

Vectra NDR for Cloud Gigamon Deployment Guide for Azure

Version: July 30, 2025

Table of Contents

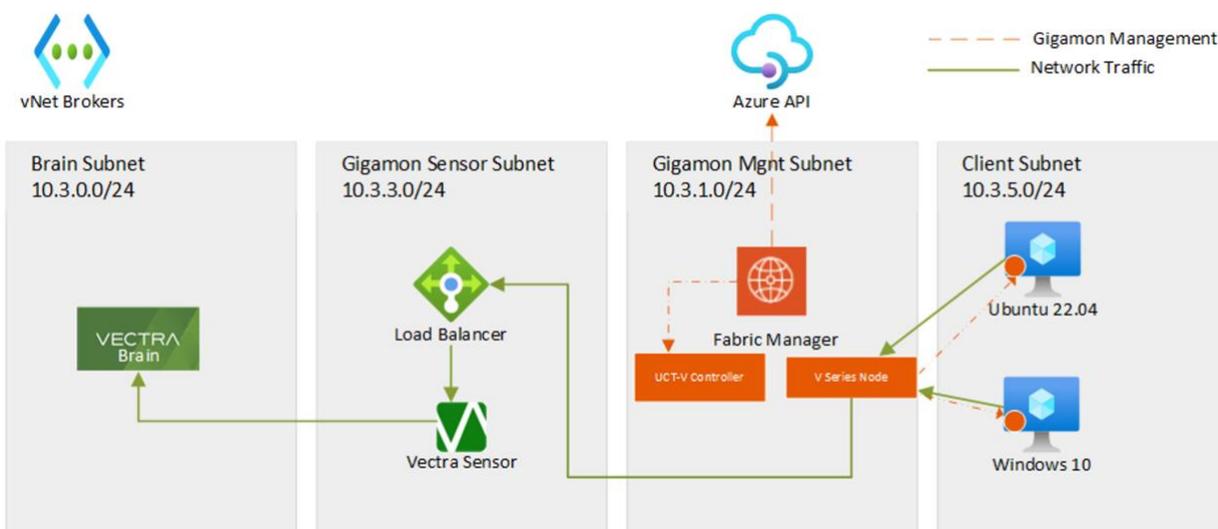
Introduction	3
Architecture Introduction	3
Gigamon Components and Terminology	4
Resources	5
Information Gathering / Scoping (Pre-Deployment).....	6
Licensing.....	6
Prerequisites	7
GigaVUE-FM Version Compatibility	7
Vectra Sensor Support	7
Supported Operating Systems for UCT-V Agents.....	7
Subscribe to Gigamon GigaVUE Cloud Suite for Azure	7
Resource Group / Virtual Network / Subnet	9
Key Pair.....	9
Default Login Credentials	9
Network Security Group (Firewall Rules)	10
Azure Security Credentials.....	12
Sourcing Required Software Components	14
Recommended Instance Types for Azure Deployments	14
Deployment.....	15
High Level Overview of Deployment Process	15
Deploying the Fabric Manager in Azure	16
Creating a Monitoring Domain	17
Deploying the Fabric	19
Deploying UCT-V Agents	20
Special notes for v6.10 and higher	21
Creating token and adding it to your client machines	21
Linux installation using .deb or .rpm package	22
Windows installation	23
Configure a Monitoring Session and Map	25
Post Deployment Guidance	27
Installing a Custom Certificate	27
Worldwide Support Contact Information	27

Introduction

Vectra NDR for Cloud combines licensing for Vectra NDR with licensing for Gigamon's GigaVUE Cloud Suite. This enables Azure IaaS network traffic visibility for Vectra using Gigamon's agent-based solution. This guide provides guidance for deploying the Gigamon components of the solution in Azure. Deployment of the Vectra components are covered in their respective deployment guides and links to those guides are provided in the [Resources](#) section below.

Vectra and Gigamon have partnered to provide simplified licensing on a per IP basis. The solution is sold and supported by Vectra. Please see the Licensing section for more details.

Architecture Introduction



The diagram above shows a simplified architecture example for Azure to introduce the basic architecture and components involved in a Vectra NDR for Cloud deployment. Every deployment will typically be unique in some way. Please see [Information Gathering / Scoping \(Pre-Deployment\)](#) for some guidance.

The diagram above depicts the following:

- ▼ VM instances in the client subnet that you desire to monitor with NDR for Cloud have a Gigamon UCT-V agent installed on them (the orange dot on the instances represents the UCT-V agent).
- ▼ The UCT-V agents communicate with the UCT-V Controller and forward traffic to the V Series Node(s).
- ▼ The V Series Node(s) forward VXLAN encapsulated traffic to the Vectra vSensor(s) which in turn produce a metadata stream that is analyzed by the Vectra Brain appliance.
- ▼ The Gigamon Fabric Manager is typically deployed in the same VNET/Subnet that other management/security tools are installed in. It deploys and manages the "Fabric" (UCT-V Controller and V Series Node(s)).

Gigamon Components and Terminology

▼ GigaVUE® Fabric Manager (GigaVUE-FM)

- GigaVUE® Fabric Manager (GigaVUE-FM) provides unified access, centralized administration, and high-level visibility for all GigaVUE traffic visibility nodes in the enterprise or data center, allowing a global perspective which is not possible from individual nodes.
- In addition to centralized management and monitoring GigaVUE-FM helps you with configuration of the virtual traffic policies for the visibility fabric thereby allowing administrators to map and direct network traffic to the tools and analytics infrastructure.
- You have the flexibility of installing GigaVUE-FM across various supported platforms. Additionally, you can effectively manage deployments in any of the cloud platforms as long as there exists IP connectivity for seamless operation.
- GigaVUE-FM can be installed on-premises as a VM, or launched from a supported public cloud marketplace.
- GigaVUE-FM manages the configuration of the following components in your Azure Virtual Networks:
 - UCT-V Controller
 - GigaVUE V Series® Nodes

▼ Fabric = V Series Nodes & UCT-V Controller

- UCT-V Controller
 - UCT-V Controller (earlier known as G-vTAP Controller) manages multiple UCT-Vs and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes. GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs. A UCT-V Controller can only manage UCT-Vs that has the same version. For example, the UCT-V Controller v6.10 can only manage UCT-Vs v6.10. If you have UCT-Vs of an older version still deployed in your instances, you must configure multiple UCT-V Controller versions. While configuring the UCT-V Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the UCT-Vs to the GigaVUE V Series nodes. The tunnel type should be VXLAN for Vectra NDR for Cloud.
 - Note: A single UCT-V Controller can manage up to 1000 UCT-Vs.
- GigaVUE V Series Node
 - GigaVUE® V Series Node is a visibility node that aggregates mirrored traffic. It distributes the optimized traffic to cloud-based tools.
 - Multiple V Series Nodes can be deployed as required to handle the traffic being mirrored. Each standard V Series node (Standard_D4s_v4) can handle approximately 7 GB of traffic.
 - If additional nodes are required for scaling on the Gigamon side, these can be deployed automatically by the Fabric Manager.

▼ UCT-V

- UCT-V (previously known as G-vTAP Agent) is an agent that is installed in a virtual instance. This agent mirrors the selected traffic from the instances (virtual machines) to the GigaVUE V Series Node. The UCT-V is offered as a Debian (.deb), Redhat Package Manager (.rpm) package, ZIP and MSI.

Resources

All NDR for Cloud deployments will typically begin with deployment of Vectra NDR or NDR for Cloud will be an add-on to an existing Vectra NDR deployment to bring visibility to cloud deployed resources. Please see the table below for resources related to the deployment of the Vectra AI platform and for public Gigamon documentation resources. Vectra's NDR for Cloud documentation will sometimes point to resources available in the online Gigamon Public Documentation library. It should be noted that NDR for Cloud is supported by directly by Vectra and not Gigamon. Also, some Gigamon public documentation will refer to features or capabilities that are not part of NDR for Cloud. Please see the [Licensing](#) section for more details.

KB Article Link or Index Category	Description
Product Documentation Index	Vectra's main index that tracks formal product documentation. Use the search box to find additional KB articles.
Analyst User Experiences (Respond vs Quadrant)	Vectra currently offers two different analyst user experiences (UX's). This article provides guidance to help users determine which UX they are working with. This is helpful when looking for documentation because some articles/documents will only apply to a specific UX.
Respond UX Deployment Guide	Starting point for Respond UX Vectra deployments.
Quadrant UX Deployment Guide	Starting point for Quadrant UX Vectra deployments.
AWS IaaS	Guides detailing best practices, Brain and network Sensor deployment in AWS IaaS environments.
Azure IaaS	Guides detailing Brain and network Sensor deployment in Azure IaaS environments.
GCP IaaS	Guides detailing network Sensor deployment in GCP IaaS environments.
CDR for AWS Deployment Guide	Guide detailing deployment of Cloud Threat Detection and Response (CDR) for AWS using CloudTrail log data as a data source.
CDR for M365, IDR for Azure AD	Guides detailing deployment of Cloud Threat Detection and Response (CDR) for Microsoft 365, and Identity Threat Detection and Response (ITDR) for Microsoft Azure AD.
CDR for Azure Deployment Guide	Guide detailing deployment of Cloud Threat Detection and Response (CDR) for Microsoft Azure using Azure platform logs as a data source.
GigaVUE 6.10 Documentation Publicly available Gigamon documentation	This online documentation provides the complete GigaVUE 6.10 documentation set in a single, searchable interface. This site is easier to navigate and is best for interactive use.
GigaVUE 6.10 Guides Publicly available Gigamon documentation	Downloadable versions of GigaVUE 6.10 documentation. Documentation for other versions can also be found here.

Information Gathering / Scoping (Pre-Deployment)

Prior to beginning deployment, it is a best practice to survey your environment and determine the overall scope of your deployment including what traffic should be captured where. This data can help to predict costs for the instances required to support the traffic acquisition and analysis (Gigamon resources and required Vectra Sensors). It can also help determine any data transfer costs that may be associated with the deployment.

Vectra SEs have tools that can help gather data from supported public clouds and tools that can help predict costs. Please work with your Vectra account team to utilize these tools and plan the deployment scope.

- ▼ PoV (Proof of Value) deployments of NDR for Cloud should be limited to a single VNET and 10 monitored hosts.
- ▼ Full production deployments of NDR for Cloud will include professional services from Vectra to assist with the deployment.

Please see the [Vectra Platform Traffic Recommendations](#) article for types of traffic that should be examined by Vectra when using network Sensors. It also covers how to enhance automated Host ID and what traffic is not required.

Licensing

When a Vectra customer licenses NDR for Cloud, it includes the following:

- ▼ 1 IP of coverage for Vectra NDR.
- ▼ 1 IP of coverage for Gigamon BaseVUE software which includes:
 - UCT-V Agents (licensed per IP)
 - Fabric Manager, V Series Nodes and UCT-V Controller (Fabric). The license allows deployment of as many of these supporting resources as are required for your deployment.
- ▼ The VBL (Volume Based License) component is arbitrarily set at 25 TB/day because Gigamon does not typically license by IP. This limit can be ignored and is not enforced by the Fabric Manager. The IP based licensing above is the contractual limit that needs to be managed with your Vectra account team.
 - Features included with the Gigamon license are: erspan, geneve, tunneling, and flowmap.

Limitations:

- ▼ Only Vectra vSensors in supported public clouds can be used as targets for mirroring traffic.
 - If you wish to direct traffic to other tools, you must purchase a different license directly from Gigamon. Please contact your Vectra and Gigamon sales teams to discuss options.
- ▼ If you wish to use other features or applications that are not part of NDR for Cloud licensing, then you must purchase a different license directly from Gigamon. Please contact your Vectra sales team to discuss options.

Tracking and Enforcement:

- ▼ GigaVUE-FM tracks the license usage for each V Series node as follows:
 - When you create and deploy a monitoring session, GigaVUE-FM allows you to use only those applications that are licensed at that point (applicable only for ACTIVE licenses, licenses in grace period are not included).
 - When a license goes into grace period (45 days), you will be notified with an audit log.
 - When a license expires (and has not been renewed yet), you can no longer configure new Monitoring Sessions.
 - Note: When the Gigamon license expires, GigaVUE-FM displays a notification on the screen.
- ▼ Vectra licensing is self-enforced except on VMware Brains. See its [deployment guide](#) for details.

Prerequisites

GigaVUE-FM Version Compatibility

Vectra NDR for Cloud requires at least version 6.6 of GigaVUE-FM (Fabric Manager). GigaVUE-FM version 6.6 supports the latest fabric components version as well as (n-2) versions. It is always recommended to use the latest version of fabric components with GigaVUE-FM, for better compatibility.

Vectra Sensor Support

NDR for Cloud only supports sending captured traffic to Vectra vSensor capture ports that have an IP address associated with them in supported public cloud platforms. This means that only AWS, Azure, and GCP Vectra Sensors can be used as targets for Gigamon to send traffic to in an NDR for Cloud deployment. Other virtual or physical Vectra Sensors cannot be used as Sensors for an NDR for Cloud deployment. This guide is focused on Azure deployment, but deployments that span multiple public clouds are supported. The Fabric Manager can be deployed anywhere that the required connectivity between components is supported. Below are links to the deployment guides for the supported vSensors.

- ▼ [Azure Sensor Deployment Guide](#)
- ▼ [AWS Sensor Deployment Guide](#)
- ▼ [GCP Sensor Deployment Guide](#)

Supported Operating Systems for UCT-V Agents

As per the GigaVUE-FM Version Compatibility above, please ensure that UCT-V agents fall no more than N-2 versions behind the FM version. It is always recommended to use the latest version of UCT-V with GigaVUE-FM, for better compatibility. Please see [Supported Operating Systems for UCT-V](#) for more detail.

Operating System	Supported Versions
Ubuntu / Debian	Versions 16.04 through 24.04
CentOS	Versions 7.5 through 9.0
RHEL	Versions 7.5 through 9.4
Windows Server	Versions 2012 through 2022
Rocky OS	Versions 8.4 and above

Subscribe to Gigamon GigaVUE Cloud Suite for Azure

While the Fabric manager can be subscribed to and deployed from the marketplace, the fabric components (V Series Nodes, UCT-V Controller, and optional V Series Proxy) are deployed through the Fabric Manager. For the Fabric Manager to be able to launch the fabric images, you must accept the terms of the end user license agreements (EULAs) for the fabric images and enable programmatic access. This can be done from the [Azure CLI](#), [Azure Cloud Shell](#), or Azure Portal (GUI). This guide will cover the subscription and term acceptance via the CLI/Cloud Shell (they are the same process). For details on the GUI process, please see: [Enable Subscription via the Azure Portal](#)

- ▼ If you are not already logged in, login to Azure using `"az login"` (not required if using the cloud shell as you already would have been logged in to access the cloud shell).

The subscription and term acceptance for the Gigamon VM images will be tied to your default Azure subscription if you don't use a `"--subscription"` option to specify your desired Azure subscription when executing the vm image acceptance command later. Please ensure your image acceptance is tied to the subscription you desire to install

into. You can see which subscription is your default subscription by executing an "az account list" command at the prompt. The default subscription will have one of them marked as default as shown in the below image:

```

> az account list
{
  "cloudName": "AzureCloud",
  "homeTenantId": "aa5e...bba7",
  "id": "b3fe...ff43e",
  "isDefault": true,
  "managedByTenants": [],
  "name": "demolab.vectra.ai",
  "state": "Enabled",
  "tenantId": "aa5...bba7",
  "user": {
    "name": "...demolab.vectra.ai",
    "type": "user"
  }
},
{
  "cloudName": "AzureCloud",
  "homeTenantId": "a6c...2d",
  "id": "ac6...a8",
  "isDefault": false,
  "managedByTenants": [],
}

```

- ▼ "az vm image list --all --publisher gigamon-inc" will display all images available from Gigamon but you may find it useful to combine this with grep to display only the versions you are interested in subscribing to (please note that at the CLI, the UCT-V Controller is still referred to by its old name "gvtap"):

```

> az vm image list --all --publisher gigamon-inc | grep 6.6
  "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:gfm-azure:6.6.00",
  "version": "6.6.00"
▶ "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:gfm-azure:6.6.01",
  "version": "6.6.01"
  "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:gigavue-netvue-v6600-2500tb:6.6.00",
  "version": "6.6.00"
  "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:gigavue-netvue-v6600-2500tb:6.6.01",
  "version": "6.6.01"
  "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:gigavue-securevue-v6600-250tb:6.6.00",
  "version": "6.6.00"
  "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:gigavue-securevue-v6600-250tb:6.6.01",
  "version": "6.6.01"
  "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:gigavue-securevue-v6600-50tb:6.6.00",
  "version": "6.6.00"
  "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:gigavue-securevue-v6600-50tb:6.6.01",
  "version": "6.6.01"
▶ "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:gvtap-ctrl:6.6.00",
  "version": "6.6.00"
▶ "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:vseries-node:6.6.00",
  "version": "6.6.00"
▶ "urn": "gigamon-inc:gigamon-gigavue-cloud-suite:vseries-proxy:6.6.00",
  "version": "6.6.00"

```

- ▼ Using the below as an example, subscribe and accept the terms for each of the highlighted images above.
 - Always use the newest image version available. Newer versions will be available in the future.
 - "az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite:gfm-azure:6.6.01"

```

> az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite:gfm-azure:6.6.01
{
  "accepted": true,
  "id": "/subscriptions/b3f...43e/providers/Microsoft.MarketplaceOrdering/offerTypes/Microsoft.MarketplaceOrdering/offertypes/publi
ers/gigamon-inc/offers/gigamon-gigavue-cloud-suite/plans/gfm-azure/agreements/current",
  "licenseTextLink": "https://mpcprodsa.blob.core.windows.net/legalterms/3E5ED_legalterms_GIGAMON%253a20INC%253a24GIGAMON%253a2DGIGAVUE%253a2DCLLOUD%253a2DSUIT
253a24GFM%253a2DAZURE%253a24BGSZ00HPVC4M4GL4ZK5K752EDRWVRVJPTVJ7LMSHSRRRN5TYHJR47WNYMJH2ULRWBWUG5CN04E6LF34G43TGV3S0GRXJ40CBMLHLBTX0.txt",
  "marketplaceTermsLink": "https://mpcprodsa.blob.core.windows.net/marketplaceterms/3EDEF_marketplaceterms_VIRTUALMACHINE%253a24AAK20AIZEAW5H4MSP5KSTVB6NDKKR
BAU23BRFTW4YC2MQLJUB52EYU0JBVF3YK34CIVPZL2HWYASCPGDUY502FWEGRBV0XWZESY.txt",
  "name": "gfm-azure",
  "plan": "gfm-azure",
  "privacyPolicyLink": "https://www.gigamon.com/privacy-policy.html",
  "product": "gigamon-gigavue-cloud-suite",
  "publisher": "gigamon-inc",
  "retrieveDatetime": "2024-05-23T20:05:22.0638077Z",
  "signature": "E5HIH2GIAGGSMVS466IMHP5G3LTA4VG64L6XL5BIGXC0WKEPG7NSSL2HZP3XJMAYSLBMY40W0GTOCCYVZKY2LHSP4ZRLQYHRVK4Q",
  "systemData": {
    "createdAt": "2024-05-23T20:05:25.805818+00:00",
    "createdBy": "b3f...f43e",
    "createdByType": "ManagedIdentity",
    "lastModifiedAt": "2024-05-23T20:05:25.805818+00:00",
    "lastModifiedBy": "b3f...3e",
    "lastModifiedByType": "ManagedIdentity"
  },
  "type": "Microsoft.MarketplaceOrdering/offertypes"
}

```

- ▼ After you have subscribed and accepted terms for each image, you are ready to move on to the next step.

Resource Group / Virtual Network / Subnet

Before proceeding with deployment, you must create a resource group in Azure, or you can use an existing resource group that you will want to deploy the Gigamon resources into. A resource group is a container that holds all the resources for a solution. To create a resource group in Azure, refer to [Create a resource group](#) topic in the Azure Documentation.

You must also create a new VNet or be prepared to use an existing VNet. An Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. You should configure the Gigamon fabric components in a centralized VNet only. To create a virtual network in Azure, refer to [Create a virtual network](#) topic in the Azure Documentation.

Your VNet must also have subnets defined as part of it for your deployment. You can add subnets when creating a VNet or add subnets to an existing VNet. Refer to [Add a subnet topic](#) in the Azure Documentation for detailed information.

See below for the two recommended subnets that your VNet should have to configure the Gigamon components in Azure:

- ▼ Management Subnet
 - Subnet that the Fabric Manager uses to communicate with the V Series Nodes, UCT-V Controller, and optional V Series Proxy.
- ▼ Data Subnet
 - A data subnet can accept incoming mirrored traffic from UCT-T agents to the V Series Nodes or be used to egress traffic to a Vectra Sensor from the V Series Nodes. There can be multiple data subnets.
 - Ingress is VXLAN from the UCT-V Agents.
 - Egress is VXLAN to the Vectra Sensor(s).
 - ! Note - If is ok to use a single subnet, in that case the management subnet will also be the data subnet.
- ▼ Tool Subnet
 - A tool subnet can egress traffic to a Vectra Sensor from the GigaVUE V Series Nodes. There can be only one tool subnet.

!! Please note - Before moving on, you should now have a Resource Group, Virtual Network (VNet), and Subnet(s) to use with your deployment.

Key Pair

SSH keys can be easily created and stored in the Azure Portal. Please see [Generate and store SSH keys](#) in the Azure portal for details on how to create key pairs. A key pair consists of a public key and a private key. When you define the specifications for the UCT-V Controller, V Series Node(s), and optional V Series Proxy during fabric deployment, you must choose a key pair or re-use an existing one.

Please generate an SSH key pair to be used with the Fabric Manager and fabric deployment later. If desired, different key pairs can be used for the deployment of the other fabric components. It's recommended to use the same key pair for all the Gigamon components unless your security policy does not allow this.

Default Login Credentials

Component	Login Credentials
Fabric Manager	GUI Login / Password: admin / admin123A!! - SSH Login / Password: azureuser / ssh key
V Series Nodes	Login / Password: admin / use the SSH key pair you generated
UCT-V Controller	Login / Password: admin / use the SSH key pair you generated
V Series Proxy (Optional)	Login / Password: admin / use the SSH key pair you generated

Network Security Group (Firewall Rules)

When you launch the Fabric Manager, V Series Proxies, V Series Nodes, and UCT-V Controllers, a security group can be utilized to define virtual firewall rules for your instance, which in turn regulates inbound and outbound traffic. You can add rules to manage inbound traffic to instances, and a distinct set of rules to control outbound traffic. It is recommended to create a separate security group for each component.

The following table lists the overall network firewall requirements for the Gigamon components of a Vectra NDR for Cloud deployment. Please see the [GigaVUE Cloud Suite for Azure Prerequisites](#) article for more detail and any additional rules that are not required for a Vectra NDR for Cloud deployment. For the Vectra portions of your deployment, please see [Firewall Requirements for Vectra Deployments](#).

Direction	Protocol	Port	CIDR	Purpose
GigaVUE Fabric Manager (FM)				
Inbound	TCP	22	Administrator Subnet	Management connection to FM (CLI via SSH).
Inbound	TCP	443	Administrator Subnet	Management connection to FM (GUI). Allows connection to REST API.
Inbound	TCP	443	UCT-V Controller IP	Allows UCT-V Controller to communicate registration requests to FM.
Inbound	TCP	443	V Series Node(s)	Allows V Series Nodes to communicate registration requests to FM, if V Series Proxy is NOT used.
Inbound	TCP	443	V Series Proxy IP	Allows V Series Proxy to communicate the registration requests to FM.
Inbound	TCP	5671	V Series Node(s)	Allows V Series Nodes to send traffic health updates to FM.
Inbound	TCP	5671	UCT-V Controller IP	Allows UCT-V controller to send statistics to FM.
Inbound	TCP	9600	UCT-V Controller IP	Allows FM to receive certificate requests from UCT-V Controller.
Inbound	TCP	9600	V Series Proxy IP	Allows FM to receive certificate requests from V Series Proxy.
Inbound	TCP	9600	V Series Node(s)	Allows FM to receive certificate requests from V Series Node(s).
Outbound	TCP/UDP	53	DNS Servers	Allows FM to query the DNS servers specified for use by FM.
Outbound	TCP	80	UCT-V Controller IP	Allows FM to send ACME challenge requests to UCT-V Controller.
Outbound	TCP	80	V Series Proxy	Allows FM to send ACME challenge requests to V Series Proxy.
Outbound	TCP	80	V Series Node(s)	Allows FM to send ACME challenge requests to V Series Node(s).
Outbound	TCP	443	AWS Endpoints	Allows FM to communicate with the public cloud platform APIs.
Outbound	TCP	8889	V Series Node(s)	Allows FM to communicate with V Series Node(s).
Outbound	TCP	8890	V Series Proxy IP	Allows FM to communicate with V Series Proxy.
Outbound	TCP	9900	UCT-V Controller IP	Allows FM to communicate with UCT-V Controller.
UCT-V Controller				
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	Fabric Manager IP	Allows UCT-V to receive ACME challenge requests from FM.
Inbound	TCP	8300	UCT-V Subnet	Allows UCT-V Controller to receive certificate requests from UCT-V agents.
Inbound	TCP	8891	UCT-V Subnet	Only required for backwards compatibility when FM is 6.10 and fabric is n-1 or n-2 version.
Inbound	TCP	8892	UCT-V Subnet	Allows UCT-V Controller to receive registration requests and heartbeat from UCT-V agents.
Inbound	TCP	9900	Fabric Manager IP	Allows UCT-V Controller to communicate with FM.
Inbound	TCP	9900	UCT-V Subnet	Allows UCT-V Controller to receive traffic health updates from UCT-V agents.
Outbound	TCP	443	Fabric Manager IP	Allows UCT-V Controller to communicate the registration requests to FM.
Outbound	TCP	5671	Fabric Manager IP	Allows UCT-V Controller to send traffic health updates to FM.
Outbound	TCP	8301	UCT-V Subnet	Allows ACME validation flow from UCT-V Controller to UCT-V agents.
Outbound	TCP	9600	Fabric Manager IP	Allows UCT-V to send certificate requests to FM.
Outbound	TCP	9901	UCT-V Subnet	Only required for backwards compatibility when FM is 6.10 and fabric is n-1 or n-2 version.
Outbound	TCP	9902	UCT-V Subnet	Allows UCT-V Controller to communicate with UCT-V agents with versions 6.10 and above.

UCT-V Agent(s)				
Inbound	TCP	8301	UCT-V Controller IP	Allows UCT-V agent to receive ACME challenge request from UCT-V Controller.
Inbound	TCP	9901	UCT-V Controller IP	Only required for backwards compatibility when FM is 6.10 and fabric is n-1 or n-2 version.
Inbound	TCP	9902	UCT-V Controller IP	Allows UCT-V agents to communicate with UCT-V Controller.
Outbound	UDP (VXLAN)	4789	V Series Node(s)	Allows UCT-V agents to send VXLAN tunnel traffic to V Series Nodes.
Outbound	TCP	8300	UCT-V Controller IP	Allows ACME validation flow from UCT-V agents to UCT-V Controller.
Outbound	TCP	8891	UCT-V Controller IP	Only required for backwards compatibility when FM is 6.10 and fabric is n-1 or n-2 version.
Outbound	TCP	8892	UCT-V Controller IP	Allows UCT-V agent to communicate with UCT-V Controller for registration and heartbeat.
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V agent to send traffic health updates to UCT-V Controller.
Outbound	TCP	11443	V Series Node(s)	Allows UCT-V agent to securely transfer the traffic to GigaVUE V Series Nodes.
V Series Node(s)				
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	Fabric Manager IP	Allows V Series Node to receive ACME challenge requests from FM.
Inbound	TCP	80	V Series Proxy IP	Allows V Series Node to receive ACME challenge requests from V Series Node(s).
Inbound	UDP (VXLAN)	4789	UCT-V Subnet	Allows UCT-V agents to send VXLAN tunnel traffic to V Series Node(s).
Inbound	TCP	8889	Fabric Manager IP	Allows FM to communicate with V Series Node(s).
Inbound	TCP	8889	V Series Proxy IP	Allows V Series Proxy to communicate with V Series Node(s).
Inbound	TCP	11443	UCT-V Subnet	Allows UCT-V agents to securely send traffic to V Series Node(s).
Outbound	TCP	443	Fabric Manager IP	Allows V Series Node(s) to send registration requests and heartbeat messages to FM when V Series Proxy is not used.a
Outbound	UDP (VXLAN)	4789	Vectra vSensor(s)	Allows V Series Node(s) to tunnel traffic to the vSensor(s).
Outbound	TCP	5671	Fabric Manager IP	Allows V Series Node(s) to send traffic health updates to FM.
Outbound	TCP	8891	V Series Proxy IP	Only required for backwards compatibility when FM is 6.10 and fabric is n-1 or n-2 version.
Outbound	TCP	8892	V Series Proxy	Allows V Series Node to send certificate request to V Series Proxy IP.
V Series Proxy (Optional)				
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	Fabric Manager IP	Allows V Series Proxy to receive ACME challenge requests from FM.
Inbound	TCP	8300	V Series Node(s)	Allows V Series Proxy to receive certificate requests from V Series Node(s).
Inbound	TCP	8890	Fabric Manager IP	Allows FM to communicate with V Series Proxy.
Inbound	TCP	8891	V Series Node(s)	Only required for backwards compatibility when FM is 6.10 and fabric is n-1 or n-2 version.
Inbound	TCP	8892	V Series Node(s)	Allows V Series Proxy to receive registration requests and heartbeat messages from V Series Node(s).
Outbound	TCP	443	Fabric Manager IP	Allows V Series Proxy to communicate the registration requests to FM.
Outbound	TCP	8889	V Series Node(s)	Allows V Series Proxy to communicate with V Series Node(s).

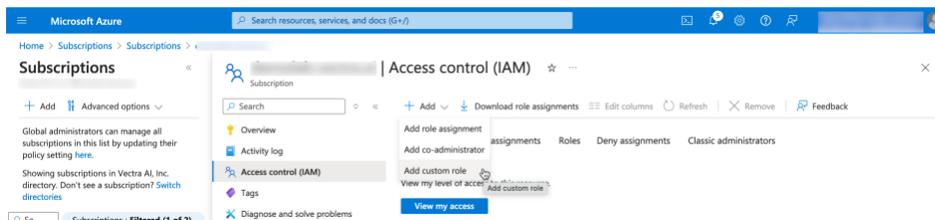
! Please note regarding the optional V Series Proxy

- ▼ V Series Nodes in Azure can be deployed in two ways – with or without the use of a V Series Proxy.
- ▼ When deployed with Proxy, the Fabric Manager communicates with the V Series Node via the Proxy node. This is typically useful when the Fabric Manager is deployed in a VNet that is different than where V Series Nodes are deployed, which makes direct communication with the V Series Nodes unfeasible.
 - If a V Series Proxy is necessary for your environment, please contact your Vectra account team for implementation guidance.

Azure Security Credentials

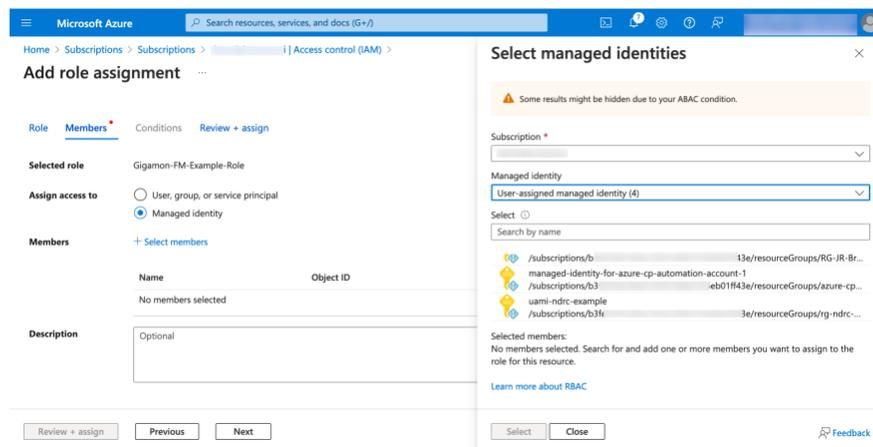
When you first connect the Fabric Manager to Azure, you need the appropriate authentication for Azure to verify your identity and check if you have permission to access the resources that you are requesting. This is used for the Fabric Manger to integrate with Azure APIs and to automate the fabric deployment and management. When deploying the Fabric Manager as a VM in Azure, this should typically be done by using a combination of a managed identity and a custom role in Azure. These will be assigned to the Fabric Manager VM so that it can launch and manage the fabric in Azure.

- ▼ It is recommended to deploy the Fabric Manager as a VM in Azure to manage Azure workloads.
- ▼ When deploying the Fabric Manger in Azure, it is recommended to use a managed identity and custom role with the Fabric Manger instance to enable its ability to perform actions within Azure.
- ▼ When the Fabric Manager is deployed outside of Azure, then an application ID and client secret can be used.
 - If the Fabric Manger is deployed outside of Azure, then the Fabric Manager encrypts and stores the application ID and the client secret in its database.
- ▼ Note: You may need the assistance of a colleague with the necessary rights in Azure to create the managed identity and assign a custom role.
- ▼ **Managed Identity and Custom Role** - If the Fabric Manger will be deployed within Azure, it is recommended to use a managed identity and custom role.
 - Managed Identities for Azure (aka MSI) are available in 2 types: System Assigned and User Assigned.
 - For more details on both types, please see: [Configure managed identities on Azure virtual machines](#).
 - We will be describing the use of a User Assigned Managed Identity in conjunction with a custom role.
 - **!! Please note** - Ultimately, it is up to the security requirements of your organization to determine the most appropriate way to authorize your Fabric Manager to deploy and manage Azure Resources as well as enabling visibility to resource groups and agents.
 - Please see [Permissions and Privileges](#) on the Gigamon Documentation site for more details and the specific permissions needed for different scenarios.
 - Create a custom role in Azure that will be assigned to the User Assigned Managed Identity later.
 - Details on custom role creation can be found in Azure documentation here:
 - [Azure custom roles](#)
 - [Create or update Azure custom roles using the Azure portal](#)
 - [Create or update Azure custom roles using the Azure CLI](#)
 - To do this at the subscription level, its easiest to start in the Azure portal from *Subscriptions > choose your subscription > Access Control (IAM) > + Add > Add custom role*



- Please see [gigamon_vectra_FM_azure.json](#) for a sample custom role that is scoped at the subscription level. Vectra has chosen the subscription scope for this as it allows for maximum flexibility and ease of deployment. If you choose more restrictive scopes, then you will need to do a more complex deployment of credentials for the Monitoring Domain and connections. This is not in scope for this document.

- Create a User Assigned Managed Identity that will be assigned to the VM instance used to run your Fabric Manager.
 - Details on User Assigned Managed Identities can be found in Azure documentation here:
 - [What are managed identities for Azure resources?](#)
 - [Manage user-assigned managed identities](#)
 - [Configure managed identities on Azure virtual machines \(VMs\)](#)
 - To create a User Assigned Managed Identity, navigate in the Azure Portal to *Managed Identities* > + *Create*
 - Choose your subscription and use the same resource group you created earlier.
 - Pick the same region that you will be using for deployment of the Fabric Manager.
 - Give you identity a name, any optional tags you desire on the next screen, and “Review + create” and then “Create” after validation.
- Assign the custom role that you created to the User Assigned Managed Identity.
 - This should be done at the Subscription level.
 - To assign the custom role, navigate in the Azure Portal to *Subscriptions* > *your subscription* > *Access control (IAM)* > + *Add* > *Add role assignment*.
 - Search for your role and select it and then click “Next”.
 - On the Members tab, click the radio button for “Managed identity”, click “+ Select members”, choose the subscription, select “User Assigned Managed Identity” and then select your identity.
 - Continue through the “Review + assign” process to completion.



- After you have **deployed** the Fabric Manager in Azure, you can assign the User Assigned Managed Identity to your VM. **Remember to complete this step after the Fabric Manger deployment.**
 - Navigate in the Azure Portal to your VM that runs the Fabric Manager.
 - Click *Security* > *Identity* (the System Assigned Managed Identity should be “Off”).
 - Click “+ Add”, and select your User Assigned Managed Identity, and click “Add”.

▼ **Application ID and Client Secret** - If the Fabric Manager is deployed outside of Azure, such as in the enterprise data center on a VM, then you must use Application ID and Client Secret to connect to Azure. For details on using this method please see the Application ID and Client Secret section of the [Permissions and Privileges](#) page in the Gigamon documentation. It is generally recommended to use the Managed Identity and Custom Role as described above.

- If you use this method, please see [Create Azure Credentials](#) for additional details.
- For VM deployment of Fabric Manager, please contact your Vectra account team for guidance.

Sourcing Required Software Components

For the Vectra portion of the deployment (Vectra AI Platform and any associated components), please see the deployment guides linked in the [Resources](#) section. This guide primarily covers the Gigamon components of the deployment.

For the Gigamon components, see below:

- ▼ Fabric Manager – This is deployed from the [Azure Marketplace](#) and will be covered in more detail in the [Deployment](#) section.
- ▼ Fabric components (UCT-V Controller, V Series Nodes) – These are deployed from the Fabric Manager after it is running.
- ▼ UCT-V Agents – Vectra will provide details for how to download the agent installation software packages.

Recommended Instance Types for Azure Deployments

The below table represents minimum instance types and vCPU and RAM requirements. Additional instance types can be used. Please contact your Vectra account team to discuss when it may be appropriate to change the instance type.

Component	Instance Type	vCPU	RAM
Fabric Manager	Standard_D4s_v3	4	16 GB
V Series Node	Standard_D4s_v4	4	16 GB
	Standard_D8s_v4	8	32 GB
UCT-V Controller	Standard_B1ms	1	2 GB
V Series Proxy (Optional)	Standard_B1ms	1	2 GB

Deployment

High Level Overview of Deployment Process

There is no one size fits all approach to deployment of NDR for Cloud. Each environment will have its own unique aspects that will need to be considered. It is critical that you have planned where the various components will be installed and that you are engaged with your Vectra team (pre-sales or professional services) depending on if this is a PoV installation or if this is a production deployment.

While this guide focuses on deployment in Azure, some NDR for Cloud deployments will include multiple public clouds and may even involve more than one Fabric Manager. Please work with your Vectra account team to determine the best deployment strategy for more complex environments.

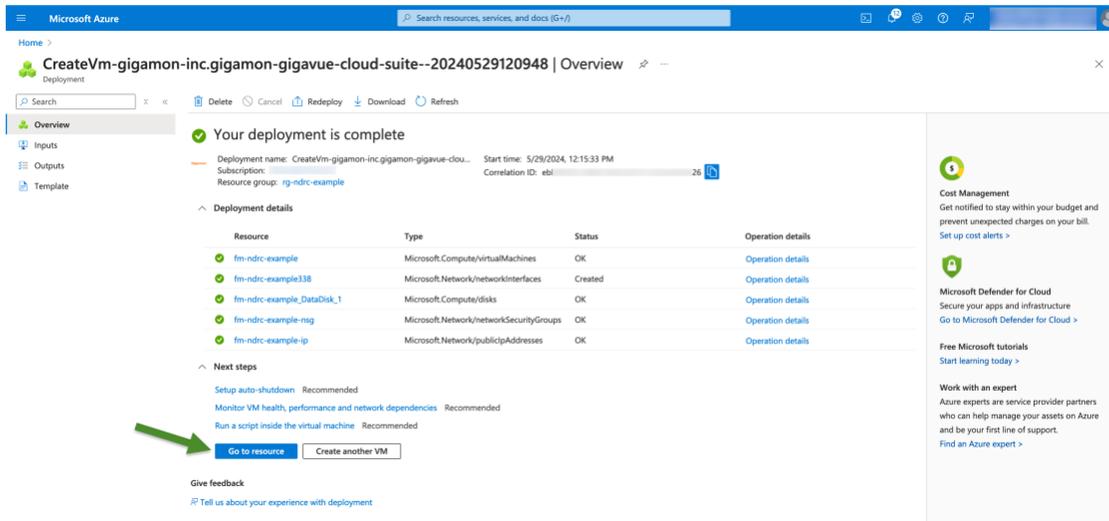
Below are the basic steps involved in a NDR for Cloud deployment:

1. Before beginning deployment.
 - Ensure you have all the necessary **Resources** you may want handy during deployment.
 - Be **engaged** with your Vectra team during deployment.
 - Vectra has SE SMEs for NDR for Cloud who are available to help with PoV deployments.
 - Vectra professional services will be involved in all production deployments.
 - Know the **scope** of your deployment and where you want to install the various components.
 - Work with Vectra to make sure you have your trial or production **license** available to install in the Fabric Manager once deployed.
 - Ensure you have satisfied all the **Prerequisites**.
2. **Deploy the Fabric Manager in Azure.**
3. **Create Monitoring Domain.**
4. **Deploy the Fabric** (V Series Node(s) and UCT-V Controller) from the Fabric Manager.
5. **Deploying UCT-V Agents.**
6. **Configure a Monitoring Session and Map.**
 - This will point to your Azure Vectra Sensors.
7. Deploy the Monitoring Session to make it live (this is covered at the end of Step 6).

Deploying the Fabric Manager in Azure

Per the [Subscribe to Gigamon GigaVUE Cloud Suite for Azure](#) in the [Prerequisites](#) section, you should already be subscribed to GigaVUE Cloud Suite components at least the 6.6 version level. If not, please refer to that section.

- ▼ Search for “Gigamon” in the Marketplace and click “Create” under Gigamon GigaVUE Cloud Suite for Azure.
- ▼ Choose the “GigaVUE-FM v6.6 - BYOL” option. (if a newer version become available, pick that)
- ▼ You should now be on a “Create a virtual machine” page with many tabs for Basics, Disks, Networking, etc.
- ▼ Be sure to configure the following before moving on “Review + create”.
 - **Subscription and Resource Group**
 - Choose your subscription and the Resource group you created earlier.
 - **Instance details**
 - **Virtual machine name** - Input a name.
 - **Region** - Choose your region.
 - **Availability options** - for simplicity, choose No infrastructure redundancy required.
 - **Security type** - typically leave this at the default of Standard.
 - **Image** - This should already be selected.
 - **VM architecture** - x64.
 - **Run with Azure Spot discount** - This is NOT recommended to be enabled because the Fabric manager needs to be persistently available. See [here](#) for more details on spot VMs.
 - **Size** - The default is Standard_D4s_v3. If other options are required, talk to you Vectra team.
 - **Administrator account**
 - Authentication type - SSH public key.
 - Username - Can be left at default of “azureuser”.
 - SSH public key source - Use existing key stored in Azure or use another source for the key. You may have created a key pair earlier in the [Prerequisites](#) section.
 - **Disks**
 - A second disk will need to be manually added on this page.
 - Click “Create and attach a new disk”.
 - **Name** - This will default to a name and does not need to be changed.
 - **Source type** - None (empty disk).
 - **Size** - Click “Change size” and choose 64 GiB and a Performance tier of P10.
 - **Key management** - Leave at default of Platform-managed key.
 - **Enable shared disk** - Leave at default of No.
 - **Delete disk with VM** - Configure at your desire but it is recommended to enable this.
 - **Networking**
 - Edit these settings as required to ensure the right Virtual network and subnet are picked based on what you determined in [Information Gathering / Scoping \(Pre-Deployment\)](#), [Resource Group / Virtual Network / Subnet](#) earlier.
 - It is not recommended to Auto-assign a public IP as this would make the installation more vulnerable to attack. Typically, private connectivity to the Fabric Manager should be used.
 - The VNet should typically be the one that has the most visibility into other VNet, is peered, has network communication, is central and used for management.
 - **Configure network security group** - Choose the [Network Security Group \(Firewall Rules\)](#) you created earlier. If you do not select an existing one a new one will be created that has a default configuration that you may want to change.
 - **Delete public IP and NIC when VM is deleted** - This recommended to be enabled.
 - Other options can be left at their defaults.
 - **Management, Monitoring, Advanced** - Nothing needs to be selected here.
 - **Tags** - It is recommended to add tags per your standard procedures for VMs in Azure.
 - **Review + create** - Validate all your selections and when satisfied, click “Create”.



- ▼ It will take a few minutes to complete the deployment in Azure
 - Once you see the “Your deployment is complete” message you can click on the “Go to resource” to go to the VM detail page where you can assign the User Assigned Managed Identity to your VM as per the earlier instructions in [Azure Security Credentials](#).
 - Login to the Fabric Manager GUI should be available within 10-15 min.
 - Use `https://the_ip_you_configured` and bypass any certificate warnings to connect initially.
 - Default username / password : admin / admin123A!!
 - SSH login using azureuser / the key pair you created is also possible but not typically required.
 - During the initial login process you will need to accept the Gigamon EULA and create a new password for the “admin” user.

Creating a Monitoring Domain

Gigamon’s documentation is available [here](#). What follows is Vectra’s suggested process.

You must establish a connection between the Fabric Manager and your Azure environment before you can perform the configuration steps. Creating a Monitoring Domain allows you to establish a connection between your Azure environment and the Fabric Manager. After establishing a connection, you will be able to use the Fabric Manager to specify a launch configuration for the UCT-V Controllers, the optional V Series Proxy, and V Series Nodes in the specified VNet and Resource Groups. The Fabric Manager connects to Azure using either an Application ID with the client secret or the MSI (Managed Identity, preferred) method of authentication. After the connection establishment, the Fabric Manager launches the fabric components.

Fabric Manager connects to Azure through the public [Azure API endpoints](#). HTTPS is the default protocol which the Fabric Manager uses to communicate with the API.

To create a Monitoring Domain:

- ▼ Navigate in Fabric Manager to *Inventory > VIRTUAL > Azure > Monitoring Domains*.
- ▼ Click “New” and fill in the following:
 - **Monitoring Domain**
 - An alias used to identify the Monitoring Domain.
 - **Traffic Acquisition Method**
 - Select UCT-V for Vectra NDR for Cloud.
 - UCT-V agents are deployed on your VMs to acquire the traffic and forward the acquired traffic to the V Series nodes. When deploying the fabric later, a UCT-V Controller will be deployed in addition to V Series Node(s).

- **Traffic Acquisition Tunnel MTU**
 - The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V agent to a V Series node.
 - The default value is 1450 and it's typical to leave this at the default.
 - Work with your Vectra team to determine if another value should be used.
 - When using IPv4 tunnels, the maximum MTU value is 1450. The UCT-V tunnel MTU should be 50 bytes less than the UCT-V destination interface MTU size.
 - When using IPv6 tunnels, the maximum MTU value is 1430. The UCT-V tunnel MTU should be 70 bytes less than the UCT-V destination interface MTU size.
- **Use FM to launch Fabric**
 - This should always be enabled / set to “Yes”. Clicking No here means that the fabric components would not be launched by the Fabric Manager and would need to be deployed manually by the administrator. If desired, this is covered by Gigamon’s docs [here](#).
- ▼ For the “Connections” part of the Monitoring Domain configuration:
 - **Name**
 - An alias used to identify the connection.
 - **Credential**
 - Choose the Managed Service Identity which references the User Assigned Managed Identity that you configured in [Azure Security Credentials](#) in the [Prerequisites](#).
 - **Subscription ID**
 - A unique alphanumeric string that identifies your Azure subscription. What you can see here will be limited by the permissions/scope of the User Assigned Managed Identity.
 - **Region**
 - Azure region for the monitoring domain. For example, West India.
 - **Resource Groups**
 - Select the Resource Groups that contain the VMs that you want to monitor with UCT-V agents..
- ▼ An example is of what you should have filled out is below:

- ▼ Click “Save” to save your Monitoring Domain configuration.
- ▼ You will immediately be placed on the “Azure Fabric Launch Configuration” wizard where you can start deployment of the fabric for the Monitoring Domain that you just created.

Additional detail about managing existing Monitoring Domains is available at [Managing Monitoring Domain](#) on the Gigamon documentation site.

Deploying the Fabric

If you left the Azure Fabric Launch Configuration page after creating the Monitoring Domain but before deploying the fabric, it's ok. Just navigate to *Inventory > VIRTUAL > Azure*, select your monitoring domain, and then from the Actions menu click "Deploy Fabric".



Fabric deployment is covered in Gigamon's documentation [here](#). What follows is Vectra's suggested process.

- ▼ The **Connections** selector will allow you to choose the connection to Azure that you want to use for the fabric deployment.
 - This will be populated by any connections that you have created. One would have been created as part of the [Monitoring Domain](#) configuration.
- ▼ **Centralized Virtual Network** - Choose the VNET that you wish to deploy the fabric components into.
- ▼ **Authentication Type** - Leave this at the default of sshPublicKey.
- ▼ **SSH Public Key** - Paste in the public key for the [Key Pair](#) you created earlier.
- ▼ **Resource Group** - Choose the [Resource Group](#) that you created earlier.
- ▼ **Security Groups** - Choose any [Security Groups](#) that you wish to be assigned to the fabric components.
- ▼ **Enable Custom Certificates** - Enable this option to validate the custom certificate during SSL Communication. The Fabric Manager validates the custom certificate with the trust store. If the certificate is not available in trust Store, communication does not happen, and a handshake error occurs.
 - Note: If the certificate expires after the successful deployment of the fabric components, then the fabric components move to a failed state.
 - Custom certificates can be added after deployment following instructions from [Installing a Custom Certificate](#).
- ▼ **Prefer IPv6** - Enables IPv6 to deploy all the fabric Controllers, and the tunnel between hypervisor to V Series node using IPv6 address. If the IPv6 address is unavailable, it uses an IPv4 address.
 - Note: This option can be enabled only when deploying a new V Series Node. If you wish to enable this option after deploying the V Series Node, then you must delete the existing V Series Node and deploy it again with this option enabled.
 - It is recommended that if you want to deploy with IPv6 to consult with your Vectra account team.
- ▼ **Configure a V Series Proxy** –
 - V Series Nodes in Azure can be deployed in two ways – with or without the use of a V Series Proxy.
 - When deployed with Proxy, the Fabric Manager communicates with the V Series Node via the Proxy node. This is typically useful when the Fabric Manager is deployed in a VNet that is different than where V Series Nodes are deployed, which makes direct communication with the V Series Nodes unfeasible.
 - If a V Series Proxy is necessary for your environment, please contact your Vectra account team for implementation guidance.
 - The vast majority of implementations do NOT need a V Series Proxy.
- ▼ **UCT-V Controller**
 - **Controller Version(s)** - If multiple UCT-V Controllers will be deployed, you can click the "Add" button to add additional Controller Versions.
 - **Image** - Choose at least the 6.6 version.
 - **Size** - Leave at the default of Standard_B1ms.
 - **Number of Instances** can remain at 1 in most deployments.
 - Please discuss with your Vectra team if you wish to deploy more than 1 UCT-V Controller.
 - Each UCT-V Controller can support 1000 monitored agents.

- **Management Subnet**
 - **IP Address Type** - This should typically be left at Private.
 - **Subnet** - Choose the subnet you wish to deploy into.
- **Agent CA** - Should be left blank.
- **IP Address Type** should typically be Private.
- **Additional Subnets** – This is typically not required.
 - If there are UCT-V agents on networks that are not IP routable from the management network, additional networks or subnets must be specified so that the UCT-V Controller can communicate with all the UCT-Vs.
 - Please work with your Vectra account team to discuss adding additional subnets.
- **Tags** – Add any Tags you wish to be associated with your UCT-V Controller EC2 instance.
- ▼ **V Series Node**
 - **SSL Key** – This can be left blank.
 - **Image** - Select the same version you are using for the UCT-V Controller. At least version 6.6
 - **Size** – Leave at the default of Standard_D4s_v4. Consult with your Vectra account team if different instance types are desired.
 - **Disk Size** – This can be left at the default of 30 GB.
 - **IP Address Type** should typically be Private.
 - **Management Subnet** - Choose the subnet you wish to deploy into.
 - **Data Subnets** - These are the networks that the V Series node uses to tunnel the captured traffic to your Vectra vSensor(s). Multiple networks are supported.
 - If you need more than 1 subnet to reach all your vSensors, the “Add Subnet” button can be used.
 - **Tool Subnet** - this is the default subnet that the V Series Nodes use to egress traffic to your Vectra vSensor(s). This subnet must have proper connectivity to your vSensors.
 - **Subnet x** – Choose the subnet that you wish to use for traffic mirroring to your vSensors.
 - **Security Groups** – Choose the security groups to apply to the interface used for traffic mirroring.
 - **Tags** - Add any Tags you wish to be associated with your UCT-V Controller EC2 instance.
 - It is recommended to consult with your Vectra account team to determine the best strategy for traffic distribution to your vSensor(s) which can impact the entries in Data Subnets.
 - **Min and Max Number of Instances** – FM will scale up and down the number of V Series Nodes that are part of the fabric as necessary to handle the load they are processing.
 - Having more than 1 node can help with High Availability but will impact Azure costs. It is recommended to discuss optimization of these numbers with your Vectra account team.
- ▼ When you are done filling in the required data, click “Save” at the top right of your screen.
 - The Fabric Manager is now making API calls to Azure to deploy the fabric components.
 - If there are errors, these can be checked in the VMM Log.
 - Navigate from the Settings cog at the bottom left of your Fabric Manager UI to *System > Logs > View Logs > VMM Log*.
 - Search near the bottom for error, not info messages.
 - If there is a failure, the Azure resources will self-terminate, and you can try deployment again.
- ▼ After successful fabric deployment, you can see the deployed components under *Inventory > VIRTUAL > Azure > Fabric*.

Deploying UCT-V Agents

Gigamon’s public documentation for UCT-V agent installation is located [here](#). Please see [Supported Operating Systems for UCT-V Agents](#) earlier in this document to see if the OS you wish to monitor is supported. In this document we’ll briefly cover Linux and Windows agent installation. Please see Gigamon’s documentation for installation instructions for other supported OS’s.

Special notes for v6.10 and higher

Gigavue Cloud Suite v6.10 introduced new encryption methods for communications between fabric components and the UCTV agents. If firewall rules are in place on client machines, they may need to be updated to allow fabric components to perform ACME challenges and communicate with each other and the UCT-V agents. Please see [Network Security Group \(Firewall Rules\)](#) in this document for full details on required FW rules for the entire NDR for Cloud deployment.

Local firewall rules (on your client machines) may need to be modified for Windows or Linux OS's. Some customers do not run local firewalls and may not need to. At a UCT-V agent level, any local firewall must allow the following:

UCT-V Agent(s)				
Inbound	TCP	8301	UCT-V Controller IP	Allows UCT-V agent to receive ACME challenge request from UCT-V Controller.
Inbound	TCP	9901	UCT-V Controller IP	Only required for backwards compatibility when FM is 6.10 and fabric is n-1 or n-2 version.
Inbound	TCP	9902	UCT-V Controller IP	Allows UCT-V agents to communicate with UCT-V Controller.
Outbound	UDP (VXLAN)	4789	V Series Node(s)	Allows UCT-V agents to send VXLAN tunnel traffic to V Series Nodes.
Outbound	TCP	8300	UCT-V Controller IP	Allows ACME validation flow from UCT-V agents to UCT-V Controller.
Outbound	TCP	8891	UCT-V Controller IP	Only required for backwards compatibility when FM is 6.10 and fabric is n-1 or n-2 version.
Outbound	TCP	8892	UCT-V Controller IP	Allows UCT-V agent to communicate with UCT-V Controller for registration and heartbeat.
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V agent to send traffic health updates to UCT-V Controller.
Outbound	TCP	11443	V Series Node(s)	Allows UCT-V agent to securely transfer the traffic to GigaVUE V Series Nodes.

Please note: that Gigamon does provide a **uctv-wizard** app as part of the UCT-V client installation that can be used to help set firewall rules and check for pre-requisites. The 6.10 version of the UCT-V wizard for both Windows and Linux have firewall rule errors that should be corrected in future versions of the wizard. Until those errors are corrected, if local firewall policies are in place, please ensure that firewall rules are modified outside of the Gigamon installation wizards or **uctv-wizard**.

Additional note: For 6.10 and higher versions of Gigamon software, a token must be created in the Fabric Manager and stored on the client machine to help allow the client to communicate with the UCT-V controller. Please see [Configure Tokens](#) on the Gigamon documentation site for full details. There are no special requirements for the user and role other than it requires the "Write" permission for "Third Party Orchestration". If you do not want to use an existing user group that may have privileges that are not needed, a new group can be created with these steps:

1. Create a new user and do not select any user group.
2. Create a custom role with at least "Write" permission for "Third Party Orchestration".
3. Create a custom user group and assign the custom role you just created and add the user you created.
4. Login to the FM with this new user and generate the token.

Creating token and adding it to your client machines

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with the Fabric Manager. The token is required only for initial registration before generating the certificate. It is used once and does not need to be maintained.

Creating Token:

- ▼ In the Fabric Manager UI, navigate to Settings > Authentication > GigaVUE-FM User Management > Tokens > Current User Tokens.
- ▼ Give your token a name, expiry, and assign the user group for the token. See "Additional note" above for requirements.
 - Since the token is only used for initial setup of encrypted communications for the UCT-V client, the expiry of the token can be limited to the time period in which you will be installing UCT-V clients.
- ▼ Click "Ok".

- ▼ Click the “...” on the right side of the token you just created and click “Copy Token”.

Adding Token to Client Machine(s):

- ▼ For Linux client installations, create a file named “**gigamon-cloud.conf**” in the `/etc` directory prior to installation of the UCT-V agent software.
- ▼ For Windows clients, create a file name “**gigamon-cloud.conf**” in the `C:\ProgramData\uctv\` directory after installing the UCT-V client software package.
- ▼ The format of the token in the text file you create should be as follows:

```
Registration:
token: <Enter the token created in GigaVUE-FM>
```

Linux installation using .deb or .rpm package

- ▼ Gigamon’s Linux installation instructions are available [here](#).
- ▼ Using the .deb or .rpm package that you received from Vectra, copy the installation package to your instance.
- ▼ Install the package with root privileges (example package name, always use the latest version available).

```
$ sudo dpkg -i gigamon-gigavue_uctv_6.10.00_amd64.deb

Or

$ sudo rpm -i gigamon-gigavue_uctv_6.10.00_x86_64.rpm
```

- ▼ After installing the UCT-V package, you can perform automated or manual configuration of UCT-V
- ▼ For automated configuration:
 - Run “`sudo uctv-wizard <argument>`” to perform pre-check, installation, and configuration functionalities.
 - Supported values for argument are explained in the following table:

Options	Use Command	Description
pre-check	<code>sudo uctv-wizard pre-check</code>	Checks the status of the required packages and firewall requirements. If there are any missing packages, it will display an appropriate message with the missing package details. If all the packages are installed, it will display a success message indicating that UCT-V is ready for configuration.
pkg-install	<code>sudo uctv-wizard pkg-install</code>	Displays the missing package and version details. To proceed with the installation, you can choose between the following: If you wish to skip the prompts and proceed with the system update, enter your option as “y”. The console interface will install the missing packages and restart the UCT-V service. Enter “n” if you wish to install missing packages manually.
configure	<code>sudo uctv-wizard configure</code>	First, it checks for any existing <code>uctv.conf</code> in the <code>etc/uctv</code> directory. If available, UCT-V will use that configuration. If unavailable, UCT-V will automatically add the interface configuration in <code>uctv.conf</code> file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination).

		You can add the required policy for the available port if a firewall is installed by answering “Y” when the wizard asks you if you want it to build FW rules. Enter “N” if you wish to configure manually.
uninstall	<code>sudo uctv-wizard uninstall</code>	Automatically stops service, removes the firewall rules, and uninstalls.

▼ For manual configuration:

- Please see the [Gigamon instructions on their documentation site](#).
- Some additional notes for manual configuration:
 - After installing the UCT-V package, modify the file `/etc/uctv/uctv.conf` to configure and register the source and destination interfaces.
 - **!! Note:** If you make any changes to the `uctv.conf` config file after the initial setup, you need to restart the agent and refresh or synchronize the inventory from the Fabric Manager to reflect the changes and start traffic mirroring again. However, if you have an ongoing monitoring session that is active and functioning well, modifying the UCT-V config file can cause traffic to be lost until the Fabric Manager performs an automatic synchronization (every 15 minutes).
 - You will need to use the interface name from `ifconfig` output. If you do not have `ifconfig` installed, you can install it using the following command:

```
$ sudo apt install net-tools
```

- Examples are included in the `/etc/uctv/uctv.conf` file.
- You may need to `sudo` the editor launch as well to modify the file.

```
$ sudo vi /etc/uctv/uctv.conf
```

- Save the file after modifying it.

▼ After either automated or manual configuration, reboot the instance or restart the service.

```
$ sudo service uctv restart
```

▼ If the UCT-V agent is successfully installed, then the status will be displayed as running.

- To check the status, run the following command:

```
$ sudo service uctv status
UCT-V is running
```

Windows installation

- ▼ Gigamon’s Windows installation instructions are available [here](#).
- ▼ Using the .msi package that you received from Vectra, copy the installation package to your instance.
- ▼ Install the downloaded MSI package as an Administrator and the UCT-V service starts automatically.
 - You will need to accept the agent EULA during the installation process.
- ▼ For automated configuration:
 - From your command prompt, run “`uctv-wizard <argument>`” to perform pre-check, installation, and configuration functionalities.
 - Supported values for argument are explained in the following table:

Options	Use Command	Description
pre-check	<code>uctv-wizard pre-check</code>	Checks the network adapter properties and firewall requirements. It notifies the user if the network adapter’s send buffer size is smaller than the required size for the agent and if any firewall rules need to be added.

		<p>Note: It is recommended to Increase the send buffer size of network adapters to 128 MB during the UCT-V installation to optimize performance and minimize traffic disruption.</p>
adapter-setup	<code>uctv-wizard adapter-setup</code>	<p>Checks the compatible network adapters, increases the send buffer size and restarts the service. Before changing the buffer size, the existing configuration is saved as a backup.</p> <p>You can choose between the following:</p> <ul style="list-style-type: none"> • If you wish to skip the prompts for changing the buffer size of compatible network adapters, enter the option as “Y”. • Enter “N” if you wish to set it up manually. Refer to the Install Windows UCT-Vs using Manual Configuration section for more details.
adapter-restore	<code>uctv-wizard adapter-restore</code>	<p>Using this command, you can restore the backup copy of the network adapter buffer size configuration saved in the in the uctv-wizard adapter-setup step.</p> <p>Note: You need to manually restart the network adapters for changes to take effect immediately.</p> <p>You can choose between the following:</p> <ul style="list-style-type: none"> • If you wish to skip the prompts for restoring the buffer size of the compatible network adapters, enter the option as “Y”. • Enter “N” if you wish to restore it manually.
configure	<code>uctv-wizard configure</code>	<p>The wizard will automatically add the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination).</p> <p>You can add the required policy for the available port if a firewall is installed.</p> <ul style="list-style-type: none"> • If you wish to skip the prompts to add the required firewall policy, enter your option as “Y”. The console interface will add the firewall rules automatically. • Enter “N” if you wish to configure manually.
uninstall	<code>uctv-wizard uninstall</code>	Automatically stops service, removes firewall rules, and uninstalls.

▼ For manual configuration:

- Please see the [Gigamon instructions on their documentation site](#).
- Some additional notes for manual configuration:
 - **!! Note:** If you make any changes to the uctv.conf config file after the initial setup, you need to restart the agent and refresh or synchronize the inventory from the Fabric Manager to reflect the changes and start traffic mirroring again. However, if you have an ongoing monitoring session that is active and functioning well, modifying the UCT-V config file can cause traffic to be lost until the Fabric Manager performs an automatic synchronization (every 15 minutes).

▼ After either automated on manual configuration, reboot the instance or restart the service.

- Here are two ways to restart the service:

- Run `"sc stop uctv"` and `"sc start uctv"` from the command prompt.
- Restart "UctV" from the Windows Task Manager.

!! Note: You may need to edit the Windows Firewall settings to grant access to the uctv process. To do this, access the Windows Firewall settings and find "uctvd" in the list of apps and features. Select it to grant access. Be sure to select both Private and Public check boxes. If "uctvd" does not appear in the list, click Add another app... Browse your program files for the uctv application (uctvd.exe) and then click Add. (Disclaimer: These are general guidelines for changing Windows Firewall settings. See Microsoft Windows help for official instructions on Windows functionality.)

Configure a Monitoring Session and Map

A monitoring session defines how traffic should be processed and sent to the Vectra vSensors. Multiple Monitoring Sessions can be created per Monitoring Domain if required. Please see [Create a Monitoring Session](#) on the Gigamon public documentation site for their documentation on this topic for more details. This guide will contain basic guidance and should be used together with advice from your Vectra team for the best way to configure the Monitoring Session(s) required for your PoV or production deployment.

The Fabric Manager automatically collects inventory data on all target instances available in the monitoring domains you have configured. You can design your monitoring session to include or exclude the instances that you want to monitor. You can also choose to monitor egress, ingress, or all traffic.

When a new target instance is added to your cloud environment, the Fabric Manager automatically detects and adds the instance to your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions.

To create a new monitoring session:

- ▼ Navigate to *Traffic > VIRTUAL > Orchestrated Flows > Azure*.
- ▼ Click the **New** and then **Monitoring Session** to begin creating a new Monitoring Session.
- ▼ Fill in the following information:
 - **Alias** - The name this Monitoring Session.
 - **Monitoring Domain** - The name of the [Monitoring Domain](#) that you want to select.
 - **Connections** - The connection(s) that are to be included as part of the monitoring domain. You can select the required connections that need to be part of the Monitoring Domain.
 - **Traffic Distribute** - Enabling the "Traffic Distribute" option identifies duplicate packets across different V Series Nodes when traffic from various targets is routed to these instances for monitoring. This setting can be ignored for Vectra NDR for Cloud deployments.
- ▼ Monitoring Sessions can also be edited after creation.

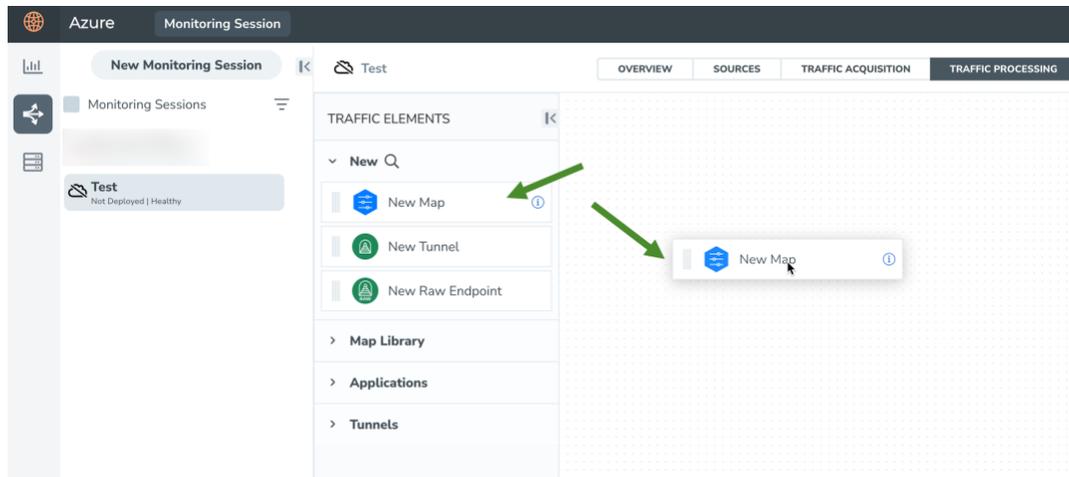
After creating a monitoring session, a map must be added to the monitoring session to tell the Fabric Manger how to direct mirrored traffic flowing through the V Series Node(s) to the Vectra vSensor(s). A map is a collection of one or more rules. The traffic passing through a map can match one or more rules defined in the map.

Creating a map can be very straight forward but they can also become very complex depending on the logic that you want to apply. We will show a simple map configuration that simply forwards all IPv4 to a single Vectra vSensor. Please work with your Vectra pre-sales or professional services team for advice on more complicated map configurations.

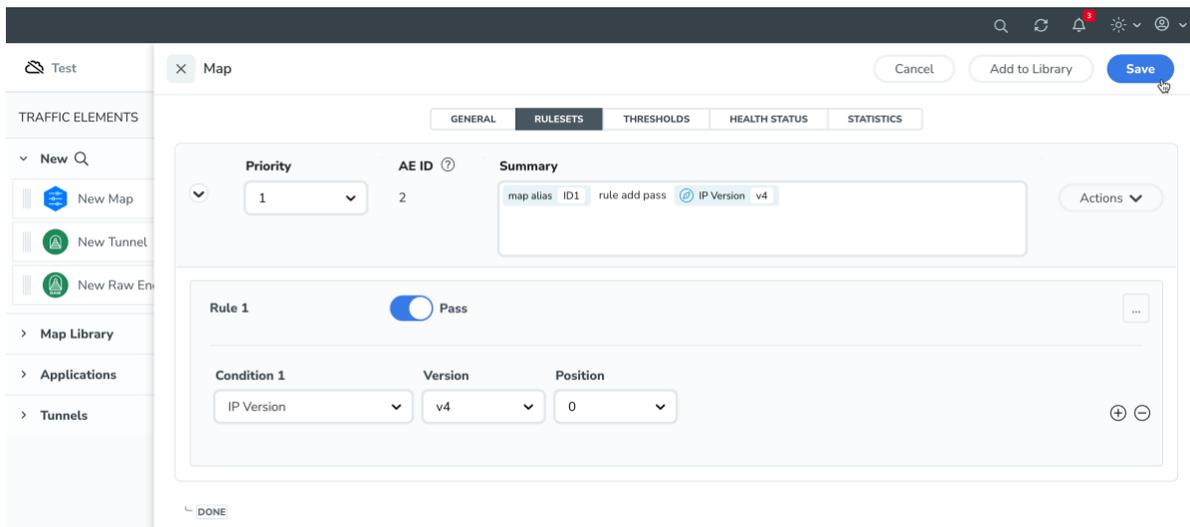
- ▼ See [Create a New Map](#) on the Gigamon documentation site for Gigamon's public documentation on map creation.

After creating the Monitoring Session, you will immediately be in the OVERVIEW tab of your monitoring session. where you can begin building the map.

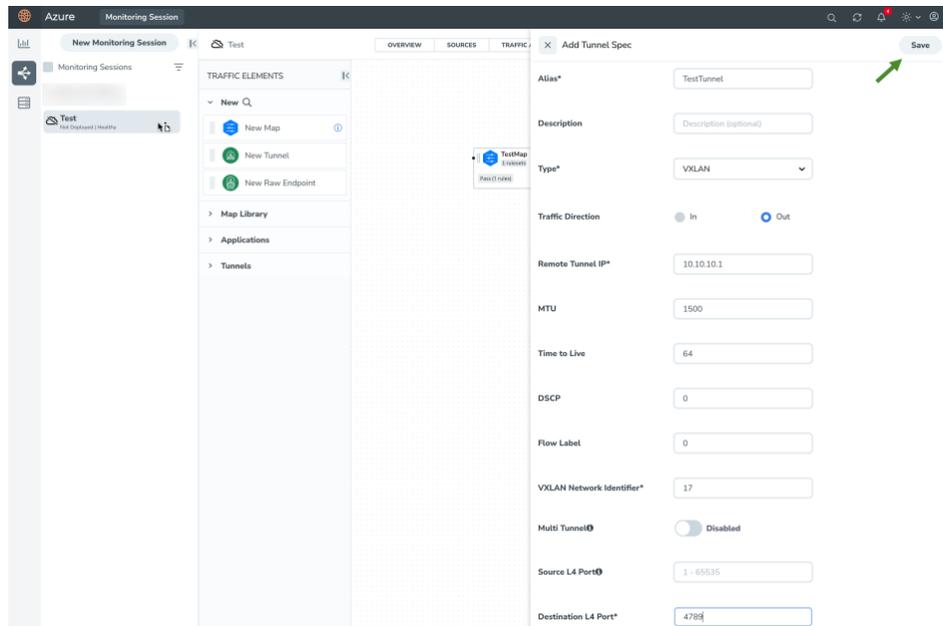
- ▼ Click and drag the **New Map** template to the workspace.



- ▼ Give it a **Name** and an optional description and then click the **RULESETS** tab.
 - Application Filtering is not licensed as part of Vectra NDR for Cloud and should not be selected.
- ▼ On the **RULESETS** tab, click **+ New Rule**, select **IP Version** for **Condition 1**, **v4** for **Version**, and **0** for **Position**, and then click **Save** at the top right.



- ▼ Drag the **New Tunnel** template to the workspace.
- ▼ Give it an **Alias** which will display in the workspace such as **Vectra_vSensor_1** or your desired Alias and you can also enter an optional **Description**.
- ▼ **Type** should be set to **VXLAN**.
 - Set the **VXLAN Network Identifier** to a positive integer that is unused in your network.
 - Set the **Destination L4 Port** to **4789**.
- ▼ **Traffic Direction** should be set to **Out**.
- ▼ **Remote Tunnel IP** should be set to the IP address associated with the capture interface of your Azure vSensor.
 - To find the IP assigned during deployment to your traffic NIC, go to your Azure resource group that was used during deployment, click on the traffic nic (it will be the interface that ends with "trafficnic"), and there you will see the private IP that was assigned to the traffic nic (capture interface of your newly deployed vSensor). Alternatively, if you can find your VM in the Azure portal, you can click into "Networking", and then select the traffic nic and see what IP is assigned to it.
 - Use this IP as the **Remote Tunnel IP**.
- ▼ MTU, Time to Live, DSCP, Flow Label, and Source L4 Port can be left at their defaults.



- ▼ Click **Save** at the top right.
- ▼ Click and drag the black dot on your map to the tunnel you created to connect the two objects.



- ▼ Click **Actions > Deploy** in the top right to deploy this update to the Monitoring Session.
 - Once the deployment is done successfully, your UCT-V agents will now be mirroring traffic through the V Series Node to the Vectra vSensor.
 - You can see details for any issues in the VMM log.
 - *Settings > System > Logs > View Logs > VMM Log*
- ▼ Another way to see status of a **Deploy** is to click **Sources** on your Monitoring Session and look in the **DEPLOYMENT STATUS** column, and click on **Target Deployment Failures** (if any).

Post Deployment Guidance

Installing a Custom Certificate

The Fabric Manager, V Series Nodes, the optional V Series Proxy, and UCT-V Controllers have default self-signed certificates installed. The communication between the Fabric Manger and the fabric components happens in a secure way using these default self-signed certificates, however you can also add your own certificates if desired.

Please see [Install Custom Certificate](#) on the Gigamon documentation site for details.

If it is required to add a CA to your deployment, please see [Adding Certificate Authority](#).

Worldwide Support Contact Information

- ▼ Support portal: <https://support.vectra.ai/>
- ▼ Email: support@vectra.ai (preferred contact method)
- ▼ Additional information: <https://www.vectra.ai/support>