

Dynatrace Managed Cluster on the AWS Cloud

Quick Start Reference Deployment

November 2018

Dynatrace

AWS Quick Start Reference Team

Contents

Overview.....	2
Dynatrace Managed Cluster on AWS.....	3
Costs and Licenses.....	3
Architecture.....	3
Prerequisites	5
Specialized Knowledge	5
Technical Requirements.....	5
Deployment Options	5
Deployment Steps	6
Step 1. Prepare Your AWS Account.....	6
Step 2. Launch the Quick Start	6
Step 3. Test the Deployment	13
Best Practices Using the Dynatrace Managed Cluster on AWS	15
High Availability and Performance.....	15
Getting Help	15
Security.....	15
Network Access to the Dynatrace Managed Cluster.....	15

Domain and TLS Certificate	15
Outbound Connections to Dynatrace Mission Control	16
IAM Capabilities Needed by the Quick Start	16
Parameters Stored in AWS Systems Manager	17
Maintaining the Dynatrace Managed Cluster	17
Protecting the Cluster against Inadvertent Termination	17
Scaling Out	18
Scaling In	18
Changing the Instance Type	19
Resizing the Amazon EBS Volumes	19
Changing Other Parameters	19
Troubleshooting	19
Git Repository	20
Additional Resources	21
Document Revisions	21

This Quick Start deployment guide was created by Amazon Web Services (AWS) in collaboration with Dynatrace.

[Quick Starts](#) are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying a Dynatrace Managed cluster on the Amazon Web Services (AWS) Cloud.

Dynatrace is available in two deployment models: SaaS and Managed. In the SaaS model, you do not need to deploy the Dynatrace cluster. In the Managed model, you can run the Dynatrace cluster in the infrastructure of your choosing and retain full control of the data.

This Quick Start is for IT infrastructure architects, administrators, and DevOps professionals who want to use the Dynatrace Managed model for deployments and run their cluster in the AWS Cloud.

Dynatrace Managed Cluster on AWS

Dynatrace is an all-in-one performance-monitoring solution. You can use a single platform to analyze application performance throughout your application's full stack, down to each individual transaction across all layers and technologies.

Using the Quick Start to deploy the Dynatrace Managed cluster in AWS greatly simplifies the deployment process. It enables the failover capacities by leveraging multiple Availability Zones, a Network Load Balancer, and an Amazon Elastic Compute Cloud (Amazon EC2) automatic recovery mechanism. It lets you easily scale the cluster both vertically and horizontally.

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 AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

To run this Quick Start, you first need to obtain the Dynatrace Managed license by contacting Dynatrace at <https://www.dynatrace.com/contact/>. You can use the trial license to try Dynatrace Managed with no additional cost.

Architecture

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

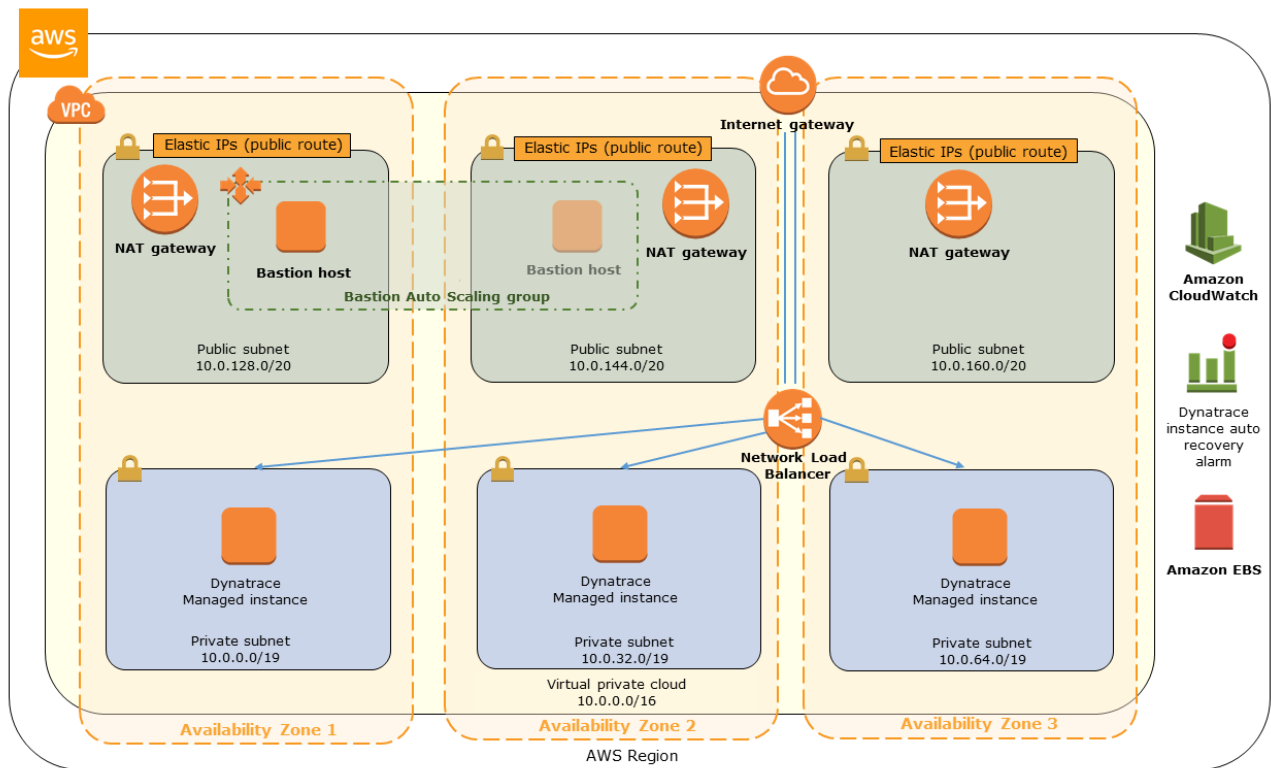


Figure 1: Quick Start architecture for a Dynatrace Managed cluster on AWS

The Quick Start sets up the following:

- A highly available architecture that spans multiple 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 Auto Scaling group to allow inbound Secure Shell (SSH) access to EC2 instances in private subnets.*
- A Network Load Balancer that can be used to access the Dynatrace Managed cluster and send monitoring data from outside of the VPC.
- Three Elastic IP addresses used by the Network Load Balancer.

- In each of the private subnets, an Amazon EC2 instance with Dynatrace Managed server installed. Each Amazon EC2 instance is using six Amazon Elastic Block Store (Amazon EBS) volumes. For each instance there is also an Amazon CloudWatch alarm defined for Amazon EC2 Auto Recovery.

* The template that deploys the Quick Start into an existing VPC skips the tasks marked by asterisks and prompts you for your existing VPC configuration.

Note We recommend using three Availability Zones for the deployment. If your Region does not support three Availability Zones, you can deploy Dynatrace Managed across two Availability Zones.

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 EC2](#)
- [Amazon EBS](#)
- [Amazon VPC](#)
- [AWS CloudFormation](#)
- [Network Load Balancer](#)

Technical Requirements

Before deploying the Dynatrace Managed cluster on AWS, you need the following:

- AWS Account
- AWS Identity and Access Management (IAM) User with permissions to use CloudFormation and create associated resources
- Amazon EC2 key pair
- Dynatrace Managed license key
- Dynatrace Managed installer download URL (provided with the license key)

Deployment Options

This Quick Start provides two deployment options:

- **Deploy the Dynatrace Managed cluster 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 the Dynatrace Managed cluster into this new VPC.
- **Deploy the Dynatrace Managed cluster into an existing VPC.** This option provisions the Dynatrace Managed cluster in your existing AWS infrastructure.

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

Deployment Steps

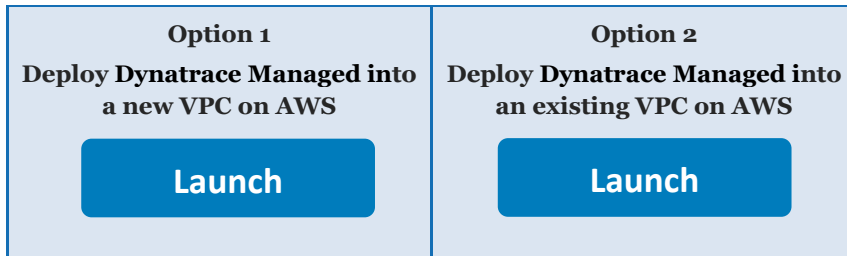
Step 1. Prepare Your AWS Account

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 the Dynatrace Managed cluster on AWS. For more information, see the [AWS Global Infrastructure](#) webpage.
3. Create a [key pair](#) in your preferred region.
4. If necessary, [request a service limit increase](#) for the Amazon EC2 r4.xlarge instance type. 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 limit](#) 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.



Important If you're deploying the Dynatrace Managed cluster into an existing VPC, make sure that your VPC has at least two but preferably three private subnets in different Availability Zones. 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.

Each deployment takes about 30 minutes to complete.

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 the Dynatrace Managed cluster will be built. The template is launched in the US East (Ohio) 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 two deployment options:

- [Parameters for deploying Dynatrace Managed cluster into a new VPC](#)
- [Parameters for deploying Dynatrace Managed cluster into an existing VPC](#)

- **Option 1: Parameters for deploying Dynatrace Managed cluster into a new VPC**

[View template](#)

Dynatrace Managed cluster configuration:

Parameter label (name)	Default	Description
Dynatrace Managed license key (LicenseKey)	<i>Requires input</i>	The license key will then be sent in email after you sign up for a license. See the Dynatrace website for information on obtaining a license.
Dynatrace Managed installer download URL (DownloadUrl)	<i>Requires input</i>	The download URL will then be sent in email after you sign up for a license. See the Dynatrace website for information on obtaining a license.
Number of Dynatrace Managed nodes (NumNodes)	3	Number of Dynatrace Managed nodes to create.

Dynatrace Managed cluster environment configuration:

Parameter label (name)	Default	Description
Admin password (AdminPassword)	<i>Requires input</i>	Initial password for the admin user. This password is used to access the Dynatrace cluster console UI.
Contact email for the cluster. (AdminEmail)	<i>Requires input</i>	Problem notifications will be sent to this email address if an issue is detected on the cluster.

Network configuration:

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	<i>Requires input</i>	The list of Availability Zones to use for the subnets in the VPC. It is recommended to use three Availability Zones or, if three are unavailable, to use two Availability Zones for this deployment. The logical order of the chosen Availability Zones is preserved.
Number of Availability Zones (NumberOfAZs)	<i>Requires input</i>	Number of Availability Zones to use in the VPC. We recommend using three Availability Zones. This must match your selections in the Availability Zones parameter
VPC CIDR (VPCCIDR)	10.0.0.0/16	The CIDR block for the VPC.
Private Subnet 1 CIDR (PrivateSubnet1CIDR)	10.0.0.0/19	The CIDR block for the private subnet located in Availability Zone 1.
Private Subnet 2 CIDR (PrivateSubnet2CIDR)	10.0.32.0/19	The CIDR block for the private subnet located in Availability Zone 2.

Parameter label (name)	Default	Description
Private subnet 3 CIDR (PrivateSubnet3CIDR)	10.0.64.0/19	The CIDR block for the private subnet located in Availability Zone 3.
Public Subnet 1 CIDR (PublicSubnet1CIDR)	10.0.128.0/20	The CIDR block for the public (DMZ) subnet located in Availability Zone 1.
Public Subnet 2 CIDR (PublicSubnet2CIDR)	10.0.144.0/20	The CIDR block for the public (DMZ) subnet located in Availability Zone 2.
Public Subnet 3 CIDR (PublicSubnet3CIDR)	10.0.160.0/20	The CIDR block for the public (DMZ) subnet located in Availability Zone 3.
Allowed Bastion external access CIDR (RemoteAccessCIDR)	<i>Requires input</i>	Allowed CIDR block for external SSH access to the bastions.

Amazon EC2 Configuration:

Parameter label (name)	Default	Description
Key pair name (KeyPairName)	<i>Requires input</i>	A name of an existing public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.
Bastion instance type (BastionInstanceType)	t2.micro	Amazon EC2 instance type for the bastion host.
Dynatrace Managed instance type (DynatraceInstanceType)	r4.xlarge	Amazon EC2 instance type for the Dynatrace Managed nodes.
Dynatrace managed instance tenancy (DynatraceInstanceTenancy)	default	Choose whether Dynatrace Managed nodes run on a dedicated or a multi-tenant host.

Amazon EBS volume sizing configuration:

Parameter label (name)	Default	Description
EBS volume size - installation (BinVolumeSize)	50	Dynatrace Managed volume for Binaries.
EBS volume size - logs and updates (MiscVolumeSize)	100	Dynatrace Managed Data Directory for Logs and Updates.
EBS volume size - transaction storage (SrvVolumeSize)	500	Dynatrace Managed Data Directory for Transaction Storage.
EBS volume size - long term storage (CassandraVolumeSize)	1200	Dynatrace Managed volume for Cassandra Long-term Metrics Repository.

EBS volume size - ElasticSearch (ElasticSearchVolumeSize)	700	Dynatrace Managed volume for ElasticSearch Store.
---	-----	---

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	aws-quickstart	The S3 bucket you have created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.
Quick Start S3 Key Prefix (QSS3KeyPrefix)	quickstart-dynatrace/	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 Dynatrace Managed cluster into an existing VPC**

[View template](#)

Dynatrace Managed cluster configuration:

Parameter label (name)	Default	Description
Dynatrace Managed license key (LicenseKey)	<i>Requires input</i>	The license key will then be sent in email after you sign up for a license. See the Dynatrace website for information on obtaining a license.
Dynatrace Managed installer download URL (DownloadUrl)	<i>Requires input</i>	The download URL will then be sent in email after you sign up for a license. See the Dynatrace website for information on obtaining a license.
Number of Dynatrace Managed nodes (NumNodes)	3	Number of Dynatrace Managed nodes to create.

Dynatrace Managed cluster environment configuration:

Parameter label (name)	Default	Description
Admin password (AdminPassword)	<i>Requires input</i>	Initial password for the admin user. This password is used to access the Dynatrace cluster console UI.
Contact email address for the cluster (AdminEmail)	<i>Requires input</i>	Problem notifications will be sent to this address if an issue is detected on the cluster.

Network configuration:

Parameter label (name)	Default	Description
Number of Availability Zones (NumberOfAZs)	<i>Requires input</i>	Number of Availability Zones to use in the VPC. This must match your subnet settings.
VPC ID (VPCID)	<i>Requires input</i>	ID of the VPC (e.g., vpc-0343606e).
Private subnet 1 ID (PrivateSubnet1ID)	<i>Requires input</i>	ID of the private subnet 1 that you want to provision the first node into (e.g., subnet-a0246dcd).
Private subnet 2 ID (PrivateSubnet2ID)	<i>Requires input</i>	ID of the private subnet 2 you want to provision the second node into (e.g., subnet-e3246d8e).
Private subnet 3 ID (PrivateSubnet3ID)	<i>Requires input</i>	ID of the private subnet 3 you want to provision the third node into. Relevant only for deployments into three Availability Zones.
Public subnet 1 ID (PublicSubnet1ID)	<i>Requires input</i>	ID of the public subnet 1 for used public-facing Network Load Balancer (e.g., subnet-a0246dcd).
Public subnet 2 ID (PublicSubnet2ID)	<i>Requires input</i>	ID of the public subnet 2 for used public-facing Network Load Balancer (e.g., subnet-e3246d8e).
Public subnet 3 ID (PublicSubnet3ID)	<i>Requires input</i>	ID of the public subnet 3 for used public-facing Network Load Balancer. Relevant only for deployments into three Availability Zones.
Bastion Security Group ID (BastionSecurityGroupID)	<i>Requires input</i>	ID of the bastion host security group to enable SSH connections (e.g., sg-7f16e910).

Amazon EC2 configuration:

Parameter label (name)	Default	Description
Key pair name (KeyPairName)	<i>Requires input</i>	The name of an existing public/private key pair, which allows you to securely connect to your instance after it launches.
Dynatrace Managed instance type (DynatraceInstanceType)	r4.xlarge	Amazon EC2 instance type for the Dynatrace Managed nodes.
Dynatrace Managed instance tenancy (DynatraceInstanceTenancy)	default	Choose whether Dynatrace Managed nodes run on a dedicated or a multi-tenant host.

Amazon EBS volume sizing configuration:

Parameter label (name)	Default	Description
EBS volume size - installation (BinVolumeSize)	50	Dynatrace Managed volume for Binaries.
EBS volume size - logs and updates (MiscVolumeSize)	100	Dynatrace Managed Data Directory for Logs and Updates.

EBS volume size - transaction storage (SrvVolumeSize)	500	Dynatrace Managed Data Directory for Transaction Storage.
EBS volume size - long term storage (CassandraVolumeSize)	1200	Dynatrace Managed volume Cassandra Long-term Metrics Repository.
EBS volume size - ElasticSearch (ElasticSearchVolumeSize)	700	Dynatrace Managed volume for ElasticSearch Store.

AWS Quick Start configuration:

Parameter label (name)	Default	Description
Quick Start S3 bucket name (QSS3BucketName)	aws-quickstart	S3 bucket name for the Quick Start assets. Quick Start bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Quick Start S3 key prefix (QSS3KeyPrefix)	quickstart-dynatrace/	S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

- On the **Options** page, you can [specify tags](#) (key-value pairs) for resources in your stack and [set advanced options](#). When you're done, choose **Next**.
- On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.
- Choose **Create** to deploy the stack.
- Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the Dynatrace Managed cluster is ready.
- Use the URL displayed in the **Outputs** tab for the nested Dynatrace stack to view the resources that were created.

Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy
Key		Value				Description	
ElasticIP1		54.86.209.52					
ElasticIP2		34.204.112.211					
ElasticIP3		54.146.133.53					
DynatraceNLB		arn:aws:elasticloadbalancing:us-east-1:██████████:loadbalancer/net/tCaT-Dynat-1CAE27F0YVV4K/d5f09febb8581f93					

Figure 2: Stack output showing the Elastic IP address that is used to access the Dynatrace Managed Console

Step 3. Test the Deployment

1. Use `https://<Elastic_IP>` obtained from the **Outputs** tab to access the Dynatrace Managed cluster console. Ignore any browser warnings regarding TLS certificate.

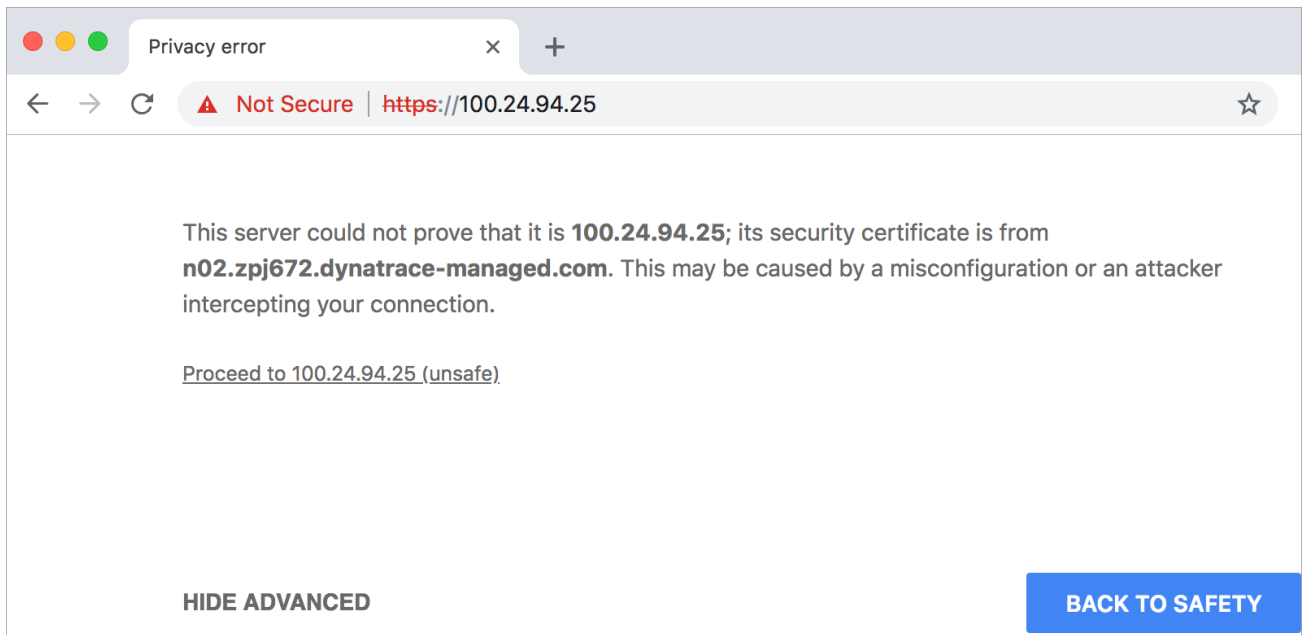


Figure 3: Ignore browser security warnings

2. Log in to the Dynatrace console, using **admin** as the user name and the password that you entered in the Quick Start **AdminPassword** parameter.

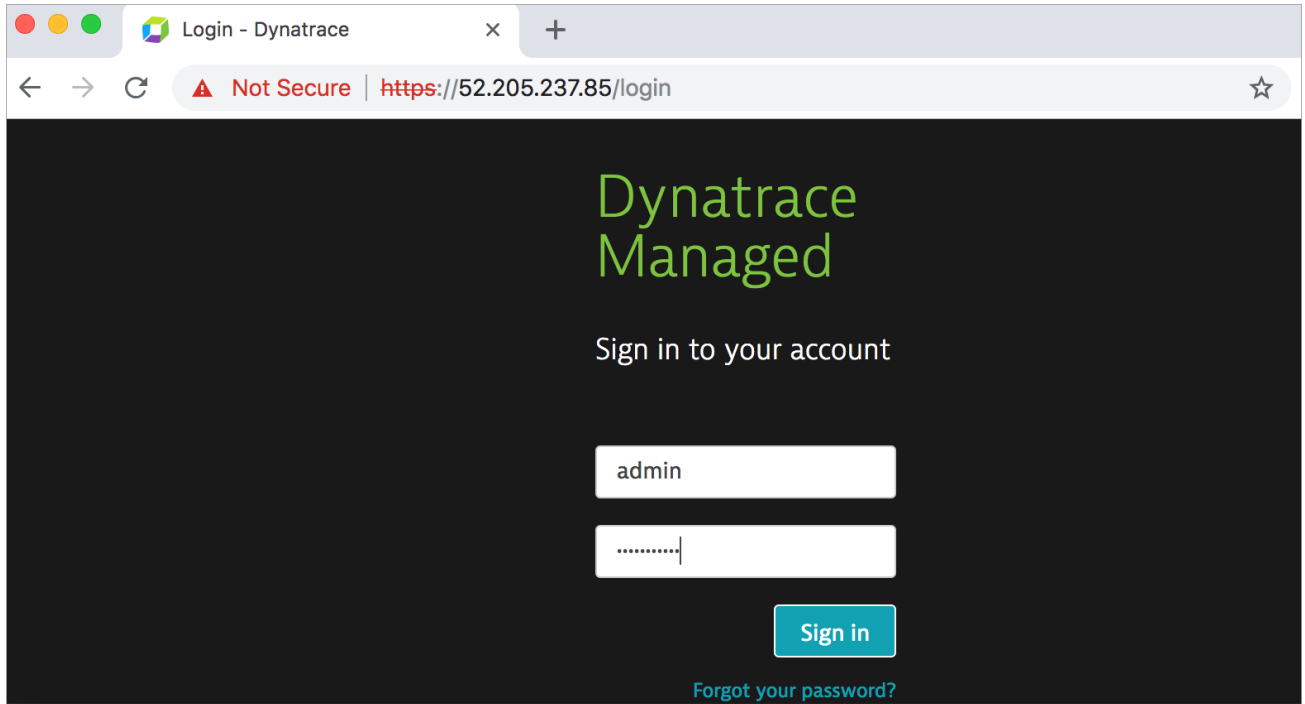


Figure 4: Dynatrace Managed login screen

3. On the Dynatrace UI Home screen, you can verify the summary of your setup.

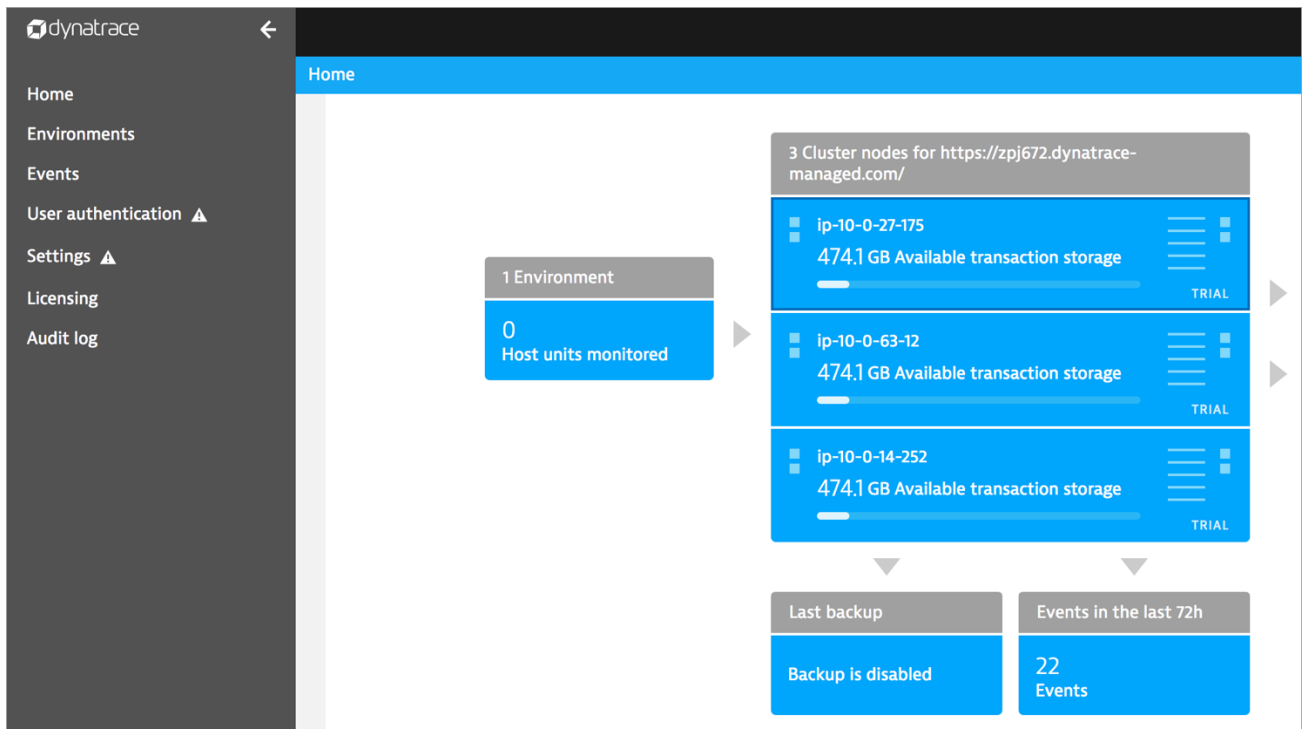


Figure 5: Dynatrace Managed Home screen after successful login

4. From the Home screen, you can navigate to the configuration of each node. You can change the IP address for each node to one of Elastic IP addresses of the Network Load Balancer. After doing this you will be able to use the pre-generated domain name to access the cluster UI.
5. Proceed with other configuration adjustments if needed.

Best Practices Using the Dynatrace Managed Cluster on AWS

High Availability and Performance

We recommend that you use three Availability Zones if possible and run at least three nodes to ensure high availability of the cluster. If you decide to start very small and use only one node, we still recommend that you configure the VPC with three Availability Zones and three public and private subnets. You can add nodes to the cluster, but you won't be able to easily reconfigure the VPC after it has been created.

While you don't need to come up with the exact cluster sizing initially, we recommend getting acquainted with the [Dynatrace Managed hardware requirements](#).

Getting Help

For Dynatrace-specific questions, see the [Dynatrace support site](#).

Security

Network Access to the Dynatrace Managed Cluster

Dynatrace Managed UI can be accessed on port 443 (HTTPS). Dynatrace Managed is also exposing secondary HTTPS port 8443, which is needed for monitoring data collection.

Public access to the cluster is facilitated by the Network Load Balancer. By default, both ports are open without restrictions. If this is not desirable, you will need to adjust the settings in the security group.

SSH access (port 22) is possible only via the bastion host. Bastion host instances and cluster node instances are configured using the same SSH key, which is provided during Quick Start deployment.

Domain and TLS Certificate

When accessing the cluster initially, you might need to ignore the browser security warnings that are caused by a TLS certificate mismatch.

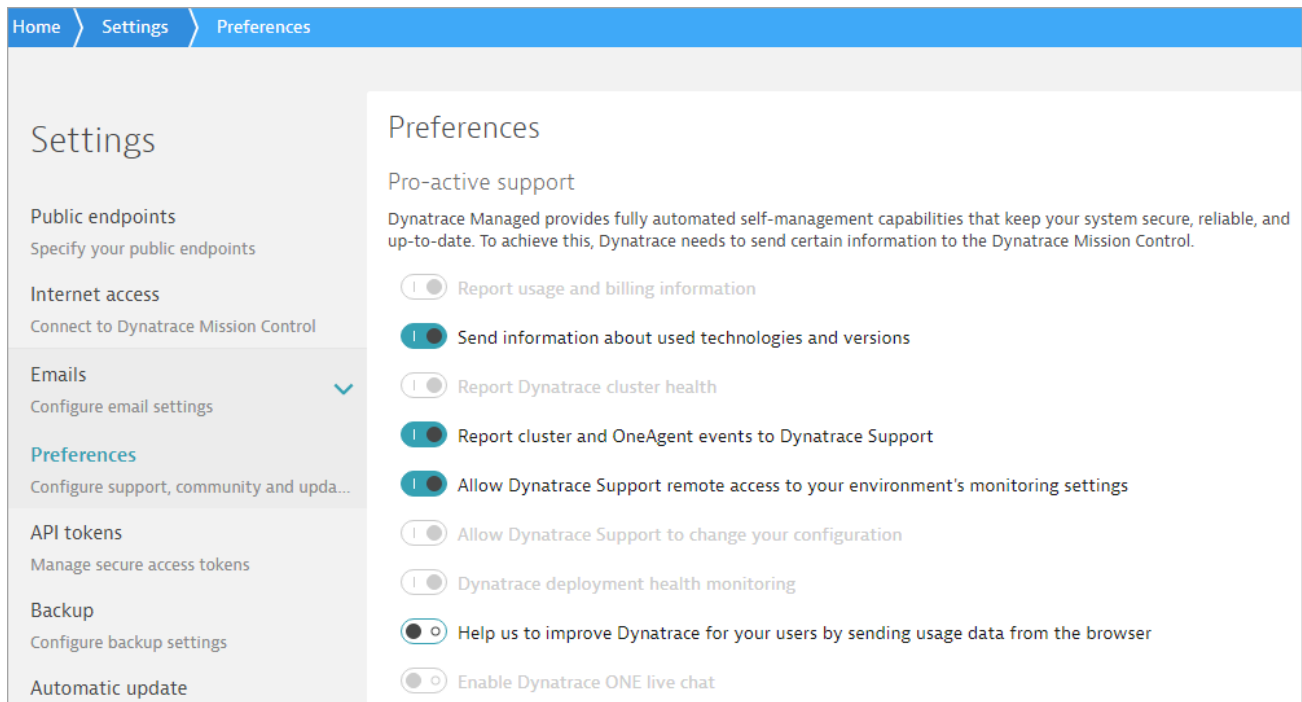
For each Dynatrace Managed cluster, a domain is created in the form *abc123.dynatrace-managed.com*, and a TLS certificate is configured. The setup uses the private IP addresses of the Amazon EC2 instances as domain records. The domain setup is done by Dynatrace and is not part of Quick Start deployment per se. For the Quick Start deployment, you would typically want to use the public IP addresses of the Network Load Balancer instead. You can reconfigure the IP address used for each node in Dynatrace Managed UI.

However, if the private IP address of the EC2 instance is not accessible—which is the case initially if you create the new VPC—the only way to access the cluster UI initially is by using an IP address instead of the domain name.

Outbound Connections to Dynatrace Mission Control

To facilitate automatic updates of Dynatrace Managed and help in supporting the installations, the Dynatrace Managed cluster periodically sends requests to the [Dynatrace Mission Control API endpoint](#).

You can control what data is sent by changing the settings in the **Pro-active support** section of Preferences in the Dynatrace Managed UI.



The screenshot shows the Dynatrace Managed UI Preferences page. The breadcrumb navigation at the top reads "Home > Settings > Preferences". On the left, a "Settings" sidebar lists various configuration areas: Public endpoints, Internet access, Emails, Preferences (highlighted), API tokens, Backup, and Automatic update. The main content area is titled "Preferences" and features a "Pro-active support" section. This section includes a descriptive paragraph and a list of nine toggleable settings:

- Report usage and billing information (disabled)
- Send information about used technologies and versions (enabled)
- Report Dynatrace cluster health (disabled)
- Report cluster and OneAgent events to Dynatrace Support (enabled)
- Allow Dynatrace Support remote access to your environment's monitoring settings (enabled)
- Allow Dynatrace Support to change your configuration (disabled)
- Dynatrace deployment health monitoring (disabled)
- Help us to improve Dynatrace for your users by sending usage data from the browser (disabled)
- Enable Dynatrace ONE live chat (disabled)

IAM Capabilities Needed by the Quick Start

The Dynatrace Managed cluster Quick Start requires IAM capabilities for the creation of the CloudFormation stack. The IAM capabilities are needed to create the IAM Role and

instance profile for the Amazon EC2 instances running Dynatrace Managed. The associated permissions do not go beyond Amazon S3 read access (restricted to the Quick Start bucket resource) and AWS Systems Manager access (restricted to parameters created by this Quick Start).

Parameters Stored in AWS Systems Manager

The Dynatrace Managed Cluster Quick Start uses AWS Systems Manager Parameter Store to persist parameters that are needed for cluster bootstrapping. One of the parameters—**seed-token**—is a Dynatrace cluster API token that should be kept secure. If you have concerns about restricting access to Parameter Store, you can remove the token parameter. Note, however, that you will need to provide it again should you decide to extend the number of cluster nodes by [updating the CloudFormation stack](#).

Maintaining the Dynatrace Managed Cluster

For detailed instructions on how to configure and maintain Dynatrace Managed cluster, refer to the [Dynatrace documentation](#), which covers some maintenance details that are specific to this Quick Start.

While this Quick Start was designed primarily with initial cluster bootstrapping in mind, it is possible to alter the setup through [AWS CloudFormation updates](#). Not all parameters may be safely changed though, and care must be taken to avoid data loss.

Protecting the Cluster against Inadvertent Termination

Because the Quick Start AWS CloudFormation template creates multiple nested stacks, it is not easy to determine if a nested resource is going to be replaced by a CloudFormation template update. To prevent inadvertent replacement of Amazon EC2 instances with the Dynatrace Managed cluster, it is paramount to apply proper stack policy to nested stacks if planning on doing CloudFormation stack updates.

For example, you can apply the following CloudFormation stack policy to each nested Dynatrace Quick Start stack:

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "Update:Replace",
        "Update>Delete"
      ]
    }
  ]
}
```

```
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ResourceType": [
          "AWS::EC2::Instance"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Principal": "*",
    "Action": "Update:*",
    "Resource": "*"
  }
]
```

Scaling Out

Because this Quick Start does not use Amazon EC2 Auto Scaling, you might need to add more nodes to the cluster if the initial sizing is not sufficient. You can add nodes by updating the AWS CloudFormation stack using the original template and increasing the value of the **NumNodes** parameter. The default value is 3, and the maximum number of nodes is currently capped at 6.

Scaling In

You can reduce the number of nodes in the cluster by using AWS CloudFormation, but we recommend that you remove only one node at a time to ensure the monitoring data can get replicated to remaining nodes. To remove a node, use the following steps:

1. Disable the last node of the cluster by using the Dynatrace UI.

The disabled node no longer accepts monitoring data, but it can be enabled again.

2. Remove the last node from the cluster by using the Dynatrace UI.
3. Update the AWS CloudFormation stack with the **NumNodes** parameter value decreased by one.

Note If you plan to remove another node from larger setups, you might need to wait a couple of hours before the data is resharded to avoid data loss.

Changing the Instance Type

You can switch to another instance type for cluster nodes by updating the AWS CloudFormation stack and changing the **DynatraceInstanceType** parameter. Make sure that the new instance type has at least as much memory as previous one. Otherwise, the services of the cluster might not be able to start. To avoid data loss, it is paramount to confirm that changing the instance type does not involve instance replacement by AWS CloudFormation.

Resizing the Amazon EBS Volumes

Resizing the Amazon EBS volumes for this Quick Start by using AWS CloudFormation update is currently **not** supported. Attempting to change the size of any Amazon EBS volume configured by AWS CloudFormation will trigger the replacement of Amazon EC2 instances and will result in data loss. If disk resize is needed, do the following:

1. You must first resize the EBS volume by following the instructions at <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/console-modify.html>.
2. Then resize the file system on each cluster node. All the volumes have been configured using LVM and can be resized without downtime. Use SSH to log in to each Amazon EC2 instance and run the `/tmp/resize_lvm.sh` script with `sudo`.

Changing Other Parameters

This Quick Start does not support changing any other cluster or VPC-related parameters by using AWS CloudFormation update.

Troubleshooting

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 `/var/log/cfn*`).

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 additional 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. The Quick Start stack has been created, but when I try to access the Dynatrace Managed cluster I get connection timeout error.

A. Try using `https://<Elastic_IP>` to log in to the cluster. You can use one of the Elastic IP addresses allocated with the stack. The Elastic IP addresses can be found on the **Outputs** tab for the CloudFormation stack.

Q. The Quick Start stack has been created, but I can't log in to the Dynatrace Managed cluster due to an authentication error.

A. For the initial login, try logging in with the user name **admin** and the password that you entered for the Quick Start **AdminPassword** parameter. Afterwards, you can configure user accounts in Dynatrace UI.

Q. I encountered a DELETE_FAILED error when deleting the Quick Start AWS CloudFormation stack.

A. If the stack deletion failed and the only resources left behind are Elastic IP addresses, please retry the deletion one more time. Sometimes AWS CloudFormation is unable to release the Elastic IP addresses because they are blocked internally by the Network Load Balancer.

Q. I want to redeploy the Quick Start by terminating the CloudFormation stack and creating it again, but the second creation attempt fails.

A. The Dynatrace license does not get released automatically when stack is terminated. You need to contact Dynatrace support to release the license or get another license key.

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 EBS
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>
- Amazon EC2
<https://aws.amazon.com/documentation/ec2/>
- Amazon VPC
<https://aws.amazon.com/documentation/vpc/>
- AWS CloudFormation
<https://aws.amazon.com/documentation/cloudformation/>
- Network Load Balancer
<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>

Dynatrace Managed cluster documentation

- Deploy Dynatrace
<https://www.dynatrace.com/support/help/deploy-dynatrace/>
- Managed deployment scenarios
<https://www.dynatrace.com/support/help/deploy-dynatrace/managed/installation/managed-deployment-scenarios/>
- Hardware & operating system requirements
<https://www.dynatrace.com/support/help/deploy-dynatrace/managed/installation/hardware-and-operating-system-requirements/>

Quick Start reference deployments

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

Document Revisions

Date	Change	In sections
November 2018	Initial publication	—

© 2018, Amazon Web Services, Inc. or its affiliates, and Dynatrace. All rights reserved.

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.