DDI 透過 DDD On-Premises 與 Vision One 整合

1. 產品版本需求

- DDI 5.7 SP3 or above
- DDD 5.2 Patch 1 or above
- 2. 透過 DDD 啟用 DDDNA SaaS
 - 2.1 在 DDD web console 上, 選擇Administration>Licenses, 輸入 XDR Addon 序號.

DDNASaaS 會自動啟動,下列訊息會出現在 DDD web console 上面.

Provisioning for Deep Discovery Director - Network Analytics as a Service is in progress...

 Deep Discovery Director

 Dashboard
 Detections •
 Threat Intelligence •
 Appliances •
 Alerts
 Reports
 Administration •
 Help

 If Provisioning for Deep Discovery Director - Network Analytics as a Service is in progress...
 Environmentation •
 Help

2.2 完成後會出現下列訊息

Deep Discovery Director - Network Analytics as a Service is ready. Go toAdministration>Network Analytics>Connected Sourcesto configure connected data sources. Deep Discovery Director

 Detections - Threat Intelli

Deep Discovery Director - Network Analytics as a Service is ready. Go to Administration > Network Analytics > Connected Sources to configure connected data License

3. 註冊 DDI 到 DDD

- 3.1 在 DDD web console, 選擇Help, 拷貝 API key.
- 3.2 在 DDD web console, 選擇 Administration > Integrated Products/Services > Deep Discovery Director, 在 Server type 選擇 On-premises version, 輸入 DDD 的 server address, DDD API key, 點選 Register.

Trend Micro XDR	Server Type:	On-premises version
Deep Discovery Directo	e l	Cloud version
Apex Central		
Threat Investigation Cer	Appliance Details	
Threat Intelligence Shar Inline Products/Services	Status:	Not registered
SAMI Authentication	Host name:	localhost
Misses R Active Disecto		
Cueles	.,	
aysiog	Connection Setting	12
litigation Products/Ser	Server address:*	
Registration		
Exceptions	Port:*	443
	API key:*	
	Use the system	proxy settings

- 4. 將 DDI 從 Unmanaged folder 搬移到 Managed folder.
 - 4.1 在 DDD web console, 選擇 Appliances > Directory, 將 DDI 搬到 managed 或其他自訂的 folder.

 Operations Directory

 Dashboard
 Detections
 Appliances
 Alerts
 Reports

 Directory
 All •
 Image: Colspan="4">Image: Colspan="4"

5. 透過 DDD web console 將 DDI 的網路流量導給 DDDNASaaS.

5.1 在 DDD web console, 選擇 Administration > Network Analytics, 點選 Connected Sources.

Th	reat Intelligence 👻	Appliances -	Administration -	Help							
N	Network Analytics										
	Status Connected Sources Domain Exceptions (Priority Watch List (Registered Services (Trusted Internal Network (
¢	Configure 1 selected Bandwidth ca										
	Status	Display Name 🕆	Host Name		IP Address	Version	Appliance	Bandwidth	Last Synchroni		
	Disabled localhost		localhost	5.7 Build 1			Disabled	250 Mbps	N/A		

5.2 勾選要設定的 DDI (預設是 Disable),點選 Configureu 並 加以 Enable

Configure Connected Sources							
Bandwidth capacity: 250 / 2,000 Mbps							
Status	Data Source ↑	Appliance Proxy Settings	Bandwidth				
Enabled	localhost (10.3.183.15)	C Enabled O Disabled	250 Mbps				

Save	Cancel

5.3 會看到 Status 已經變成 Enable

t	🕖 Deep Discovery Director										
Da	ashboard Detection	ons - Threat Inte	lligence - Appliances	- Alerts	Reports Admin	inistration - Help					
N	Network Analytics										
	Status Connected Sources Domain Exceptions (i) Priority Watch List (i) Registered Services (i) Trusted Internal Network (i)										
	Status	Display Name 🕆	Host Name	IP Addre	ss Versio	on Appliand	ce Pr Bandwidth				
	Enabled	localhost	localhost	10.3.183	15 5.7 Bu	ild 1178 Disabled	250 Mbps				

- 6. Onboard DDD 到 Trend Micro Vision One
 - 6.1 登入 Trend Micro Vision One console. 選擇 INVENTORY MANAGEMENT > Network Inventory.



6.2 點選 Deep Discovery Director on-premises version,點選 Next.

Connect Network Sensors

Network Inventory allows you to manage network sensors directly from the console. Select the product or service to use to connect network sensors.

O Network Inventory Service

Deep Discovery Director on-premises version

6.3 點選 Finish

Connect Network Sensors

Connecting Deep Discovery Director on-premises version will automatically connect all managed network sensors (Deep Discovery Inspector appliances) to Trend Micro Vision One.

Click Finish to confirm your choice, or click Back to return to the selection.

Appliance prerequisites

< Back

Finish

6.4 輸入 DDD 的 IP address, 點選 Go

0	Trend Micro Vision One [™] Network Inventory						Ging	۰	Crimbert S	8	
Ð				Connect Network Sensor							
						Connecting Deep Discovery Director on-premises version will automatically connect all managed network sensors (Deep Discovery					
<u>[8]</u>]					Inspecto	or appliances) to Trend Mic	ro Vision	One.			
Х					Deep D	iscovery Director Version:				í.	
•					5.2 Pa	itch 1 and above					
≣≾					Applian	ce IP address or FQDN:					
					193.1	60 H				Go	
Ę					Instruct	ions:				_	
					Step 1:	Specify the IP address or Director and click Go . The	FQDN of t product	he dep console	loyed Deep Disco will open.	overy	
ŝ					Step 2:	Log on to the Deep Disco Continue in the registrati Director will proceed with	very Direc on promp the onbo	tor cor t dialog arding	nsole, and then cli g. Deep Discovery process.	ick /	
			No network se	ensors connec							

6.5 點選 Continue



6.6 在 Administration > Trend Micro Vision One 頁面,可以 看到註冊成功的結果

D	ashboard	Detections -	Threat Intelligence -	Appliances -	Alerts	Reports	Administration -	Help			
٦	Trend Micro Vision One										
	Status	Connected Sources									
	Note: Regis	stering Deep Discove	ry Director to Trend Micro Visi	ion One sends the act	ivity data of all	registered Deep	Discovery appliances to	Trend Micro	Vision One.		
	Status:	Registered	Connected								
	Last connect	cted: N/A									

7. 回到 Trend Micro Vision One Console,到 Network Inventory 頁面可以看到 DDI 已經註冊為一個 Network Sensor.

0	Trend Micro Vision One [™] Network Inventory										
Ð	Bandwidth usage: 250 / 1										
(R)	Connected Network Sensors (
	Identifier	Network Analytics	Connection status	Sensor version	Bandwidth	License expiration	Actions				
X		date									
	localhost (#001458/14)	Enabled	 Healthy 	5.7 Service Pack 3	250 Mbps	2021-12-31					
±£											