citrix

White Paper

Machine Learning in Citrix ADM Service

Powerful analytics, stronger application security, and predictive forecasting with machine learning algorithms

The Growing Importance of Insight

In case the trends were not apparent before, the COVID-19 pandemic has only further revealed the need for businesses to embrace modern AI and machine learning technologies to translate massive amounts of historical data into actionable analytics, predictive models, and stronger security policies. A sudden, widespread shift to remote work has prompted companies to reconsider their digital transformation strategies—while bad actors are simultaneously leveraging uncertainty to attack.

The Machine Learning Advantage

With the sheer amount of data available in a modern application delivery infrastructure, machine learning is critical for detecting trends and anomalies that are not necessarily apparent.

Harnessing historical data helps teams create better, more personalized user experiences by ensuring applications are performing properly, routine tasks are automated, and future trends are forecasted accurately to facilitate preemptive action. At the same time, machine learning algorithms can continually learn what normal usage looks like to rapidly identify potentially malicious behavior—and take action promptly.

Citrix Application Delivery Management (ADM) service is uniquely positioned to take in an immense amount of data from the application delivery infrastructure—application, server, client, and individual transaction requests and response data, for example. Artificial intelligence and machine learning in Citrix ADM service are useful for more than just insights on this data; these technologies are key drivers of business strategy and user experience. After all, companies that use AI and machine learning as part of their business strategies and operations see increased revenue, reduced costs, and greater customer retention.

Citrix ADM service is a cloud-based controller that provides simple, agile management for the entire application delivery infrastructure, including all Citrix Application Delivery Controller (ADC) instances across hybrid, multi-cloud environments. Routine workflow activities such as onboarding and updating ADCs, renewing SSL certificates, allocating licenses, and remediation are managed through a single pane of glass. AI and machine learning capabilities assist administrators in making decisions and enforcing a consistent security posture. And with Citrix ADM service in Citrix Cloud, there are no installations or updates necessary to enjoy the latest features.

Powerful Analytics with Citrix ADM Service

Citrix ADC is available in a number of form factors and can be deployed in a number of flexible ways across hybrid, multi-cloud environments. Citrix ADM is an essential management and analytics tool as it provides a unified, holistic view across all Citrix ADC instances with a number of features that make managing capacity, analytics, and security straightforward. Machine learning on Citrix ADM service expands on the already wide breadth of features to drive a better experience for both users and customers.

With the considerable number of applications and Citrix ADC instances in any given application delivery environment, the machine learning capabilities of Citrix ADM service are invaluable for transmuting massive amounts of data into valuable, actionable insights that drive business decisions and user experience. Using a variety of algorithms and statistical techniques, Citrix ADM creates live models that are quite literally unique to each application environment.

By defining typical thresholds for performance, resources, and security, Citrix ADM service relieves admins of labor-intensive modeling tasks, enabling them to focus on more valuable activities.

At the same time, Citrix ADM is incredibly effective at separating real performance or security concerns from miscellaneous noise, alerting the admin only when their attention is needed. The result is a better, more reliable application experience for users and less worry for the security and application administrators behind the scenes.

Server Response Time Baselining

When load balancing application traffic, Citrix ADC distributes client requests across multiple backend servers to optimize resource utilization. Citrix ADC utilizes a number of load balancing algorithms to determine how to most logically distribute this potentially high volume of requests. While backend servers will often perform well with similar response times, there is always the potential for unexpected server response degradation in real world scenarios.

Realistically, it is a difficult, time-consuming chore for administrators to manually assess and define appropriate thresholds for server response time, especially considering the sheer volume of applications and backend servers that are likely being utilized. Additionally, "typical performance" is a moving target that can be difficult to determine manually. This is where Citrix ADM service with its machine learning capabilities really excels.

Citrix ADM service's intelligent analytics leverages machine learning in order to accurately define a baseline performance for server response times of each application. The server delay model for Citrix ADM service uses the Breakout Detection algorithm at its core to determine significant deviations from the baseline performance levels that persist over significant periods of time. This algorithm is specialized for level shifts, robust against anomalies and noise, and has been extensively tested and verified to work well in this use case.

It's also critical that Citrix ADM is not only able to notify administrators about anomalous performance degradation, but it is also able to distinguish and avoid notifying users of insignificant events like short-term spikes.

In the case that there is a change in server response time performance, Citrix ADM service will determine whether or not this change is statistically significant. When the response time deviates from the mean significantly and consistently over a period of time, this is flagged as anomalous.

Citrix ADM service is constantly digesting data on server response times for applications and reevaluating on a rolling basis in order to automatically and accurately calculate acceptable thresholds and identify significant anomalies. Administrators are alerted only when significant anomalies are detected while short spikes and other miscellaneous noise are ignored. This frees up time and resources for administrators, who are able to focus on more important work and only take corrective action when Citrix ADM service determines that it is actually needed.

Predictive Analytics for Resource Utilization

To provide the best possible application experience for users and customers, it is critical that there is sufficient resource capacity to satisfy the demands of fluctuating traffic. In this case, "resources" refers to CPU, memory, and disk usage, and demands can vary wildly across different deployments.

Administrators typically monitor resource utilization to ensure demands are within acceptable thresholds and look for traffic increases that come during peak hours, seasonal demand, and other events. Because of how critical the user experience is, thresholds are generally set low out and resources are overprovisioned in advance out of an abundance of caution. Autoscaling on cloud deployments serves a similar purpose, but even this is a reactive solution.

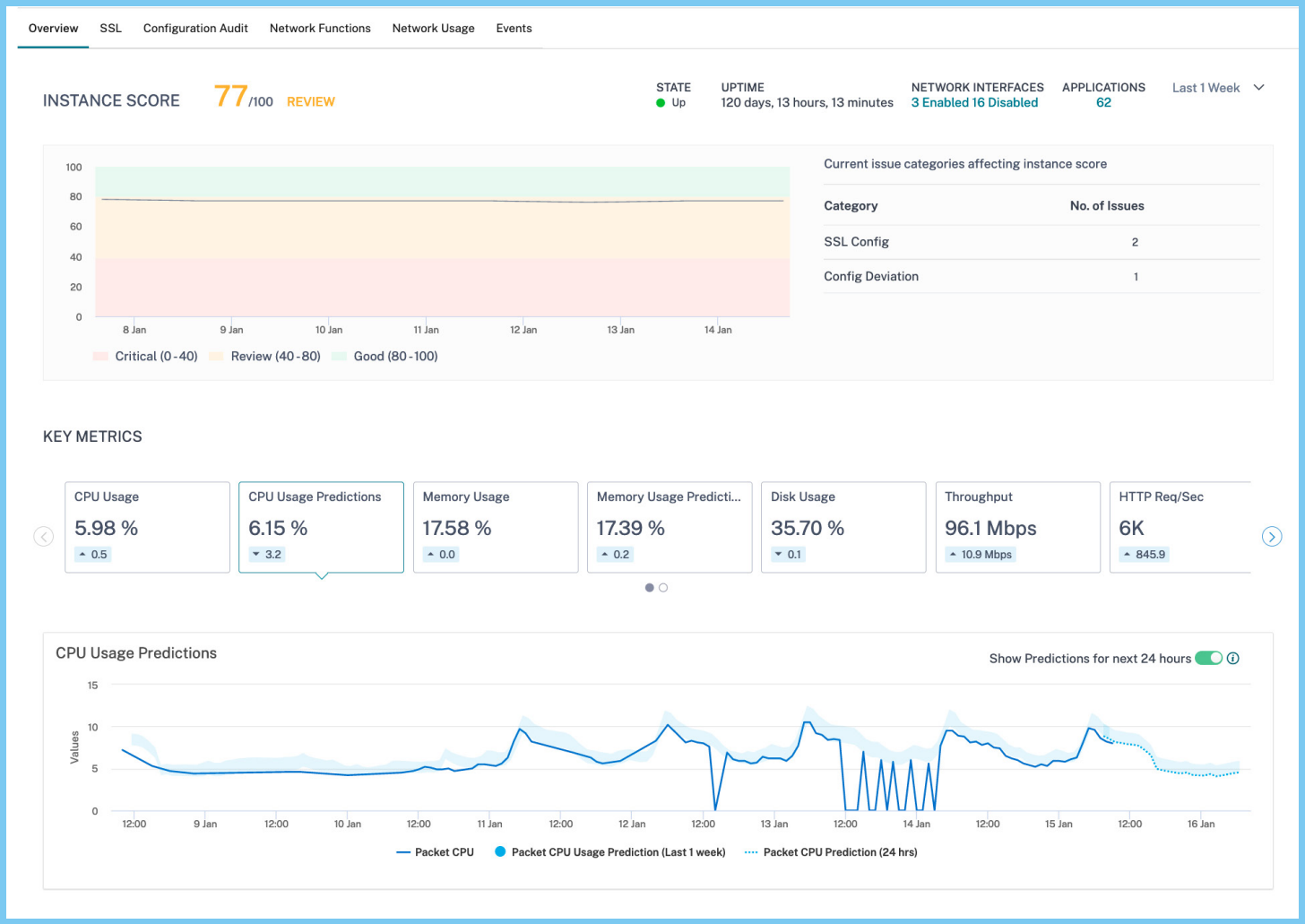
For a proactive and efficient approach, Citrix ADM service utilizes machine learning to observe trends in resource utilization to forecast and scale to meet future demand with a relatively high degree of accuracy. Using time series decomposition and estimation techniques, Citrix ADM breaks down the time series to better understand the elements of baseline level, trends, seasonal fluctuations, and irregular noise.

The result is that Citrix ADM service is able to intelligently determine acceptable thresholds for resource utilization, relieving administrators of the need to manually define them. Citrix ADM service also predicts future hourly resource demand for the next 24 hours using the aforementioned machine learning techniques and with a specified accuracy index.

This means that if demand is expected to exceed acceptable boundaries, administrators are able to take a proactive approach by provisioning resources optimally. This ensures that demand is met and user experience for applications remains top-notch.

Application Security and Anomaly Detection

With Citrix ADM service, machine learning capabilities are used not only to keep applications performing at their best, but also to ensure they are secure and protected against increasingly complex attacks and malicious actors. This can help ensure a consistent security profile across all deployments while using



aggregate data from all Citrix ADC, Web App Firewall (WAF), and bot management instances to continually train Citrix ADM machine learning models.
When a bad actor attempts an account takeover attack, for example, they may utilize stolen or otherwise compromised credentials for other accounts to gain account access with credential stuffing or automatic password spraying attacks. Because Citrix ADM service creates a model of the typical ratio of login successes and failures, it is able to notify security administrators of subtle deviations which may have otherwise gone unnoticed by human observers.

Using machine learning techniques similar to those used to predict resource utilization, Citrix ADM service builds an expected threshold for typical client connections factoring in considerations like seasonality, trends, and noise. If an anomalous excess of client connections is detected, security administrators are again alerted and able to take timely action.

Citrix ADM service is able to detect other anomalous deviations across a number of categories, including excessively high upload or download numbers, large data transactions, high request rates, and unique IP addresses from any particular location. More information on Citrix ADM service protection against web scraping attacks and anomaly detection is available in the respective Citrix blogs.

With cyberattacks increasing in sophistication and subtlety, Citrix ADM service machine learning models built around each unique deployment situation are invaluable in detecting and stopping these violations in their tracks. Because Citrix ADM service is cloud-delivered, it's available from a central, unified console accessible anytime, anywhere. This also means that the latest features and attack detection capabilities are available in Citrix ADM service the moment they are released without any updates necessary.

Application Usage Anomaly Detection

Just like Citrix ADM service is able to intelligently determine typical usage thresholds for resources, so too is it able to monitor traffic behavior for individual applications for anomalies. This traffic pattern analysis extends to key metrics such as response time, throughput, data volume, and requests per second for each application.

Traffic to an application can be unpredictable, and unusual application performance deviations can occur over specific periods of time. Administrators need to respond to these anomalies to troubleshoot accordingly and ensure that user experience remains uncompromised.

When Citrix ADM service's intelligent analytics determine that one application's usage is increasing suddenly and may exceed the application delivery controller's license limit, administrators are notified and able to allocate more licenses or throttle the application request rate if the baseline increase isn't desirable. If this is an indicator of a potential security threat, it will be logged, and details will be available in the Citrix ADM service's Security Violations tab.

In other cases, Citrix ADM service can identify applications whose usages tend to be especially volatile with frequent spikes or drops. These applications are suggested as ideal candidates for transition to the public cloud or use with the flexible pooled capacity licensing options offered by Citrix ADC.

Application usage anomaly detection on Citrix ADM service can also be invaluable for catching usage issues after rolling out new code for an application. Here, IT Ops administrators are able to better understand the impact that key events including new code deployment, app maintenance, and application or ADC-level failures may have on usage. More information on these features is available in the Citrix ADM service documentation.

Get Started with Citrix ADM Service

Citrix ADM service offers holistic, centralized visibility and management for your entire application delivery infrastructure across hybrid, multi-cloud from a single pane. With Citrix ADM service on Citrix Cloud, the latest features and functionalities are available anytime, anywhere, with no update installations necessary. Learn more and get started with Citrix ADM service today.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States