Vectra NDR for Cloud

Gigamon Deployment Guide for AWS

Version: June 5, 2025

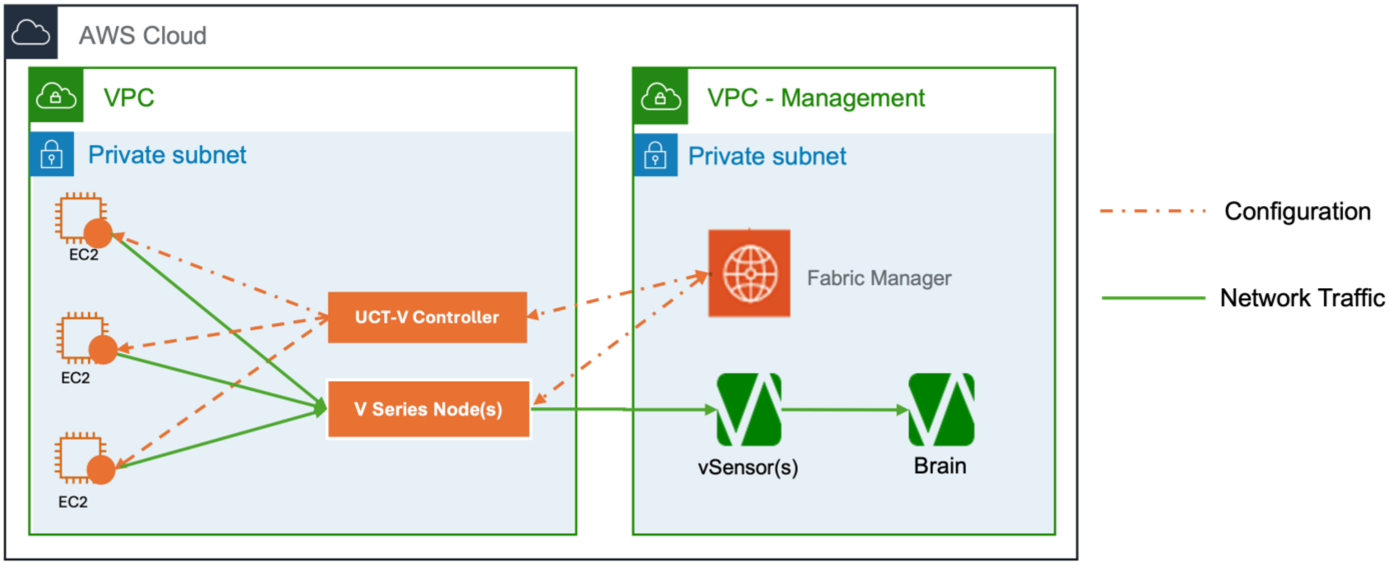
Table of Contents

Introduction

Vectra NDR for Cloud combines licensing for Vectra NDR with licensing for Gigamon's GigaVUE Cloud Suite. This guide provides guidance for deploying the Gigamon components of the solution in AWS. 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 AWS 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:

- EC2 instances 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 VPC/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 Amazon Virtual Private Clouds (VPC):
    - 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 NDR4C.
    - 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 (c5n.xlarge) can handle approximately 7 GB of traffic.

- **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.

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 VPC 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.

Additionally, when deploying in AWS, the Vectra AWS IaaS Best Practices Guide provides general guidance for Vectra deployments in AWS.

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:
    - Fabric Manager, UCT-V Agents, V Series Nodes and UCT-V Controller (Fabric).
- 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, 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 and Gigamon sales teams 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 AWS 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.

- AWS Sensor Deployment Guide
- Azure 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 (**Note:** Ensure the send buffer size of the network adapters is set to 128 MB for optimal performance and to minimize traffic disruption)
Rocky OS	Versions 8.4 through 8.8

Subscribe to GigaVUE Cloud Suite BYOL Version

- Login to your AWS account.
- Go to https://aws.amazon.com/marketplace/.
- In the Search field, type Gigamon and click Search.
- Select the latest GigaVUE Cloud Suite BYOL (Bring Your Own License) version link from the list for Gigamon products. Your license will be provided by your Vectra account team.
- Click Continue to Subscribe. Repeat these steps in each child account if you have parent /child accounts.

AWS Security Credentials

To establish the initial connection between the Fabric Manager and AWS, you will require the security credentials for AWS. These credentials are necessary to verify your identity and determine whether you have authorization to access the resources you are requesting. AWS employs these security credentials to authenticate and authorize your requests.

You need one of the following security credentials:

- **Identity and Access Management (IAM) role** - If GigaVUE-FM is running within AWS, it is recommended to use an IAM role. By using an IAM role, you can securely make API requests from the instances. Create an IAM role and ensure that the permissions and policies listed in Permissions and Privileges on the Gigamon documentation site are associated to the role and also ensure that you are using Customer Managed Policies or Inline Policies. Vectra NDR for Cloud uses UCT-V agents for traffic acquisition, other permissions listed in the article above may not be required. Please see gigamon_vectra_ndrc_aws.json for a sample IAM role.
- **Access Keys** - If GigaVUE-FM is configured in the enterprise data center on a VM, then you must use the access keys or basic credentials to connect to the VPC. Basic credentials allow full access to all the resources in your AWS account. An access key consists of an access key ID and a secret access key. For detailed instructions on creating access keys, refer to the AWS documentation on Managing Access Keys for Your AWS Account. For VM deployment of Fabric Manager, please contact your Vectra account team for guidance.
- Note: To obtain the IAM role or access keys, contact your AWS administrator.

VPC and Subnet

You must have an Amazon Virtual Private Cloud (VPC) to launch Gigamon components into your virtual network.

- Note: To create a VPC, refer to Create a VPC topic in the AWS documentation.

The VPC must have a subnet to configure the Gigamon components. You can either have the components deployed in a single subnet or in multiple subnets.

- **Management Subnet** that the Fabric Manager uses to communicate with the V Series nodes and UCT-V Controllers.
- **Data Subnet** that can accept incoming mirrored traffic from agents or be used to egress traffic to a tool.

If a single subnet is used, then the Management subnet is also used as a Data Subnet.

Key Pair

A key pair consists of a public key and a private key. When you define the specifications for the UCT-V Controllers, GigaVUE V Series nodes, and GigaVUE V Series Proxy in your VPC, you must create a key pair and specify the name of this key pair.

- To create a key pair, refer to Create a key pair using Amazon EC2 topic in the AWS Documentation.

Default Login Credentials

Component	Login Credentials
Fabric Manager	Login / Password: admin / instance-id in AWS EC2 after deployment of FM is complete
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

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 Prerequisites for AWS 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 AWS 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 VPC 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.

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 AWS 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.

Other Points to Note

Keep in mind the following notes and rules when deploying GigaVUE Cloud Suite:

- It is recommended to deploy the Fabric Manager in AWS to manage AWS workloads.
- If the Fabric Manger is deployed outside of the AWS, then the Fabric Manager encrypts and stores the access key and the secret key in its database.
- Always attach an IAM role to the instance running Fabric Manager in AWS to connect it to your AWS account.
- If you are launching the Fabric Manager instance from the AWS Marketplace, you need to have only the IAM roles.
- Fragmentation in the network should be avoided from UCT-V to V Series node and from V Series nodes to your Vectra Sensors by setting appropriate MTU for the interfaces. If the Vectra Sensor VM MTU is less than that of V Series node, then the V Series nodes will fragment the packets. This results in packet loss, that is, all fragments over 200 packet per second gets dropped by ENA (Elastic Network Adapter) of AWS.

Recommended Instance Types for AWS 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.

The UCT-V Agent is installed on other EC2 instances that you want to monitor within you AWS environment. This is the minimum recommended instance type that the agent can be installed on.

Component	Instance Type	vCPU	RAM
Fabric Manager	m5.xlarge	4	16 GB
V Series Node	c5n.xlarge (AMD)	4	10.5 GB
	C7gn.xlarge (ARM)	4	8 GB
UCT-V Controller	t2.medium	2	4 GB
UCT-V Agent	t2.micro	1	1 GB
V Series Proxy (Optional)	t2.medium (AMD)	2	4 GB
	t4g.micro (ARM)	2	1 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 AWS, 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.

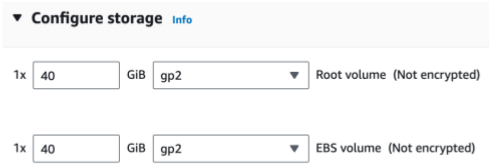
Below are the basic steps involved in a NDR for Cloud deployment:

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 AWS.
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 AWS 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 AWS

Per the Subscribe to GigaVUE Cloud Suite BYOL Version in the Prerequisites section, you should already be subscribed to GigaVUE Cloud Suite BYOL edition at least the 6.6 version level. If not, please refer to that section.

- Locate the subscription in *AWS Marketplace > Manage subscriptions* and click “Launch new instance”.
- On the “Configure this software page”:
    - Delivery method should be 64-bit (x86) Amazon Machine Image.
    - Software version should be 6.6 or later. This should always show the latest available version.
    - Choose the Region you wish to deploy in.
    - Click “Continue to launch through EC2”.
- In the “Launch an instance” page configure the following:
    - **Name and tags**
        - Configure any name and tags you want for the instance.
    - **Application and OS Images (Amazon Machine Image)**
        - Nothing required.
    - **Instance type**
        - This should be left at the default of m5.xlarge.
    - **Key pair (login)**
        - Use the key pair that you configured previously or use the link to “Create new key pair”.
        - Instructions were earlier in this doc at: Key Pair.
    - **Network settings**
        - Edit these settings as required to ensure the right VPC, subnet, and security groups are picked based on what you determined in Information Gathering / Scoping (Pre-Deployment), VPC and Subnet, and Security Group (Firewall Rules) 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 VPC should typically be the one that has the most visibility into other VPCs, is peered, connected via transit gateway, has network communication, is central and used for management.
    - **Configure storage**
        - There should be 2 40 GiB gp2 volumes by default (one Root, one EBS). If not, make sure the configuration matches the below (encryption can be enabled if required):



▼ Configure storage Info

1x 40 GiB gp2 ▼ Root volume (Not encrypted)

1x 40 GiB gp2 ▼ EBS volume (Not encrypted)

-
    - **Advanced details**
        - The IAM instance profile that you created earlier should be selected.
            - This can be added later if you miss adding it now (go to the ec2 instance and edit it).
        - All other advanced details can be left unchanged.
- Click “Launch Instance”.
    - Once you see the green “Success” message you can click on the Instance ID to go to the instance detail page where you can follow the initialization process.
    - 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 / instance-id
        - SSH login using admin / 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.

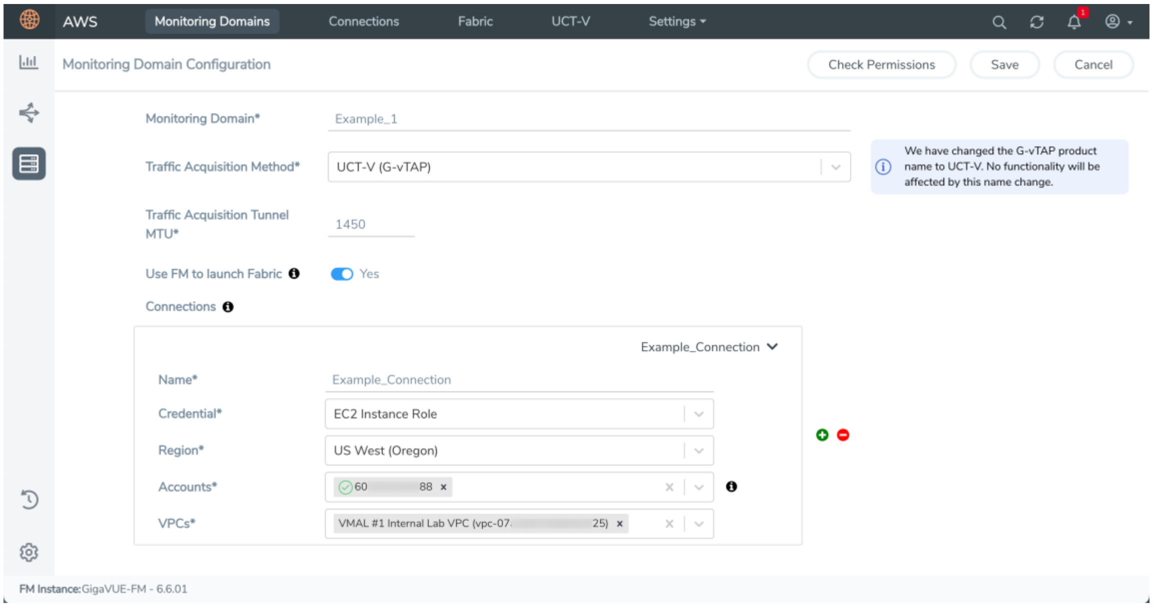
Fabric Manager connects to the AWS Platform through the public AWS API endpoint. HTTPS is the default protocol which GigaVUE-FM uses to communicate with the API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

Fabric Manager provides you the flexibility to monitor multiple VPCs. You can choose the VPC ID and launch the GigaVUE Cloud Suite for AWS components in the desired VPCs.

Note: To configure the monitoring domain and launch the fabric components in AWS, you must be a user with fm_super_admin role or a user with write access to the Physical Device Infrastructure Management category.

To create a Monitoring Domain:

- Navigate in Fabric Manager to *Inventory* > *VIRTUAL* > *AWS* > *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 8951 but it's typical to set this to a lower value, especially in non-green field deployments.
      - Vectra recommends setting this to 1450 for most deployments. Work with your Vectra team to determine if another value should be used.
    - When using IPv4 tunnels, the maximum MTU value is 8951. The UCT-V tunnel MTU should be 50 bytes less than the agent's destination interface MTU size.
    - When using IPv6 tunnels, the maximum MTU value is 8931. The UCT-V tunnel MTU should be 70 bytes less than the agent's destination interface MTU size.
  - **Use FM to launch Fabric**
    - This should always be enabled 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.
- For the "Connections" part of the Monitoring Domain configuration:
  - **Name**
    - An alias used to identify the connection.
  - **Credential**
    - Choose the IAM role that you configured in AWS Security Credentials in the Prerequisites.
  - **Region**
    - AWS Region for the Monitoring Domain.
  - **Accounts**
    - Select the desired AWS account(s).
  - **VPCs**
    - Select the VPC(s) that you want to monitor.
- An example is of what you should have filled out is below:



Monitoring Domain Configuration

Monitoring Domain* Example_1

Traffic Acquisition Method* UCT-V (G-vTAP)

We have changed the G-vTAP product name to UCT-V. No functionality will be affected by this name change.

Traffic Acquisition Tunnel MTU* 1450

Use FM to launch Fabric: Yes

Connections

Example_Connection

Name* Example_Connection

Credential* EC2 Instance Role

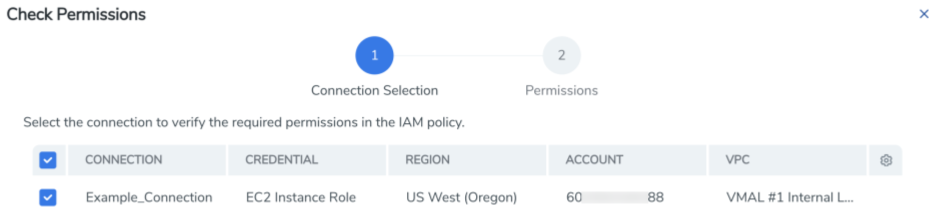
Region* US West (Oregon)

Accounts* 60[redacted]88

VPCs* VMAL #1 Internal Lab VPC (vpc-07[redacted]25)

FM Instance:GigaVUE-FM - 6.6.01

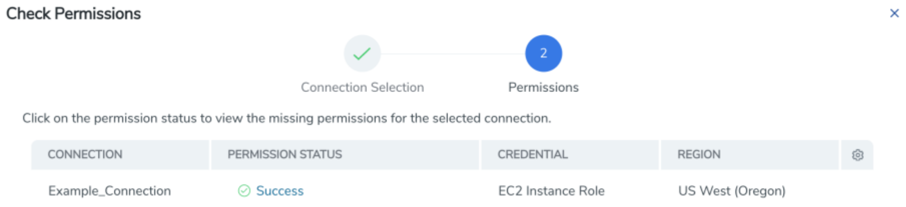
- Click “Check Permissions” and validate whether you have the required permissions.
  - Be careful to not hit “back” in your browser or you will need to start over.
  - A dialog box will come up where you can select you connection and then click “Next”.



Select the connection to verify the required permissions in the IAM policy.

☑	CONNECTION	CREDENTIAL	REGION	ACCOUNT	VPC
☑	Example_Connection	EC2 Instance Role	US West (Oregon)	60[redacted]88	VMAL #1 Internal L...

  - “Success” in the Permission Status column means all is good.



Click on the permission status to view the missing permissions for the selected connection.

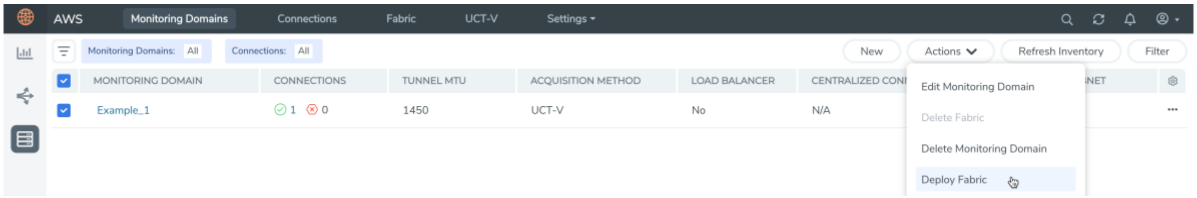
CONNECTION	PERMISSION STATUS	CREDENTIAL	REGION
Example_Connection	✓ Success	EC2 Instance Role	US West (Oregon)

- Click “Close” and then “Save” to save your Monitoring Domain configuration.
- You will immediately be placed on the “AWS Fabric Launch Configuration Page” 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 AWS Fabric Launch Configuration page after creating the Monitoring Domain but before deploying the Fabric, it's ok. Just navigate to *Inventory* > *VIRTUAL* > *AWS*, select your monitoring domain, and then from the Actions menu click "Deploy Fabric".



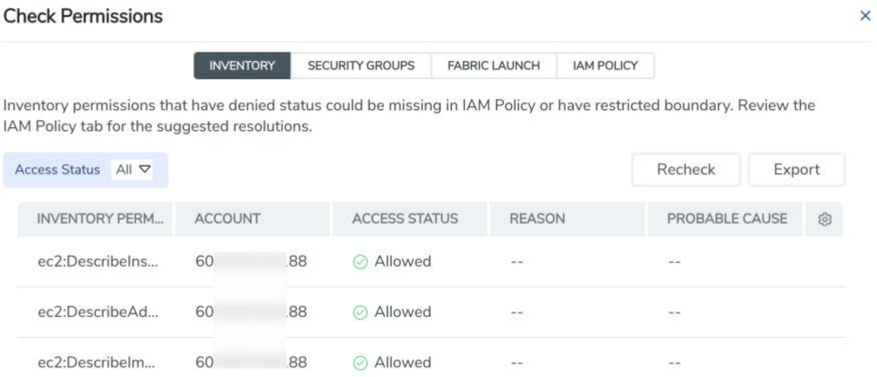
MONITORING DOMAIN	CONNECTIONS	TUNNEL MTU	ACQUISITION METHOD	LOAD BALANCER	CENTRALIZED CONI	NET
Example_1	✓ 1 ⊗ 0	1450	UCT-V	No	N/A	

Fabric deployment is covered in Gigamon's documentation here. What follows is Vectra's suggested process.

The Check Permissions button on the top right of the AWS Fabric Launch Configuration page is a useful tool but to enable it to work fully, you must fill in some of the information in the tables on this page before it will function.

- The **Centralized VPC** must be selected before Check Permissions will open at all.
  - This will be the VPC where the fabric (V Series Node(s) and UCT-V Controller) is deployed.
- Leave **EBS Volume Type** at the default of gp2 (General Purpose SSD).
- **Enable Encryption** is optional and if enabled will enable volume encryption. It is typical to leave this unencrypted unless there is a specific requirement to enable it as part of your policy.
- Select the desired **SSH Key Pair** in the top section of the page. This will be used for the UCT-V Controller.
- Select the desired **Management Subnet.** This will be the subnet used for the management interface of the UCT-V Controller.
- Select the **Version** under Controller Versions for the UCT-V Controller.
  - Always select at least version 6.6 for Vectra NDR for Cloud. Match the Fabric Manager version.
- Select the **Version** under V Series Node
  - Select the same version number you chose for the UCT-V Controller.

At this point, all functionality in the "Check Permissions" area will be available.



Inventory permissions that have denied status could be missing in IAM Policy or have restricted boundary. Review the IAM Policy tab for the suggested resolutions.

INVENTORY PERM...	ACCOUNT	ACCESS STATUS	REASON	PROBABLE CAUSE
ec2:DescribeIns...	60[redacted]88	✓ Allowed	--	--
ec2:DescribeAd...	60[redacted]88	✓ Allowed	--	--
ec2:DescribeIm...	60[redacted]88	✓ Allowed	--	--

- Check permissions is a capability that can be used in several areas of Fabric Manager. For additional details, please see Check for Required IAM Permissions on the Gigamon documentation site.
  - The INVENTORY tab checks if Fabric Manager can use the AWS API to describe what it needs to.
  - The SECURITY GROUPS tab checks if required security group rules are in place and can point out issues that need to be corrected.
  - The FABRIC LAUNCH tab will check if Fabric Manager can launch instances properly. Executing this check will take a few minutes.
  - The IAM POLICY tab provides a sample policy that contains the required permissions for deploying the GigaVUE Cloud Suite.
- After checking permissions (this is an optional step, but it is recommended to complete checking permissions if you have never deployed fabric previously), you can move on to fill out the rest of the information in the AWS Fabric Launch Configuration screen.

- **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 moves 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 AWS 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 VPC 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**
    - You should have already selected at least **Version** 6.6 (Match Fabric Manager). If not, do so now.
        - You should use the same UCT-V Agent versions when deploying agents.
    - The **Instance Type** can remain at the default of t2.micro.
    - **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.
    - **Agent Tunnel Type** should be VXLAN for Vectra NDR for Cloud. This selection is for the tunnel used for sending traffic from the UCT-V agents to the V Series Node(s).
    - **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.
    - You should have already selected at least **Version** 6.6. If not, do so now. Select the same version you are using for the UCT-V Controller. Typically, just match the version you used for the Fabric Manager.
    - **Instance Type** – Leave at the default of c5n.xlarge. Consult with your Vectra account team if different instance types are desired. A c5n.xlarge instance can support around 7 Gbps of traffic.
    - **Volume Size** – This can be left at the default of 8 GB.
    - **IP Address Type** should typically be Private.
    - **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 AWS costs. It is recommended to discuss optimization of these numbers with your Vectra account team.

- ○ **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.

- 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 AWS 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 AWS resources will self-terminate, and you can try deployment again.
- After successful Fabric deployment, you can see the deployed components under *Inventory > VIRTUAL > AWS > 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 .deb 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 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	**sudo uctv-wizard pre-check**	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	**sudo uctv-wizard pkg-install**	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	**sudo uctv-wizard configure**	First, it checks for any existing uctv.conf in the etc/uctv directory. If available, UCT-V will use that configuration. If unavailable, UCT-V 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). 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	**sudo uctv-wizard uninstall**	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 on 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 you 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	**`uctv-wizard pre-check`**	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. **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.
adapter-setup	**`uctv-wizard adapter-setup`**	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. You can choose between the following: • 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	**`uctv-wizard adapter-restore`**	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. Note: You need to manually restart the network adapters for changes to take effect immediately. You can choose between the following: • 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	`uctv-wizard configure`	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). You can add the required policy for the available port if a firewall is installed. • 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	`uctv-wizard uninstall`	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 Configure 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* > *AWS.*

- Click the **New Monitoring Session** button 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.

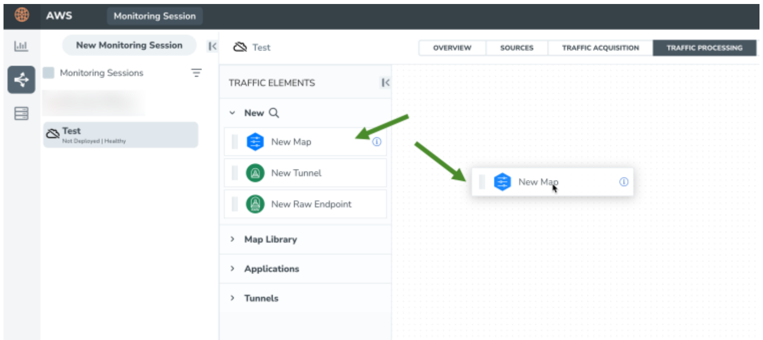
After creating a monitoring session, a map must be added to the monitoring session to tell the Fabric Manger how to direct mirrored traffic flowing through the V Series Node(s) to the Vectra vSensor(s). A map is a collection of one or more rules. The traffic passing through a map can match one or more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

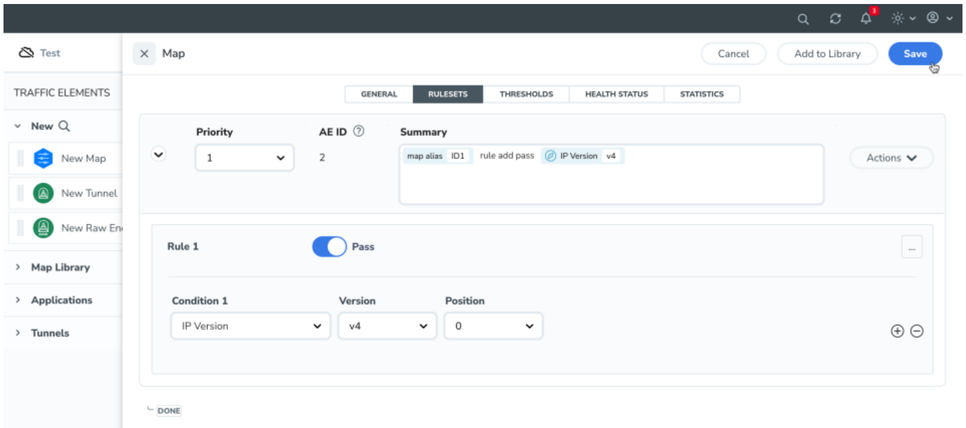
- See Create a New Map on the Gigamon documentation site for Gigamon's public documentation on map creation.

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.

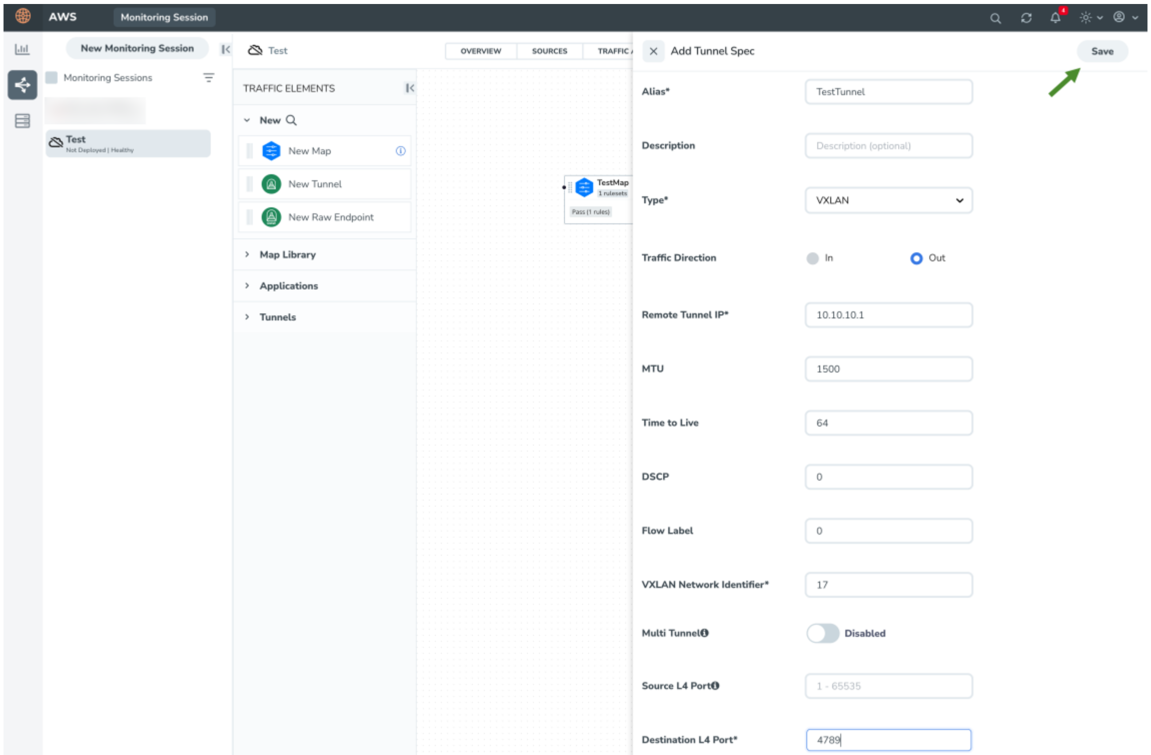


Priority: 1
AE ID: 2
Summary: map alias ID1 rule add pass IP Version v4

Rule 1 Pass

Condition 1: IP Version
Version: v4
Position: 0

- 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 AWS vSensor.
  - To find this IP, it is helpful if you know the Management IP (MGT IP) of the vSensor. In your Vectra GUI, the MGT IP can be seen at *Data Sources, > Network > Sensors > Click on your Sensor name* and the MGT IP is listed as the **Sensor IP**.
  - In your AWS console, navigate to EC2 and find your vSensor instance. Look at the **Networking** tab of the instance details and the capture interface IP is the IP that isn't your MGT IP. 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.

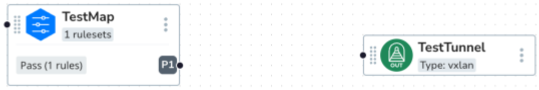


[redacted]

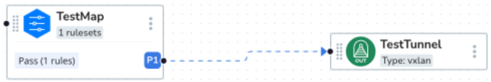
Add Tunnel Spec

Alias*	TestTunnel
Description	Description (optional)
Type*	VXLAN
Traffic Direction	○ In ● Out
Remote Tunnel IP*	10.10.10.1
MTU	1500
Time to Live	64
DSCP	0
Flow Label	0
VXLAN Network Identifier*	17
Multi Tunnel	Disabled
Source L4 Port	1 - 65535
Destination L4 Port*	4789

- 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.



< before --- after >



- 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