AppDynamics Pro

Documentation

Get Started with AppDynamics SaaS

Get Started with AppDynamics SaaS

AppMan Advice

"Deploying APM in the Enterprise... the Path of the Rock Star"

Follow these steps to get started with AppDynamics.

If you are reading a PDF of this document, use your Help Center login to access the documentation at http://docs.appdynamics.com.

Get Your SaaS Account Information from AppDynamics

After signing up for AppDynamics SaaS, you receive a Welcome email containing important account information, including the Account Owner login. Save this information.

Design Your AppDynamics Deployment

- Learn about Business Transaction Monitoring and identify which critical business transactions you want to monitor.
- Learn about End User Experience and decide whether you want to use this feature.
- Learn about how to map your application components to the AppDynamics business application, tier, and node model. See Logical Model and Name Business Applications, Tiers, and Nodes.
- Based on the model, plan how you will specify AppDynamics application, tier, and node names during installation.
- For Java environments, decide whether you want to use object instance tracking.

Download the AppDynamics Agents

Download the AppDynamics agents from the Download Center. AppDynamics agents collect data from your application servers and other monitored systems and report to the Controller. Select the agents that are appropriate for your environment:

- Java Agent
- .NET Agent
- Machine Agent
  For details see Download AppDynamics Software.

Install the AppDynamics Agents

Install agents on the application servers you want to instrument and any other machines you want to monitor. Follow the instructions to install the AppDynamics Agents.

SaaS Login Credentials

SaaS Controller login credentials are included in the welcome email from AppDynamics.

To add additional login accounts contact the AppDynamics Support Team.

The SaaS Controller login is an Account Administrator credential. The Account Administrator can create other users for the account. See Account Administrator.

Connecting Agents to Your SaaS Controller Service

For agents to successfully connect to the Controller, configure the Controller host and port information using either the controller-info.xml file or the system properties of your JVM startup script.

To use HTTPS communication, enable SSL by setting the <controller-ssl-enabled> agent configuration property to "True". For details see App Agent for Java Configuration Properties, App Agent for .NET Configuration Properties, and Machine Agent Configuration Properties.

- The default ports for the SaaS Controller service are:
  - Port 80 for HTTP
  - Port 443 for HTTPS

If you need to specifically open up the communication ports (80 or 443) for the AppDynamics SaaS Controller IP address please request the IPs from the AppDynamics Support Team.

Access the AppDynamics UI from a Browser

Once you have installed the agents, launch your web browser and connect to the AppDynamics User Interface (UI). For SaaS, the URL includes the account name from the Welcome email:

```
http://<account-name>.saas.appdynamics.com/controller
```

When using SSL, use port 443 or https to access the Controller.

Review the Dashboards and Flow Maps

AppDynamics automatically discovers the Business Transactions in your application environment. Browse the Application Dashboard and see the Flow Maps to visualize your application. You can resize and move icons around on the flow maps.

Review Defaults and Configure Business Transactions, if Needed

The default configurations may need to be further customized for your environment. For example, AppDynamics may have discovered

transactions that you want to group together or even exclude, because you want to concentrate on the most important transactions. There may be business transactions that are not yet discovered for which you need to configure detection rules. See:

- Monitor Business Transactions
- Configure Business Transaction Detection

Review Defaults and Configure Databases and Remote Services, if Needed

AppDynamics automatically discovers "backends" such as databases, message queues, etc. by following calls in the Java or .NET code. Look at the databases and remote services dashboards to make sure all necessary backends are revealed. If needed, configure how backends are detected.

Review Default Heath Rules and Set Up Policies

AppDynamics provides default health rules that define performance parameters for business transactions, such as the conditions that indicate a slow transaction, or when too much memory is being used. You can adjust the thresholds that define when a health rules is violated, create new health rules, and set up policies to specify actions to automate when health rules are violated.

Review Default Error Detection

AppDynamics detects errors and exceptions. You can review and, if needed, modify the error detection rules. For example, some errors you may want to ignore.

Explore Additional Data and Metric Features

Explore these features to gain more insight into application performance:

- Data Collectors
- Business Metrics
- (for Java environments) JMX Metrics
- Machine Agent Custom Metrics

Configure Advanced Features

Additional features you may want to use include:

- End User Monitoring
- Custom Dashboards
- Automation
- System Integrations

Start Monitoring and Troubleshooting

Start getting the benefits of AppDynamics! See:

- AppDynamics in Action Videos
- AppDynamics Features

Questions?

For questions about using AppDynamics contact the AppDynamics Support Team.

Use a SaaS Controller

- Your SaaS Controller URL

If you are using the SaaS service for the AppDynamics Controller, simply open a web browser at the URL of the AppDynamics UI and log in with your AppDynamics credentials.

Your SaaS Controller URL

Your SaaS Controller URL is included in the welcome email from AppDynamics.

The URL is of the following form:

```
http(s)://<customer>.saas.appdynamics.com/controller
```

Login Credentials

Login credentials are included in the welcome email from AppDynamics.

To add additional login accounts contact the AppDynamics Support Team.

Connecting Agents to Your SaaS Controller Service

For agents to successfully connect to the Controller, configure the Controller host and port information using either the controller-info.xml file or the system properties of your JVM startup script.

To use HTTPS communication, enable SSL by setting the <controller-ssl-enabled> agent configuration property to "True". For details see App Agent for Java Configuration Properties, App Agent for .NET Configuration Properties, and Machine Agent Configuration Properties.

- The default ports for the SaaS Controller service are:
  - Port 80 for HTTP
  - Port 443 for HTTPS

Important: If you need to specifically open up the communication ports (80 or 443) for the AppDynamics SaaS Controller IP address please request the IPs from the AppDynamics Support Team.

SMTP Service for SaaS

To enable email and SMS notifications you must configure SMTP. See Configure the SMTP Server.

For SaaS users, AppDynamics has an SMTP service running on every machine.

The configuration is:

host: localhost
port: 25

No authentication is needed.

SaaS Limitations

Compared to an on-premise installation, the following are limitations in the SaaS environment:

- Flow maps show a maximum of the last 60 minutes of data, regardless of whether the Time Range is set to a larger range. Other graphs will display according to the selected Time Range.
- There is a minimum time lag of 4 minutes before data is displayed in the UI.

- Custom action scripts are not supported.
- LDAP integration is limited.
- The business transaction limit is 200 per business application, unless you are using a dedicated Controller.
- Configuration settings related to data retention is limited.

Contact AppDynamics Support for details.

See also http://www.appdynamics.com/products-saas-on-premise.php.

Contact Support

For questions about the service contact the AppDynamics Support Team.

SaaS Availability and Security

This topic summarizes the service availability and security AppDynamics provides for customers who use the AppDynamics SaaS platform.

Service Availability

AppDynamics makes every best effort to operate and manage the AppDynamics SaaS platform with a goal of 99.5% uptime Service Level Agreement (SLA), excluding planned maintenance windows. AppDynamics actively monitors the latency of the SaaS platform 24/7 from different locations around the world to ensure AppDynamics delivers the best quality of service.

Customer Account Login Security

The AppDynamics user interface (UI) uses TLS 1.0 with AES 256 bit encryption terminated at the server to ensure end-to-end security over the wire. For additional security, AppDynamics can restrict UI access to customer corporate networks.

Hosting

The AppDynamics SaaS platform (servers, infrastructure and storage) is hosted in one of the largest Tier III data centers in North America. The data center is designed and constructed to deliver world-class physical security, power availability, infrastructure flexibility, and growth capacity. The data center provider is SSAE 16 SOC 1 Type II compliant, which means that it has been fully independently audited to verify the validity and functionality of its control activities and processes.

Every server is operated in a fully redundant fail-over pair to ensure high availability. Data is backed up nightly, stored redundantly and can be restored rapidly in case of failure. AppDynamics also provides an off-site backup service that is available at additional cost.

Security updates and patches are actively evaluated by engineers and are deployed based upon the security risks and stability benefits they offer to the AppDynamics SaaS platform and customers.

Data Access

Access to the AppDynamics SaaS platform infrastructure and data is secured by multiple authentication challenges including RSA and DSA key pairs, passwords, and network access control lists. Infrastructure and data access is restricted to AppDynamics employees and contractors, all of whom are under strict confidentiality agreements.

System and Network activity is actively monitored by a team of engineers 24/7. Failed authentication attempts are audited and engineers are paged immediately so that any possible intrusion or threat can be investigated promptly. Standard firewall policies are deployed to block all access except to ports required for AppDynamics SaaS platform and agent communication.

Data Collection

AppDynamics agents collect metrics that relate to the performance, health and resources of an application, its components (transactions, code libraries) and related infrastructure (nodes, tiers) that service those components.

Data Communication

AppDynamics agents typically push data using one-way HTTP or HTTPS connections to a single host (a Controller) which has been allocated to one or more customer accounts. AppDynamics offers dedicated Controllers for customers who require their data to be isolated.

For added security, agents can be configured to send data using encrypted transmission by simply selecting HTTPS port 443 and setting "controller-ssl-enabled" to true in the agent configuration. AppDynamics agents also have built-in support for outbound HTTP proxies for customers using these security mechanisms.

A single agent with the default configuration will typically push between 300KB to 500KB of data per minute depending on application characteristics. AppDynamics uses random staggering on agent data communication to the AppDynamics SaaS platform so traffic is spread evenly to minimize bursts and spikes of network traffic from your data center to the AppDynamics SaaS platform.

# of Agents	Typical Network Bandwidth Used (per min)
1	300KB to 500KB
100	4Mbit to 6.4Mbit
1000	40Mbit to 64Mbit

These figures assume a 1:1 relationship between an agent and a JVM/CLR.

