McAfee ePolicy Orchestrator on AWS

Quick Start Reference Deployment

July 2018
Last update: August 2020 (revisions)

McAfee, Inc.
AWS Quick Start Reference Team

Contents

This guide was created by Amazon Web Services (AWS) in collaboration with McAfee, Inc.

Quick Starts are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices. Amazon may share who uses AWS Quick Starts with the AWS Partner Network (APN) Partner that collaborated with AWS on the content of the Quick Start.

Overview

This Quick Start deployment guide discusses architectural considerations, configuration steps, and best practices for deploying McAfee ePolicy Orchestrator (McAfee ePO) on the AWS Cloud using Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC), and Amazon Relational Database Service (Amazon RDS).

It also provides links for viewing and launching AWS CloudFormation templates that you can launch directly into your AWS account to automate the deployment. You can use these AWS CloudFormation templates to deploy McAfee ePO and its supported products to suit your specific business needs.

This guide is for IT infrastructure architects, administrators, and DevOps professionals who are planning new deployments of McAfee ePO on the AWS Cloud. It provides IT infrastructure decision-makers and system administrators with technical guidance on how to configure, deploy, and run McAfee ePO in a highly available manner on AWS. It also outlines a reference architecture for McAfee ePO that addresses common scalability, high availability, and security requirements.

McAfee ePO is an extensible platform that enables centralized management and enforcement of your security policies. It performs network management by detecting threats and helping to protect endpoints against these threats.

By using McAfee ePO, you can perform many network and client tasks, including:

- Managing and enforcing network and endpoint security, by using the Policy Assignments and Client Tasks functionality in the platform.
- Monitoring the health of your network.

- Collecting data on events and alerts.
- Creating reports, by using the Queries and Reports feature, which displays configurable charts and tables of your network security data.
- Automating product deployments, patch installations, and security updates.

For more information, see the McAfee documentation.

McAfee ePolicy Orchestrator on AWS

Use this Quick Start to deploy McAfee ePO on AWS. In less than an hour, you can use a single console—the McAfee ePO console—to manage endpoint security, data loss prevention, encryption, server security in the public cloud, and the information-sharing Data Exchange Layer (DXL).

By using the components that make up the McAfee ePO security management platform:

- You can manage a comprehensive threat defense lifecycle, so that you can protect, detect, and correct from a common view across your IT environment.
- Gain global, contextual visibility into changing events, with a cross-product, command and control core.
- Intelligently connect dynamic context from the McAfee Global Threat Intelligence service, enterprise risk, and system security posture in real time.

This interlacing of threat intelligence and risk management instantly blocks damaging attacks and enables you to adjust your security posture as risks change.

For in-depth information about installing and using McAfee ePO, see the McAfee ePO documentation.

Costs and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The cost of the resources created by the Quick Start varies based on how many instances you want to protect and the products that are being managed. Prices are subject to change. See the pricing pages for each AWS service that you will be using in this Quick Start for full details.

Bring Your Own License (BYOL) is the supported licensing option with this Quick Start–based deployment. By using this Quick Start reference deployment, you agree to terms and conditions outlined in the product End User License Agreement (EULA).

You can use your current, valid license for McAfee ePO. To purchase products that McAfee ePO manages, please contact McAfee Sales or a McAfee authorized partner or reseller.

Architecture

Deploying this Quick Start for a new virtual private cloud (VPC) with **default parameters** builds the following McAfee ePolicy Orchestrator environment in the AWS Cloud.

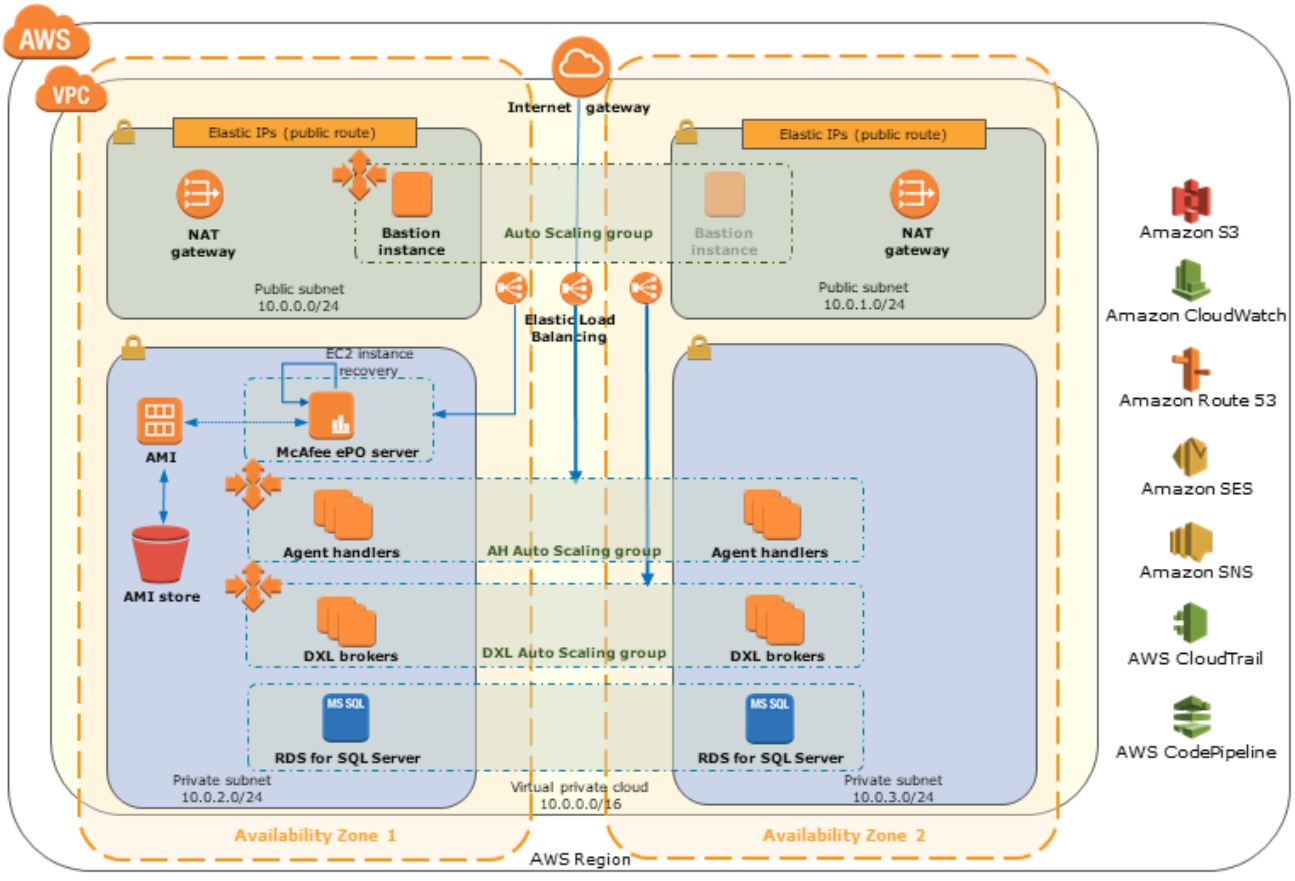

Figure 1: Quick Start architecture for McAfee ePolicy Orchestrator on AWS

The Quick Start sets up the following:

- A highly available architecture that spans two Availability Zones.
- A VPC configured with public and private subnets according to AWS best practices, to provide you with your own virtual network on AWS.

- An internet gateway to allow access to the internet. This gateway is used by the bastion hosts to send and receive traffic.
- In the public subnets, managed NAT gateways to allow outbound internet access for resources in the private subnets.
- In the public subnets, a Linux bastion host in an AWS Auto Scaling group to allow inbound Secure Shell (SSH) access to EC2 instances in public and private subnets.
- In the private subnets, a McAfee ePO server.
- In the private subnets, Agent Handlers in an Auto Scaling group.
- In the private subnets, DXL brokers in an Auto Scaling group.
- In the private subnets, Amazon Relational Database Service (Amazon RDS) for Microsoft SQL Server.

Prerequisites

Specialized Knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see Getting Started with AWS.)

- Amazon CloudWatch
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Route 53
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Email Service (Amazon SES)
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS Auto Scaling
- AWS Certificate Manager (ACM)
- AWS CloudFormation
- AWS CodePipeline
- AWS Identity and Access Management (IAM)
- AWS Lambda
- Elastic Load Balancing

Supported Regions and Availability Zones

Before you deploy the AWS CloudFormation template, familiarize yourself with AWS Regions, Availability Zones, and endpoints, which are components of the AWS secure global infrastructure. For more information about AWS Regions, Availability Zones, and endpoints, see the AWS documentation.

You can launch the McAfee ePO on AWS Quick Start in many regions across the Americas, Europe, and Asia Pacific. If you have an AWS GovCloud (US) account, you can also launch this Quick Start in the AWS GovCloud (US) region. For the latest list of regions supported, see the McAfee Knowledge Base article.

Deployment Options

This Quick Start provides the following deployment options:

- **Deploy McAfee ePolicy Orchestrator into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, bastion hosts, and other infrastructure components, and then deploys McAfee ePolicy Orchestrator into this new VPC.
- **Deploy McAfee ePolicy Orchestrator into an existing VPC**. This option provisions McAfee ePO in your existing AWS infrastructure.
- **AWS GovCloud (US) Region—Deploy McAfee ePolicy Orchestrator into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, bastion hosts, and other infrastructure components, and then deploys McAfee ePolicy Orchestrator into this new VPC.
- **AWS GovCloud (US) Region—Deploy McAfee ePolicy Orchestrator into an existing VPC**. This option provisions McAfee ePO in your existing AWS infrastructure.

The Quick Start provides separate templates for these options. It also lets you configure CIDR blocks, instance types, and McAfee ePolicy Orchestrator settings, as discussed later in this guide.

Deployment Steps

Step 1. Prepare Your AWS Account

1. If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.

2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy McAfee ePolicy Orchestrator on AWS. For the latest list of regions supported, see the McAfee Knowledge Base article.
3. Create a key pair in your preferred region.
4. If necessary, request a service quota increase for the Amazon EC2 instance types you plan to use for the bastion host and McAfee ePO server instances as well as other AWS resources, such as Amazon RDS and the VPC that you intend to deploy.

   You might need to do this if you already have an existing deployment that uses this instance type, and you think you might exceed the default quota with this deployment.

Step 2. Launch the Quick Start

> **Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see deployment options earlier in this guide.

Option 1	Option 2
Deploy McAfee ePO into a new VPC on AWS	**Deploy McAfee ePO into an existing VPC on AWS**
Launch	Launch

   If you have an AWS GovCloud (US) account, you can use one of the following options to launch the Quick Start in the AWS GovCloud (US) Region.

Option 1	Option 2
Deploy into a new VPC in AWS GovCloud (US) Region	**Deploy into an existing VPC in AWS GovCloud (US) Region**
Launch	Launch

> **Important** If you're deploying McAfee ePO into an existing VPC, make sure that your VPC has two private subnets in different Availability Zones for the database instances. These subnets require NAT gateways or NAT instances in their route tables, to allow the instances to download packages and software without exposing them to the internet. You will also need the domain name option configured in the DHCP options as explained in the Amazon VPC documentation. You will be prompted for your VPC settings when you launch the Quick Start.

2. Check the region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for McAfee ePO will be built. The template is launched in the US West (Oregon) Region by default.
3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

   In the following tables, parameters are listed by category and described separately for the following deployment options:

   - Parameters for deploying McAfee ePO into a new VPC
   - Parameters for deploying McAfee ePO into an existing VPC

> **Note** The templates and parameters for deploying to the GovCloud (US) Region, are similar to those for other regions. However, as indicated in the descriptions of the following tables, certain parameters aren't available in the GovCloud (US) Region.

- **Option 1: Parameters for deploying McAfee ePO into a new VPC**

  View template

  View template: GovCloud (US) Region

  Network Configuration:

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	*Requires input*	The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.
VPC CIDR (VPCCIDR)	10.0.0.0/16	The CIDR block to create the VPC (e.g., 10.0.0.0/16).
Private Subnet 1 CIDR (PrivateSubnet1CIDR)	10.0.2.0/24	The CIDR block to create the private subnet in Availability Zone 1 (e.g., 10.0.2.0/24).
Private Subnet 2 CIDR (PrivateSubnet2CIDR)	10.0.3.0/24	The CIDR block to create the private subnet in Availability Zone 2 (e.g., 10.0.3.0/24).
Public Subnet 1 CIDR (PublicSubnet1CIDR)	10.0.0.0/24	The CIDR block to create the public subnet in Availability Zone 1 (e.g., 10.0.0.0/24).
Public Subnet 2 CIDR (PublicSubnet2CIDR)	10.0.1.0/24	The CIDR block to create the public subnet in Availability Zone 2 (e.g., 10.0.1.0/24).
External Bastion Access CIDR (RemoteAccessCIDR)	*Requires input*	The CIDR block that's allowed external SSH access to the bastion hosts, e.g., x.x.x.x/16-28. We recommend that you set this value to a trusted CIDR block. For example, you might want to restrict access to your corporate network.

  McAfee ePolicy Orchestrator Platform Configuration:

Parameter label (name)	Default	Description
Number of Endpoints (ProtectedInstances)	1-10K	The number of endpoints that you want to manage.
Deployment Environment (Environment)	Production	The targeted deployment environment.
Domain Name (DomainName)	—	[Optional] Amazon Route 53 registered domain name (e.g., mcafee.com). We recommend that you either register the Amazon Route 53 domain name so that public DNS records can be propagated automatically OR add the sub domain name server records into your main domain server. **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.

Parameter label (name)	Default	Description
Sub Domain Name (SubDomainName)	*Requires input*	The non-existent sub domain name to be used for the management solution (e.g., manage.mcafee.com). We recommend that you either register the Amazon Route 53 domain name so that public DNS records can be propagated automatically OR add the sub domain name server records into your main domain server. **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.
High Availability (Availability)	Yes	We recommend selecting **Yes** for production environments. It is applicable for Agent Handlers, Data Exchange Layer (DXL) brokers, and Amazon RDS.
AWS Key Pair Name (KeyPairName)	*Requires input*	The name of an existing public/private key pair. If you do not have one to select, you need to create one. This is required to securely connect to instances.

On-Premises Domain Configuration:

Parameter label (name)	Default	Description
On Premises Domain Name (OnPremiseDomainName)	—	[Optional] The on-premises domain name that you want to resolve from inside the VPC (e.g., mcafee.com). This is required for DNS resolution between the ePO instance in the VPC and on-premises services like LDAP (ldap.mcafee.com). **Note** This is only required if you are planning to use Microsoft Active Directory and if you are planning to use a domain name instead of an IP address for the LDAP server.
On Premises Server DNS (OnPremiseServerDNS)	—	[Optional] The on-premises DNS (e.g., 192.168.1.1) that will be used to resolve the domain name queries. This is required for DNS resolution between the ePO instance in the VPC and services like LDAP (ldap.mcafee.com). **Note** This is only required if you are planning to use Microsoft Active Directory and if you are planning to use a domain name instead of an IP address for the LDAP server.

ePO Application Server Configuration:

Parameter label (name)	Default	Description
Enable FIPS Mode (FIPSEnabled)	No	Allow the ePO and Agent Handlers to be installed in FIPS mode.
License Key (EPOLicenseKey)	—	The McAfee ePO license key (xxx-xxx-xxx-xxxx) that you enter. If you don't enter a license key, the environment will launch in evaluation mode.
Admin Username (EPOAdminUserName)	*Requires input*	Your global administrator user name that you create for logging in to the McAfee ePO console.
Admin Password (EPOAdminPassword)	*Requires input*	Your global administrator password that you create for logging in to the McAfee ePO console. The password must be a minimum of 8 characters and contain alpha, numeric, and a special character.
Confirm Admin Password (ConfirmEPOAdmin Password)	*Requires input*	Your global administrator password that you confirm for logging in to the McAfee ePO console. The password must be a minimum of 8 characters and contain alpha, numeric, and a special character.
DR Passphrase (EPOPassphraseDR)	*Requires input*	The keystore encryption passphrase that you create, which is required for disaster recovery. The server recovery passphrase must be 14 to 200 characters in length. It must not contain backslashes (\), spaces, or any double quotes (").
Confirm DR Passphrase (ConfirmEPO PassphraseDR)	*Requires input*	The keystore encryption passphrase that you confirm. This is required for disaster recovery. The server recovery passphrase must be 14 to 200 characters in length. It must not contain backslashes (\), spaces, or any double quotes (").
Console Port (EPOConsolePort)	8443	The secure port number to access the McAfee ePO console.
Enable Product Improvement Program (TelemetryOption)	Yes	Allows the collection of product performance and usage information to help McAfee provide better products and services.
Load Balancer Certificate ARN (EPOELBCertificateARN)	—	[Optional] The Amazon Resource Name (ARN) of the certificate stored in AWS Certificate Manager (ACM) or imported in AWS IAM. Generally, the certificate associated with the sub domain needs to be presented. The certificate will be attached with the Application Load Balancer for McAfee ePO (e.g., arn:aws:*:us-west-1:*:certificate/* or arn:aws-us-gov:*:us-west-1:*:certificate/*). **Note** For production servers, we recommend attaching the certificate with the Application Load Balancer for McAfee ePO.
External Access CIDR (EPOAccessCIDR)	*Requires input*	The CIDR block that's allowed external access to the McAfee ePO console (e.g., x.x.x.x/16-28). We recommend that you set this value to a trusted CIDR block. For example, you might want to restrict access to your corporate network.

ePO Database - Amazon RDS for SQL Server Configuration:

Parameter label (name)	Default	Description
DB Master Username (DBMasterUsername)	*Requires input*	The login ID that you create for the master user of the database. The ID must contain 2 to 8 characters.
DB Master Password (DBMasterUserPassword)	*Requires input*	The password that you create for the master user of the database. This password can contain any printable ASCII character except "/", """, or "@" and must contain 8 to 255 characters.
Confirm DB Master Password (ConfirmDBMasterUser Password)	*Requires input*	The password that you confirm for the master user of the database. This password can contain any printable ASCII character except "/", """, or "@" and must contain 8 to 255 characters.
DB Port (DBPort)	1433	The TCP/IP port that the database instance will use for application connections.
Allocated Storage (DBAllocatedStorage)	—	Applies to a new database instance. Specify how much storage to allocate to the McAfee ePO database. Leave it blank to use the default recommended size.
DB Backup Retention Period (DBBackupRetentionPeriod)	7	Applies to a new database instance. The number of days for which automatic database snapshots are retained.
DB Instance Identifier (DBInstanceIdentifier)	—	The existing database instance identifier that you specify. Leave it blank to create a new database instance.

Client Communication Configuration:

Parameter label (name)	Default	Description
Agent Handler Http Port (AHHttpPort)	80	The agent server communication (ASC) http port used by the McAfee Agent to communicate to server.
Agent Handler Port (AHPort)	443	The agent server communication port that the McAfee agent uses to securely communicate to the server.
DXL Port (DXLPort)	8883	The DXL communication port that the DXL client uses to enable secure messaging to the DXL fabric.
External Access CIDR (ClientAccessCIDR)	*Requires input*	The CIDR block that's allowed to connect from on-premises endpoints to the Agent Handlers/DXL brokers (e.g., x.x.x.x/16-28). Keep default setting to allow roaming endpoints.

Administration Configuration:

Parameter label (name)	Default	Description
Updates for Stack Components (EnableAutoUpdate)	Yes	Recommended. Enables automatic updates of the McAfee server stack components (e.g., Agent Handler, DXL broker). **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.
Application of Updates (AutoApproval)	Automatic	Auto or manual approval to review the change sets on auto updates of stack components. **Note** If you don't want auto approval (i.e. with Update after Approval selected), provide the email address of the approver. This enables notifications to be sent for approval. Otherwise, the approver will have to watch the pipeline periodically for approvals. **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.
Approver Email (ApproverEmailAddress)	—	The email address of the approver where approval of auto updates will be sent, if Application of Updates/AutoApproval is not selected. **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.
Operator Email (AdminEmailAddress)	*Requires input*	The email address where notifications of any operations will be sent. This address is also used for tagging ownership of resources.
Auto Cleanup (AutoCleanup)	Enable	Enables auto cleanup of backup logs and data in Amazon S3.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
S3 Bucket Name (QSS3BucketName)	aws-quickstart	The S3 bucket name for the Quick Start assets. The Quick Start bucket name can include numbers, lowercase letters, uppercase letters, periods (.), and hyphens (-). It cannot start or end with a hyphen (-) or period (.).
S3 Key Prefix (QSS3KeyPrefix)	quickstart-mcafee-epo/	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.'

- **Option 2: Parameters for deploying McAfee ePO into an existing VPC**

  View template

  View template: GovCloud (US) Region

  Network Configuration:

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	*Requires input*	The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.
VPC ID (VPCID)	*Requires input*	The ID of your existing VPC for deployment (e.g., vpc-fd990584).
Private Subnet 1 ID (PrivateSubnet1ID)	*Requires input*	The ID of private subnet 1 in Availability Zone 1 for the McAfee application components (e.g., subnet-a0246dcd).
Private Subnet 2 ID (PrivateSubnet2ID)	*Requires input*	The ID of private subnet 2 in Availability Zone 2 for the McAfee application components (e.g., subnet-b1f432cd).
Public Subnet 1 ID (PublicSubnet1ID)	*Requires input*	The ID of public subnet 1 in Availability Zone 1 for the ELB load balancer (e.g., subnet-9bc642ac).
Public Subnet 2 ID (PublicSubnet2ID)	*Requires input*	The ID of public subnet 2 in Availability Zone 2 for the ELB load balancer (e.g., subnet-e3246d8e),
Bastion Security Group ID (BastionSecurityGroupID)	*Requires input*	The ID of the bastion host security group to enable SSH connections (e.g., sg-7f16e910).

  McAfee ePolicy Orchestrator Platform Configuration:

Parameter label (name)	Default	Description
Number of Endpoints (ProtectedInstances)	1-10K	The number of endpoint instances that you want to manage.
Deployment Environment (Environment)	Production	The targeted deployment environment.
Domain Name (DomainName)	—	[Optional] Amazon Route 53 registered domain name (e.g., mcafee.com). We recommend that you either register the Amazon Route 53 domain name so that public DNS records can be propagated automatically OR add the sub domain name server records into your main domain server. **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.

Parameter label (name)	Default	Description
Sub Domain Name (SubDomainName)	*Requires input*	The non-existent sub domain name to be used for the management solution (e.g., manage.mcafee.com). We recommend that you either register the Amazon Route 53 domain name so that public DNS records can be propagated automatically OR add the sub domain name server records into your main domain server. **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.
High Availability (Availability)	Yes	We recommend selecting **Yes** for production environments. It is applicable for Agent Handlers, Data Exchange Layer (DXL) brokers, and Amazon RDS.
AWS Key Pair Name (KeyPairName)	*Requires input*	The name of an existing public/private key pair. If you do not have one to select, you need to create one. This is required to securely connect to instances.

On-Premises Domain Configuration:

Parameter label (name)	Default	Description
On Premises Domain Name (OnPremiseDomainName)	—	[Optional] The on-premises domain name that you want to resolve from inside the VPC (e.g., mcafee.com). This is required for DNS resolution between the ePO instance that is in the VPC and on-premises services like LDAP (ldap.mcafee.com). **Note** This is only required if you are planning to use Microsoft Active Directory and are planning to use a domain name instead of an IP address for the LDAP server.
On Premises Server DNS (OnPremiseServerDNS)	—	[Optional] The on-premises server DNS (e.g., 192.168.1.1) that will be used to resolve the domain name queries. This is required for DNS resolution between an ePO instance that is in the VPC and on-premises services like LDAP (ldap.mcafee.com). **Note** This is only required if you are planning to use Microsoft Active Directory and are planning to use a domain name instead of an IP address for the LDAP server.

ePO Application Server Configuration:

Parameter label (name)	Default	Description
Enable FIPS Mode (FIPSEnabled)	No	Allow the ePO and Agent Handlers to be installed in FIPS mode.
License Key (EPOLicenseKey)	—	The McAfee ePO license key (xxx-xxx-xxx-xxxx) that you enter. If you don't enter a license key, the environment will launch in evaluation mode.
Admin Username (EPOAdminUserName)	*Requires input*	The administrator user name that you create for logging in to the McAfee ePO console.
Admin Password (EPOAdminPassword)	*Requires input*	The administrator password that you create for logging in to the McAfee ePO console. The password must be a minimum of 8 characters and contain alpha, numeric, and a special character.
Confirm Admin Password (ConfirmEPOAdmin Password)	*Requires input*	The administrator password that you confirm for logging in to the McAfee ePO console. The password must be a minimum of 8 characters and contain alpha, numeric, and a special character.
DR Passphrase (EPOPassphraseDR)	*Requires input*	The keystore encryption passphrase that you create. This is required for disaster recovery. The server recovery passphrase must be 14 to 200 characters in length. It must not contain backslashes (\), spaces, or any double quotes (").
Confirm DR Passphrase (ConfirmEPO PassphraseDR)	*Requires input*	The keystore encryption passphrase that you confirm. This is required for disaster recovery. The server recovery passphrase must be 14 to 200 characters in length. It must not contain backslashes (\), spaces, or any double quotes (").
Console Port (EPOConsolePort)	8443	The secure port number to access the McAfee ePO console.
Enable Product Improvement Program (TelemetryOption)	Yes	Allows the collection of product performance and usage information to help McAfee provide better products and services.
Load Balancer Certificate ARN (EPOELBCertificateARN)	—	[Optional] The Amazon Resource Name (ARN) of the certificate stored in AWS Certificate Manager (ACM) or imported in AWS IAM. Generally, the certificate associated with the sub domain needs to be presented. The certificate will be attached with the Application Load Balancer for McAfee ePO (e.g., arn:aws:*:us-west-1:*:certificate/*). **Note** For production servers, we recommend attaching the certificate with the Application Load Balancer for McAfee ePO.
External Access CIDR (EPOAccessCIDR)	*Requires input*	The CIDR block that's allowed external access to the McAfee ePO console (e.g., x.x.x.x/16-28). We recommend that you set this value to a trusted CIDR block. For example, you might want to restrict access to your corporate network.

ePO Database - Amazon RDS for SQL Server Configuration:

Parameter label (name)	Default	Description
DB Master Username (DBMasterUsername)	*Requires input*	The login ID that you create for the master user of the database. The ID must contain 2 to 8 characters.
DB Master Password (DBMasterUserPassword)	*Requires input*	The password that you create for the master user of the database. This password can contain any printable ASCII character except "/", """, or "@" and must contain 8 to 255 characters.
Confirm DB Master Password (ConfirmDBMasterUser Password)	*Requires input*	The password that you confirm for the master user of the database. This password can contain any printable ASCII character except "/", """, or "@"and must contain 8 to 255 characters.
DB Port (DBPort)	1433	The TCP/IP port that the database instance will use for application connections.
Allocated Storage (DBAllocatedStorage)	—	Applies to a new database instance. Specify how much storage to allocate to the McAfee ePO database. Leave it blank to use the default recommended size.
DB Backup Retention Period (DBBackupRetentionPeriod)	7	Applies to a new database instance. The number of days for which automatic database snapshots are retained.
DB Instance Identifier (DBInstanceIdentifier)	—	The existing database instance identifier that you specify. Leave it blank to create a new database instance.

Client Communication Configuration:

Parameter label (name)	Default	Description
Agent Handler Http Port (AHHttpPort)	80	The agent server communication (ASC) http port used by the McAfee Agent to communicate to server.
Agent Handler Port (AHPort)	443	The agent server communication port that the McAfee agent uses to securely communicate to the server.
DXL Port (DXLPort)	8883	The DXL communication port that the DXL client uses to enable secure messaging to the DXL fabric.
External Access CIDR (ClientAccessCIDR)	*Requires input*	The CIDR block that's allowed to connect from on-premises endpoints to Agent Handlers/DXL brokers. e.g., x.x.x.x/16-28. Keep default setting to allow roaming endpoints.

Administration Configuration:

Parameter label (name)	Default	Description
Updates for Stack Components (EnableAutoUpdate)	Yes	Recommended. Enables auto updates of McAfee server stack components (e.g., Agent Handlers, DXL). **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.
Application of Updates (AutoApproval)	Automatic	Auto or manual approval to review the change sets on auto updates of stack components. **Note** If you don't want auto approval (i.e. with Update after Approval selected), provide the email address of the approver. This enables notifications to be sent for approval. Otherwise, the approver will have to watch the pipeline periodically for approvals. **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.
Approver Email (ApproverEmailAddress)	—	The email address of the approver where approval of auto updates will be sent, if Application of Updates/AutoApproval is not selected. **Note** This parameter is not available when setting up McAfee ePO in the GovCloud (US) region.
Operator Email (AdminEmailAddress)	*Requires input*	The email address where notifications of any operations will be sent. This address is also used for tagging of ownership of resources.
Auto Cleanup (AutoCleanup)	Enable	Enables auto cleanup of backup logs and data in Amazon S3.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
S3 Bucket Name (QSS3BucketName)	aws-quickstart	The S3 bucket name for the Quick Start assets. The Quick Start bucket name can include numbers, lowercase letters, uppercase letters, periods (.), and hyphens (-). It cannot start or end with a hyphen (-) or period (.).
S3 Key Prefix (QSS3KeyPrefix)	quickstart-mcafee-epo/	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.'

Step 3. Test the Deployment

In the AWS CloudFormation console, select the **Outputs** tab. Choose the link for the Website URL key, **ePOConsoleURL**, as shown in Figure 2.

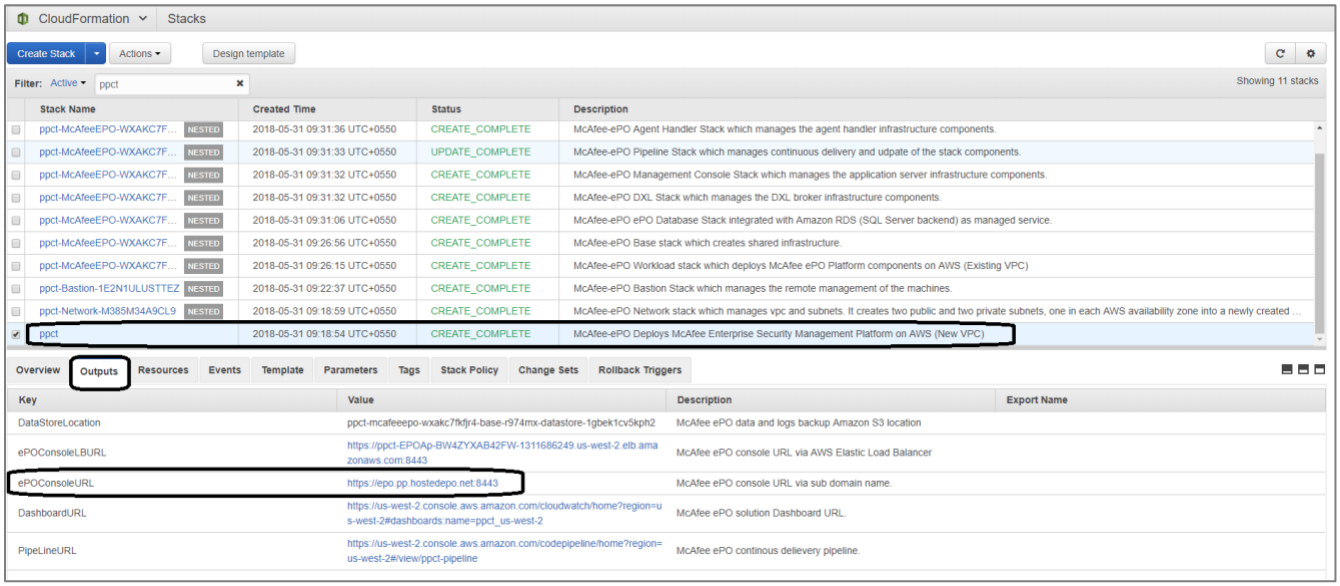

Figure 2: Validating ability to launch the McAfee ePO console

This link launches the McAfee ePO console. After you have validated that you can log in to the console, follow the McAfee ePO documentation to use McAfee ePO.

Best Practices for McAfee ePO on AWS

Complete the installation of your McAfee ePO infrastructure:

1. Use your permanent license key, if applicable. If you created a stack without specifying a BYOL key, McAfee ePO will be set up in evaluation mode. When you buy an ePO license, you can go back to the McAfee ePO console and enter your new license key.
2. Set up your Microsoft Active Directory connection to your VPC running on AWS.

> **Note** Setting up the connection is required if you plan to use McAfee products that rely on data/connection to Active Directory. For details on how to set up a VPN between your VPC running on AWS and Active Directory that your company uses on premises, see the McAfee Knowledge Base article.

3. Deploy the McAfee Agent and Data Exchange Layer (DXL) components to the endpoints you want to protect using either the Client Tasks or Product Deployment feature in the McAfee ePO console.
4. Set up and deploy security products available to install in the McAfee ePO console.

Security

The AWS Cloud provides a scalable, highly reliable platform that helps customers deploy applications and data quickly and securely. When you build systems on the AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

In turn, you assume responsibility and management of the guest operating system (including updates and security patches) and other associated applications, as well as the configuration of the AWS-provided security group firewall. For more information about security on AWS, visit the AWS Security Center.

FAQ

Q. I encountered a CREATE_FAILED error when I launched the Quick Start.

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state will be retained and the instance will be left running, so you can troubleshoot the issue. (Look at the log files in `%ProgramFiles%\Amazon\EC2ConfigService` and `C:\cfn\log`.)

> **Important** When you set **Rollback on failure** to **No**, you will continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For more information, see Troubleshooting AWS CloudFormation on the AWS website.

Q. I encountered a size limitation error when I deployed the AWS CloudFormation templates.

A. We recommend that you launch the Quick Start templates from the location we've provided or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

Q. How do I log in to the console on which the various components of McAfee ePO run?

A. To log in to the console of various ePO components:

- Access the bastion server. Launch a Remote Desktop Protocol (RDP) session to the bastion server. This must be initiated from the computer within your company's network whose IP address range has been allowed to access the bastion server as per the security group configuration.
- Access the McAfee ePO server. Launch an SSH session to the bastion server. Create a tunnel the ePO server IP as the destination host. This opens the ePO server console.
- Access the Agent Handler servers. Launch an SSH session to the bastion server. Create a tunnel with the destination host being the Agent Handler server IP. This opens the Agent Handler server console.
- Access the DXL servers. Launch an SSH session to the bastion server. Copy the key file to the bastion server. Connect via SSH from the bastion server to the DXL server IP using the key copied.

Q. How can I access logs of the different components of McAfee ePO if I need to pass them to McAfee technical support team for any support cases?

A. The logs of all key components of McAfee ePO components are replicated from the individual EC2 instances into Amazon CloudWatch, and are backed up daily into your S3 bucket. This S3 bucket is created in your account at the time of McAfee ePO stack creation. You can find the name of the S3 bucket in the **Output**s tab of the first/master stack that has been created, as shown in Figure 3.

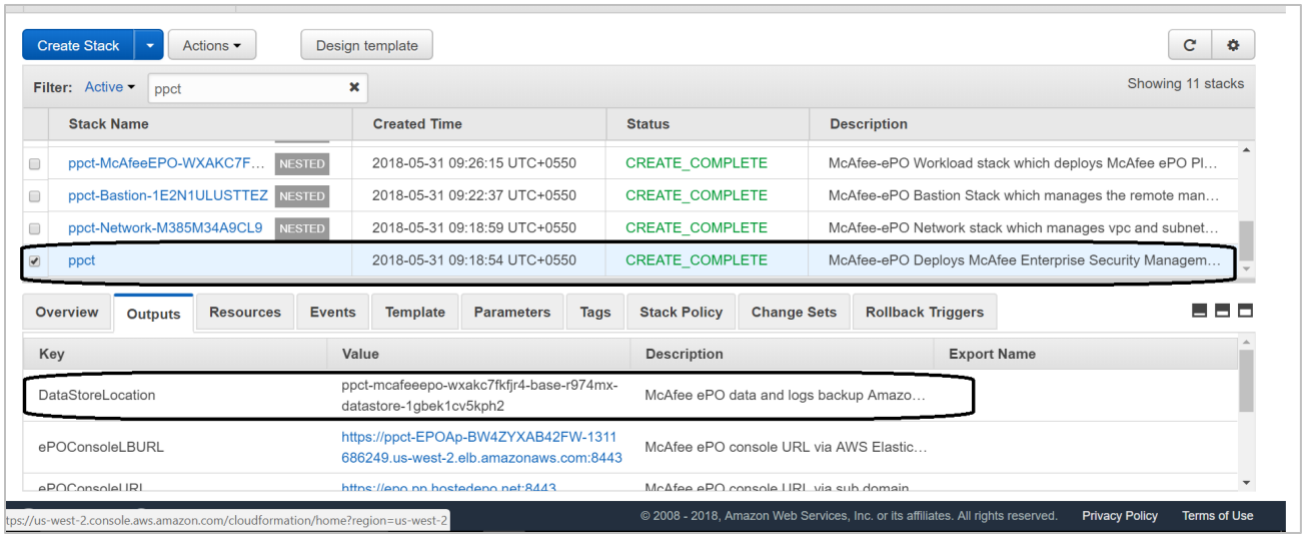

Figure 3: Data store location of McAfee ePO data and logs

Known Issues

For known issues related to setting up McAfee ePO on AWS and using McAfee ePO to manage security, see the McAfee Knowledge Base article.

Git Repository

You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Additional Resources

AWS services

- Amazon EC2
  https://aws.amazon.com/documentation/ec2/
- Amazon Route 53
  http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/
- Amazon S3
  http://aws.amazon.com/documentation/s3/
- Amazon VPC
  https://aws.amazon.com/documentation/vpc/
- AWS Auto Scaling
  http://aws.amazon.com/documentation/autoscaling/
- AWS Certificate Manager
  http://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html
- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/
- AWS IAM
  http://aws.amazon.com/documentation/iam/

McAfee ePolicy Orchestrator documentation

McAfee ePO
https://docs.mcafee.com/bundle?value=183

- McAfee documentation portal
  https://docs.mcafee.com
- McAfee Release Notes
  https://kc.mcafee.com/corporate/index?page=content&id=PD27627

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/

Document Revisions

Date	Change	In sections
August 2020	Added two parameters: `FIPSEnabled` and `AHHttpPort`; adjusted page breaks for at-a-glance groupings; changed *service limits* to *service quotas* and updated those links.	Parameters for deploying McAfee ePO into a new VPC Parameters for deploying McAfee ePO into an existing VPC
March 2019	Added Enable Product Improvement Program parameter to support version 1.0.154	Parameters for deploying McAfee ePO into a new VPC Parameters for deploying McAfee ePO into an existing VPC
October 2018	Added template support for deploying in the GovCloud (US) Region	Templates for GovCloud (US) Region Parameters for deploying McAfee ePO into a new VPC Parameters for deploying McAfee ePO into an existing VPC
August 2018	Updated parameters, table names, and descriptions	Parameters for deploying McAfee ePO into a new VPC Parameters for deploying McAfee ePO into an existing VPC
July 2018	Initial draft	—

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.