

Dynatrace Managed – Cluster Management Console

Dynatrace Training Module

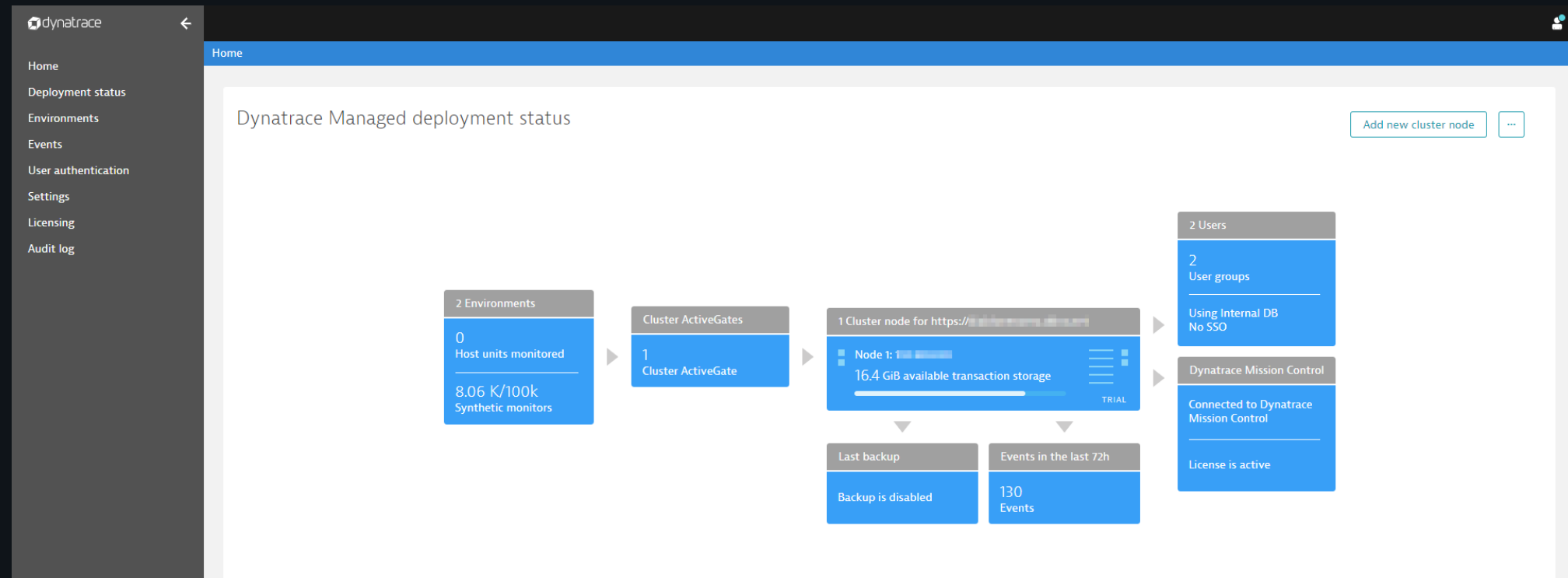


Agenda

- Home
- Deployment Status
- Environments
- Events
- User Authentication
- Settings
 - Preferences - Domain and Certificate Management
- Licensing
- Audit log

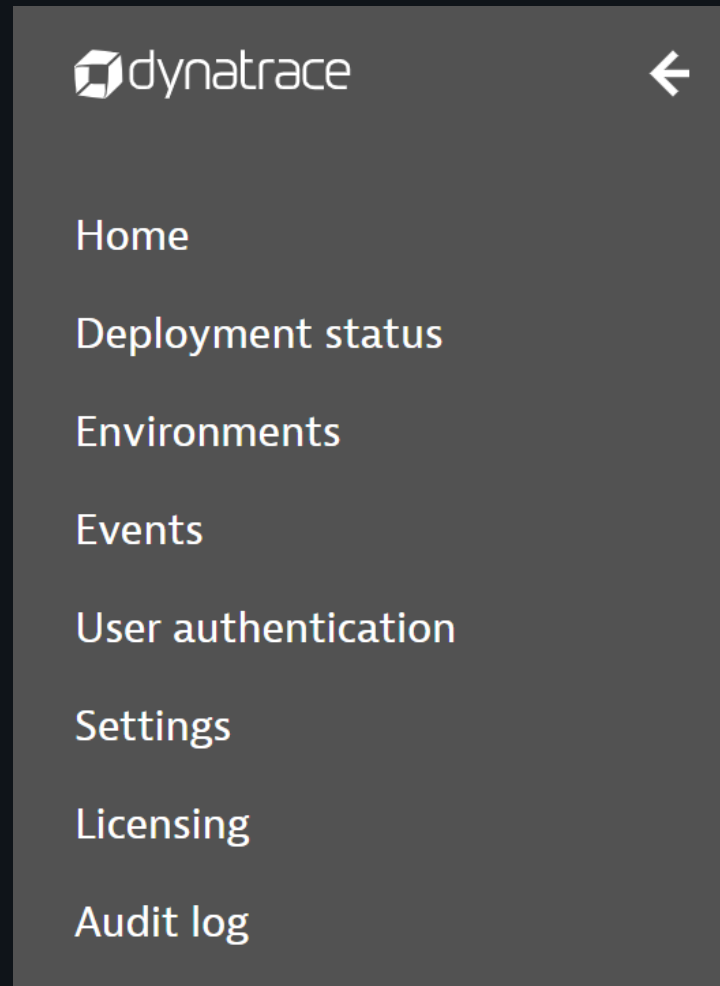
Log into the Cluster Management Console (CMC)

- Access the Cluster Management Console (CMC) for your cluster
 - <https://{clusterID}.dynatrace-managed.com>



Main Menu

- List of all views that can be accessed for configuration and analysis of cluster specific information

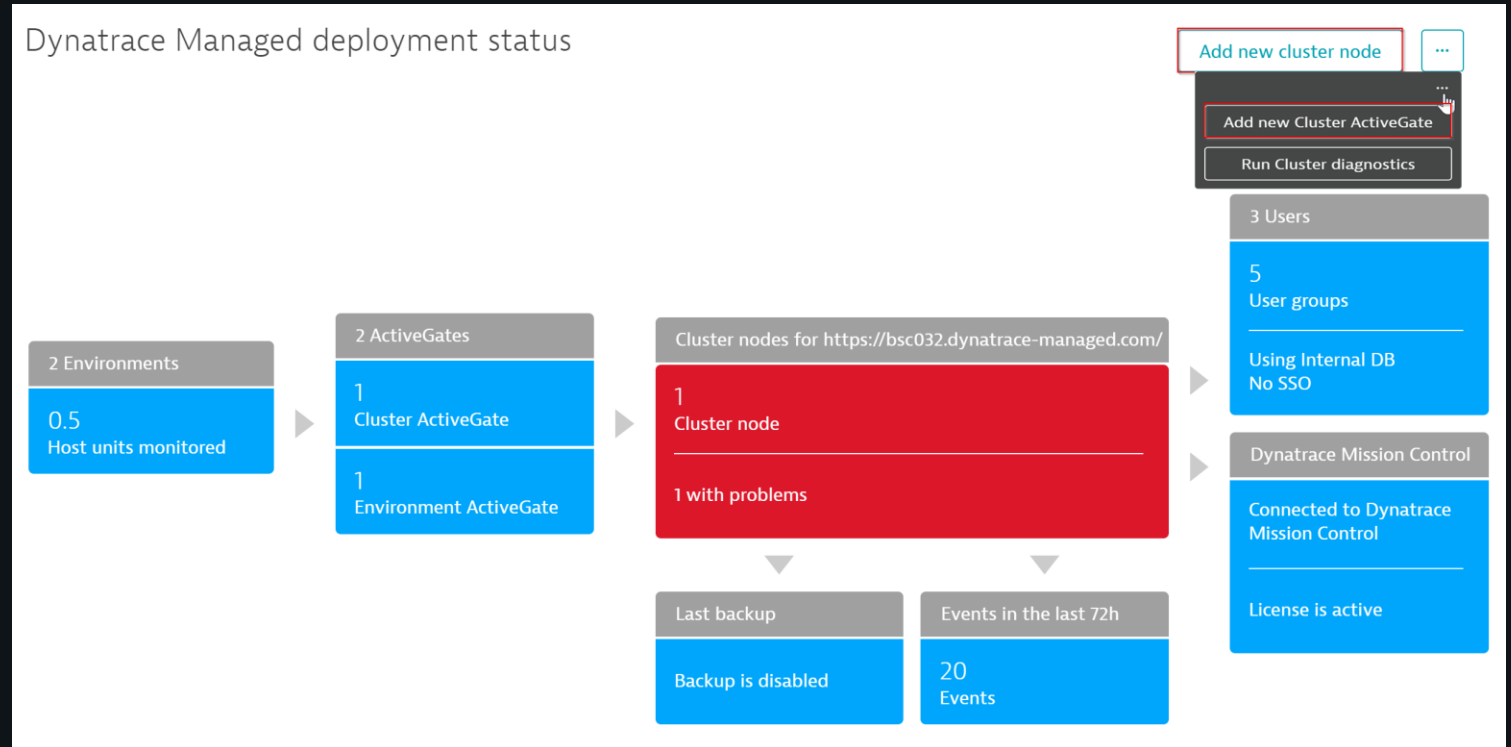


Home



Home

- Provides overall status of the cluster.
- Link to add new cluster nodes
- Link to add Cluster ActiveGates
- Click on any status box to link to details for the item



Deployment Status

Deployment Status – Cluster Node Information

- Select cluster nodes from the home screen or Deployment Status -> Cluster Nodes to view more information
- Select a node to view the details
- Select Configure to view details about the node

Deployment status

Cluster nodes

ActiveGates

Network zones

Cluster nodes

for https://[redacted].dynatrace-managed.com/

Filter by

Showing 1 cluster node.

Problematic node

There is 1 node having an issue currently.

Apply filter

ID	Hostname	State	Transaction storage	CPU usage	Data transfer	Details
1	192.168.192.85 Attached RAM/CPU is below hardware recomr	Running	17.4 GB free	34 %	1.91 kB/s	⬆

Properties

Version1.216.107.20210505-135918

SizeLeight, John (john.leight@dynatrace.com) is signed in

OneAgent Address192.168.192.85:443

Web UI IP192.168.192.85

Configure

Responsibilities

OneAgent trafficEnabled


Enabled

Confidential

8

Deployment Status – Cluster Node Information


- The ellipsis allows you to:
 - Disable OneAgent Traffic
 - Remove the Node
- Storage allocation and utilization can be viewed


 192.168.192.85


Version 1.216.107.20210505-135918, Rack rack1

Micro

You can use this node to try Dynatrace out, but you should increase your hardware capabilities to make the most of the product. Node size category is decided based on the host's memory and the number of CPU cores.


 34 %
2 CPU cores


 1.3 KiB/s
Total data transfer

 SSL certificate


Issuer: R3, Let's Encrypt
Subject: n01.bsc032.dynatrace-managed.com
Expires: Jun 29, 2021

Edit SSL certificate

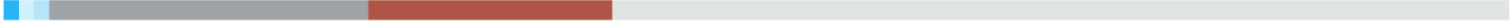
 SSL certificate management is **enabled**.
To install a custom certificate, first [Disable management of SSL certificates](#).
If you lose the connection following install of a new certificate, refresh the page.


 Insufficient hardware


It is recommended to use a host with at least 8 cores and 32 GB RAM.
Currently there are 2 cores and 15.9 GB memory available.


 Storage


Disk space on **/var/opt/dynatrace-managed (/dev/sdb)**: 22.4 GiB free space left out of 29.4 GiB





 72.0 MiB
Metrics storage


 326.2 MiB
Elasticsearch storage

 227.0 MiB
Transaction storage

 6.4 GiB
Other files

 5.0 GiB
Reserved disk space

 17.4 GiB
Available disk space



Disable OneAgent traffic

Disable Web UI traffic

Remove node

Confidential

9

Node Endpoints

Customize node endpoints

Dynatrace automatically detects node IP addresses. You can override this behavior if, for example, you have multiple interfaces or you use IP-forwarding.

IP address and port for OneAgent traffic

Update configuration

This address will be used by OneAgent to send monitoring data to this cluster node. Use an IP address and port number or a domain name. Note: the listen port of this cluster node is not affected by this setting. The default port is 8443, but you can also use 443.

Web UI IP address

This affects the domain name you use to access Dynatrace.

- Allows for customization of the node IP address and port number that the Cluster AG and the OneAgent connect to
- Allows for customization of Web UI IP address

Deployment Status - ActiveGates

Deployment Status – ActiveGates Information

- Select ActiveGates from the home screen or Deployment Status -> ActiveGates to view more information
- ActiveGate modules, type and version are listed in the table
- Select a node to view the details
- Select Configure to view details about the node

Deployment status

Cluster nodes

ActiveGates

Network zones

ActiveGates

Manage your ActiveGates. ActiveGates can be deployed to either:

- route OneAgent traffic, monitor cloud environments or monitor remote technologies with extensions, or
- run synthetic monitors from a private location, or
- route z/OS traffic to Dynatrace.

Learn more about [ActiveGate purposes](#).

Filter by

Showing 2 ActiveGates.

OS	ActiveGate	Active modules	Update status	Environment	Version	Details
192.168.192.80		Up to date	Cluster	1.215.163		

Properties

ID	0x0f901592
OS	Linux
Type	Cluster
Version	1.215.163.20210428-232414
Running in container	False
Network zone	default
Group	default
Address #1	192.168.192.80
Address #2	97104.70.29

☒ AutoUpdate Update ActiveGate

Modules

AWS	Enabled
Azure	Enabled
Beacon forwarder	Enabled
Cloud Foundry	Enabled
DB Insight	Enabled
Extensions 1.0	Disabled
Extensions 2.0	Disabled
HTTP Metric API	Enabled
Kubernetes	Enabled
Log Monitoring	Enabled
Memory dumps	Enabled
OneAgent Routing	Enabled
REST API	Enabled
VMware	Enabled

If additional modules need to be enabled then learn more about how to [configure this ActiveGate](#).

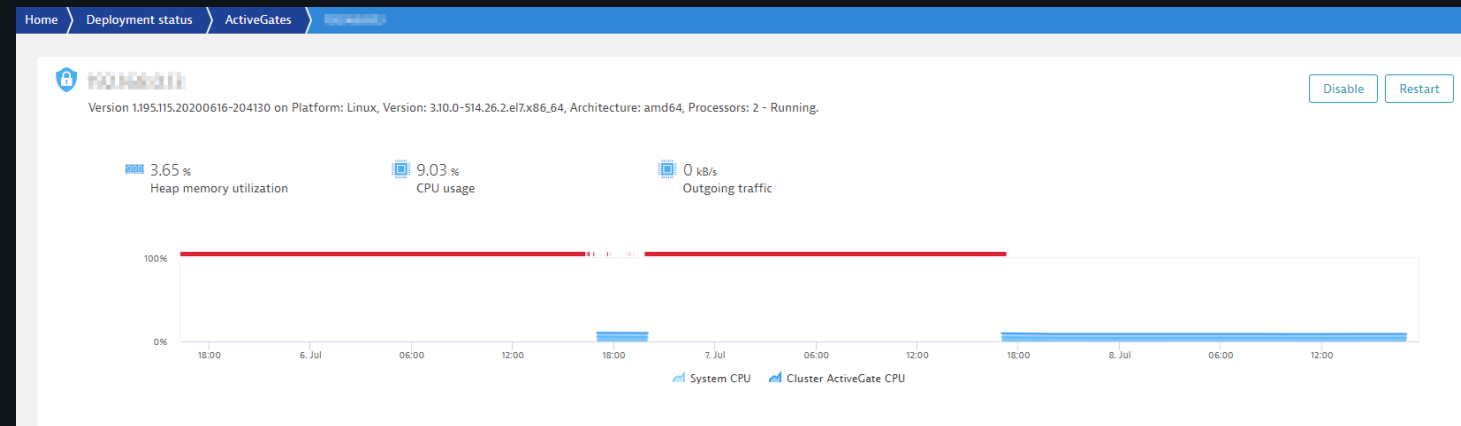
Configuration

Public IP address

Configure

Cluster ActiveGates

- Cluster ActiveGates are only managed through the CMC
- Environment Active Gates can be managed in the CMC or from the Environment
- Disable and Restart options are available
- Heap Memory Utilization, CPU Usage, and Outgoing Traffic of the Active Gate Host are displayed
- Allows for quick analysis of the infrastructure that the Active Gate is deployed on



Cluster ActiveGate Configuration

- Ability to customize the IP address and port number that the OneAgent uses to connect to the ActiveGate
- Ability to supply custom ActiveGate SSL Certificate
- If customer SSL certificate is not specified, Dynatrace will issue a valid certificate as long as the IP address of the AG is public

Customize Cluster ActiveGate endpoints

Dynatrace automatically detects the IP address of the Cluster ActiveGate. You can override that, for example if you have multiple interfaces or IP-forwarding in place.

IP address and port for OneAgent traffic


This address will be used by OneAgent to send monitoring data to this Cluster ActiveGate. You can customize IP, port or use a domain name. Note: the listen port of this Cluster ActiveGate is not affected by this setting.

Update Cluster ActiveGate configuration

Publicly available IP address

This address is used to send data from external [synthetic monitors](#) locations and for [agentless RUM](#). Dynatrace automatically generates a public DNS name for this address.

Cluster ActiveGate SSL certificate

 **Current SSL certificate**

Issuer:
Subject:
Expires:

Edit SSL certificate

Deployment Status – Network Zones

Deployment Status – Network Zone Information

- Select Deployment Status -> Network Zones to view more information
- Network Zone names, Number of OneAgents and number of ActiveGates are listed
- Select a Network Zone to view the details

Deployment status

Cluster nodes

ActiveGates

Network zones

Network zones

Early adopter

Network zones allow you to effectively manage the Dynatrace monitoring environment. Thanks to them, you can group ActiveGates in any way adopted to the needs of the monitored environment.

Search...

Network zone	OneAgents	ActiveGates
default	2	2

Deployment Status – Network Zone Information

- Network Zone Details include
 - Infographic with details
 - Alternate Network Zones

default Early adopter [Edit](#)

The default network zone. This is the network zone for OneAgents or ActiveGates that do not have any network zone configured.

ActiveGates

2
all ActiveGates

OneAgents

2
all OneAgents

2
OneAgents configured in Network Zone

0
OneAgents using this zone as alternative

Alternative network zones

By adding an alternative network zones, you can specify how routing will occur if this network zone is unavailable.

Alternative network zone	OneAgents	ActiveGates
No alternative network zones		
Edit this network zone to add another network zones as the alternative routing.		

Environments

Environments

- A list of environments are shown
- New Environments can be created



The screenshot displays the 'Environments' management page. At the top, a breadcrumb shows 'Home' and 'Environments'. Below this, a summary states '2 environments enabled, 0 disabled'. A 'Sort by Name' dropdown and view toggles (grid and list) are on the right. A left sidebar contains a 'Filter for...' section with a funnel icon, and two expandable filter sections: 'Environment state' (showing 'Enabled' with a count of 2) and 'Environment type' (showing 'Regular' with a count of 2). The main content area lists two environments: 'DEV' and 'Test'. Each environment card shows three metrics: 'Host units monitored' (19 for DEV, 15 for Test), 'Last hour user sessions' (0 for both), and 'Transactional visibility' (10 days for both). A third card with a large plus icon and the text 'Monitor another environment' is also present.

Environment	Host units monitored	Last hour user sessions	Transactional visibility
DEV	19	0	10 days
Test	15	0	10 days





Environment Details

- Environment License Quotas can be modified
- Environment data retention times can be viewed/changed

Total environment quotas

Name	Current value	Max limit
Host units	0	Unlimited 
Custom metrics	0	Unlimited 







Monthly and annual quotas

Name	Current consumption (monthly / annual)	Monthly limit	Annual limit
User sessions	0 / 0	Unlimited 	Unlimited 
Web application user sessions	0 / 0		
Mobile app user sessions	0 / 0		
Synthetic monitors	0 / 0	Unlimited 	Unlimited 
Avg. daily log volume	0 / 0	Unlimited	Unlimited

Log Monitoring is available on your cluster license but won't work until you configure a network path. To do that, go to [Log Monitoring settings](#)

Storage settings

Change the volume of disk space to be reserved or the amount of time the specified disk space is to be retained. Service code level retention time can't be greater than service request level retention time and both can't exceed one year. The maximum limit for other retention times is 35 days.

Name	Current value	Max limit
Transaction storage	0 MiB	Unlimited 
Symbol files from mobile apps	0 B	1 GiB 
Service request level retention	<1 hour	365  days
Service code level retention	<1 hour	365  days
Real user monitoring retention	<1 hour	35  days
Synthetic monitoring retention	<1 hour	35  days
Log monitoring storage	0 B	0 MiB
Log monitoring retention	0 days	30

Events

Event Types

86 of 1558 Events

Only show log events that have minimum severity level of severe ^

Search

Message

Timestamp (UTC-05:00)

! Insufficient system privileges on SERVER at location '...' (i)

Dynatrace is not able to gain elevated privileges. This means that ... nodes and adding/removing nodes to cluster will not work. Check if the executable /opt/dtrun/dtrun has the root privileges granted.

The following error occurred during validation:

chown: changing ownership of '/opt/dtrun/dtrun.conf': Operation not permitted

chmod: changing permissions of '/opt/dtrun/dtrun.conf': Operation not permitted

informational

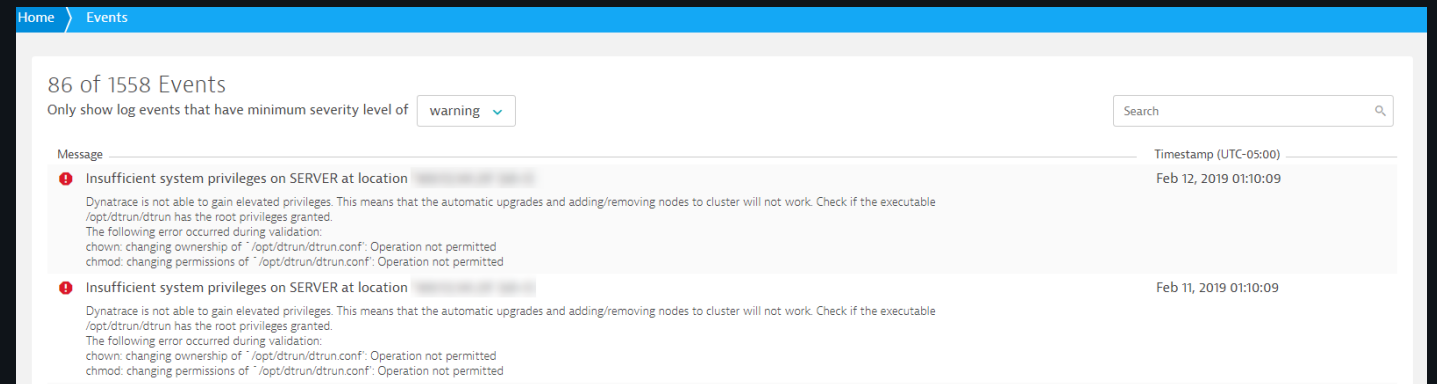
warning

severe

- There are 3 types of events:
 - Informational – AG connectivity data, successful logins, etc...
 - Warning – License check errors, insufficient privileges, etc...
 - Severe – insufficient system privileges, shutdowns, etc...
- Some of the information can be displayed in both warning and severe categories

Warning & Severe Events

- Great source of information to understand whether all of the infrastructure components of the cluster are performing as expected
- Can be used for debugging cluster related issues



The screenshot shows the 'Events' page in the Dynatrace interface. At the top, there's a navigation bar with 'Home' and 'Events'. Below it, the page title is '86 of 1558 Events'. A filter bar indicates 'Only show log events that have minimum severity level of' with a dropdown menu set to 'warning'. A search bar is on the right. The main content area displays a list of events. Two events are visible, both with a red warning icon. The first event is dated 'Feb 12, 2019 01:10:09' and the second is dated 'Feb 11, 2019 01:10:09'. Both events have the same message: 'Insufficient system privileges on SERVER at location [REDACTED]'. The message details state: 'Dynatrace is not able to gain elevated privileges. This means that the automatic upgrades and adding/removing nodes to cluster will not work. Check if the executable /opt/dtrun/dtrun has the root privileges granted. The following error occurred during validation: chown: changing ownership of "/opt/dtrun/dtrun.conf": Operation not permitted; chmod: changing permissions of "/opt/dtrun/dtrun.conf": Operation not permitted'.

Home > Events

86 of 1558 Events

Only show log events that have minimum severity level of warning

Search

Message	Timestamp (UTC-05:00)
<p>Insufficient system privileges on SERVER at location [REDACTED]</p> <p>Dynatrace is not able to gain elevated privileges. This means that the automatic upgrades and adding/removing nodes to cluster will not work. Check if the executable /opt/dtrun/dtrun has the root privileges granted.</p> <p>The following error occurred during validation:</p> <p>chown: changing ownership of "/opt/dtrun/dtrun.conf": Operation not permitted</p> <p>chmod: changing permissions of "/opt/dtrun/dtrun.conf": Operation not permitted</p>	Feb 12, 2019 01:10:09
<p>Insufficient system privileges on SERVER at location [REDACTED]</p> <p>Dynatrace is not able to gain elevated privileges. This means that the automatic upgrades and adding/removing nodes to cluster will not work. Check if the executable /opt/dtrun/dtrun has the root privileges granted.</p> <p>The following error occurred during validation:</p> <p>chown: changing ownership of "/opt/dtrun/dtrun.conf": Operation not permitted</p> <p>chmod: changing permissions of "/opt/dtrun/dtrun.conf": Operation not permitted</p>	Feb 11, 2019 01:10:09

Informational Events

1558 Events

Only show log events that have minimum severity level of informational

Search

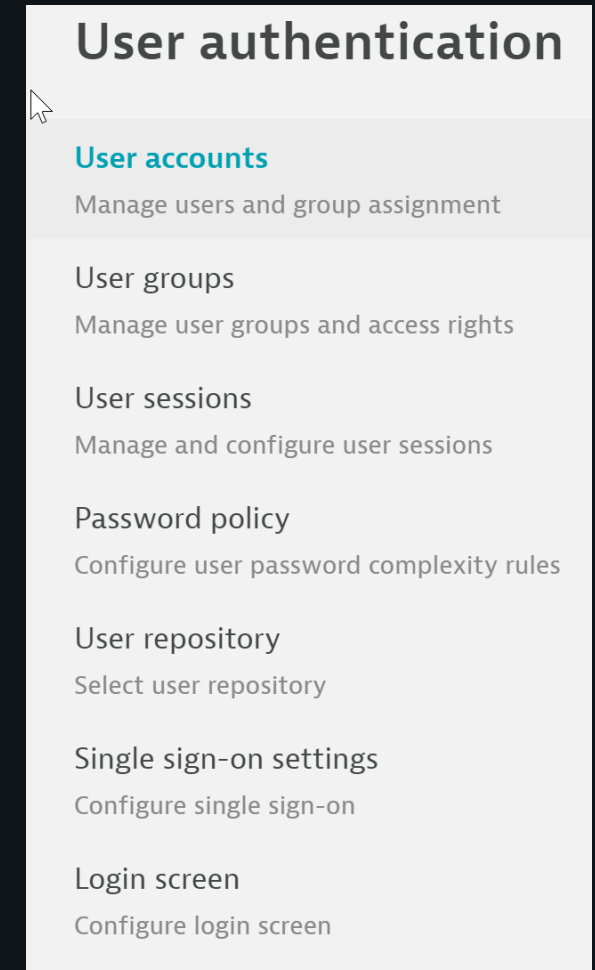
Message	Timestamp (UTC-05:00)
i Successful login. Successful login for Dynatrace pro-active support.	Feb 12, 2019 20:59:31
i Request for remote access Request for remote access to node, host [REDACTED]	Feb 12, 2019 20:58:59
i Dynatrace update 1.1.0.20190213-001200 was successfully downloaded. List of downloaded updates: 1.1.0.20190213-001200: NGINX_OFFSET	Feb 12, 2019 18:50:32

- Provides general information about the cluster
- Allows you to track statistics about the number of logins to the cluster as well as number of updates performed to the cluster

User Authentication

User Authentication

- User Account – create users and assign users to groups
- User Groups – Create Groups and assign permissions to environments and/or management zones
- User Sessions – View and manage user sessions accessing the cluster
- Password Policy – Customize the password policy when using the Internal Cluster Database
- User Repository – Select whether to use the Internal Cluster Database or LDAP
- Single Sign-on Settings – Configure SSO (Single sign-on) to use OpenID Connect or SAML 2.0
- Login Screen – Customize the Dynatrace Cluster Login Screen



User Authentication – Special Notes

- User Group and Permission Details: <https://www.dynatrace.com/support/help/shortlink/managed-user-groups>
- User Management via LDAP. After you switch to LDAP authentication
 - Local accounts (other than the administrator account) will stop working: it will be impossible to log in with a local account.
 - The administrator account you created during installation will continue to work regardless of the selected authentication provider.
 - LDAP configuration: <https://www.dynatrace.com/support/help/shortlink/managed-ldap#connection-configuration>
- LDAP Groups section can map LDAP groups to the Dynatrace User Groups
- SSO SAML 2.0 integration: <https://www.dynatrace.com/support/help/shortlink/managed-saml#set-up-saml-20-integration>
- OpenID integration: <https://www.dynatrace.com/support/help/shortlink/managed-openid>

Settings

Public Endpoints

- Dynatrace Web UI URL can be configured
- Dynatrace can generate an SSL certificate for your Cluster AGs as long as they all have publicly exposed IPs
- Cluster AG URL specifies a URL that the synthetic tests as well as agentless RUM use
- The CDN path is required for JavaScript tag for all of the manually injected applications
 - This will enable Dynatrace to fetch all of the CDN resources

Public endpoints

Dynatrace Web UI URL

The address you normally use to access your Dynatrace cluster UI. Changing this will affect the links in problem notification emails.

Manage domain name and SSL certificates

Enable this setting to generate a domain name (a subdomain of dynatrace-managed.com) with a trusted certificate for your Cluster ActiveGates.
Currently there is at least one Cluster ActiveGate with no public IP configured. This setting will be disabled.

☐

 Enable management of domain name and SSL certificates

Cluster ActiveGate URL

This URL is used to transmit the results of synthetic tests to your Dynatrace cluster. Also agentless real user monitoring requires this endpoint to transmit the monitoring signals to Dynatrace.

Test connection to URL

CDN for JavaScript tag (mandatory only for manually injected applications)

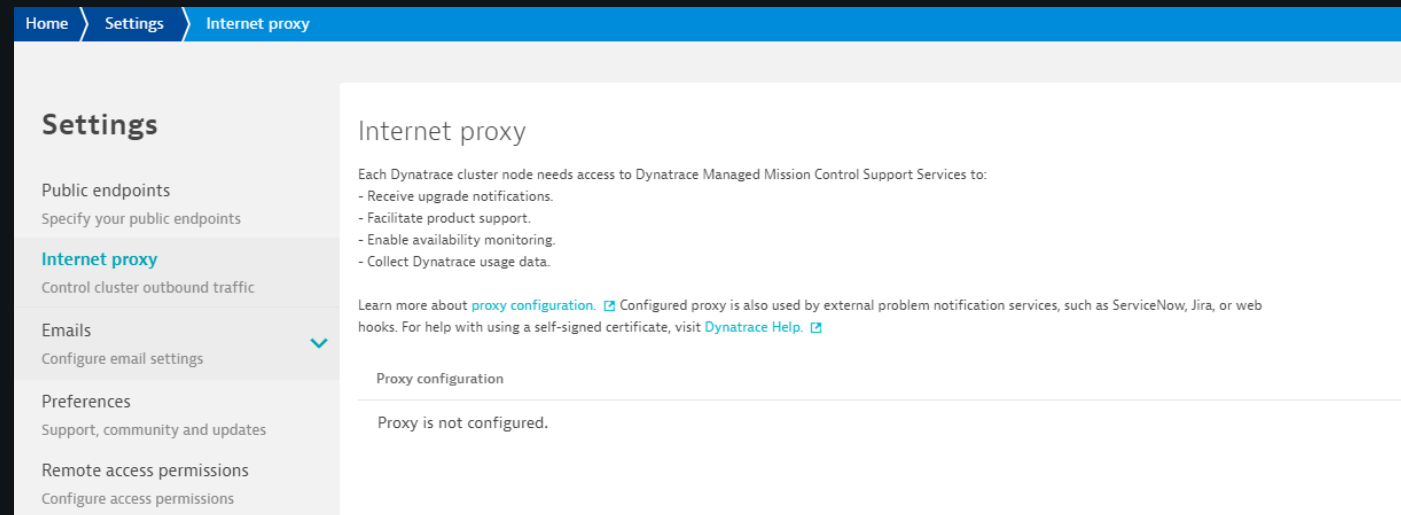
Enter a path to your CDN

Test connection to URL

Specify the root path to your CDN which should be configured to fetch all resources under "/jstag" from a Cluster ActiveGate.
Examples for resources that need to be served:
http[s]://<ClusterActiveGateHostname>/jstag/managed/d01dcab3-ff58-4263-b92f-a399999e0287/c952fe29f7e54277.bs.js
http[s]://<ClusterActiveGateHostname>/jstag/managed/ruxitagentjs_2fhjnqrtx_10102160727210304.js

Internet Proxy

- Access to Dynatrace Managed Mission Control is required for:
 - Usage and billing information
 - Dynatrace cluster health
 - Dynatrace Cluster event reporting
 - Upgrade notifications and packages
 - Facilitating product support
- Configure a proxy for the Managed Cluster to communicate back to Mission Control if necessary
- <https://www.dynatrace.com/support/help/shortlink/managed-support>



Emails – SMTP Server

- Configure the SMTP Server for cluster email notifications

Home

Settings

Emails

SMTP server

Settings

Public endpoints
Specify your public endpoints

Internet access
Connect to Dynatrace Mission Control

Emails
Configure email settings

SMTP server
Email notifications

Preferences
Configure support, community and upda...

API tokens
Manage secure access tokens

Backup
Configure backup settings

Automatic update
Automatic update settings

Log monitoring
Network storage configuration

SMTP server

To configure how email notifications for this cluster are delivered, select a notification mechanism and provide the connection and authentication information for the mail server.

Select **SMTP server with Mission Control fallback** to have Mission Control send notifications when your SMTP server is unavailable.

Use

SMTP server with Mission Control fallback

 to send email notifications

Confirm

SMTP server

No Mission Control

Mail server

Port

25

Username

Password

Sender email address

noreply@dynatrace.com

Email test address

Send test message

Emails - notifications

- Setup recipients of email notifications for Managed events, including updates

The screenshot shows the Dynatrace Settings interface. The top navigation bar includes links for Home, Settings, Emails, and Email notifications. The left sidebar is titled 'Settings' and contains a list of configuration categories: Public endpoints, Internet access, Emails (highlighted), SMTP server, Email notifications (highlighted), Preferences, API tokens, Backup, Automatic update, and Log monitoring. The main content area is titled 'Email notifications' and contains two sections: 'Notifications recipients' and 'Emergency notifications recipients'. Both sections have text boxes for entering email addresses. The 'Notifications recipients' section also includes two toggle switches: 'Also notify all active users with cluster admin rights' (checked) and 'Send email notification when update is available' (unchecked).

Home > Settings > Emails > Email notifications

Settings

- Public endpoints
Specify your public endpoints
- Internet access
Connect to Dynatrace Mission Control
- Emails**
Configure email settings
- SMTP server
- Email notifications**
- Preferences
Configure support, community and upda...
- API tokens
Manage secure access tokens
- Backup
Configure backup settings
- Automatic update
Automatic update settings
- Log monitoring
Network storage configuration

Email notifications

Notifications recipients

Recipients who will receive notifications about important cluster-, environment-, and account-related events. Please separate email addresses using commas.

[Email address input field]

☒ Also notify all active users with cluster admin rights

☐ Send email notification when update is available

Emergency notifications recipients

Recipients who will be contacted by the Dynatrace ONE team only in case of emergency. Please separate email addresses using commas.

[Email address input field]

Preferences – Pro-active support

- To facilitate pro-active support, your Dynatrace server transmits status information to Dynatrace Mission Control
- Some information is optional

Preferences

Dynatrace Managed Mission Control Support Services

Dynatrace Managed provides fully automated self-management capabilities that keep your system secure, reliable, and up-to-date. To achieve this, Dynatrace needs to send certain information to the Dynatrace Mission Control.



Report usage and billing information



Report Dynatrace cluster health



Report cluster and OneAgent events to Dynatrace Managed Mission Control Support Services



Dynatrace deployment health monitoring

Preferences – Use and Integration

- Send information about monitored technologies to pro-actively support any incompatibilities or technology-specific risks.
- Select product integrations for chat, help and support.

Monitored technologies and product adoption

Dynatrace pro-actively alerts you to any incompatibilities or technology-specific risks related to your environment. We report information about OneAgents, code modules, process technologies, hosts, ActiveGates, and related entities for support, product improvement and research purposes.

Relevant logs are accessible on each cluster node at <datastore_dir>\log\server\audit.rest.proxy.log.

Dynatrace companies (Dynatrace LLC and subsidiaries) [operate globally](#). Data may be transferred to, and processed by cloud services in the United States and other locations. For details, see [Dynatrace security policies and data-privacy settings](#).

☒ Send information about monitored technologies and feature usage

Dynatrace services and support

Dynatrace services and support ensure you get the most out of the Dynatrace Software Intelligence Platform. They include documentation, University, in-product chat, Community forum and support resources. You can read more at [Dynatrace services and support](#) website.

☒ Enable in-product Dynatrace ONE live chat

☒ Send users an invitation to the Dynatrace Community upon first login. Users will be able to ask questions in Dynatrace forums, access Dynatrace University and create Support tickets

☒ Integrate Dynatrace Help and Answers user forum content into search results

Preferences – Domain name and SSL Certificate Management


- The Dynatrace UI is only accessible over encrypted HTTPS connections.
- Allow automatic certificate management or provide your own.
- If disabled each cluster node and Cluster ActiveGate will need to be configured with a valid certificate
 - <https://www.dynatrace.com/support/help/shortlink/managed-ssl>

Domain name and SSL certificates management

Enable this setting to generate a domain name (a subdomain of dynatrace-managed.com) with a trusted certificate for your Dynatrace Managed cluster. All users in your environment can then access Dynatrace at <https://bsc032.dynatrace-managed.com/>.

Please note that this process may take a few minutes, once complete, you'll be redirected to the new URL.
Disabling this option results in SSL certificates and the cluster URL being rolled back to the previous version.

☒ Enable management of domain name and SSL certificates

 SSL certificate

Issuer: R3, Let's Encrypt
Subject: bsc032.dynatrace-managed.com
Expires: Sep 19, 2021

Date of renewing the certificate: Sep 03, 2021

Remote Access Permissions

- Dynatrace ONE can assist you remotely with Dynatrace Managed cluster upgrades and troubleshooting when you run into problems.
- To make this happen, a Dynatrace ONE product specialist must have permission to remotely access your Dynatrace Managed cluster.
- You can configure remote access permissions for your Dynatrace Managed cluster to authorize Dynatrace ONE to provide you with updates and pro-active support.
 - <https://www.dynatrace.com/support/help/shortlink/cluster-remote-access>

Remote access permissions

Configure remote access permissions for your Dynatrace Managed cluster so that authorized Dynatrace Support employees can provide you with updates, and pro-active support.
[How does Mission Control pro-active support work?](#)

☒ Allow Dynatrace Support employees remote access to this cluster's monitoring settings

Allow

all ^

all

approved

 Dynatrace employees who have appropriate permissions to access this cluster for purposes of pro-active support

API tokens

- Use the CMC API Tokens setting to manage cluster tokens
- Cluster APIs are available for easy automation of:
 - Environment Management
 - Configuration Management
 - Cluster Management
 - User/Group Management



API tokens

Generate a secure access API token that enables access to your Dynatrace Managed cluster management interface via our REST-based automate cluster management tasks with your 3rd party tools. Multiple API tokens can be created for different purposes. [Read API doc](#)

Token settings

Check out this [blog post](#) to find out more about the new Dynatrace API token format.

Create Dynatrace API tokens in the new format

Environment token management tokens

[Generate token](#)

Token name	Owner
------------	-------

Cluster tokens

[Generate token](#)

Token name	Owner	Disable/enable	Delete	Edit
------------	-------	----------------	--------	------

admin

Featured product news

Environment

Cluster Management

Support resources

Support Center

Release notes

Documentation

University

Community

Product ideas

Dynatrace API

Cluster API v1

Cluster API v2

Sign out

Dynatrace version

Backup

- Automatically backup the Dynatrace Cluster
- Determine what to backup
 - Cluster Configuration
 - User Sessions (consider GDPR)
 - Time-series metric data
- Define backup location
 - Shared cluster node NFS mount
- Define backup schedule
- <https://www.dynatrace.com/support/help/shortlink/managed-cluster-restore>

Configure backup

When enabled, Dynatrace Managed will automatically back up your configuration and monitoring data. For more information, see [Back up and restore a cluster](#).

☒ Enable cluster backup

☒ Include backup of user sessions (disable for GDPR compliance)

☒ Include time series metric-data (disable to retain configuration data only)

Set storage location

Network attached storage path for backup:

/dt-cluster-backup

Available storage

Unavailable - The path must point to a valid directory.

Backup schedule

Cassandra backups are performed on a daily basis.

Perform backups each day at 23:00 UTC-04:00.

Elasticsearch storage backups are triggered every 120 minutes.

Backup status

Automatic backup has not been performed yet.

Backup Sizing

- All important Dynatrace Server configuration files and monitoring data can be backed up automatically
 - All cluster nodes should be accessing the same NFS share mounted as a filesystem on each node in the cluster
 - The configuration files and Cassandra metrics are contained in an uncompressed tar archive, with one tar file per cluster node, which is updated daily
 - Elasticsearch is contained in a snapshot file, which is updated hourly
 - Transaction storage isn't backed up
 - Backup history isn't preserved, so the Dynatrace Server keeps only the latest backup
 - Network bandwidth utilization is limited to 30MB/s which is appropriate for 1 Gbps connections.
 - <https://www.dynatrace.com/support/help/shortlink/managed-cluster-backup-estimate>
-
- Size of a cluster backup = ("sum of metrics storage on all nodes" x 0.20) + sum of elasticsearch storage on all nodes

Automatic updates

- Choose a convenient time to update the managed cluster off-hours.
- Multiple nodes will be upgraded one-by-one to maintain cluster availability
- Older update packages will be removed automatically
- To save storage space, you can exclude specific update packages

Automatic update

Updates download from Mission Control is enabled.

☒ Install Dynatrace cluster updates automatically

Dynatrace updates are run automatically during the time frame that you select. Because installation causes brief downtime for all users, it's recommended that you select an 'off hours' time. Monitoring data is typically not lost during an update.

Update starts on Sunday at 02:00

To save storage space, you can exclude specific update packages. If you need excluded packages later, you can download them again. Some updates might be already deleted from Dynatrace repository, you can remove them from cluster permanently without option to re-download. You can't exclude a OneAgent update package for a OneAgent that is [configured as a standard agent](#).

Installation files

Type	Version	Size	Status	Action	Standard OneAgent version
OneAgent	1.217162.20210609-185653	1.38 GiB	available	<button>Exclude</button>	in 0 environments
JS agent	1.217152.20210531-134607	955.74 KiB	available	<button>Exclude</button>	-
ActiveGate	1.217144.20210526-112924	545.69 MiB	available	<button>Exclude</button>	-
Synthetic module	1.21740.20210603-030501	255.15 MiB	available	<button>Exclude</button>	-
Docker OneAgent	1.21734.20210428-091645	189.19 MiB	available	<button>Exclude</button>	-
ODIN	1.2170.20210526-105030	197 B	available	<button>Exclude</button>	-
OneAgent	1.215192.20210519-150820	1.37 GiB	removed	<button>Re-download</button>	in 0 environments
JS agent	1.215172.20210506-155120	943.28 KiB	removed	<button>Re-download</button>	-

Log Analytics

- Allow monitored host and process log file storage on the Dynatrace cluster
- Define patterns and custom log metrics
- Otherwise logs are only available as long as they are stored on the monitored hosts' disks
- <https://www.dynatrace.com/support/help/shortlink/log-monitoring-hub>

Log monitoring

By default, log data is stored on monitored hosts and is available on-demand.

You can optionally store log data on a network attached storage device that's accessible across all your cluster nodes as a virtual directory.

Note: Cluster restart is required following change to the file storage path.

☒ Use network attached storage

Network attached storage path:



Domain and Certificate Management

Let's start with the domain name name and cert management

Home > Settings > Preferences

Settings

- Public endpoints
Specify your public endpoints
- Internet access
Connect to Dynatrace Mission Control
- Emails
Configure email settings
- Preferences**
Configure support, community and upda...
- API tokens
Manage secure access tokens
- Backup
Configure backup settings
- Automatic update
Automatic update settings

Preferences

Pro-active support

Dynatrace Managed provides fully automated self-management capabilities that keep your system secure, reliable, and up-to-date. To achieve this, Dynatrace needs to send certain information to the Dynatrace Mission Control.

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

Dynatrace community

- ☒ Create Dynatrace community user account upon login
- ☒ Integrate Dynatrace Help and Answers user forum content into search results

Manage domain name and SSL certificates

Enable this setting to generate a domain name (a subdomain of [dynatrace-managed.com](https://aif633.dynatrace-managed.com/)) with a trusted certificate for your Dynatrace Managed cluster. All users in your environment can then access Dynatrace at <https://aif633.dynatrace-managed.com/>. Please note that this process may take a few minutes, once complete, you'll be redirected to the new URL. Disabling this option results in SSL certificates and the cluster URL being rolled back to the previous version.

- ☒ Enable management of domain name and SSL certificates

Activated by default

So what does it do?

For the cluster UI

Configure public endpoints

Dynatrace Web UI URL

<https://aif633.dynatrace-managed.com/> 

The address you normally use to access your Dynatrace cluster UI. Changing this will affect the links in problem notification emails.

☒ Enable automatic failover

Manage domain name and SSL certificates

Enable this setting to generate a domain name (a subdomain of dynatrace-managed.com) with a trusted certificate for your Security gateways.

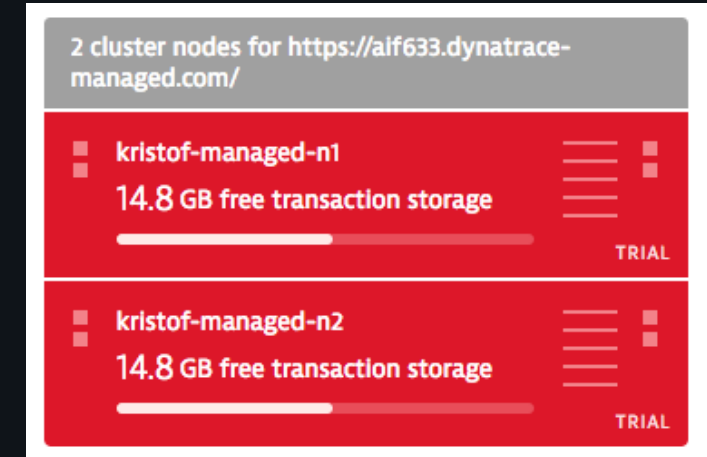
☒ Enable management of domain name and SSL certificates

Generated Security gateway domain name: **lbp047.dynatrace-managed.com**
IP addresses associated with this domain: **52.166.6.68**

For the Cluster ActiveGate

So what does it do?

- Creates a subdomain for dynatrace-managed.com
 - And a node subdomain: n[node-id].subdomain.dynatrace-managed.com
 - E.g.: <https://n01.aif633.dynatrace-managed.com/>
- Users can access the cluster through there
- The cluster nodes **do not** need to be exposed to the internet, only reachable by the user
- This subdomain is used in all emails, problem notifications sent by the cluster
- 3 month "Let's Encrypt" Certificates are generated and automatically renewed
- When DNS lookup is performed by the user, it will redirect to a particular node



Agent traffic
always load-
balanced

In order for it to work

Subdomain generated for each node

2 cluster nodes for https://alf633.dynatrace-managed.com/

 kristof-managed-n1.westeurope.cloudapp.azure.com

Version 1.132.95.20171127-132916

Size category of this node: TRIAL

You can use this node to try Dynatrace out, but you should increase your hardware capacity.
Node size category is decided based on the host's memory and the number of CPU cores.

Dynatrace can manage SSL certificate, disable to set own certificate

 kristof-managed-n1 

14.8 GB free transaction storage

TRIAL


 kristof-managed-n2 

14.8 GB free transaction storage

TRIAL

Storage

Disk space on / (/dev/sda1): 14.8 GB free space left out of 31.2 GB

 50.5 MB
Metrics storage

 1.6 GB
Dynatrace installation

 14.8 GB
Other files

Customize node endpoints

Dynatrace automatically detects node IP addresses. You can override this behaviour if you have multiple

IP address and port for OneAgent traffic

kristof-managed-n1.westeurope.cloudapp

Update configuration

✓ Current DNS entry point set on this node: kristof-managed-n1.westeurope.cloudapp.azure.com:8443

Web UI IP address

52.166.240.55

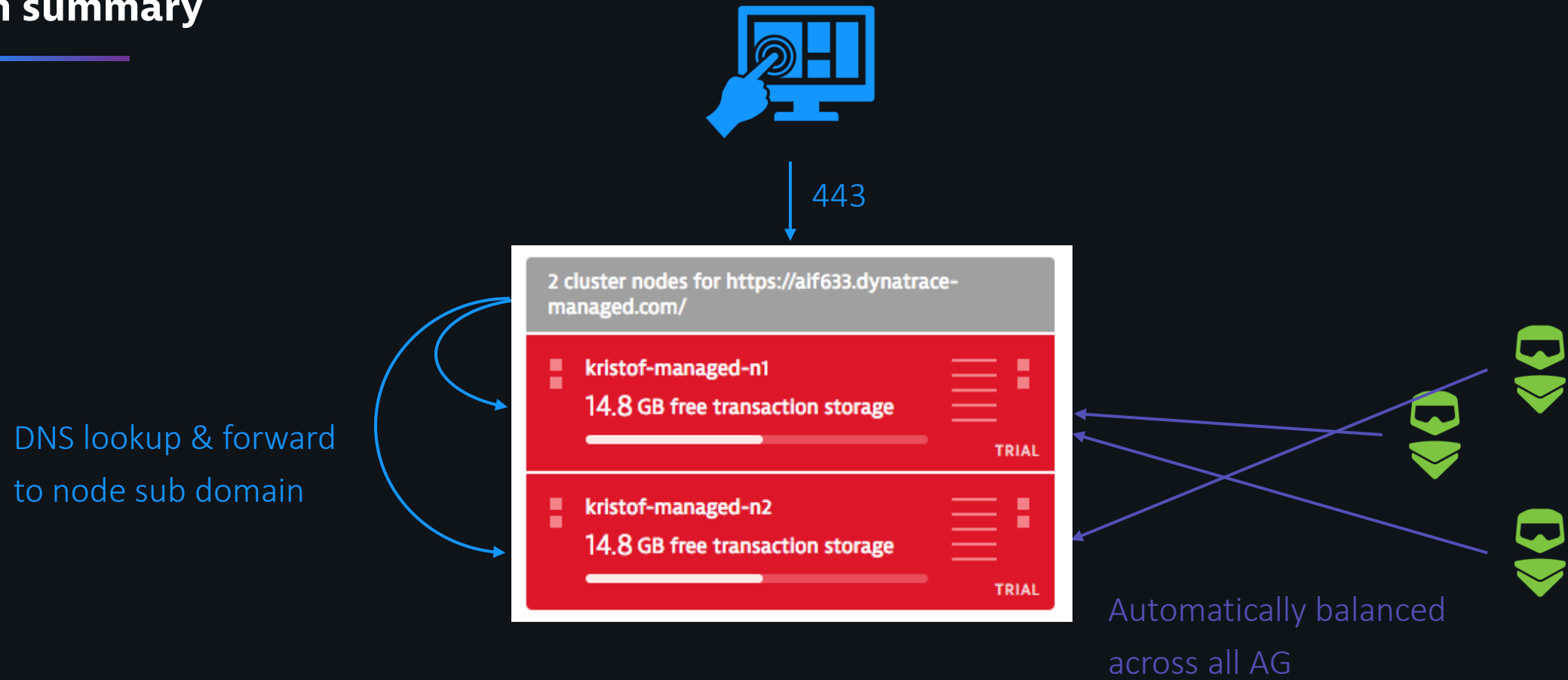
This address will be used by OneAgent to send monitoring data to this cluster node. Use an IP address and port number or a domain name. Note: the listen port of this cluster node is not affected by this setting.

DNS entry or ip address for Embedded ActiveGate to receive agent traffic.
Reachable by agents

IP address for node subdomain redirect.
Reachable by UI users

...ate management is **enabled**.
... custom certificate, first [Disable management of SSL certificates](#).
... ate, refresh the page.

In summary



What if you want to control your DNS and Certificates?

- You can add your own certificates for each node
- And enter your own DNS name
- Load balancer included (Nginx)
- Note for custom load balancer: context root cannot be changed
 - **Works:** dynatrace.customerdomain.com
 - **Does not work:** customerdomain.com/dynatrace
- Load balancer config
 - Probing URL: /rest/health
 - Stickiness: HTTP cookie, any cookie not used by Dynatrace
 - Algorithm: least connections

Cluster ActiveGate

- Public endpoint separated from the cluster nodes
- Reachable from the internet and correct certificate required
 - Domain and cert can also be managed by Dynatrace

1 Security Gateway

kristof-managed-sgw.w
esteurope.cloudapp.azu
re.com

Setting it up

DNS entry or ip address for AG to receive agent traffic.

Reachable by **OneAgents**

1 Security Gateway

kristof-managed-sgw.westeurope.cloudapp.azure.com

Customize Security Gateway endpoints

Dynatrace automatically detects the IP address of the Security Gateway. You can override that, for example if you have multiple interfaces or IP-forwarding in place.

IP address and port for OneAgent traffic

kristof-managed-sgw.westeurope.clouda

Update Security gateway configuration

This address will be used by OneAgent to send monitoring data to this Security gateway. You can customize IP, port or use a domain name. Note: the listen port of this Security Gateway is not affected by this setting.

Publicly available IP address

52.166.6.68

This address is used to send data from external **synthetic web check** locations and for **agentless RUM**. Dynatrace automatically generates a public DNS name for this address.

IP address where Synthetic and Agentless RUM data is sent to. Public DNS name is managed elsewhere.

Manage domain name and SSL certificates

Enable this setting to generate a domain name (a subdomain of dynatrace-managed.com) with a trusted certificate for your Security gateways.

☒ Enable management of domain name and SSL certificates

Generated Security gateway domain name: **lbp047.dynatrace-managed.com**

IP addresses associated with this domain: **52.166.6.68**

Turning off domain and certificate management

Manage domain name and SSL certificates

Enable this setting to generate a domain name (a subdomain of dynatrace-managed.com) with a trusted certificate for your Security gateways.

☒ Enable management of domain name and SSL certificates

Generated Security gateway domain name: **ibp047.dynatrace-managed.com**
IP addresses associated with this domain: **52.166.6.68**

Manage domain name and SSL certificates

Enable this setting to generate a domain name (a subdomain of dynatrace-managed.com) with a trusted certificate for your Security gateways.

☐ Enable management of domain name and SSL certificates

Security Gateway URL

https://kristof-managed-sgw.westeurope.cloud...

This URL is used to transmit to your Dynatrace cluster. Also agentless real user monitoring to transmit the monitoring signals.

Test connection to URL

This Security Gateway can receive monitoring data from:

- ✓ Synthetic monitoring
- ✗ external users of web applications (for agentless real user monitoring)
- ✗ internal users of web applications (for agentless real user monitoring)
- ✓ externally deployed OneAgent installations

⚠ There were some SSL certificate problems detected. They need to be fixed to enable agentless real user monitoring.

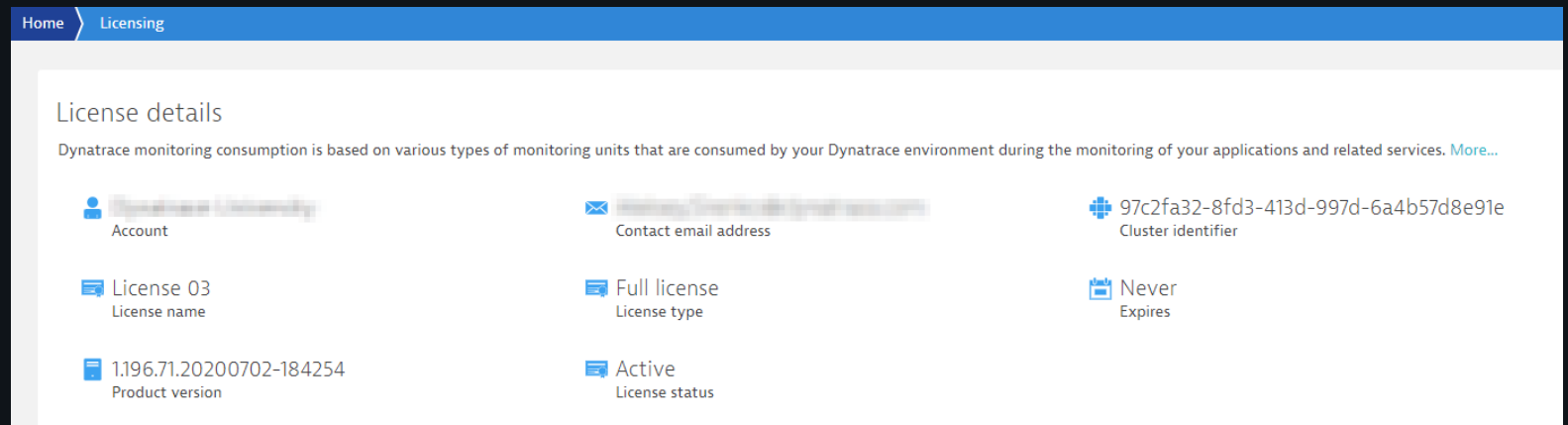
Custom DNS name that routes to Cluster ActiveGate
(can be load balanced)

Valid certificate required for Agentless RUM and Mobile App monitoring

Licensing

License Details

- Displays the following:
 - Account Name
 - License Name
 - Server Version
 - License Type
 - License Status
 - Contact Email Address
 - Cluster Identifier
 - Expiration date

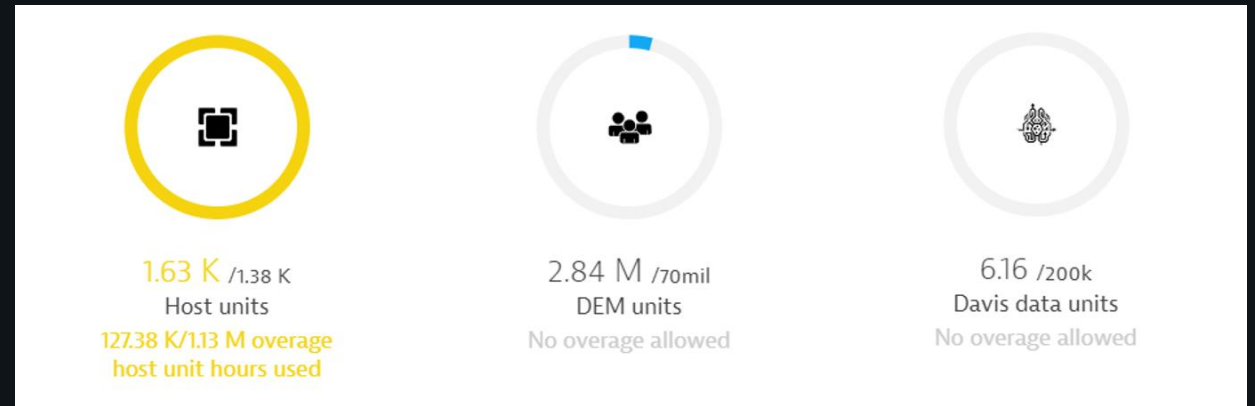


The screenshot shows the 'Licensing' section of the Dynatrace interface. It displays the following details:

Icon	Value	Label
Person icon	[Redacted]	Account
Envelope icon	[Redacted]	Contact email address
Plus icon	97c2fa32-8fd3-413d-997d-6a4b57d8e91e	Cluster identifier
Document icon	License 03	License name
Document icon	Full license	License type
Calendar icon	Never	Expires
Document icon	1.196.71.20200702-184254	Product version
Document icon	Active	License status

License Details Cont.

- Show the License Key
- Displays the license consumption and amount remaining for:
 - Host Units
 - DEM Units
 - Davis Data Units
- <https://www.dynatrace.com/support/help/shortlink/monitoring-consumption>





Overall License Consumption

- Displays the overall license consumption per environment for the following metrics
 - Host Units
 - DEM Units
 - Davis Data Units
- Edit license quotas per environment

Overall license consumption

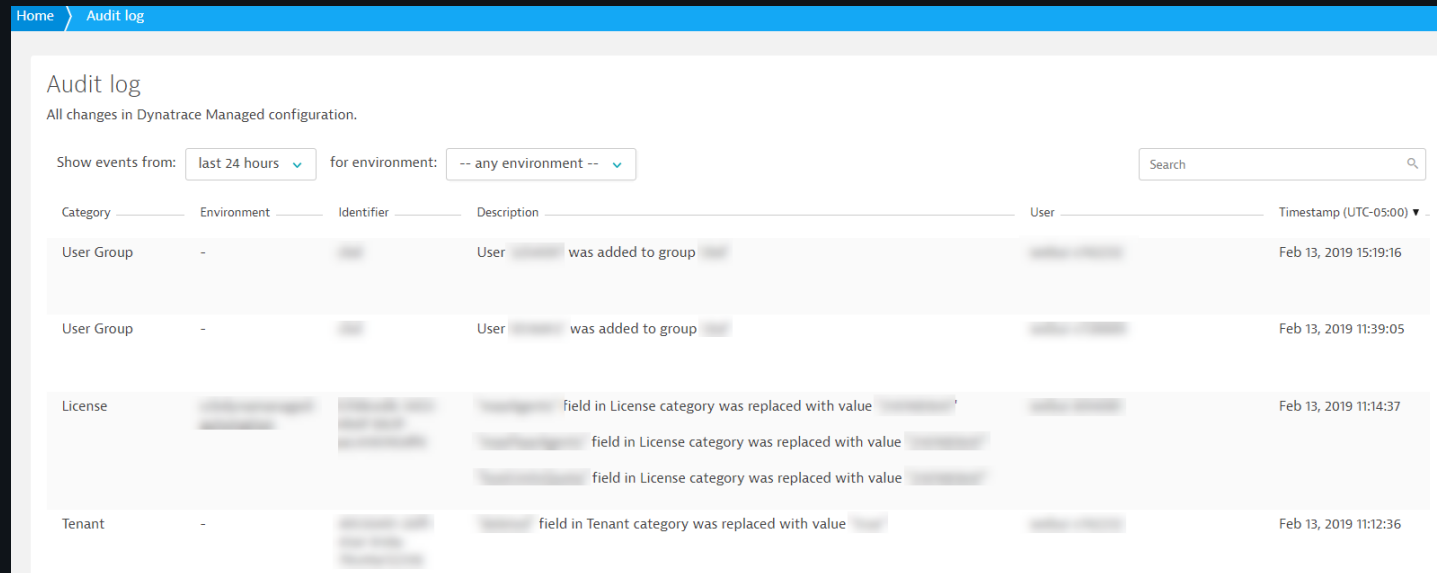
Shows an overview of your current consumption per environment. Total usage for the current license key includes usage under contracts from past years.

Filter this table

Environment ▲	Host Units ▾	DEM Units ▾	Davis Data Units ▾	Edit Quotas
PROD, Dev	0	0	0	
PROD, Testing/Dev	0.5	2.37 K	0	

Audit Log

Audit Log



The screenshot displays the 'Audit log' page in the Dynatrace interface. At the top, there's a navigation bar with 'Home' and 'Audit log'. Below the title, a subtitle reads 'All changes in Dynatrace Managed configuration.' The interface includes filters for 'Show events from:' (set to 'last 24 hours') and 'for environment:' (set to '-- any environment --'). A search bar is also present. The main content is a table with columns: Category, Environment, Identifier, Description, User, and Timestamp (UTC-05:00). The table lists several events, including 'User Group' additions and 'License'/'Tenant' field replacements.

Category	Environment	Identifier	Description	User	Timestamp (UTC-05:00)
User Group	-		User [redacted] was added to group [redacted]	[redacted]	Feb 13, 2019 15:19:16
User Group	-		User [redacted] was added to group [redacted]	[redacted]	Feb 13, 2019 11:39:05
License	[redacted]	[redacted]	[redacted] field in License category was replaced with value [redacted]	[redacted]	Feb 13, 2019 11:14:37
		[redacted]	[redacted] field in License category was replaced with value [redacted]	[redacted]	
		[redacted]	[redacted] field in License category was replaced with value [redacted]	[redacted]	
Tenant	-	[redacted]	[redacted] field in Tenant category was replaced with value [redacted]	[redacted]	Feb 13, 2019 11:12:36

- Allows for tracking changes performed within each monitoring environment
- Each change is associated to the username of the user that performed the change
- Helpful tool in tracking changes in environments

Questions?



Simply smarter clouds