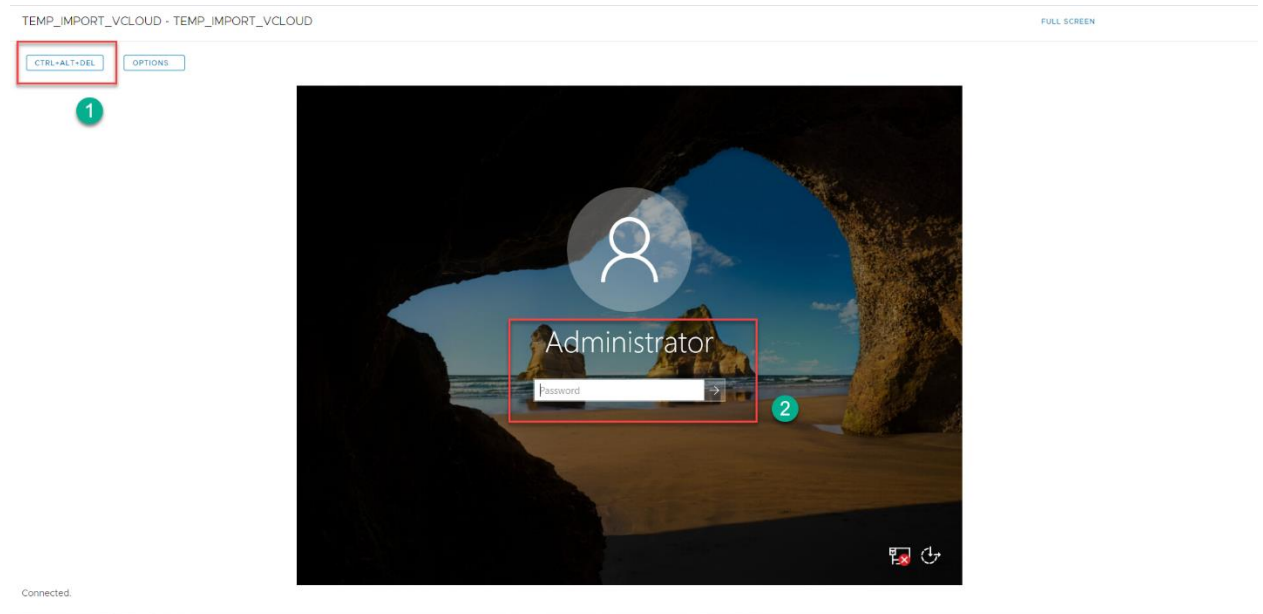
Recent Tasks | Running: 0 Failed: 0

2. การใช้งาน Web Console ของ Virtual Machine

2.1 ขั้นตอนการ Launch Web Console



2.2 ขั้นตอนการ Login เข้าใช้งาน Virtual Machine



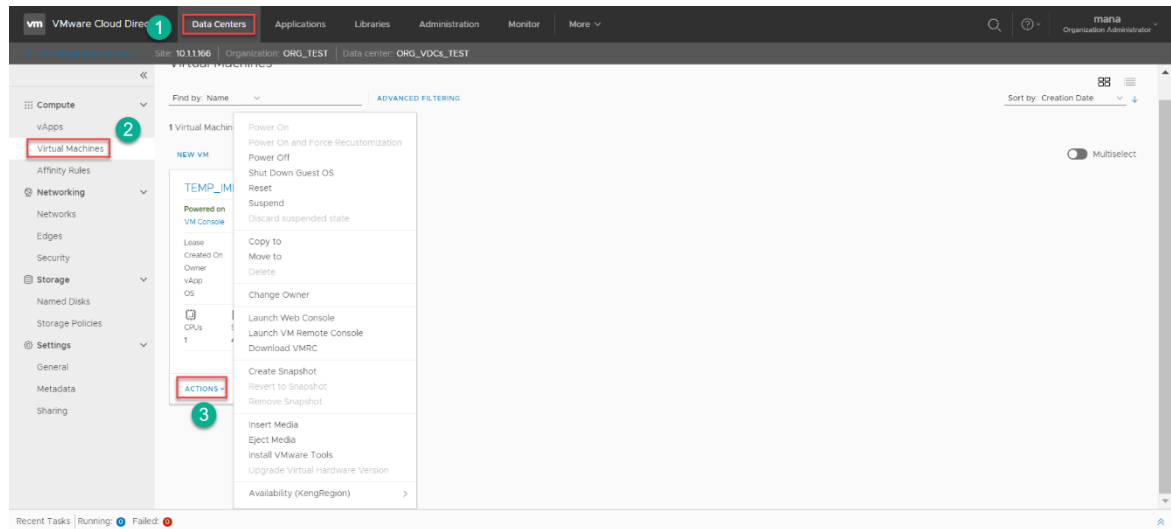
3. วิธีการดำเนินการ Operate Virtual Machine

Power on : เปิดเครื่อง Virtual Machine

Power off : ปิดเครื่อง Virtual Machine (Force shut down)

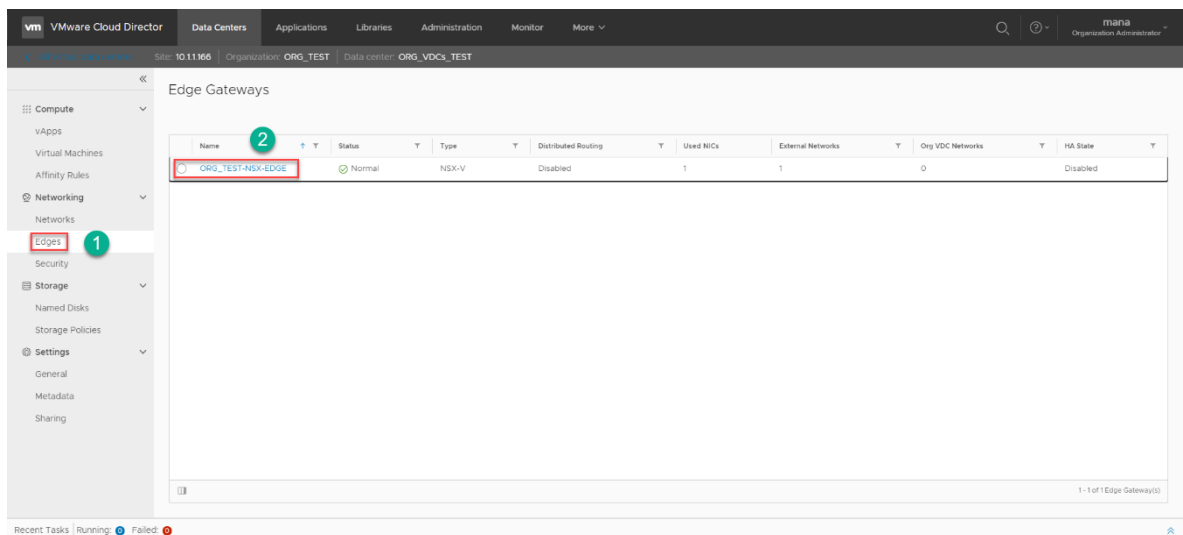
Shut Down Guest OS : Shut down os ในขณะที่เครื่องกำลัง Power on

Reset : Clear State ของ Virtual Machine (Hard reset os)



4. วิธีการจัดการ Service NSX Edges (Firewall) เลือก NSX Firewall ที่ต้องการแก้ไข

4.1 Click Edge



4.2 Select Tab Firewall > Edit Rules

General
Services
Firewall
NAT
IPSec VPN
Load Balancer
General Settings

EDIT RULES

#	Name	Category	State	Applications	Source	Destination	Action
1	External-To-Internal	User defined	Enabled	-	Any	VM	Allow
2	Internal-To-External	User defined	Enabled	-	VM	Any	Allow
	default_rule	Default	Enabled	-	Any	Any	Deny

4.3 Page for manage NSX Firewall

Edit Rules

NEW ON TOP
NEW ABOVE
REMOVE
MOVE UP
MOVE DOWN
MOVE TO
GO TO USER RULES

	#	Name	Category	State	Applications	Source	Destination	Action	IP Protocol	Logging
<input type="radio"/>	1									Enabled
<input type="radio"/>	2									Enabled
<input type="radio"/>										Disabled

3 rule(s)

DISCARD SAVE

4.4 How to Add Rule Firewall

4.4.1 Click NEW ON TOP for add new rule firewall

Edit Rules

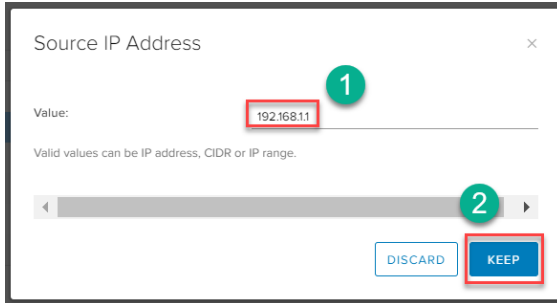
NEW ON TOP
NEW ABOVE
REMOVE
MOVE UP
MOVE DOWN
MOVE TO
GO TO USER RULES

	#	Name	Category	State	Applications	Source	Destination	Action	IP Protocol	Logging
<input checked="" type="radio"/>	1	TEST	User defined	<input checked="" type="checkbox"/>	-	< select >	< select >	Allow	IPv4	<input type="checkbox"/>
<input type="radio"/>	2									Enabled
<input type="radio"/>	3									Enabled
<input type="radio"/>										Disabled

4 rule(s)

DISCARD SAVE

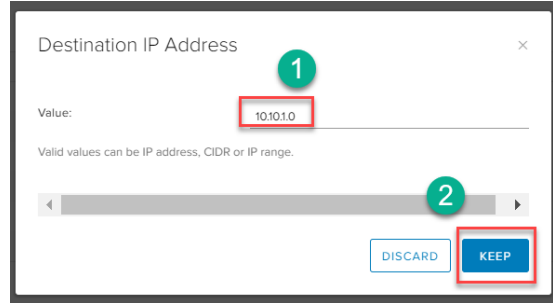
4.4.2 Click  for add IP Address value



Source IP Address

Value:

Valid values can be IP address, CIDR or IP range.



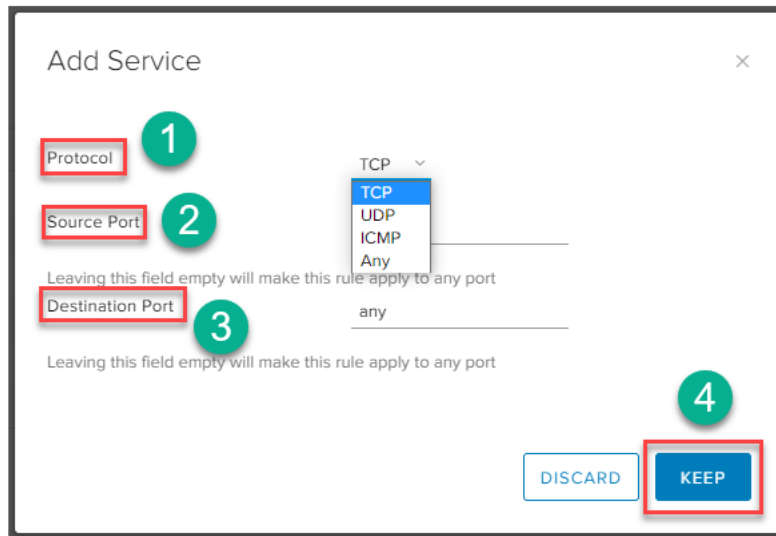
Destination IP Address

Value:

Valid values can be IP address, CIDR or IP range.

4.4.3 Select Service Port (Default = Any)

Protocol, Source Port และ Destination Port



Add Service

Protocol

Source Port

Destination Port

Leaving this field empty will make this rule apply to any port

any

4.4.4 Action for Rule

Allow: Accept all traffic and port

Deny: Drop all traffic and port

4.4.5 Click Save Changes for apply rules

