

FortiSIEM - AWS Installation and Migration Guide

Version 6.1.0



FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE https://video.fortinet.com

FORTINET BLOG https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com



10/04/2023 FortiSIEM 6.1.0 AWS Installation and Migration Guide

TABLE OF CONTENTS

Change Log	
Fresh Installation	5
Pre-Installation Checklist	5
All-in-one Installation	6
Launch an Instance Using FortiSIEM 6.1.0 AMI	
Configure FortiSIEM via GUI	
Upload the FortiSIEM License	
Choose an Event Database	
Cluster Installation	
Install Supervisor	
Install Workers	
Register Workers	
Install Collectors Register Collectors	
0	
Migrating from FortiSIEM 5.3.0, 5.3.1 or 5.3.2	
Pre-Migration Checklist	
Migrate All-in-one Installation	
Download the Backup Script	
Run the Backup Script and Shutdown System	
Detach 5.3.0, 5.3.1 or 5.3.2 Root Disk	
Attach the 6.1.0 Root Disk to the 5.3.0, 5.3.1 or 5.3.2 Instance Boot Up the 5.3.0, 5.3.1 or 5.3.2 Instance and Migrate to 6.1.0	
(Optional) Change Instance Type to the Latest Generation	
Migrate Cluster Installation	
Delete Workers	
Migrate Supervisor	
Install New Worker(s)	
Register Workers	
Set Up Collector-to-Worker Communication	
Working with Pre-6.1.0 Collectors	
Install 6.1.0 Collectors	
Register 6.1.0 Collectors	

Change Log

Date	Change Description
05/09/2019	Initial release of ForiSIEM - AWS Installation Guide
03/22/2019	Revision 2: updated instructions for Service Provider deployments.
11/11/2019	Revision 3: small change to installation instructions for FortiSIEM and FortiSIEM Report Server.
03/30/2020	Released document for 5.3.0.
08/15/2020	Revision 4: Updated deployment and installation for FortiSIEM 6.1 on AWS.
12/03/2020	Revision 6: Small addition to Pre-Installation Checklist.
12/07/2020	Revision 7: Small addition to Register Collectors.
02/04/2021	Revision 8: Updated Migration.
03/23/2021	Revision 9: Released for 6.2.0.
4/16/2021	Revision 10: Minor update to Run the Backup Script and Shutdown System section.
09/28/2021	Revision 11: Updated volume type information for 6.x guides.
11/19/2021	Revision 12: Updated Register Collectors section for 6.x guides.
08/18/2022	Revision 13: Updated All-in-one Installation section.
10/20/2022	Revision 14: Updated Register Collectors instructions for 6.x guides.

Fresh Installation

This section describes how to install FortiSIEM for the current release.

- Pre-Installation Checklist
- All-in-one Installation
- Cluster Installation

Pre-Installation Checklist

Before you begin, check the following:

- Ensure that your system can connect to the network. You will be asked to provide a DNS Server and a host that can be resolved by the DNS Server and can respond to a ping. The host can either be an internal host or a public domain host like google.com.
- Deployment type Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Whether FIPS should be enabled
- Install type:
 - All-in-one with Supervisor only, or
 - Cluster with Supervisor and Workers
- Storage type
 - Online Local or NFS or Elasticsearch
 - Archive NFS or HDFS
- Fortinet recommends that you do not choose AWS Spot instances for Supervisor and Worker nodes. Such instances can go down at any time with short notice, causing instability and performance issues.
- Before beginning FortiSIEM deployment, you must configure external storage
- Determine hardware requirements and choose AWS instance type accordingly:

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum without UEBA – 24GB with UEBA - 32GB Recommended without UEBA – 32GB with UEBA - 64GB 	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum without UEBA – 24GB with UEBA - 32GB Recommended without UEBA – 32GB with UEBA - 64GB 	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB

Node	vCPU	RAM	Local Disks
Workers	Minimum – 8 Recommended - 16	Minimum – 16GB Recommended – 24GB	OS – 25GB OPT – 100GB
Collector	Minimum – 4 Recommended – 8 (based on load)	Minimum – 4GB Recommended – 8GB	OS – 25GB OPT – 100GB

Note: compared to FortiSIEM 5.x, you need one more disk (OPT) which provides a cache for FortiSIEM.

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when configFSM.shruns.

Before proceeding to FortiSIEM deployment, you must configure the external storage.

- For NFS deployment, see FortiSIEM NFS Storage Guide here.
- For Elasticsearch deployment, see FortiSIEM Elasticsearch Storage Guide here.

All-in-one Installation

This is the simplest installation with a single Virtual Appliance. If storage is external, then you must configure external storage before proceeding with installation.

- Launch an instance using FortiSIEM 6.1.0 AMI
- Configure FortiSIEM via GUI
- Upload the FortiSIEM License
- Choose an Event Database

Launch an Instance Using FortiSIEM 6.1.0 AMI

- 1. Navigate to the EC2 AMIs page and find FortiSIEM 6.1.0 AMI (or in AWS Marketplace after the GA release).
- **2.** Launch FortiSIEM-6.1.0.0112.

-	Launch EC2 Image Builder Actions *		
	Owned by me 👻 🔍 search : 1255 💿 Add filter		
	Name	AMI Name	~ AMI ID ~ :
	FortiSIEM-VA-6.1.0.1255	FortiSIEM-VA-6.1.0.1255	ami-036b92a1377106e04

3. Go to Step 3: Configure Instance Details in AWS Services. Configure instance details such as VPC, Subnet, IP, etc. Click Next.

Number of instance Launch into Aufo Scaling Group () Purchasing option Pu	p 3: Configure Instar gure the instance to suit your requi			, requ	est Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Network i vpc.5ddeb38 [Default us-asst VPC Submet i submet.68ddb18a [default-submet-11] us-asst-11 Create new submet Submet i submet.68ddb18a [default-submet-11] Create new submet Auto-assign Public IP i Use submet setting (Enable) Create new submet Auto-assign Public IP i Use submet setting (Enable) Create new submet Auto-assign Public IP i Use submet setting (Enable) Create new submet Placement group I Add to assting placement group. Create new Capacity Reservation Placement group name Open Create new Capacity Reservation IM role Mone Create new IAcreate new IAcreate Studdown behavior Specify CPU options Create new IAM role Studdown behavior Specify CPU options Create new IAM role Studdown behavior Specify CPU options Create new IAM role EBS-optimized instance Enable Hoernation as an additional stop behavior Enable CoudVatch detailed montoring Additional charges nety. Additional charges nety apply. EBS-optimized instance Enable CoudVatch detailed montoring Additional charges nety. EBS-optimized instance	Number of instances	(j)	1 Launch into Auto	Scalin	ng Group (j)
Subnet implementation Subnet implementation Subnet implementation 231 IP Addresses available Create new subnet Auto-assign Public IP implementation Auto-assign IPvid IP implementation Auto-assign IPvid IP implementation Placement group implementation implementation implementation Placement group implementation implementation implementation Add to a new placement group. implementation implementation implementation Add to a new placement group. implementation implementation implementation Add to a new placement group. implementation implementation implementation Add to a new placement group. implementation implementation </td <td>Purchasing option</td> <td>(i)</td> <td>Request Spot instances</td> <td></td> <td></td>	Purchasing option	(i)	Request Spot instances		
23 IP Addresses available Auto-assign Public IP Use subnet setting (Enable) Auto-assign IPv6 IP Use subnet setting (Enable) Placement group Add instance to placement group. Add to a new placement group. Add to a new placement group. Add to a new placement group. Add to a new placement group. Capacity Reservation Open C create new Capacity Reservation IAM role Open C create new IAM role Shutdown behavior Stop C spacity Reservation Stop - Hibernate behavior Stop C spacity CPU options Stop - Hibernate behavior Placendual taccidental termination Monitoring Protoct against accidental termination Monitoring Enable Notemation Beso-optimized instance Enable Add and EBS-optimized instance Koditonal charges amply when launching Dedicated instances. Additional charges amply when launching Dedicated instances.	Network	(i)	vpc-5d4eb938 Default us-east VPC	\$	C Create new VPC
Auto-assign IPv6 IP 0 Placement group 0 Add to assign Ipv6 IP 0 0 Add to assign Ipv6 IP 0 0 Add to assign Ipv6 IP 0 0 Add to a new placement group. 0 Add to a new placement group. 0 0 </td <td>Subnet</td> <td>(j)</td> <td></td> <td>\$</td> <td>Create new subnet</td>	Subnet	(j)		\$	Create new subnet
Placement group I Add instance to placement group Placement group name I Add to a sexisting placement group. Add to a new placement group. Scalability (cluster) Capacity Reservation Open IAM role Open IAM role None CPU options Specify CPU options Shutdown behavior Stop Ibernate behavior Stop Ibernate behavior Protect against accidental termination Monitoring Image: Specify CPU options Enable termination protection Image: Protect against accidental termination Monitoring Image: Enable Cloud/Watch detailed monitoring Additional charges apply. EBS-optimized instance Launch as EBS-optimized instance Tennacy Shared-hardware instance Tennacy Add in Elastic Inference accelerator	Auto-assign Public IP		Use subnet setting (Enable)	\$	
Placement group name Add to existing placement group. Add to a new placement group. scalability (cluster) Capacity Reservation Open C create new Capacity Reservation None C create new Capacity Reservation IAM role None C create new IAM role CPU options Specify CPU options Shutdown behavior Stop C protect against accidental termination C Protect against accidental termination C Protect against accidental termination C Enable CloudWatch detailed monitoring Additional charges apply. EBS-optimized instance Launch as EBS-optimized instance Shaddomal charges any apply when launching Dedicated instances. Elastic Inference Additional charges may apply when launching Dedicated instances. 	Auto-assign IPv6 IP	(i)	Use subnet setting (Enable)	\$	
Placement group name Add to a rew placement group. Add to a new placement group. Scalability (cluster) Capacity Reservation Open C reate new Capacity Reservation IAM role None C create new IAM role None Specify CPU options Shutdown behavior Specify CPU options Specify CPU options Shutdown behavior Stop Hibernate behavior Enable hibernation as an additional stop behavior Protect against accidental termination Protect against accidental termination Monitoring Enable CoudWatch detailed monitoring Additional charges apply. EBS-optimized instance Launch as EBS-optimized instance Launch as EBS-optimized instance Shared Andware instance Shared Andware instance Additional charges any apply when launching Dedicated instances. Elastic Inference Add an Elastic Inference accelerator 	Placement group	(i)	Add instance to placement group		
Add to a new placement group. capacity Reservation Open C Capacity Reservation IMmole None C CPU options Shutdown behavior Stop Shutdown behavior Stop C PU options C PU options Shutdown behavior Stop C PU options Stop Potect against accidental termination Monitoring C Protect against accidental termination Monitoring C Protect against accidental termination Additional charges apply. EBS-optimized instance EBS-optimized instance C Pana e hared hardware instance Additional charges may apply when launching Dedicated instances. Additional charges may apply when launching Dedicated instances. Additional charges may apply when launching D	Placement group name	(i)			
Capacity Reservation Open C create new Capacity Reservation IAM role None C Create new IAM role CPU options Specify CPU options Shutdown behavior Stop Stop - Hibernate behavior Enable hibernation as an additional stop behavior Enable termination protection Protect against accidental termination Monitoring Finable follow/Watch detailed monitoring Additional charges apply. EBS-optimized instance Launch as EBS-optimization smax apply when launching Dedicated instances. Shared - Run a shared hardware instance Additional charges may apply when launching Dedicated instances. Elastic Inference Additional charges may apply when launching Dedicated instances. 		0			
IAM role Image: Contract new Capabity Heservation IAM role Image: None Image: Contract new IAM role CPU options Image: Specify CPU options Shutdown behavior Image: Specify CPU options Stop - Hibernate behavior Image: Specify CPU options Stop - Hibernate behavior Image: Contract new IAM role Image: CPU options Image: Contract new IAM role Stop - Hibernate behavior Image: Contract new IAM role Image: CPU options Image: Contract new IAM role Image: CPU options Image: Contract new IAM role Stop - Hibernate behavior Image: Contract new IAM role Image: CPU options Image: C			scalability (cluster)	\$	
CPU options Specify CPU options Shutdown behavior Stop Enable hibernation as an additional stop behavior Enable hibernation protection Protect against accidental termination Monitoring Protect against accidental termination Additional charges apply. EBS-optimized instance Launch as EBS-optimized instance Stared - Run a shared hardware instance Additional charges may apply when launching Dedicated instances. Elastic Inference Add an Elastic Inference accelerator 	Capacity Reservation	(i)	Open	\$	C Create new Capacity Reservation
Shutdown behavior i Stop I Stop - Hibernate behavior i Enable hibernation as an additional stop behavior Enable termination protection i IP Protect against accidental termination Monitoring i IP Enable CloudWatch detailed monitoring Additional charges apply. EBS-optimized instance i I Launch as EBS-optimization instance Tenancy i Shared - Run a shared hardware instance Additional charges may apply when launching Dedicated instances. Additional charges and and previous accelerator	IAM role	(j)	None	\$	C Create new IAM role
Stop - Hibernate behavior □Enable hibernation as an additional stop behavior □Enable hibernation as an additional stop behavior Enable termination protection □Protect against accidental termination □Enable termination □Enable cloudWatch detailed monitoring Additional charges apply. EBS-optimized instance	CPU options	(i)	Specify CPU options		
Stop - Hibernate behavior □Enable hibernation as an additional stop behavior □Enable hibernation as an additional stop behavior Enable termination protection □Protect against accidental termination □Enable termination □Enable cloudWatch detailed monitoring Additional charges apply. EBS-optimized instance	Shutdown behavior	(i)	Stop	\$	
Monitoring Image: CouldWatch detailed monitoring Additional charges apply. EBS-optimized instance Image: CouldWatch detailed monitoring Additional charges apply. EBS-optimized instance Image: CouldWatch detailed monitoring Additional charges apply. EBS-optimized instance Image: CouldWatch detailed monitoring Additional charges may apply when launching Dedicated instances. Elastic Inference Image: CouldWatch detailed monitoring Additional charges may apply when launching Dedicated instances.	Stop - Hibernate behavior	(i)	Enable hibernation as an additional stop behavior		
Additional charges apply. EBS-optimized instance Image: I	Enable termination protection	(i)	Protect against accidental termination		
Tenancy () Shared - Run a shared hardware instance (*) Additional charges may apply when launching Dedicated instances. Elastic Inference (i) □ Add an Elastic Inference accelerator	Monitoring	(j)			
Additional charges may apply when launching Dedicated instances. Elastic Inference I Add an Elastic Inference accelerator	EBS-optimized instance	i	Launch as EBS-optimized instance		
	Tenancy	(j)			instances.
	Elastic Inference	(j)			

4. In Step 4: Add Storage, add additional disks in the Add Storage page. These will be used for the additional partitions in the virtual appliance. An All In One deployment requires the following additional partitions. Then click Next.

Volume Type	Ð	Device (i)	Snapshot (i)	Size (GiB) (i)	Volume Type (i)			Throughput (MB/s)	Delete on Termination (i)	Encryption (i)		
	~					_		0				
Root		/dev/sda1	snap-0b341032a6aa1b17a	25	General Purpose SSD (gp3)	*	3000	125		Not Encrypted	*	
BS	~	/dev/sdb ∨	Search (case-insensit	100	General Purpose SSD (gp3)	~	3000	125		Not Encrypted	•	•
EBS	~	[/dev/sdc ♥]	Search (case-insensit	60	General Purpose SSD (gp3)	~	3000	125	0	Not Encrypted	-	•
EBS	*	/dev/sdd 🖌	Search (case-insensit	60	General Purpose SSD (gp3)	~	3000	125	0	Not Encrypted	*	6
	pose (SSI		the ability to burst to 3000 IOPS p tent baseline of 3 IOPS/GiB. Set r		nt of volume size, to meet the perform eral Purpose (SSD).	ance n	eeds of]				

Note: If you plan to onboard greater than 500 devices, or 5000 eps, please consider increasing IOPS and Throughput for the disk used to mount / cmdb in FortiSIEM.

For instance, you can run the following command once FortiSIEM is initially deployed to determine which disk mounts the cmdb folder.

[admin@6 data-definition]\$ lsblk | grep cmdb └_sdc1 8:33 0 60G 0 part /cmdb

In this case /dev/sdc.

You can go into EBS volumes in AWS, and increase the IOPS to 5000, and Throughput to 400MB/s to be more in line with SSD performance.

Use these partition values:

Volume Name	Size	Disk Name
EBS Volume 2	100GB	/opt For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when configFSM.sh runs.
EBS Volume 3	60GB	/cmdb
EBS Volume 4	60GB	/svn
EBS Volume 5	60GB+	/data (see the following note)

Note on EBS Volume 5:

- Add a 5th EBS Volume if using local storage in an All In One deployment. Otherwise, a separate NFS share or Elasticsearch cluster must be used for event storage.
- 60GB is the minimum event DB disk size for small deployments, provision significantly more event storage for higher EPS deployments. See the FortiSIEM Sizing Guide for additional information.
- NFS or Elasticsearch event DB storage is mandatory for multi-node cluster deployments.
- Choose GP3 volume type for all volumes (GP3 is better than GP2 at a slightly lower cost). For the CMDB partition, you can choose to modify your volume type and IOPS based on your system workload if you see the consistently high IOPS requirement in your deployment.
- 5. In Step 5: Add Tags: click click to add a new Name Tag and provide a name for the instance. Click Next.

dWS Services v Resource Groups v	*	
1. Choose AMI 2. Choose Instance Type 3. Configure Instance	4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review	
Step 5: Add Tags A tag consists of a case-sensitive key-value pair. For example, you A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more abo	- ·	
Key (128 characters maximum)	Value (256 characters maximum)	Instances () Volumes ()
	This resource currently has no tags	
	Choose the Add tag button or click to add a Name tag. Make sure your IAM policy includes permissions to create tags.	
Add Tag (Up to 50 tags maximum)		
	Cancel Pre	vious Review and Launch Next: Configure Security Group

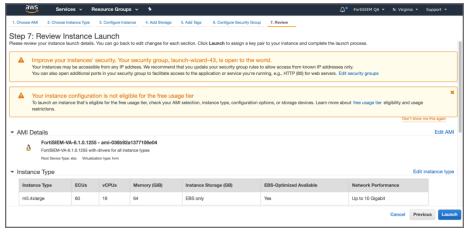
Add a new Name Tag.

aws Services - Resource Groups - 1		4 •	FortiSIEM QA 👻 N. V	/irginia 👻 Support 👻
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Store	age 5. Add Tags 6. Configure Security Group 7. Review			
Step 5: Add Tags htsg consists of a case-sensitive key-value pair. For example, you could define A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging you				
Key (128 characters maximum)	Value (256 characters maximum)	Instances	(i) Volumes (i)	
Name	FSM-610-Super			0
Add another tag (Up to 50 tags maximum)				
	Ca	ncel Previous Revi	ew and Launch Nex	t: Configure Security Grou

6. In Step 6: Configure Security Group, add the allowed inbound protocols for your instance. You will need ssh and https to begin with. Depending on whether this node will receive syslog or other inbound data, you may need to open additional protocols/ports. Click Review and Launch.

. Choose AMI 2. Choose		ce Groups ~	4. Add Storage 5. Add Tags	6. Configure Security Group	7. Review	Å® FortiSIEM QA ▾ N. Virginia ▾ Support ▾
	rewall rules that control	ol the traffic for y				or example, if you want to set up a web server and allow Intern ng one below. Learn more about Arnazon EC2 security groups
Assign	a security group: 🧕	Create a new se	acurity group			
	0	Select an existin	ng security group			
Secu	rity group name:	launch-wizard-	43]	
	Description:	launch-wizard-	43 created 2020-07-15T12:43:	00.232+07:00]	
Туре ()	Protocol	()	Port Range (i)	Source ()		Description (j)
SSH ¥	TCP		22	Custom	♥ 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS V	TCP		443	Custom	✔ 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
Add Rule						
A Warning						
Rules with source	of 0.0.0.0/0 allow all	IP addresses to	access your instance. We reco	mmend setting security group rule	s to allow access from known	IP addresses only.
						Cancel Previous Review and Launci
						Cancel Previous Review and Launc

7. In Step 7: Review Instance Launch, click Launch.



8. Select an existing key pair or create a new key pair, then click Launch Instances.

Select an existing key pair or create a new key pair	×
A key pair consists of a public key that AWS stores, and a private key file that you store. Togeth they allow you to connect to your instance securely. For Windows AMIs, the private key file is rec to obtain the password used to log into your instance. For Linux AMIs, the private key file allows securely SSH into your instance.	luired
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn m about removing existing key pairs from a public AMI.	
Choose an existing key pair	~
Select a key pair	
and the	~
✓ I acknowledge that I have access to the selected private key file (ga-ec2-ht.pem), and tha	
without this file, I won't be able to log into my instance.	
Cancel Launch Instan	ces

9. Select the instance that you just created and click Connect.

New EC2 Experience Tell us what you think	Launch Instanc	co 🗸 Connec	Actions 👻	Connect to your	instance	×	æ	•	0
EC2 Dashboard New	Q, search : i-0	Da7742ded6c568e8	Ado Ster	Connection method	A standalone SSH client (1)		of 1		
Events New	Name				Session Manager () EC2 Instance Connect (browser-based SSH connection)		us Ch	hecks	
Tags	FSM-610-5	Super					2/2 ch	ecks .	
Limits	-			To access your instance					
▼ Instances					t. (find out how to connect using PuTTY)				
Instances	Instance: i-0a	7742ded6c568e8a	(FSM-610-Super)	Locate your private to launch the instar	key file (qa-ec2-ht.pem). The wizard automatically detects the key you used nce.				
Instance Types	Description	Status Checks	Monitoring T	3. Your key must not l	be publicly viewable for SSH to work. Use this command if needed:				
Launch Templates		Instance ID	i-0a7742ded6c568el	chmod 400 q	a-ec2-ht.pem				
Spot Requests				4. Connect to your ins	stance using its Public DNS:				
Savings Plans		Instance state		007-54-161-1	175-251.compute-1.amazonaws.com				
Reserved Instances		Finding	Opt-in to AWS Comp	Example:	173-231. Compute-1. anazonaws. com				æ
Dedicated Hosts New			recommendations. L			~			
Scheduled Instances		Private DNS	ip-10-0-0-25.ec2.int	ssh -i "🏢 🖩	.pem" root@ec2-54-161-175-251.compute-1.amazonaws.co	m			
Capacity Reservations		Private IPs	10.0.25		t in most cases the username above will be correct, however please ensure				
capacity Reservations	Sec	condary private IPs		that you read yo default AMI use	our AMI usage instructions to ensure that the AMI owner has not changed the	•			
▼ Images		VPC ID	vpc-4c0d8528 (PS-A						
AMIs				If you need any assistance	e connecting to your instance, please see our connection documentation.				
▼ Elastic Block Store		Subnet ID Network interfaces	subnet-53969e78 (P						
			-		Close				
Volumes									
Snapshots									

10. Using the example above in the **Connect** popup, ssh to the instance you created. Replace root user with ec2user. Once logged in, you can execute the sudo su - command to become root user

Configure FortiSIEM via GUI

Follow these steps to configure FortiSIEM by using a simple GUI.

- 1. At the root command prompt, go to /usr/local/bin and enter configFSM.sh, for example:
 # configFSM.sh
- 2. In VM console, select 1 Set Timezone and then press Next.

Set TimeZone	Conf igure	TIMEZONE
	2	Yes No
l		
	< <u>N</u> ext >	< Exit >

3. Select your Location, and press Next.



4. Select your Continent, and press Next.



5. Select the Country and City for your timezone, and press Next.



6. Select 1 Supervisor. Press Next.





Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

7. If you want to enable FIPS, then choose 2 install_with_fips. Otherwise, choose 1 install_without_fips. You have the option of enabling FIPS (option 3) or disabling FIPS (option 4) later.

Select Operation	onfigure Supervisor
1 2 3 4 5 7	install_without_fips install_with_fips enable_fips disable_fips change_ip migrate_6_1_1 upgrade
< ext >	< BACK > < Exit >

8. Configure the network by entering the following fields. Press Next.

172.30.52.32

< Next >

Option	Description		
Host Name	The Supervisor's host name		
IPv4 Address	The Supervisor's IPv4 address		
NetMask	The Supervisor's subnet		
Gateway	Network gateway address		
FQDN	Fully-qualified domain name		
DNS1, DNS2	Addresses of the DNS servers		
Configure N Host name: IPv4 Addre Netmask: Gateway:	sp5782.fortinet.com ss: 172.30.57.82 255.255.252.0 172.30.56.1		
FQDN: DNS1:	sp5782.fortinet.com 172.30.52.31		

< Back >

9. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.

< Exit >

DNS2:

Confi Enter host for checkin	gure Supervis g network cor]
myhost.com_			
K Next >	< Back >	< Exit >	

10. The final configuration confirmation is displayed. Verify that the parameters are correct. If they are not, then press **Back** to return to previous dialog boxes to correct any errors. If everything is OK, then press **Run**.

Configure Supervisor -
Run Configuration Command:
python /usr/local/bin/configureFSM.py -r super -z US/Pacific -i 172.30.57.82 -m 255.255.252.0 -g 172.30.56.1host sp5782.fortinet.com -f sp5782.fortinet.com -t 4dns1 172.30.52.32dns2 172.30.52.31 -o install_with_fipstestpinghost myhost.com
<pre></pre>

The options are described in the following table.

Option	Description
-r	The FortiSIEM component being configured
-Z	The time zone being configured
-i	IPv4-formatted address
-m	Address of the subnet mask
-g	Address of the gateway server used
host	Host name
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either 4 (for ipv4) or 6 (for v6) Note: the 6 value is not currently supported.
dns1,dns2	Addresses of the DNS server 1 and DNS server 2.
-0	Installation option (install_without_fips , install_with_fips, enable_fips, disable_fips, change_ip, or migrate_6_1_0)
-Z	Time zone. Possible values are US/Pacific ,

Option	Description
	Asia/Shanghai, Europe/London, or Africa/Tunis
testpinghost	The host used to test connectivity

11. It will take some time for this process to finish. When it is done, proceed to Upload the FortiSIEM License. If the VM fails, you can inspect the ansible.log file located at /usr/local/fresh-install/logs to try and identify the problem.

Upload the FortiSIEM License



Before proceeding, make sure that you have obtained valid FortiSIEM license from Forticare. For more information, see the Licensing Guide.

You will now be asked to input a license.

- 1. Open a Web browser and log in to the FortiSIEM UI.
- 2. The License Upload dialog box will open.

🔀 FortiSIEM				
Hardware ID:	1. 2			
Select license file:	Browse			
User ID:				
Password:				
License Type:	● Enterprise ○ Service Provider			
	Upload			

- Click Browse and upload the license file.
 Make sure that the Hardware ID shown in the License Upload page matches the license.
- 4. For User ID and Password, choose any Full Admin credentials. For the first time installation, enter admin as the user and admin*1 as the password. You will then be asked to create a new password for GUI access.
- Choose License type as Enterprise or Service Provider. This option is available only for a first time installation. Once the database is configured, this option will not be available.
- 6. Proceed to Choose an Event Database.

Choose an Event Database

For a fresh installation, you will be taken to the Event Database Storage page. You will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options. For more details, see Configuring Storage.

Fresh Installation



After the License has been uploaded, and the Event Database Storage setup is configured, FortiSIEM installation is complete. If the installation is successful, the VM will reboot automatically. Otherwise, the VM will stop at the failed task.

You can inspect the ansible.log file located at /usr/local/fresh-install/logs if you encounter any issues during FortiSIEM installation.

After installation completes, ensure that the phMonitor is up and running, for example:

phstatus

The response should be similar to the following.

Every 1.8s: /opt/phoenix/bin/phstatus.py					
System uptime: 21:12:82 up 1:11, 1 user, load average: 0.16, 0.28, 0.36 Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie Cpu(s): 16 cores, 6.2xus, 2.1xsy, 0.8xui, 91.4xid, 0.0xus, 0.8xhi, 0.1xsi, 0.8xst Mem: 65782100K total, 10560836k used, 55330604K free, 4352k utifers Swap: 2621436k total, 0k used, 2621436k free, 24650820k cached					
PROCESS	UPTIME	CPU:	VIRT_MEM	RES_MEM	
phParser	41:23	0	2176m	558m	
phQueryMaster	41:41	0	1020m	77m	
phRuleMaster	41:41	0	1079m	504m	
phRuleWorker	41:41	0	1363m	285m	
phQueryWorker	41:41	0	1383m	279m	
phDataManager	41:41	0	1419m	285m	
phDiscover	41:41	0	513m	53m	
phReportWorker	41:41	0	1433m	95m	
phReportMaster	41:41	0	603m	67m	
phlpIdentityWorker	41:41	0	1027m	58m	
phIpIdentityMaster	41:41	0	491m	39m	
phagentManager	41:41	0	1425m	54m	
phCheckpoint	42:31	0	325m	34m	
phPerfMonitor	41:41	0	782m	70m	
phReportLoader	41:41	0	769m	278m	
phBeaconEventPackager	41:41	0	1125m	65m	
phDataPurger	41:41	0	588m	58m	
phEventForwarder	41:41	0	548m	46m	
phMonitor	37:24		2888m	53m	
Apache	01:10:40	0	310m	16m	
Node.js-charting	01:10:19		916m	71m	
Node.js-pm2	01:10:13			26m	
AppSor	01:10:07	0	15172m	3026m	
DBSvr	01:10:38		317m	30m	
phAnoma ly	01:08:07		987m	64m	
phFortiInsightAI	01:10:40		23432m	438m	
Redis	01:10:18	0	55m	25m	

Cluster Installation

For larger installations, you can choose Worker nodes, Collector nodes, and external storage (NFS or Elasticsearch).

- Install Supervisor
- Install Workers
- Register Workers
- Install Collectors
- Register Collectors

Install Supervisor

Follow the steps in All-in-one Install with two differences:

- Setting up hardware you do not need to add an EBS Volume 5 for Event database.
- Setting up an Event database Configure the cluster for either NFS or Elasticsearch.
 NFS

×	FortiSIEM
Event Database stora	age:
🔿 Local Disk	
NFS	
Server IP/Host:	Server IP/Host
Exported Directory:	Exported Directory
 Elasticsearch 	
	Test Save

Elasticsearch

🔀 FortiSIEM					
Event Database storage:					
○ Local Disk					
○ NFS	O NFS				
Elasticsearch					
Client:	● Java Transport ○ REST API				
Cluster Name:	Elasticsearch				
Cluster IP/Host:	127.0.0.1 / Host Name				
HTTP Port:	9200				
Java Port:	9300				
User Name:	(Optional)				
Password:	(Optional)				
Shard Allocation:	• Fixed O Dynamic				
Shards:	5				
Replicas:	1				
Per Org Index					
	Test Save				

You must choose external storage listed in Choose an Event Database.

Install Workers

Once the Supervisor is installed, follow the same steps in All-in-one Install to install a Worker except you need to only choose OS and OPT disks. The recommended CPU and memory settings for Worker node, and required hard disk settings are:

- CPU = 8
- Memory = 24 GB
- Two hard disks:
 - OS-25GB

• OPT - 100GB

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when configFSM.shruns.

	inched with the followi pot volume. You can a			BS volumes and instance store vo istance, but not instance store volu					
Volume Type 🕕	Device (j)	Snapshot ①	Size (GiB) (j)	Volume Type (j)	IOPS ()	Throughput (MB/s)	Delete on Termination (j)	Encryption ①	
Root	/dev/sda1	snap-0a71481d3c7816fb3	25	[General Purpose SSD (gp3)	✔ 3000	125	0	Not Encrypted	*
EBS v	/dev/sdb ✔	Search (case-insensit	100	General Purpose SSD (gp3)	✓ 3000	125	8	Not Encrypted	*
Add New Volume	stomers can get up to	30 GB of EBS General Purpose (\$	SD) or Magnetic sto	rage. Learn more about free usag	e tier eligibility and]			

Register Workers

Once the Worker is up and running, add the Worker to the Supervisor node.

- 1. Go to ADMIN > License > Nodes.
- 2. Select Worker from the drop-down list and enter the Worker's IP address. Click Add.

🌣 Setup	General Usage Nodes	
🖨 Device Support	Add Delete	
📑 Health	Mode	IP Address
License	Supervisor	172.30.57.2
🕫 Settings	Add Node	×
	Type: Worker	~
	Worker IP Address: 172.30.57.3	
	OK Cancel	_

3. See ADMIN > Health > Cloud Health to ensure that the Workers are up, healthy, and properly added to the

system.										
🏟 Setup	Cloud Health Colle	ector Health								
🖨 Device Support	Search	Columns 🕶							Lines: 2 Last update at 8:4	9:17 PM 🟾
⊟ Health	Name	IP Address	Module Role	Health	Versi	on	Load Average	CPU	Swap Used	
	sp572.fortinet.com	1 2	Supervisor	Normal	6.1.0	.1238	0.95,0.47,0.4	3 4%	0 KB	
Icense License	wk573.fortinet.com	1 3	Worker	Normal	6.1.0	.1238	0.1,0.2,0.16	2%	0 KB	
📽 Settings										
	Search	Columns 🕶		1	Process le	vel metrics for wk5	73.fortinet.com (17	2.30.57.3)		Lines: 17
	Process Name	Status	Up Time	C	PU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position	
	Node.js-charting	Up	1h 3m	0	1%	70 MB	916 MB			*
	httpd	Up	14m 6s	0	1%	16 MB	310 MB			
	Redis	Up	14m 6s	0	1%	22 MB	51 MB			_
	Node.js-pm2	Up	1h 3m	0	1%	44 MB	899 MB			
	rsyslogd	Up	1h 3m	0	%	7 MB	189 MB			
	phDataManager	Up	14m 6s	0	%	103 MB	1229 MB	1	126108	*
Copyright © 2020 Fortinet, Inc. All rights	reserved.		Organization	: Super Use	er: admin	Scope: Global				FortiSIEM

Install Collectors

Once Supervisor and Workers are installed, follow the same steps in All-in-one Install to install a Collector except in Edit FortiSIEM Hardware Settings, you need to only choose OS and OPT disks. The recommended CPU and memory settings for Collector node, and required hard disk settings are:

- CPU = 4
- Memory = 8GB
- Two hard disks:
 - OS 25GB
 - OPT 100GB

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when configFSM.shruns.

1. Choose AMI	2. Choose	Instance Type	3. Configure Instance 4. Add	Storage 5. Add Tags	6. Configure Security Group	7. Review						
	be launche f the root v	ed with the follow olume. You can	ving storage device settings. Ye also attach additional EBS volu									
Volume Type	D	Device (j)	Snapshot ①	Size (GiB) ①	Volume Type 🕕		IOPS (j)	Throughput (MB/s)	Delete on Termination (j)	Encryption ①		
Root		/dev/sda1	snap-0a71481d3c7816fl	b3 25	General Purpose SSD	(gp3) 🗸	3000	125		Not Encrypted	•	
EBS	*	/dev/sdb ✔	Search (case-insensit	100	General Purpose SSD	(gp3) 🗸	3000	125	•	Not Encrypted	*	۲
Add New Volum	ole custom	ers can get up t	o 30 GB of EBS General Purpo	use (SSD) or Magnetic ste	orage. Learn more about free	o usage tier eligibi	ity and					

Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

- Enterprise Deployments
- Service Provider Deployments

Enterprise Deployments

For Enterprise deployments, follow these steps.

- 1. Log in to Supervisor with 'Admin' privileges.
- 2. Go to ADMIN > Settings > System > Event Worker.
 - a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
 Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
 - b. Click OK.
- 3. Go to ADMIN > Setup > Collectors and add a Collector by entering:
 - a. Name Collector Name
 - **b.** Guaranteed EPS this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
 - c. Start Time and End Time set to Unlimited.

4. SSH to the Collector and run following script to register Collectors:

phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization>
<CollectorName>

The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

- a. Set user and password using the admin user name and password for the Supervisor.
- **b.** Set Super IP or Host as the Supervisor's IP address.
- c. Set Organization. For Enterprise deployments, the default name is Super.
- d. Set CollectorName from Step 2a.

The Collector will reboot during the Registration.

5. Go to ADMIN > Health > Collector Health for the status.

Cloud Health	ollector Health											
Show Processes	Tunnels 🏚 🗸	Action 👻	Search	Colum	ns 🕶				Lines: 1	Last update at 8	8:54:17 PM	ø
Organization	Name	IP Ad	dress Statu	s i H	lealth Up 1	ïme (CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	1	t up	,	iormal 3m ·	45	65%	5%	200	0	6.1.0	100
Close Panel Se	arch	Col	umns 🕶						Lir	es: 9 Last upda	te at 8:54:2	▶ 24 PM
Process Name	5 S	tatus Up	Time	CPU	Physical Memory	Virtual Memory	/ Sha ID	redStore	SharedStore P	osition		
phMonitorAgent	U	Jp 299	5	0%	575 MB	1116 MB						*
phParser	u	Jp 179	5	0%	106 MB	1190 MB	99		0			
phPerfMonitor	U	Jp 17s	5	0%	79 MB	766 MB						
phEventForwarder	U	Jp 17s	s	0%	48 MB	547 MB						
phDiscover	U	Up 17s	5	0%	53 MB	513 MB						
	Show Processes Organization Super Close Panel Se Process Name PhMonitor Agent phParser phPerfMonitor phPerfMonitor	Show Processes Tunnets Drganization Name Super CO-ORG Close Panel Search Close Panel Search Process Name S phMonitor Agent I phParser I phPer/Monitor I phEventForwarder I	Show Processes Tunnels Action - Organization Name IP Ad Super CO-ORG 1 Close Panel Search Col Process Name Status Up phMonitor Agent Up 29 phParser Up 17 phPer/Monitor Up 17 phEventForwarder Up 17	Show Processes Tunnels Action Search Organization Name IP Address Statu Super CO-ORG 1 4 Close Panel Search Columns • Process Name Status Up PhMonitorAgent Up 29s phParser Up 17s phPertMonitor Up 17s phEventForwarder Up 17s	Show Processes Tunnels Action Search Column Organization Name IP Address Status IH Super CO-ORG 1 4 up 1 Close Panet Search Columns - ************************************	Show Processes Tunnets Action Search Columns + Organization Name IP Address Status Health Up T Super CO-ORG 1 up Normal 3m Close Panet Search Columns + Process Name Status Up Time CPU Physical Memory phonitorAgent Up 29s 0% 575 M8 pherrifinitor Up 17s 0% 10e M8 pherrifinitor Up 17s 0% 48 M8	Show Processes Tunnets Action Search Columns • Organization Name IP Address Status Health Up Time Image: Columns • Super CO-ORG 1 up Normal Jm 4s Image: Columns • Close Panel Search Columns • Columns • Image: CPU Physical Memory Virtual Memory PhonolitorAgent Up 29s 0% 575 M8 1116 M8 phParser Up 17s 0% 106 M8 1190 M8 phPerfMonitor Up 17s 0% 79 M8 766 M8 phEventForwarder Up 17s 0% 48 M8 547 M8	Show Processes Tunnets Celumns - Organization Name IP Address Status Health Up Time CPU Super CO-ORG 1 up Normal 2m 4s 65% Close Panet Search Columns - 100 Normal 2m 4s 65% Process Name Status Up Time CPU Physical Memory Virtual Memory Shab phaner Up 29s 0% 575 MB 1116 MB 99 pharer Up 17s 0% 79 MB 766 MB 99 pherfMonitor Up 17s 0% 48 MB 547 MB 547 MB	Show Processes Tunnels Search Columns • Organization Name IP Address I Status Health Up Time CPU Memory Super CO-ORG 1 3 up Normal 3m 4s 65s 5s Close Panet Search Columns • SparedStore Process Name Status Up Time CPU Physicat Memory Virtual Memory SharedStore phonitor/agent Up 29s 0% 575 M8 1116 M8 99 phorer/Monitor Up 17s 0% 79 M8 766 M8 99 phorer/Monitor Up 17s 0% 48 M8 547 M8	Show Processes Tunnets Columns - Columns - Lines: 1 Organization Name IP Address Status Health I Up Time CPU Memory Allocated EPS Super CO-ORG 1 3 up Normal 3m 4s 65% 5% 200 Close Panet Search Columns - Virtual Memory Virtual Memory SharedStore PharedStore PharedStore	Show Processes Tunnets Earch Columns - Line: t Line	Show Processes Tunnets Address Status Health Up Time CPU Memory Allocated EPS Incoming EPS Version Super C0-ORG 1 1 up Normal 3m 4s 65% 5% 200 0 6.11.0 Close Panel Search Columns • CPU Physical Memory Virtual Memory SineredStore SineredStore 8.544:154:17 PM Process Name Status Up Time CPU Physical Memory Virtual Memory SineredStore SineredStore Position phonitorAgent Up 29% 0% 575 M8 1116 M8 9 0 - phorefr/Monitor Up 175 0% 106 M8 1190 M8 99 0 - - phorefr/Monitor Up 175 0% 26% A8 547 M8 - </th

Service Provider Deployments

For Service Provider deployments, follow these steps.

- 1. Log in to Supervisor with 'Admin' privileges.
- 2. Go to ADMIN > Settings > System > Event Worker.
 - a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.

Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.

b. Click OK.

Setup	← All Settings > System > Event Worker
🗇 Device Support	Worker Address: 1
📰 Health	
I License	Save
🛱 Settings	

3. Go to ADMIN > Setup > Organizations and click New to add an Organization.

Organization Definiti	on (ORG)			×
Organization:	ORG	Include IP/IP Range:		
Full Name:		Exclude IP/IP Range:		
Admin User:	admin	Agent User:		
Admin Password:	•••••	Agent Password:		
Confirm Admin Password:	•••••	Confirm Agent Password:		
Admin Email:	Required	Max Devices:		
Phone:		Address:		
Account Number:		Account Type:		
Support Tier:		Account Status:		
Support Team:		Account Manager:		
Collectors:	New Edit Delete			
	Collector Name Collector EPS	UpLoad Rate Limit	Valid Start Date Valid End Dat	е
				- ,
	Save	Cancel		

- 4. Enter the Organization Name, Admin User, Admin Password, and Admin Email.
- 5. Under Collectors, click New.
- Enter the Collector Name, Guaranteed EPS, Start Time, and End Time.
 The last two values could be set as Unlimited. Guaranteed EPS is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.

Fresh Installation

Organization Definiti	on (ORG) - Add Collector X
Name:	Required
Guaranteed EPS:	Required
Upload Rate Limit (Kbps):	Unlimited
Start Time:	Unlimited
End Time:	Unlimited
	✓ Save

7. SSH to the Collector and run following script to register Collectors:

```
phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization>
<CollectorName>
```

The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

- a. Set user and password using the admin user name and password for the Organization that the Collector is going to be registered to.
- **b.** Set Super IP or Host as the Supervisor's IP address.
- c. Set Organization as the name of an organization created on the Supervisor.
- d. Set CollectorName from Step 6.



The Collector will reboot during the Registration.

8. Go to ADMIN > Health > Collector Health and check the status.

🌣 Setup	Cloud Health	Collector Health												
🖨 Device Support	Show Processes	Tunnels 🕻	Action	• Search		Columns -					Lines: 1	Last update at I	8:54:17 PM	ø
🗮 Health	Organization	Name	11	P Address	Status	Heal	th Up T	ime (CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Icense	Super	CO-ORG	1	-	up	Norr	nal 3m 4	s i	65%	5%	200	0	6.1.0	100
✿C Settings														
	<													•
	Close Panel	Search		Columns -							Lir	nes: 9 Last upda	te at 8:54:2	24 PM
	Process Name		Status	Up Time	i Ci	PU Ph	vsical Memory	Virtual Memory	/ Sha	aredStore	SharedStore P	osition		
	phMonitorAgent		Up	29s	0	% 57	5 MB	1116 MB						^
	phParser		Up	175	0	% 10	6 MB	1190 MB	99		0			
	phPerfMonitor		Up	175	0	% 79	MB	766 MB						
	phEventForwarde	r	Up	17s	0	% 48	MB	547 MB						
	phDiscover		Up	175	0	% 53	MB	513 MB						
														*

Migrating from FortiSIEM 5.3.0, 5.3.1 or 5.3.2

WARNING: FortiSIEM 5.3.3 and 5.4.0 cannot be upgraded to FortiSIEM 6.1.0. You must upgrade to FortiSIEM 6.1.1.

This section describes how to migrate from FortiSIEM 5.3.0, 5.3.1 or 5.3.2 to FortiSIEM 6.1.0. FortiSIEM performs migration in-place. The migration process backs up some important information from the original 5.3.0, 5.3.1 or 5.3.2 root disk, and then changes the root disk to boot up from a new 6.1.0 root disk. There is no need to copy disks. The instance identity remains the same.

- Pre-Migration Checklist
- Migrate All-in-one Installation
- Migrate Cluster

Pre-Migration Checklist

To perform the migration, the following prerequisites must be met:

- Delete the Worker from the Super GUI.
- Stop/Shutdown the Worker.
- Note the /svn partition by running the df -h command. the partition is used to mount /svn/53x-settings. You will need this information for a later step.
- Create a /svn/53x-settings directory and symlink it to /images. In AWS, you need only a small amount of space to backup 5.3.0, 5.3.1 or 5.3.2 system settings, so use the /svn partition (that is, a partition other than root) instead of a new disk. See the following example:

<pre>[root@fsm-531-to-610-migrate ~]# cat /opt/phoenix/bin/VERSION</pre>	
Version: 5.3.1.1668	
DSVersion: 5.3.1.1668	
CommitHash:725c388e6	
Built on: 1590816258	
Local time: Fri May 29 22:24:18 PDT 2020	
[root@fsm-531-to-610-migrate ~]#	
[root@fsm-531-to-610-migrate ~]# mkdir /svn/53x-settings	
<pre>[root@fsm-531-to-610-migrate ~]# ln -sf /svn/53x-settings /image</pre>	es:
[root@fsm-531-to-610-migrate ~]#	

Migrate All-in-one Installation

- · Download the Backup Script
- Run the Backup Script and Shutdown

- Detach 5.3.0, 5.3.1 or 5.3.2 Root Disk
- Attach the 6.1.0 Root Disk to the 5.3.0, 5.3.1 or 5.3.2 Instance
- Boot Up the 5.3.0, 5.3.1 or 5.3.2 Instance and Migrate to 6.1.0
- (Optional) Change Instance Type to the Latest Generation

Download the Backup Script

Download FortiSIEM AWS backup script to start migration. Follow these steps:

- 1. # Download the file FSM_Backup_5.3_Files_6.1.0_0112.zip from the support site and copy it to the 5.3.x AWS instance that you are planning to migrate to 6.1.0 (for example, /svn/53x-settings).
- 2. Unzip the .zip file, for example: # unzip FSM_Backup_5.3_Files_6.1.0_0112.zip

Run the Backup Script and Shutdown System

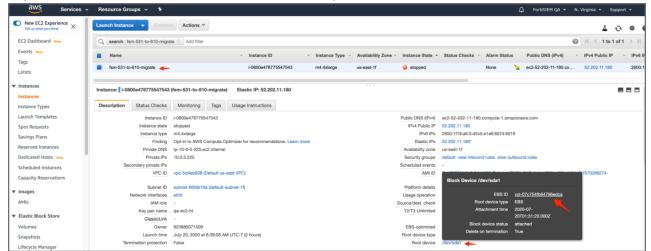
Follow these steps to run the backup script and shut down the system:

- 1. Go to the directory where you downloaded the backup script, for example: # cd /svn/53x-settings/FSM_Backup_5.3_Files_6.1.0_0112
- 2. Run the backup script with the sh backup command to backup 5.3.0, 5.3.1 or 5.3.2 settings that will be migrated later into the new 6.1.0 OS. For example:
 - # sh backup
- 3. Run the shutdown command to shut down the FortiSIEM instance, for example:

Detach 5.3.0, 5.3.1 or 5.3.2 Root Disk

Follow these steps to detach the 5.3.0, 5.3.1 or 5.3.2 root disk from the AWS console.

1. Log in to the AWS Console, select EC2 service, and select your FortiSIEM 5.3.0, 5.3.1 or 5.3.2 instance.



- 2. Click the /dev/sda1 volume and navigate to the volume by clicking the volume EBS ID.
- 3. Click Action > Detach Volume.

aws services ~	Resource Groups 🤟 🔭	🗘 FortiSIEM QA 👻 N. Virginia 👻 Support 👻
New EC2 Experience Tell us what you think	Create Volume Actions ^	∆ ⊕ ♦ Ø
EC2 Dashboard New	Q search: vol Creat Bragdort Delar Bragdort	
Tags	Attach Volume + size + volume type + runce + onapanot + uneaso + Availability zone + osate + At	arm Attachment Information
Limits	Foros Detach Volume	
▼ Instances	Change Auto-Enable ID Setting Add/Tidt Tags	
Instances	Add/ticlt Taga	
Instance Types		
Launch Templates		
Spot Requests		
Savings Plans		
Reserved Instances		
Dedicated Hosts New		
Scheduled Instances		
Capacity Reservations		
▼ Images	Description Status Linexis Monitoring lags	
AMIs	Volume ID vol-67c754fb54798edca Outposts ARN -	
▼ Elastic Block Store	Alam status None Size 80 GB Snapht snap-07a15500(2284403 Crested July 19, 2229 at 6.31.21 PM 1	mo-7
	Availability Zone un-set-11 State in-use	
Volumes	Enoryption Net Enorypted Attachment Information +0800e4787755432643 (tem-5	31-to-610-migrate):/dev/sda1 (attached)
Snapshots	KMS Key ID Volume type gp2	
Lifecycle Manager	KMS Key Aliases Product codes marketplace: 8edm7at0404	ho2kte2tma9g

4. Confirm the operation in the popup by clicking Yes, Detach.



Attach the 6.1.0 Root Disk to the 5.3.0, 5.3.1 or 5.3.2 Instance

Follow these steps to attach the 6.1.0 root disk to the 5.3.0, 5.3.1 or 5.3.2 instance which you obtained from a fresh 6.1.0 instance.

- 1. Navigate to the EC2 AMIs page and find FortiSIEM 6.1.0 AMI (or in AWS Marketplace after GA).
- 2. Launch FortiSIEM-6.1.0.0112.

aws services v	R	lesource Groups 👻 🧚									
New EC2 Experience Tell us what you think	La	EC2 Image Builder	Actions ~								
EC2 Dashboard New											
Events New Tags		Name	v	AMI Name		AMI ID ~	Source ~	Owner ~	Visibility	- Sta	itus ~
Limits		FortiSIEM-VA-6.1.0.1260		FortiSIEM-VA-6.1.0.1260		ami-0d9e0d46e6c653f81	623885071509/	623885071509	Private	ava	ilable
▼ Instances	1	•									

3. In Step 2: Choose an Instance Type, select the m5.2xlarge instance type (it does not matter if you pick another instance type). The purpose of this is only to get a root volume. Click Next: Configure Instance Details.

aws	Services - Reso	urce Groups 🗸 🔺				Ĺ	📍 FortiSIEM QA 👻 N. Virginia	- Support -
1. Choose AM	2. Choose Instance Type 3	Configure Instance 4.	Add Storage 5. Add Ta	igs 6. Configure Sect	urity Group 7. Review			
Step 2:	Choose an Instance	Туре						
	General purpose	m5.2xlarge	н в	32	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose m5.4xlarg		16	64	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose m5.8xlarge		32	128	EBS only	Yes	10 Gigabit	Yes
	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
	General purpose	m5.16xlarge	64	256	EBS only	Yes	20 Gigabit	Yes
	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
	General purpose m5.metal		96	384	EBS only	Yes	25 Gioabit	Yes
					Ca	ncel Previous Ren	riew and Launch Next: Configu	re Instance Details

4. In Step 3: Configure Instance Details choose the same VPC and subnet where you deployed your 5.3.0, 5.3.1 or 5.3.2 instance. The remaining details can be default values.

dWS Services v	Resour	ce Groups 👻	*						Δ•	FortiSIEM QA 👻	N. Virginia 🔻	Support *
1. Choose AMI 2. Choose Instance Typ	• 3. Co	onfigure Instance	4. Add Storage	5. Add Tags	6. Cont	figure Security Group	7. Review					
Step 3: Configure Insta												
Configure the instance to suit your requ	irements.	You can launch m	ultiple instances	from the same A	AMI, reque	est Spot instances to	o take advantage	e of the lower pricing,	assign an access m	nanagement role to t	he instance, an	d more.
Number of instance	s ()	1		Launch into Au	uto Scalin	ng Group 🕕						
Purchasing option	n (j)	Request Spore	t instances									
Networ	k 🕕	vpc-5d4eb938	Default us-east	VPC	4	C Create new VP	с					
Subne	t 🕕	subnet-66fdb16 228 IP Addresse	5a default-subn	et-1f us-east-11	f 4	Create new sub	bnet					
Auto-assign Public II	P (1)	Use subnet set			\$							
Auto-assign IPv6 II	P ()	Use subnet set	ting (Enable)		4							
Placement grou	p (1)	Add instance	to placement gr	oup								
Capacity Reservation	n (i)	Open			\$	C Create new Ca	pacity Reservation	on				
IAM rol	• ①	None				C Create new IAM	f min					
		TAOLIO				Create new pow	TOUE					
CPU option	•	Specify CPU	options									
Shutdown behavio	r ()	Stop			4							
Stop - Hibernate behavio	r (j	C Enable hiberr	nation as an add	itional stop beha	ivior							
Enable termination protection	n ()	Protect again	ist accidental ter	mination								
Monitorin		Enable Cloud Additional charg	Watch detailed r ges apply.	monitoring								
EBS-optimized instance	0	🛙 Launch as EE	3S-optimized ins	tance								
Tenanc	y (i)		shared hardware ges may apply w		edicated i	instances.						
Elastic Inference	• ()	Add an Elasti Additional charg	ic Inference acce ges apply.	lerator								
File system	• (i)	Add file syste	em C Crea	ite new file syste	m							
 Network interfaces (i) 												
Device Network Interface	Subnet	Pri	mary IP	Seco	ondary IP	addresses		IPv6 IPs				
eth0 New network interface >	subnet-6	66fdb16a V AL	uto-assign	Add	IP			Auto-assign	Add IP			
									Cancel Previ	ous Review an	d Launch	Next: Add Storage
												↑

5. In Step 4: Add Storage, click Next: Add Tags.

AWS 651531 Mantis	ervices - Reso	urce Groups 🗸	*					۵	FortiSIEM QA 👻	N. Virginia 👻	Support 👻
1. Choose AMI 2. Cho	se Instance Type 3.	Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review					
	ched with the followin ot volume. You can als				IS volumes and instance sto tance, but not instance stor						
Volume Type (i)	Device (i)	Snapshot (i)		Size (GiB) (i)	Volume Type (i)		IOPS ()	Throughput (MB/s) (i)	Delete on Termination (i)	Encryptic	n ()
Root	/dev/sda1	snap-07894c407	375ab841	25	General Purpose SSD (g	p2) 🗸	100 / 3000	N/A		Not Encry	pted 🔻
Add New Volume											
Free tier eligible cust usage restrictions.	omers can get up to 3	0 GB of EBS Genera	I Purpose (SSD) or Magnetic stora	ge. Learn more about free u	sage tier eligibil	ity and				7
								Cancel	Previous Review a	nd Launch	Next: Add Tags

6. In Step 5: Add Tags click the Add Tag button.

aWS Services → Resource Groups → ト	🎝 [●] FortiSIEM QA 👻 N. Virginia 👻 Support 👻
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review	
Step 5: Add Tags A tag consists of a case-sensity evolve pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to valuese, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.	
Key (128 characters maximum) Value (256 characters maximum) Inst	stances () Volumes ()
This resource currently has no tags	
Choose the Add tag button or click to add a Name tag.	
Add Tag (Up to 50 tags maximum)	
Cancel Previo	ious Review and Launch Next: Configure Security Group

7. Provide a Key name and Value for the tag. Click Next: Configure Security Group.

aWS Services v Resource Groups v t	₽ •	FortiSIEM QA 👻	N. Virginia 👻	Support 💌
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review				
Step 5: Add Tags A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of at ag on a be applied to volumes, Instances or both. Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.				
Key (128 characters maximum) Value (256 characters maximum) Instances (0	Volumes (i)		
Name fsm-6.1.0-instance-to-detach-root-volume 2		2	8	
Add another tag (Up to 50 tags maximum)				
			•	
Cancel Previous	Revie	w and Launch	Next: Configure	Security Group

8. In Step 6: Configure Security Group, select any security group because FortiSIEM will not be logging into this instance. Click Review and Launch.

aws	Services 🗸	Resource Groups ~	*				4 °	FortiSIEM QA 👻	N. Virginia 👻	Support 👻
1. Choose AMI 2.	hoose Instance Ty	pe 3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review				
	et of firewall rule	s that control the traffic for			add rules to allow specific n create a new security gro					
	ssign a security	group: O Create a new	security group							
		Select an exis	ting security grou	p						
									Filter VPC	security groups 🗸
Security Group	ID Name				Description					
sg-624f9807	default				default VPC security gro	up				
Inbound rules for s	1-62419807 (Sele	cted security groups: sg	-624f9807)							
Туре 🕕		Protocol ()		Port R	ange ()	Source (D	Descriptio	in (j)	
Custom UDP Rule		UDP		161		0.0.0/0				+
								Cancel	Previous	wiew and Launch

9. In Step 7: Review Instance Launch. Click Launch.

4	ws	Services ~	Resource Groups 🐱	*							4 •	FortiSIEM QA 👻	N. Virgini	ia ♥ Si	upport 👻	
1. Choose	e AMI	2. Choose Instance Type	e 3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure S	Security Group	7. Review	_							1
		view Instance r instance launch deta	e Launch ails. You can go back to ed	it changes for ea	ch section. Clic	k Launch to as	isign a key pair	r to your instar	nce and comple	ete the launch j	process.					l
			ration is not eligible for eligible for the free usage to			istance type, co	onfiguration op	itions, or stora	ge devices. Lea	arn more about	t free usag	e tier eligibility a	-	strictions.		
A	Your in	stances may be acce	es' security. Your security is address all ports in your security groups and the security group is a secur	We recommend	i that you updat	te your security (group rules to					ıps				
▼ AMI	Detai	s													Edit AMI	
4	· ·		260 - ami-0d9e0d46e6c AMI with drivers for all instar												+	
													Cancel	Previou	s Launch	I

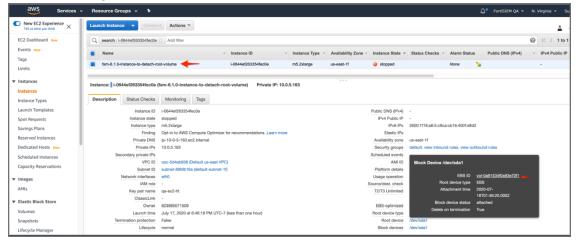
10. Select an existing key pair or create a new key pair. Click Launch Instances.

Select an existing key pair or create a new key pair	×
A key pair consists of a public key that AWS stores, and a private key file that you store. To they allow you to connect to your instance securely. For Windows AMIs, the private key file to obtain the password used to log into your instance. For Linux AMIs, the private key file all securely SSH into your instance.	is required
Note: The selected key pair will be added to the set of keys authorized for this instance. Lea about removing existing key pairs from a public AMI.	Irn more
Choose an existing key pair	~
Select a key pair	
qa-ec2-ht	~
✓ I acknowledge that I have access to the selected private key file (qa-ec2-ht.pem), and without this file, I won't be able to log into my instance.	d that
Cancel Launch Ins	stances

11. Navigate to Instances. Select, then stop the instance.

Services .	 Hesource Groups ~ * 									4.	OPEISTEM QA 👻	N. Virginia +
New EC2 Experience Tell us what you think	Launch Instance 💌 Connect	Actions ^	_									
EC2 Dashboard	Q search: i-0644ot263354fec0e O	Connect Get Windows Password										0 K K (
Events New Tags	Name	Create Template From Instance Launch More Like This	tance ID	 Instance Type 	Availability Zone ~	Instance State *		Alarm Status	Public DNS (IPv4)	 IPv4 Public IP 	 IPv6 IPs 	
Limits	fsm-6.1.0-instance-to-detach-root-v		Start	m5.2xlarge	us-east-1f	🥥 running	🚡 Initializing	None	ec2-35-175-133-162.co	35.175.133.162	2 2600:1118:	a6.5:c9 q
		Instance Settings										
▼ Instances												
Instances	Instance: I-0644ef263354fec0e (fsm		Fleboot Terminate	k: ec2-35-175-133-162.0	ompute-1.amazona;	iws.com						
Instance Types	Description Status Checks	CloudWatch Monitoring										
Launch Templates			_									

12. Select, then navigate to the root volume.



13. Click Actions > Detach Volume.

aws Services	 Resource Gro 	oups v 🔸											4	FortiSIEM QA	 N. Virginia 	• Suppo	rt =
New EC2 Experience Tell us what you think	Create Volume	Actions ^														40	\$ E
EC2 Dashboard New	Q, search : vi	Modify Volume Create Snapshor													0 K	1 to 1 of	\rightarrow \rightarrow
Events New	Name Name	Delete Volume Attach Volume			Size	- Volume Type	- IOPE-	Snapshot	Created	- Availability 2	lone - State	^ Ala	rm At	tachment Informat	ion		
Tags Limits	fsm-531-lo	-6 Detach Volume		dca	80 GiB	gp2	240	snap-07a1350	July 19, 2020 at 6:3.	us-east-1f	🥥 in-us	e N	Ъ н	000e47877554754	3 (fsm-531-to-6	10-migrate) :/d	ev/sda1 (att
Instances		Force Detach Vo Change Auto-En															
Instances		Add/Edit Tags															
Instance Types																	
Launch Templates																	
Spot Requests																	
Savings Plans																	
Reserved Instances																	
Dedicated Hosts New																	
Scheduled Instances																	
Capacity Reservations																	
Images	Description	Status Unecks	Monitoring	rags													
AMIs		Volume ID		64795edca						Outposts ARN							
		Alarm status									80 GiB						
 Elastic Block Store 			snap-07a135	00622267403	3						July 19, 2020 at	6:31:21 PM U	TC-7				
Volumes		Availability Zone	Us-east-1f Not Encrypte						111	State hment information	in-use			-migrate);/dev/sda1	(attached)		
Snapshots		KMS Key ID							Attach	Volume type		** 0*3 (f97)-00	1-10-610	-mgruny/devisida:	persected)		
Lifecycle Manager		KMS Key Aliases									marketplace: 8le	8m7a/049q4h	c2kte2tm	wila T			

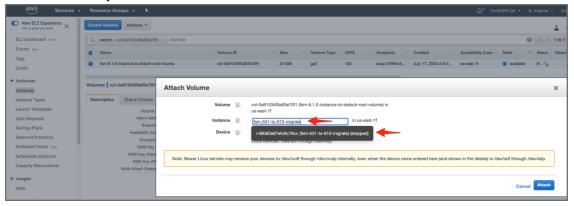
14. Click Yes, Detach in the popup window. Wait for the instance state to be Available.

651166 Mantis Services		
New EC2 Experience Tell us what you think	Create Volume Actions *	2
EC2 Dashboard New	Q search : vol-0x315340x30a7011	@ K < 1
Events New Tags	Name Volume ID Size Volume Type + IOP5 Snapshot Created Availability Zone + State	Alarm A
Limits	📕 fam 8.1.0-instance-to-detach-root-volume vol-Casi+1534/DatKle70f1 25 G/B gp2 100 snap-0789404 July 17, 2020 at 8.4 us-east-1f 🥥 in	Huse N's H
 Instances 	Volumes: vol-0a91554f0atDe7011 (fam-6.1.0-instance-to-detach-root-volume)	
Instance Types	Description Status Checks Monitoring Tags Detach Volume X	
Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Item Scheduled Instances Capacity Reservations	Waters Box var-Bell/SNR/BS/RT A	cot-volume):/dev/sda1
	Nuti-Attach Enabled No	

15. Click Actions > Attach Volume.

aws Services	- Resource Groups 🗸 🔹					Δ • ۱	ortiSIEM QA 👻	N. Virginia	v Sup
New EC2 Experience Tell us what you think	Create Volume Actions ^								Δ.
EC2 Dashboard New	Q, search : vol- Create Snapsho							0 K <	1 to 1
Events New Tags	Name Delete Volume Attach Volume		Volume ID ~	Size - Volume Typ	e - IOPS - Snapshot -	Created ~ Availability Zone	- State	^ Alarm	Attach
Tags Limits	fsm-6.1.0-ins Detach Volume Force Detach V		vol-0a91534f0a93a70f1	25 GiB gp2	100 snap-07894o4	July 17, 2020 at 6:4 us-east-1f	 available 	N	
 Instances Instances 	Volumes: vol-0at Add/Edit Tags	nable IO Setting	tach-root-volume)						
Instance Types	Description Status Checks	Monitoring Tags							
Launch Templates	Volume II	D vol-0a91534f0a93e70f1			Outposts ARN				
Spot Requests	Alarm statu	s None			Size	25 GIB			
Savings Plans		snap-07894o407375ab841	1		Created				
Reserved Instances	Availability Zone Encryption	e us-east-1f n Not Encrypted			State Attachment information	available			
Dedicated Hosts New	KMS Key II				Volume type	gp2			
Scheduled Instances	KMS Key Aliaser	6			Product codes				
Capacity Reservations	KMS Key ARM Multi-Attach Enabled				IOPS	100			
▼ Images									

16. Enter the name of your 5.3.0, 5.3.1 or 5.3.2 instance in the Instance search box and select it.



17. Enter the Device as /dev/sda1 and click Attach.

aws Services	Resource Groups 🗸 🔭 🖈 🗘		* Support
New EC2 Experience Tell us what you think	Create Volume Actions *		∆ ⊕
EC2 Dashboard New	Q search : vol-Ga91554f0at0e7011	0 K <	1 to 1 of 1
Events New	Name - Volume ID - Size - Volume Type - IOPS - Snapshot - Created - Availability Zone - State	+ Alarm	Attachmen
Tags Limits	tem-6.1.0-instance-to-detach-root-volume vol-0a915340a9307011 25 G-B gp2 100 snap-9789404 July 17, 2020 at 6.4 us-east-11 envilable	ie N');	
▼ Instances Instances	Volume: vol-0utr1554/f0utr304/707 Attach Volume		×
Instance Types	Description Status Checks Volume () vol-0a91554fta93e70f1 (fsm-8.1.0-instance-to-detach-root-volume) in		
Launch Templates Spot Requests	Volume us-east-11 Alem stat Instance () Loge-stue?74cf-278cc () in us-east-11		
Savings Plans Reserved Instances	Singapi Availability Zin Device () (devi/daf Encrypti Linux Devices: (devi/daf through /devi/adp		
Dedicated Hosts New Scheduled Instances	KMS Key KMS Key Alase Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through	h /dev/sdp.	1
Capacity Reservations	KNIS KNJ AH Mulli-Attach Enabl	1	
▼ Images AMIs	Car	Attach	
▼ Elastic Block Store			

18. Create a new 100GB volume for /opt in the same availability zone where your 5.3.0, 5.3.1 or 5.3.2 instance is running. Click **Create Volume**.

aws Services - Re	asource Groups 👻 🔭
Create Volume	
Volume Type	General Purpose SSD (gp2) 👻 🖲
Size (GiB)	100 (Min: 1 GiB, Max: 16384 GiB)
IOPS	300 / 3000 (Baseline of 3 IOPS per GIB with a minimum of 100 IOPS, burstable to 3000 IOPS)
Availability Zone*	us-easi-11 🗸 🗸
Throughput (MB/s)	Not applicable 🚯
Snapshot ID	Select a snapshot - C 0
Encryption	Encrypt this volume
	Key (128 characters maximum) Value (256 characters maximum) Name 6.1.0-100GB-opt-volume) 🖏
	Add Tag 49 remaining (Up to 50 tags maximum)
* Required	Cancel Create Volume

19. Navigate to **Volumes**, then click **Actions > Attach Volume**.

dWS Services v	Resource Grou	ıps∨ 1×										tISIEM QA 👻	N. VI
New EC2 Experience Tell us what you think	Create Volume	Actions ^		_									
EC2 Dashboard New	Q, Volume ID :	Modify Volume Create Snapshot											0
Events New	Name	Delete Volume			Volume ID	- Size	Volume Type -	IOPS .	Snapshot -	Created ~	Availability Zone	State	
Tags	6.1.0-100GE			_	vol-0cbb01709256f04b7	100 GiB	gp2	300		July 17, 2020 at 7:1	us-east-1f	 availabi 	
Limits		Force Detach Vol			10-0000110020010401	100 010	Shor.	000		ooy 11, 2020 at 1111	00-0001-11	- aronaur	- 1
▼ Instances		Change Auto-En Add/Edit Tags											
Instances		Abdreak light											
Instance Types													
Launch Templates	Volumes: Vol-00	bb01709256f04b7	(6.1.0-100GB-	ont-volume)									
Spot Requests			(
Savings Plans	Description	Status Checks	Monitoring	Tags									
Reserved Instances		Volume ID	vol-0cbb017	09256f04b7					Outposts ARN	-			
Dedicated Hosts New		Alarm status							Size	100 GiB			
Scheduled Instances		Snapshot							Created		0 PM UTC-7		
Capacity Reservations		Availability Zone	us-east-1f Not Encrypte						State ttachment information	available			
		KMS Key ID	NOT ENDTYPOI	0					Volume type	ap2			
▼ Images		KMS Key Aliases							Product codes				
AMIs		KMS Key ARN							IOPS	300			
▼ Elastic Block Store		Multi-Attach Enabled	No										

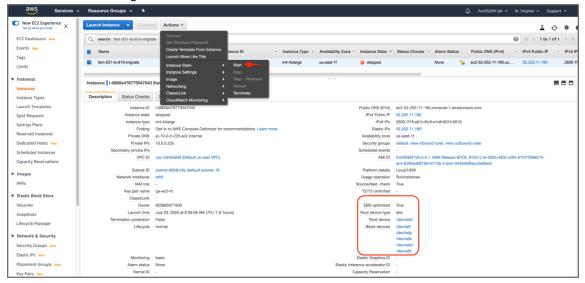
20. Navigate to Instances page and select the 5.3.0, 5.3.1 or 5.3.2 instance that you want to migrate to 6.1.0.

GS1166 Mantis																
New EC2 Experience Tell us what you think	• ×	Create Volume	Actions ~													
EC2 Dashboard New		Q Volume ID	: vol-0cbb01709256f0	4b7 🔿 Add fi	Iter											0
Events New		Name				Volume ID	- Size		Volume Type -	IOPS	- Snapshot	- Created		Availability Zor	ne - State	^
Tags		610-1000	B-opt-volume			vol-0cbb01709256f04b7	100 Gil		gp2	300		July 17, 202			avai	ilable
Limits		()				101 0000011 0000010101			97-						0 010	
▼ Instances																
Instances						Attach Volume							,	×		
Instance Types						Attach volume							,	^		
Launch Templates		Volumes: vol-0	0cbb01709256f04b7	(6.1.0-100GB-	opt-volume		Volume (Ð	vol-0cbb0170925	56f04b7 (6.1	0-100GB-opt-volu	me) in us-east-1f				
Spot Requests							Instance (D	fsm-531-to-610	-migrate		in us-east-1f				
Savings Plans		Description	Status Checks	Monitoring	Tags		Device (Ð								
Reserved Instances				vol-0cbb017	09256f04b7		Device	U	1-06b83e87etcs	9c78cc (fsm	-531-to-610-migrat	e) (stopped)				
Dedicated Hosts New			Alarm status										_			
Scheduled Instances			Snapshot Availability Zone									Cancel	Attach	ЛС-7		
Capacity Reservations				Not Encrypte	ed						Attachment informa	ation				
▼ Images			KMS Key ID									type gp2				
AMIs			KMS Key Aliases								Product co					
MMIS			KMS Key ARN Multi-Attach Enabled	Al.							Þ	OPS 300				
▼ Elastic Block Store			mun-Anaon Enabled	140												
Volumes																
Coonchote																

Boot Up the 5.3.0, 5.3.1 or 5.3.2 Instance and Migrate to 6.1.0

Follow these steps to complete the migration process:

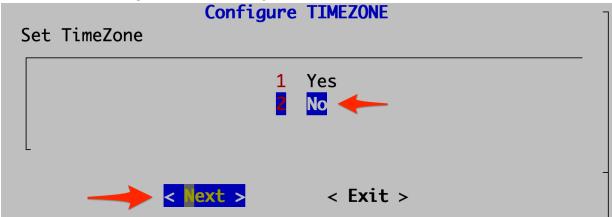
1. Start the instance using Actions > Instance State > Start.



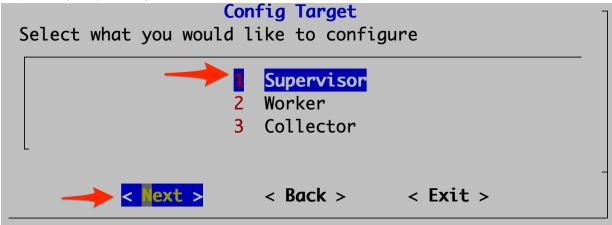
2. Use the /svn partition noted earlier and mount it to /mnt. This contains the backup of the 5.3.0, 5.3.1 or 5.3.2 system settings that will be used during migration. Copy the 5.3.0, 5.3.1 or 5.3.2 settings that were previously backed up and umount /mnt. For example:

```
# mount /dev/xvdg1 /mnt
# mkdir /restore-53x-settings
# cd /restore-53x-settings
# rsync -av /mnt/53x-settings/. .
# ln -sf /restore-53x-settings /images
# umount /mnt
```

- **3.** Run the command configFSM. sh script to open the configuration GUI:
 - a. Select 2 No in the Configure TIMEZONE dialog. Click Next.



b. In **Config Target**, select your node type: Supervisor, Worker, or Collector. This step is usually performed on Supervisor (**1 Supervisor**). Click **Next**.



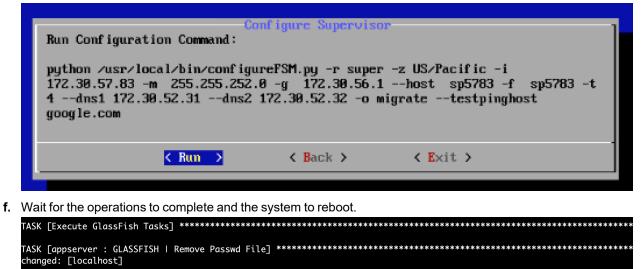
c. In Configure Supervisor, select the 6 migrate_6_1_0 operation. Click Next.

Configure Supervisor							
Select Operation							
2 3 4	<pre>install_without_fips install_with_fips enable_fips disable_fips change_ip migrate_6_1_0</pre>						
< Next >	< BACK >	< Exit >					

d. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a ping. The host can either be an internal host or a public domain host like google.com. Click **Next**.

Enter host for checking	<mark>igure Super∨i</mark> s ng network cor		
myhost.com_			
< Next >	< Back >	< Exit >	

e. Click **Run** on the confirmation page once you make sure all the values are correct. The options are described in the table here.



TASK [reboot : Reboot the machine] ************************************
TASK [reboot : Wait for machine to come back] ************************************
Connection to ec2-52-202-11-180.compute-1.amazonaws.com closed by remote host.
Connection to ec2-52-202-11-180.compute-1.amazonaws.com closed.

g. Wait for about 2 minutes before logging in to the system. Wait another 5-10 minutes for all of the processes to start up. Execute the phstatus command to see the status of FortiSIEM processes.

\$ ssh ec2-user@ec2-52-202-11-180.compute-1.amazonaws.com
Last login: Mon Jul 20 14:54:35 2020 from 69.181.213.37
[ec2-user@fsm-531-to-610-migrate ~]\$ sudo su -
Last login: Mon Jul 20 14:54:39 EDT 2020 on pts/0
[root@fsm-531-to-610-migrate ~]# phstatus.py
System uptime: 14:55:11 up 2 min, 1 user, load average: 1.55, 0.84, 0.33
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 16 cores, 0.2%us, 0.1%sy, 0.0%ni, 99.6%id, 0.0%wa, 0.1%hi, 0.0%si, 0.0%st
Mem: 65675424k total, 9388188k used, 56287236k free, 9184k buffers
Swap: 26058744k total, 0k used, 26058744k free, 2493084k cached

PROCESS	UPTIME	CPU%	VIRT_MEM	RES_MEM
phParser	00:55	0	2161m	585m
phQueryMaster	00:55	0	954m	74m
phRuleMaster	00:55	0	638m	56m
phRuleWorker	00:55	0	1357m	281m
phQueryWorker	00:55	0	1377m	277m
phDataManager	00:55	0	1196m	60m
phDiscover	00:55	0	516m	67m
phReportWorker	00:55	0	1420m	90m
phReportMaster	00:55	0	558m	58m
phIpIdentityWorker	00:55	0	1030m	57m
phIpIdentityMaster	00:55	0	492m	50m
phAgentManager	00:55	0	1452m	53m
phCheckpoint	00:55	0	325m	33m
phPerfMonitor	00:55	0	809m	82m
phReportLoader	00:55	0	763m	277m
phBeaconEventPackager	00:55	0	1129m	64m
phDataPurger	00:55	0	583m	60m
phEventForwarder	00:55	0	549m	45m
phMonitor	00:58	0	1455m	612m
Apache	02:33	0	311m	15m
Node.js-charting	02:26	0	913m	84m
Node.js-pm2	02:26	0	0	7164
AppSvr	02:24	0	15111m	2852m
DBSvr	02:33	0	317m	30m
phAnomaly	00:56	0	1495m	67m
phFortiInsightAI	02:33	0	23425m	296m
Redis	02:26	0	53m	22m

h. Remove the restored settings directories because you no longer need them, for example:

- # rm -rf /restore-53x-settings
- # rm -rf /svn/53x-settings
- # rm -f /images

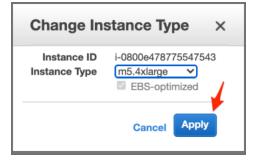
(Optional) Change Instance Type to the Latest Generation

If you would like to change the instance type to one in the current generation for higher performance, this is a good time to do it. 5.3.0, 5.3.1 or 5.3.2 and earlier versions do not support m5 (AWS Nitro) instance types. FSM 6.1.0 supports all instance types that have the recommended vCPU/memory levels. This step may require a reset of FortiSIEM license for the UUID change.

New EC2 Expe 4 0 0 0 EC2 Dashb 0 1 to 1 of 1 Q, Events New Nam IPv4 Public IP IPv6 IP Public DNS (IPv4 Tags **fsm-53** stop ec2-52-202-11-180.co. 2600:1f Limits ▼ Instance ... Instances Instance Typ Launch Templat ec2-52-202-11 52.202.11.180 Spot Requests IPv6 IPs Bastic IPs 2600:1f18:a6:5:d5c5:e1e6:6074:6019 Savings Plans Opt-in to 52,202,11 served Ins p-10-0-5-225.ec2.in ast-1f 10.0.5.225 Dedicated Hosts default, view Private IPs Scheduled In: VPC ID VDC AMI ID Capacity Reservat ▼ Images AMIs IAM role qa-ec2-ht Elastic Block Store Volumes July 20, False Snapshots Lifecycle Ma Network & Security Security Gro Elastic IPs New basic None

To do this, stop the instance and change instance type as follows, then start the instance again.

Select the **Instance Type** from the drop-down list and click **Apply**.



Migrate Cluster Installation

This section provides instructions on how to migrate Supervisor, Workers, and Collectors separately in a cluster environment,

- Delete Workers
- Migrate Supervisor
- Install New Worker(s)
- Register Workers
- Set Up Collector-to-Worker Communication
- Working with Pre-6.1.0 Collectors
- Install 6.1.0 Collectors
- Register 6.1.0 Collectors

Delete Workers

- 1. Login to the Supervisor.
- 2. Go to Admin > License > Nodes and delete the Workers one-by-one.
- **3.** Go to the **Admin > Cloud Health** page and make sure that the Workers are not present. Note that the Collectors will buffer events while the Workers are down.
- Shutdown the Workers.
 SSH to the Workers one-by-one and shutdown the Workers.

Migrate Supervisor

Follow the steps in Migrate All-in-one Installation to migrate the supervisor node. **Note:** FortiSIEM 6.1.0 does not support Worker or Collector migration.

Install New Worker(s)

Follow the steps in Cluster Installation > Install Workers to install new Workers. You can either keep the same IP address or change the address.

Register Workers

Follow the steps in Cluster Installation > Register Workers to register the newly created 6.1.0 Workers to the 6.1.0 Supervisor. The 6.1.0 FortiSIEM Cluster is now ready.

Set Up Collector-to-Worker Communication

- 1. Go to Admin > Systems > Settings.
- 2. Add the Workers to the Event Worker or Query Worker as appropriate.
- 3. Click Save.

Working with Pre-6.1.0 Collectors

Pre-6.1.0 Collectors and agents will work with 6.1.0 Supervisor and Workers. You can install 6.1.0 collectors at your convenience.

Install 6.1.0 Collectors

FortiSIEM does not support Collector migration to 6.1.0. You can install new 6.1.0 Collectors and register them to 6.1.0 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. Follow these steps:

- 1. Copy the http hashed password file (/etc/httpd/accounts/passwds) from the old Collector.
- 2. Disconnect the pre-6.1.0 Collector.
- 3. Install the 6.1.0 Collector with the old IP address by the following the steps in Cluster Installation > Install Collectors.
- 4. Copy the saved http hashed password file (/etc/httpd/accounts/passwds) from the old Collector to the 6.1.0 Collector. This step is needed for Agents to work seamlessly with 6.1.0 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.0 migration, this password is lost.

Register 6.1.0 Collectors

Follow the steps in Cluster Installation > Register Collectors, with the following difference: in the phProvisionCollector command, use the --update option instead of --add. Other than this, use the exactly the same parameters that were used to register the pre-6.1.0 Collector. Specifically, use this form of the

phProvisionCollector command to register a 6.1.0 Collector and keep the old associations:

The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

Re-install new Windows Agents with the old InstallSettings.xml file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.





Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet shall be change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.