NetScaler Intelligent Traffic Management

Machine translated content

Disclaimer

Contents

Neue Features

April 29, 2022

Neue Funktion/Erweiterung	Version
Warnungen —Diese Funktion überwacht Leistungsprobleme oder Anomalien Ihrer konfigurierten Plattformen von einem Endbenutzer-Netzwerk auf der ganzen Welt aus.	2022.02.15
Lokale Persistenz —Diese Funktion bietet die Möglichkeit zur Entscheidungssicherheit, wenn sie aktiviert ist. Die Anforderungen werden mithilfe der IP-Subnetzmaske identifiziert, deren Länge konfigurierbar ist. Wenn ein Kunde beispielsweise innerhalb eines bestimmten Zeitraums (Persistence TTL) eine Anfrage an dieselbe Anwendung wiederholt (Persistence TTL), wird die ursprüngliche Entscheidung zurückgestellt.	2021.12.09
AWS ELB Connector —Dieser neue Connector ruft die Metriken `HealthyHostCount`, `UnHealthyHostCount` und `Load Balancer Capacity Units (LCUs)` von AWS ELB über Fusion ab. Es bietet Kunden ein integriertes Load-Balancing-Erlebnis und Einblick in Fusion-Metriken, die in ihren Openmix-Anwendungen verfügbar sind.	2019.08.16
Plattformtyp ändern (Privat in Community): Mit dieser neuen Funktion können Kunden die aktuellen Einstellungen ihrer privaten Plattform oder GSLB ändern, um stattdessen auf die Community-Plattform zu verweisen. Diese Funktion ist nützlich für Kunden, deren private Plattformen in einem öffentlichen Rechenzentrum oder einer Cloud-Region gehostet werden.	2019.07.03

Neue Funktion/Erweiterung	Version
Neues Dashboard —Das neue ITM-Dashboard ist jetzt betriebsbereit, informationsreich, anpassbar und insgesamt nützlicher als die Vorgängerversion. Im neuen Dashboard können Sie Diagramme zu Radarsitzungen, Radarleistung, Openmix Traffic Management Decisions und Sonar Monitoring Status anzeigen. Sie können mehrere Dashboards erstellen, die jeweils auf eine Ansicht zugeschnitten sind, die Ihnen wichtig ist. Sie können auch den ITM Visualizer oder das Dashboard als Standardlandesseite festlegen.	2019.06.27
Fusion-Quarantäne: Diese Funktion verschiebt den fehlgeschlagenen Fusion-Datenfeed eines Kunden in Quarantäne, wenn der Feed ausfällt oder in einem Abfrageintervall von weniger als 24 Stunden ausgeführt wird. Fusion wendet die Quarantänelogik an, um zu verhindern, dass diese fehlerhaften Feeds ausgeführt werden, um Ressourcen (CPU/Speicher) zu sparen und Auswirkungen auf andere gute oder gültige Fusion-Datenfeeds zu vermeiden.	2019.06.19
Plattformen für Openmix aktivieren/deaktivieren - Eine Plattform kann jetzt für Openmix aktiviert oder deaktiviert werden, indem die Schaltfläche **Openmix Enabled** in den Plattformeinstellungen ein- oder ausgeschaltet wird. Wenn eine bestimmte Plattform für Openmix deaktiviert ist, wird diese Plattform in Openmix-Entscheidungen nicht berücksichtigt.	2019.04.09

Neue Funktion/Erweiterung	Version
Platform Geo —Mit dieser Funktion können Kunden den einer Plattform zugewiesenen Geo-Standort anzeigen und verwalten. Standardmäßig ist privaten Plattformen kein **Geo-Standort** zugewiesen. Wenn ein Benutzer eine private Plattform erstellt und einen Radar-Sonde konfiguriert, verwenden wir die Sonde-URL, um die Plattform zu lokalisieren. Alternativ kann der Benutzer einen Geo manuell zuweisen, ohne sich auf den Radar-URL-Pfad zu verlassen. Für GSLB- und F5-Konfigurationsimporte finden wir die öffentliche IP und verwenden diese als **Geo** der Plattform. Community-Plattformen erben standardmäßig den ursprünglichen Speicherort der Plattform.	2019.04.09
Visualizer: Drilldown zur Bundesstaatsebene: Aktive Warnungen mit Informationen über die Leistung und Verfügbarkeit von Clouds, Rechenzentren, CDNs und anderen Diensten. Diese Warnungen werden auf Bundesstaatsebene innerhalb der Vereinigten Staaten gemessen und angezeigt.	2019.04.01
Visualizer: F5- und GSLB-Importe - F5- und GSLB-Importe: Sie können jetzt eine Plattform über eine GSLB- oder F5-Konfiguration importieren. Die grundlegenden Site-Informationen (IP und Name) werden als ITM-Plattformen importiert. ITM lokalisiert die Site und ermöglicht die Anzeige der Plattform im Visualizer zur Leistungsanalyse.	2019.03.29
G-Core Purge Adapter —Der G-Core CDN-Spüladapter wurde jetzt zur Liste der Adapter hinzugefügt, die ITM für die Ausführung von Purges unterstützt.	2019.03.29

Neue Funktion/Erweiterung	Version
Radar DSA 3 für alle Community-Anbieter —Um die Radar-Community und die Genauigkeit unserer Benchmarks kontinuierlich zu verbessern, haben wir kürzlich einen neuen Dynamic Content Benchmark veröffentlicht. Dieser neue Benchmark hat eine dynamische HTML-Seite und eine Signatur, mit der die Messung verifiziert werden kann.	2019.03.21
Visualizer —Der ITM-Visualizer ist ein intuitives und intelligentes Tool, mit dem Sie die globale Leistung von ISPs und Services überwachen und analysieren können. Die ITM Visualizer-Benutzeroberfläche bietet aktive Warnmeldungen mit Informationen zur Leistung und Verfügbarkeit von Clouds, Rechenzentren, CDNs und anderen Diensten. Die ITM-Community misst diese Warnungen auf der ganzen Welt. ITM Radar sammelt über die Radar-Community Milliarden von Messungen von echten Benutzern auf der ganzen Welt. Es verwendet ein Crowdsourcing-Modell, um diese Alarme zu messen.	2019.03.08
Guided Tours (Walk-throughs) für Visualizer und Openmix sind ab sofort im **ITM Demo Portal** verfügbar. Das Demo-Portal kann über das Hilfesymbol im ITM-Portal aufgerufen werden. In der rechten unteren Ecke des **Demo-Portals** sehen Sie ein Symbol, das die Führungen startet.	2019.03.08

Hinweise zu Drittanbietern

September 14, 2023

NetScaler Intelligent Traffic Management Benachrichtigungen von Drittanbietern (PDF)

Glossar

September 14, 2023

Begriff	Beschreibung
Anwendung	Eine Openmix-Anwendung ist eine Spezifikation einer Load-Balancing-Logik, die innerhalb des Portals konfiguriert werden kann. Die Anwendung wird für jede Anfrage an Openmix bearbeitet und eine Routing-Entscheidung wird auf der Grundlage der angegebenen Logik getroffen. Anwendungen können für eine oder mehrere Arten von Inhalten verwendet werden. Ein Kunde hat möglicherweise eine Anwendung für einen Inhaltstyp mit hohem Geschäftswert und eine andere Anwendung für Inhalte, die einen geringeren Wert haben und unterschiedlich weitergeleitet werden müssen. Beispielsweise kann der Kunde eine Anwendung für Inhalte haben, die allen Benutzern angezeigt werden, wobei der Schwerpunkt auf der Weiterleitung zum schnellsten Anbieter liegt, unabhängig von den Kosten. Der Kunde hat möglicherweise auch eine andere Anwendung für selten gezeigte Inhalte, die sich auf die Kostenoptimierung zwischen Anbietern für Inhalte mit geringerem Wert konzentriert. Im obigen Szenario hätte der Kunde zwei Openmix-Anwendungen.

Begriff	Beschreibung
Messungen der Gemeinschaft	Community-Messungen werden im Rahmen eines Crowdsourcing-Modells durchgeführt, das dem Kunden einen Überblick über die Leistung und Verfügbarkeit eines Anbieters auf geografischer und logischer Ebene weltweit bietet. Community-Messungen stehen teilnehmenden Community-Mitgliedern kostenlos zur Verfügung (Installation des JavaScript-Tags erforderlich). Der Zugang zu Community-Daten für nicht beitragende (d. h. nicht JS-integrierende) Organisationen wird in Rechnung gestellt.
Entscheidung	Eine Openmix-Entscheidung wird als einzelne Anfrage an einen der Load-Balancer von NetScaler spezifiziert. Bei DNS handelt es sich um eine einzelne DNS-Anfrage an die DNS-Load-Balancer. Bei HTTP ist es eine GET- oder HEAD-Anfrage an den Openmix-HTTP-Endpunkt.
Messung	Eine Messung bezieht sich auf Radar und die Erfassung von Daten von Endbenutzern über die Leistung einer Dienstanwendung. Für Gemeinschaftsmessungen siehe Gemeinschaftsmessungen.
Plattform	Eine Plattform ist ein CDN, eine Cloud, ein Rechenzentrum oder ein anderer Endpunkt, den der Kunde entweder in Radar überwachen oder innerhalb der Openmix-Anwendung verwenden möchte.

Begriff	Beschreibung
Private Messung	Bei privaten Radarmessungen werden Messungen oder Telemetrie (im Fall von Streaming) über die Erfahrung der Endbenutzer zurückgemeldet, die nicht mit der Community geteilt werden. Dies kann der Fall sein, wenn ein Kunde Folgendes messen möchte: + seine eigene Rechenzentrumsarchitektur (n) + Verwendung seines eigenen Testobjekts oder seiner eigenen Seite + Verwendung seines eigenen Vertrags mit einem Anbieter + Qualität der Audio/Video-Erfahrung für Endbenutzer

Radardatendefinitionen

April 21, 2020

Benchmark-Partner und Radar-Community-Mitglieder, die das Radar-Tag eingesetzt haben, können optional Zugriff auf ihre Radar-Messungen erhalten. Bei Benchmark-Partnern teilen wir Messungen dieses Partners unabhängig von der Seite, auf der das Radar-Tag eingesetzt wurde oder wann die Messung durchgeführt wurde. Community-Mitglieder können alle Messungen ihrer Webbesucher sehen, unabhängig davon, welcher Benchmark-Partner gemessen wird.

Kundenradar-Datenfreigabe

Radar-Tag-Bereitsteller können optional auf eine Teilmenge der Felder zugreifen, die wir vom Radar-Client erhalten, wenn eine Radarmessung auf ihrer Website durchgeführt wird. Benutzer-IP-Adressen werden anonymisiert, bevor Berichte generiert werden. Protokollbeschreibungen finden Sie in der Netscope (NEM) Dokumentation.

Raw-Radar-Messungen

Raw-Radar-Messungen enthalten eine Teilmenge der Felder, die wir vom Radar-Client erhalten, wenn eine Radar-Messung durchgeführt wird. Benutzer-IP-Adressen werden anonymisiert, bevor Berichte generiert werden.

Die Berichte können täglich oder in Echtzeit zur Verfügung gestellt werden, die Messdaten in weniger als 5 Minuten liefern.

Die Dateien können TAB-Trennzeichen, CSV- oder JSON-Format sein. Protokollbeschreibungen und Berichte finden Sie in der Netscope-Dokumentation.

Autonome Systemnummern

https://s3-eu-west-1.amazonaws.com/community-radar/ref/asns.json.gz

Community-Provider-IDs (öffentliche)

https://s3-eu-west-1.amazonaws.com/community-radar/ref/providers.json.gz

Sondenarten (Messarten)

https://s3-eu-west-1.amazonaws.com/community-radar/ref/probetypes.json.gz

---

Antwortcodes

Code	Modul	Beschreibung	Wert
0	Alle	Erfolg	Messwert
1	Fernsondierung	HTTP-Anforderung-Timeout	0
2	Fernsondierung	RTMP-Verbindung fehlgeschlagen	0
3	Fernsondierung	RTMP-Stream nicht gefunden	0
4	Fernsondierung	Ungültige HTTP-Datei	0
5	Navigation Timing	Navigation Timing API nicht unterstützt	0

Marktkodizes

Code	Name	ISO-Abkürzung
0	Unbekannt	XX
1	Nordamerika	Nicht verfügbar
2	Ozeanien	OC
3	Europa	EU
4	Asien	AS
5	Afrika	AF
6	Südamerika	SA

Ländercodes

Basierend aufISO 3166 -1 Alpha 2

https://s3-eu-west-1.amazonaws.com/community-radar/ref/countries.json.gz

Regionscodes

Es gibt keine ISO-Standards für Regionen, die uns bekannt sind. Darüber hinaus bietet unser GEO-Anbieter Regionen nur für eine kleine Teilmenge von Ländern an. Nach ihren Dokumenten besteht das Ziel von "Regionen"darin, bestimmte Länder in Gebiete zu unterteilen, die größer sind als Staaten. Zum Beispiel "US - Southwest"

Zunächst stellen wir Ihnen unsere eigenen numerischen "Regions-IDs"und ein Mapping zur Verfügung:https://s3-eu-west-1.amazonaws.com/community-radar/ref/regions.json.gz

> **HINWEIS:** Wir behalten uns das Recht vor, das Format dieser Datei zu ändern. Jeder Code, der zum Laden in diesen Zuordnungen erstellt wurde, muss in diesem Sinne erstellt werden. Langfristig wird es einen API-Aufruf geben, um diese Mappings herunterzuladen.

Zustandscodes

Es gibt einen ISO-Standard für Zustände3166-2. Wir prüfen, ob dieser Standard unseren Anforderungen entspricht. Also fang an, wir verwenden unsere eigenen numerischen, um Mappings zu string. Ähnlich wie Region kann sich das Format ändernhttps://s3-eu-west-1.amazonaws.com/community-radar/ref/states.json.gz

Städtecodes

Wir verwenden unsere eigenen numerischen, um Mappings zu string. Ähnlich wie Region kann sich das Format ändern und wir können diese Zuordnungen eventuell als API-Aufruf bereitstellen. https://s3-eu-west-1.amazonaws.com/community-radar/ref/cities.json.gz

Visualisierer

September 14, 2023

Einführung

Der ITM Visualizer ist ein intuitives und intelligentes Tool, mit dem Sie die globale Leistung von ISPs und Services überwachen und analysieren können. Die ITM Visualizer-Benutzeroberfläche bietet aktive Warnmeldungen mit Informationen zur Leistung und Verfügbarkeit von Clouds, Rechenzentren, CDNs und anderen Diensten. Die ITM-Community misst diese Warnungen auf der ganzen Welt. ITM Radar sammelt über die Radar-Community Milliarden von Messungen von echten Benutzern auf der ganzen Welt. Es verwendet ein Crowdsourcing-Modell, um diese Alarme zu messen.

Für einen neuen Benutzer wird die Visualisierer-Seite mit allen verfügbaren Community-Alerts auf der Karte geöffnet. ITM Radar misst Leistungsanomalien und generiert Warnmeldungen in fast jedem Netzwerk und an jedem Standort auf der ganzen Welt.

Die vier Kacheln über der Visualizer-Karte zeigen die folgenden Daten.

Aktive Radarwarnungen

Aktive Radarwarnungen sind aktuell und laufend.

Radarwarnungen

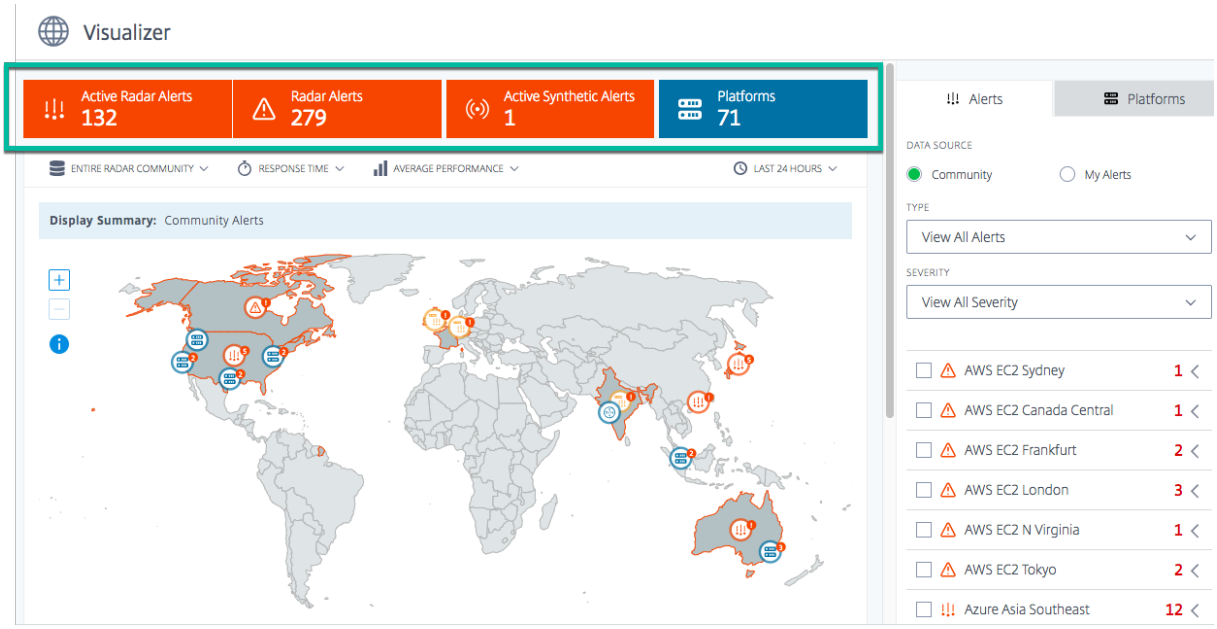
Aktive Radarwarnungen sind aktuell und laufend. Standardmäßig zeigt diese Kachel alle Benachrichtigungen der letzten 24 Stunden an, ändert sich jedoch je nach dem von einem Benutzer ausgewählten Zeitraum.

Aktive synthetische Warnungen

Diese Warnungen erfolgen in Echtzeit. Sonar, unser synthetisches Überwachungssystem, das die globale Verfügbarkeit eines Dienstes oder Rechenzentrums misst, generiert diese Warnungen.

Plattformen

Die Anzahl der im Kundenkonto konfigurierten Plattformen.



Optionen anzeigen

Sie können Benachrichtigungen und Plattformen auf der Karte anhand der folgenden Kriterien anzeigen:

Die gesamte Radar-Community oder nur Ihre Besucher

Wählen Sie **Radar Community**, um die Leistung der Plattformen in der Radar-Community zu sehen. Oder wählen Sie „Nur Ihre Besucher“, um die Leistung nur für Ihre Besucher auf **Ihren privaten Plattformen zu sehen**.

Reaktionszeit oder Verfügbarkeit

Klicken Sie auf eine beliebige Plattform auf der Karte oder in der Liste, um deren Leistung basierend auf **Verfügbarkeit** oder **Reaktionszeit**anzuzeigen.

Beste Leistung oder durchschnittliche Leistung

Wählen Sie **Durchschnittliche Leistung** oder Beste Leistung aus, um die durchschnittliche/beste Leistung anzuzeigen, die Sie für Ihre Plattformen erhalten würden.

Die durchschnittliche Leistung ist vergleichbar mit einem Round-Robin-Verfahren zwischen Ihren Plattformen. Die **beste Leistung** ist die Leistung, die wir durch die Verwendung von ITM erzielen.

Wenn Sie „ **Beste Leistung** "wählen, wird die Leistung auf der Karte angezeigt, die auf der Plattform mit der besten Leistung basiert. Wenn Sie sich beispielsweise die Leistung für ein bestimmtes Land ansehen und zwei Plattformen ausgewählt haben, färbt „ **Beste Leistung** "die Länderkarte auf der Grundlage der Plattform ein, die für dieses Land die beste Leistung zwischen den beiden (höchste Verfügbarkeit oder niedrigste Reaktionszeit) aufwies.

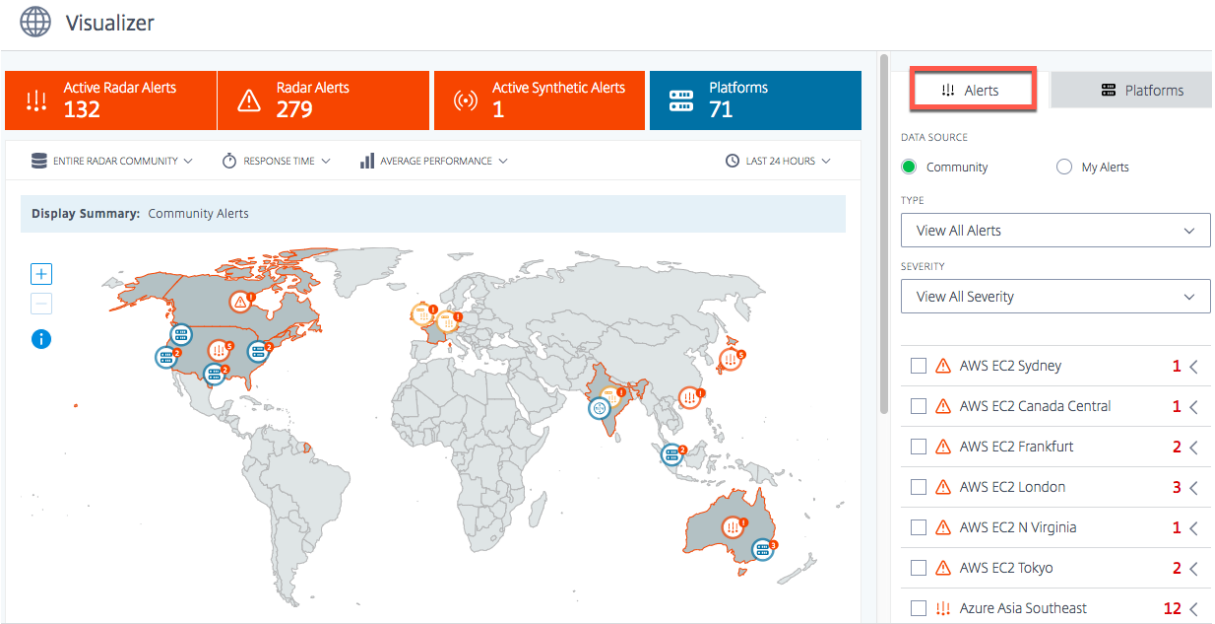
Wenn Sie "**Durchschnittliche Leistung**"wählen, wird die Performance auf der Karte basierend auf dem Durchschnitt aller ausgewählten Plattformen angezeigt. Es färbt die Länderkarte mit der durchschnittlichen Verfügbarkeit (oder Reaktionszeit) der beiden Plattformen ein.

Zeitraum

Benachrichtigungen auf der Karte können mit einem Zeitraum von „ **Letzte 60 Minuten", „Letzte 24 Stunden", „Letzte 48 Stunden", „Letzte 7 Tage", „Letzte 30 Tage"oder mit einem benutzerdefinierten Bereich**generiert werden. Die Standardansicht ist die Letzte 24 Stunden. Jedes Mal, wenn Sie den Zeitraum ändern, werden die Daten auf der Karte aktualisiert und die ausgelösten Alerts für diesen Zeitraum angezeigt.

Warnungen

Die Registerkarte „ **Benachrichtigungen** "ist die Standardregisterkarte, die angezeigt wird, wenn Sie auf der Visualizer-Seite landen. Die Standarddatenquelle, die für einen neuen Benutzer ohne eigene Benachrichtigungen angezeigt wird, ist **Community.** Das bedeutet, dass alle Benachrichtigungen, die Sie als neuer Benutzer auf der Karte ansehen, Community-Benachrichtigungen sind. Selbst wenn Sie Warnungen eingerichtet haben, aber keine aktiven oder laufenden Warnungen haben, werden in Ihrer Ansicht standardmäßig Community-Warnungen angezeigt. Wenn Sie jedoch Ihre Alerts eingerichtet haben und aktive laufende Alerts haben, dann sind Ihre eigenen Alerts Ihre Standardansicht. Weitere Informationen zu Alerts finden Sie unter Alerts.



Gemeinschaft

Community-Warnungen sind Leistungsprobleme oder Anomalien, wie ITM Radar in der ITM-Community auftreten. Diese Alarme werden über Endbenutzer-Netzwerke aus der ganzen Welt gemessen. Wenn Sie den **Visualizer** zum ersten Mal als neuen Benutzer öffnen, werden alle Community-Alerts auf der Karte angezeigt. Sobald Sie Ihre eigenen Benachrichtigungen eingerichtet haben, sehen Sie diese Benachrichtigungen anstelle der Community-Benachrichtigungen.

Wenn Sie jedoch private Plattformen und Benachrichtigungen eingerichtet haben, werden Ihre eigenen Benachrichtigungen als **Meine Benachrichtigungen angezeigt**, der Standardansicht.

Meine Warnungen

Bei diesen Warnungen handelt es sich um Leistungsprobleme oder Anomalien Ihrer privaten Plattformen. Es verwendet Endbenutzer-Netzwerke auf der ganzen Welt, um diese Warnungen zu messen.

Wenn Sie als neuer Benutzer keine Warnungen sehen, bedeutet dies, dass Sie keine Warnungen eingerichtet haben. Sie können in der linken Seitenleiste auf die Seite “**Warnungen**”gehen, um Warnungen für die Leistung Ihrer Plattformen einzurichten. Sie müssten jedoch zuerst Ihre privaten Plattformen einrichten. Um Plattformen einzurichten, können Sie entweder von der linken Seitenleiste auf die Seite **Plattformen** gehen oder im laufenden Betrieb über die Registerkarte “**Plattformen**”tun.

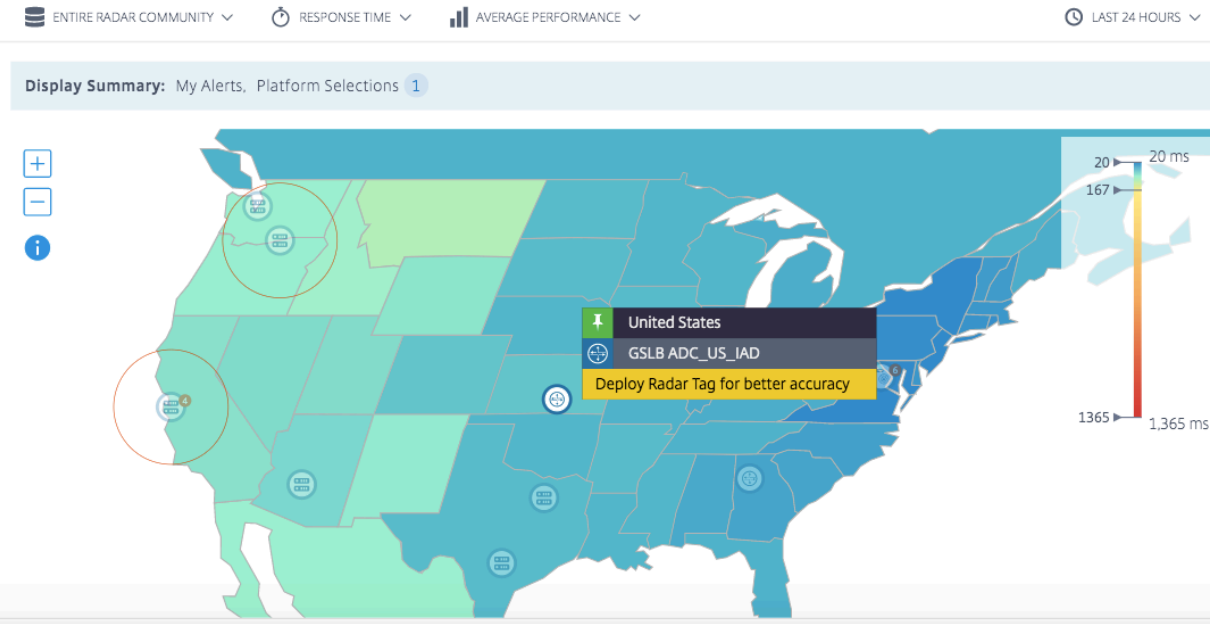
Einzelheiten der Warnung

Sie können den Mauszeiger über die Warnung auf der Karte bewegen, um das Land und die Dienste anzuzeigen, für die die Benachrichtigungen ausgelöst werden. Weitere Informationen zu einer bestimmten Warnmeldung erhalten Sie

1. Klicken Sie auf das Warnungssymbol auf der Karte, um das Kästchen für die Service-Trigger-Warnung zu aktivieren und sie in der Liste hervorzuheben.
2. Klicken Sie auf den Pfeil rechts neben der ausgewählten Plattform oder dem ausgewählten Dienst, um die Details der Warnung anzuzeigen, einschließlich

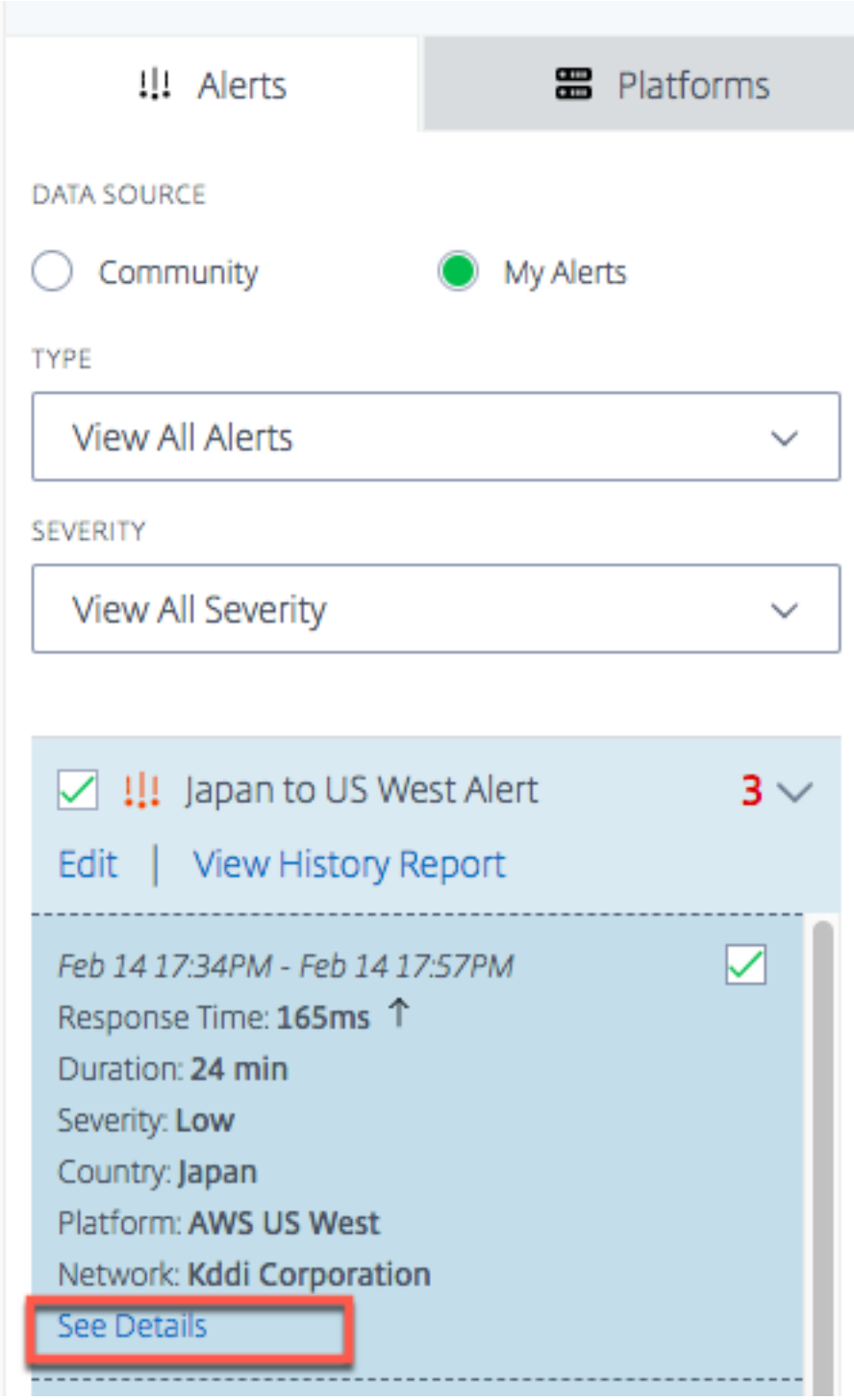
   a) **Verfügbarkeits-** oder **Antwortzeit** der Datenquelle
   b) **Dauer** der Warnung
   c) **Schweregrad** der Warnung
   d) **Land** des Netzwerks, von dem aus die Probleme gemessen werden
   e) Name der **Plattform**, für die die Warnung ausgelöst wird.
   f) Name des **Netzwerks**, von dem die Probleme gemessen werden.

Alerts auf Bundesstaatsebene: Aktive Alerts mit Informationen über die Leistung und Verfügbarkeit von Clouds, Rechenzentren, CDNs und anderen Diensten. Diese Warnungen werden auf Bundesstaatsebene innerhalb der Vereinigten Staaten gemessen und angezeigt.



Um tiefer in die Details der Warnung einzutauchen, klicken Sie auf **Details anzeigen**, um zur Seite **Warnungen** zu gelangen.

> **HINWEIS:** Sie können den Link „ **Details** anzeigen“nur für Ihre eigenen Benachrichtigungen aufrufen.

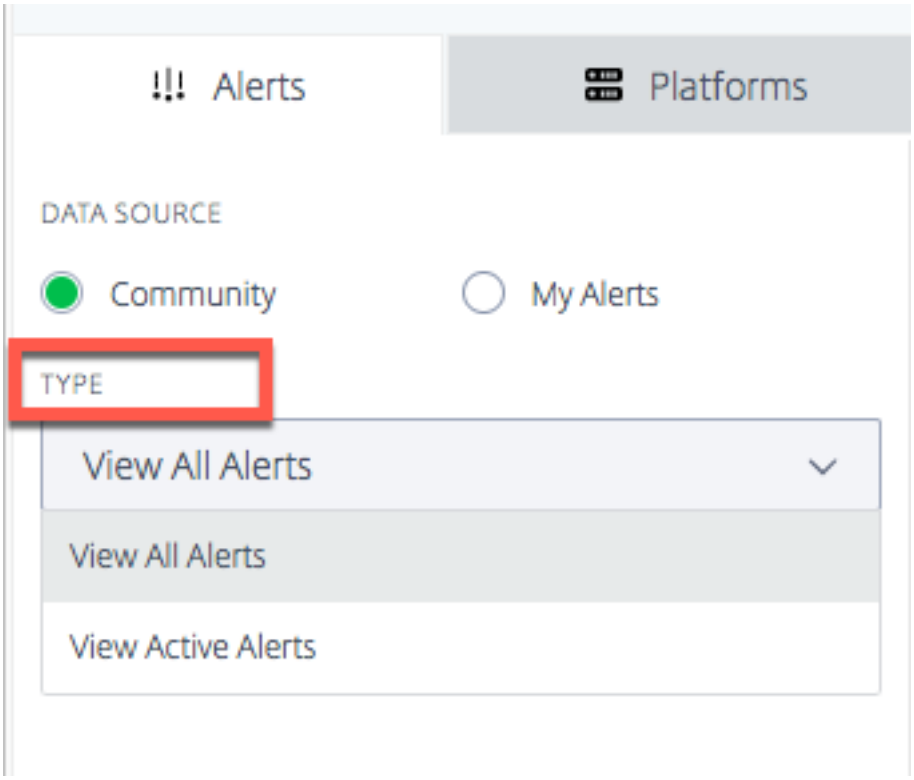


Warnungstyp

Im Menü **Typ** können Sie die folgenden Arten von Benachrichtigungen anzeigen.

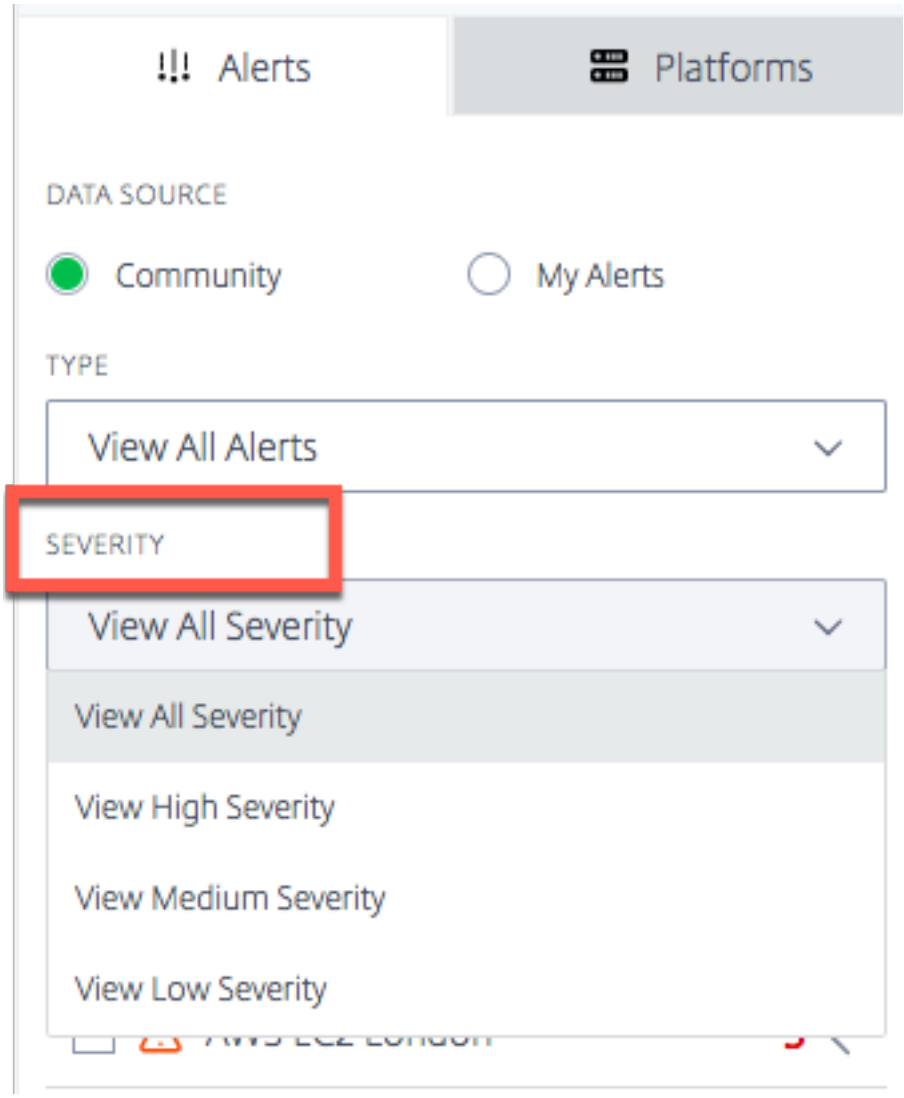
Alle Benachrichtigungen Alle Benachrichtigungen beinhalten aktive und historische Benachrichtigungen. Historische Benachrichtigungen sind Benachrichtigungen, die zu einem späteren Zeitpunkt im ausgewählten Zeitraum entstanden sind.

Aktive Benachrichtigungen Zu den aktiven Benachrichtigungen gehören auch Benachrichtigungen, die aktuell sind. Sie sind gültig und aktuell für den vom Benutzer angegebenen Zeitraum.



Warnschweregrad

Warnmeldungen können nach Schweregrad **Hoch, Mittel**und **Niedrig** gefiltert werden. Der**gesamte Schweregrad** ist die Standardanzeige.



Logik des Schweregrads Zur Verfügbarkeit:

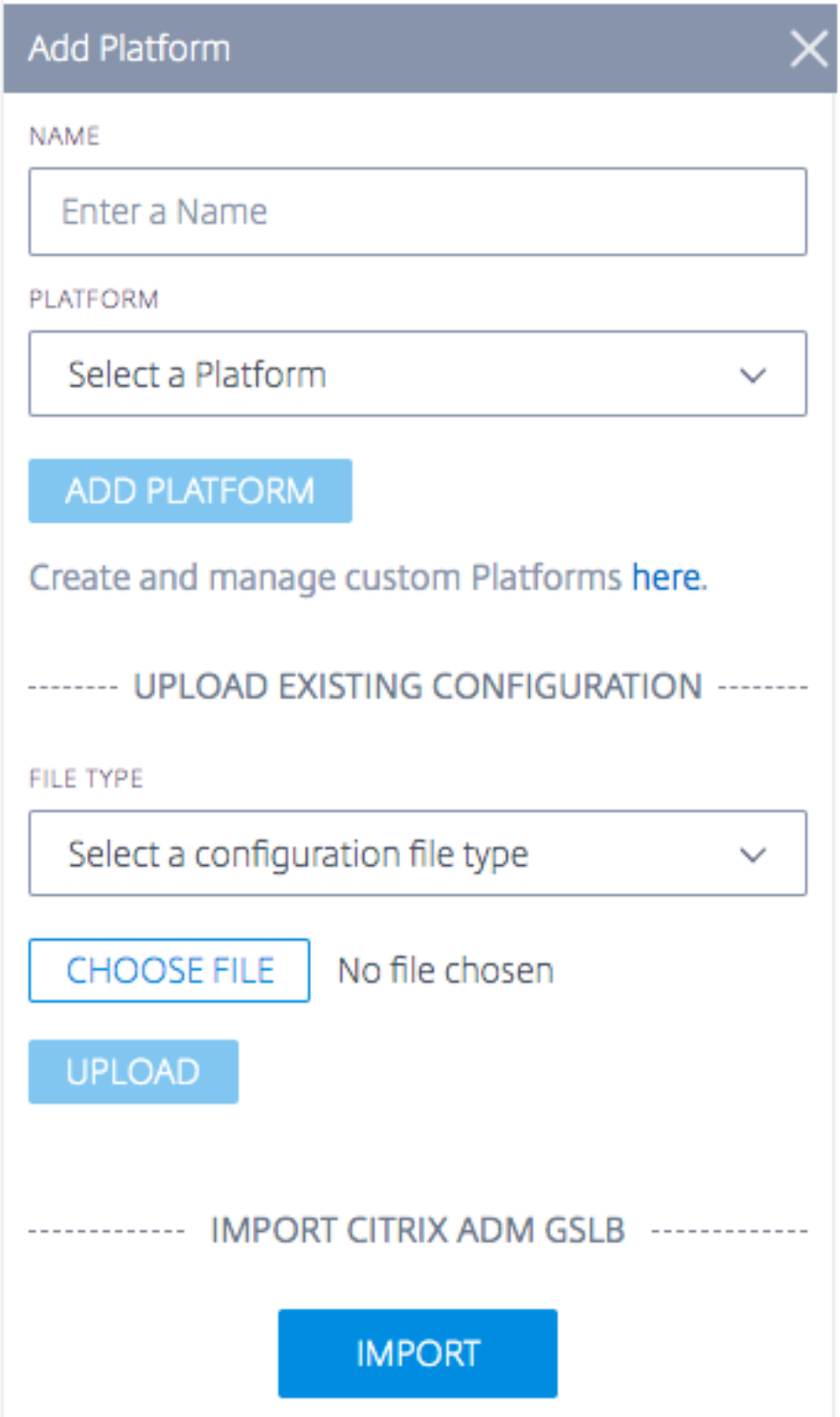
- Wenn mehr als 50% unter dem Schwellenwert liegen -> Schweregrad ist **hoch**
- Wenn mehr als 25%, aber weniger als 50% unter dem Schwellenwert liegen -> Schweregrad ist **Mittel**
- Wenn weniger als 25% unter dem Schwellenwert liegen -> Schweregrad ist **Niedrig**

Für die Reaktionszeit:

- **Wenn der Schwellenwert um mehr als 200% überschritten wird -> Schweregrad ist hoch**
- **Wenn mehr als 100% über dem Schwellenwert, aber weniger als 200% liegt -> Schweregrad ist Mittel**
- Wenn der Schwellenwert um weniger als 100% überschritten wird -> Schweregrad ist **Niedrig**

Plattformen

Wenn Sie die Registerkarte **Plattformen** auswählen, wird die Liste der Plattformen angezeigt, die Sie hinzugefügt haben. Wenn Sie jedoch ein neuer Benutzer sind und noch keine Plattformen eingerichtet haben, können Sie hier entweder spontan eine Community-Plattform hinzufügen oder eine private Plattform einrichten, indem Sie **hier auf den Link Benutzerdefinierte Plattformen erstellen und verwalten** klicken.



Eine Community-Plattform hinzufügen

1. Um eine Community-Plattform hinzuzufügen, klicken Sie auf das Pluszeichen neben der Leiste **Plattform hinzufügen** .
2. Geben Sie einen Namen für die Plattform ein und wählen Sie die Plattform aus der Liste der Community-Plattformen im **Plattformmenü** aus.
3. Klicken Sie auf **Plattform hinzufügen**.

Fügen Sie eine benutzerdefinierte/private Plattform hinzu

1. Um eine private Plattform hinzuzufügen, klicken Sie auf das + -Symbol neben der **Add Platform** Leiste.
2. Klicken Sie auf den Link **Benutzerdefinierte Plattformen hier erstellen und verwalten**, um zur Seite **Plattformen** zu gelangen, auf der Sie eine neue private Plattform hinzufügen können. Alternativ können Sie in der linken Seitenleiste auf die Seite **Plattformen** gehen.

Bestehende Konfiguration hochladen: NetScaler und F5 BIG-IP DNS

Mit dieser Option können Sie eine NetScaler oder F5 BIG-IP DNS-Konfigurationsdatei auswählen und die Konfiguration (Ihrer vorhandenen Plattformen) direkt importieren. Es erstellt automatisch private Plattformen für Ihre NetScaler- oder F5-BIG-IP-DNS-Konfiguration.

Importieren von Citrix GSLB aus ADM Service

Mit dieser Option können Sie alle Ihre im ADM-Dienst konfigurierten GSLBs direkt importieren.

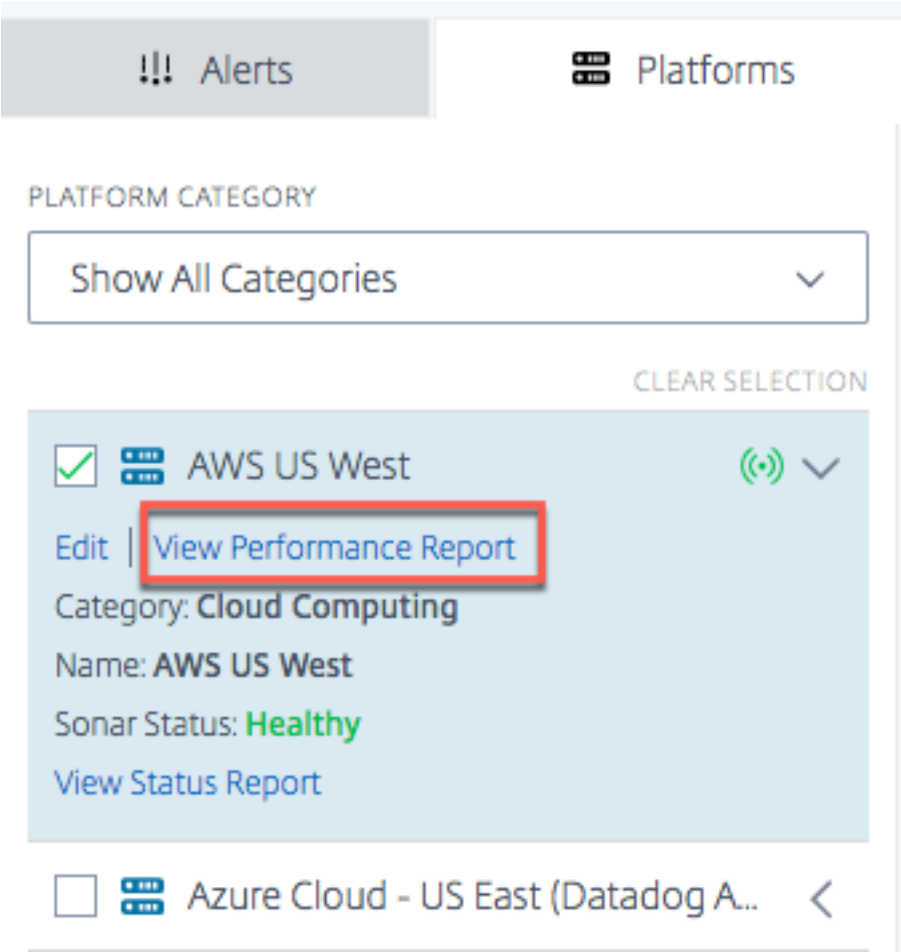
Wenn Sie Citrix Cloud ADM Service verwenden, können Sie die dort konfigurierten GSLBs importieren. Die grundlegenden Site-Informationen - IP und Name - werden als ITM-Plattformen importiert. ITM lokalisiert die Site und ermöglicht die Anzeige der Plattform im Visualizer zur Leistungsanalyse.

Leistungsbericht

Der Radar-Leistungsbericht enthält Details zu bestimmten Plattformen, ausgelösten Warnmeldungen und jedem Netzwerk, von dem aus sie gemessen wurden. Der Bericht zeigt Messungen der Reaktionszeit oder Verfügbarkeit und den Zeitraum für das gemessene Problem an. Es beinhaltet alle Filter, die im **Visualizer**angewendet wurden.

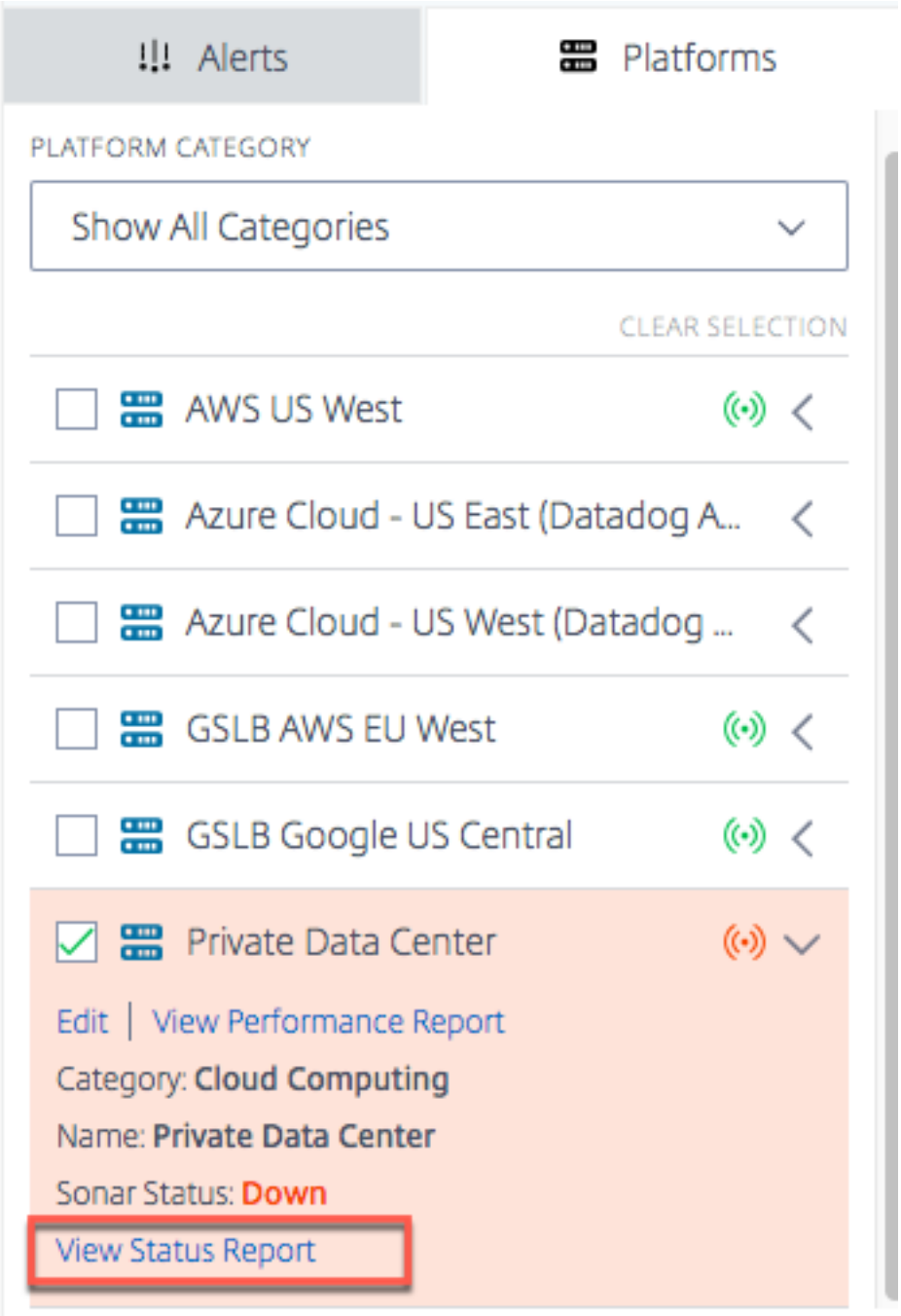
Gehen Sie wie folgt vor, um die Leistungsdetails einer bestimmten Plattform anzuzeigen, für die die Warnung ausgelöst wurde.

1. Klicken Sie auf das Plattformsymbol oder das Warnsymbol auf der Karte, um es zu markieren, und aktivieren Sie das Kästchen in der Liste auf der rechten Seite.
2. Klicken Sie auf den Pfeil neben der Plattform oder Warnung, um sie zu erweitern.
3. Klicken Sie auf den Link **Leistungsbericht anzeigen**, um zur Seite **Radar-Leistungsbericht** zu gelangen.

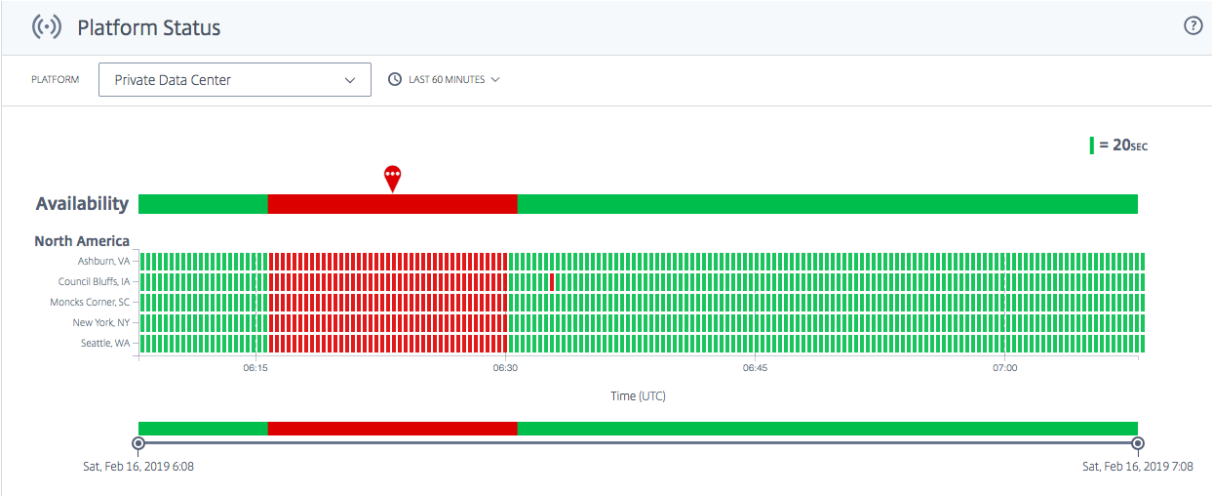


Statusbericht

Bei synthetischen Überwachungswarnungen können Sie die Warndetails anzeigen, indem Sie die Plattform erweitern, um Details anzuzeigen, und dann auf **Statusbericht anzeigen**klicken.



Über den Link **Statusbericht anzeigen** gelangen Sie zur Seite mit dem **Status der Sonar-Plattform**. Dort finden Sie anhand synthetischer Überwachungsprüfungen in Echtzeit detaillierte Informationen zum Zustand Ihrer Plattform.



Radar

September 14, 2023

Übersicht

Radar bildet das Rückgrat der Datenerhebungsmethodik. Radar verwendet ein JavaScript-Skript, das in die Seiten einer Inhaltsseite oder eines Anwendungsanbieters eingebettet ist, um Informationen über die Leistung und Verfügbarkeit eines Rechenzentrums oder einer Bereitstellungsplattform zu sammeln.

Der Radar-Client ist eine JavaScript-Anwendung, die auf Kundenwebseiten und in mobilen Anwendungen ausgeführt wird. Sein Hauptzweck besteht darin, Netzwerkleistungsdaten zu sammeln, die für intelligente Routing-Entscheidungen über Openmix verwendet werden, und optionale Plug-ins bereitzustellen, um andere NetScaler Intelligent Traffic Management-Dienste wie Page Load Time, Page Resource Timing und Video Playback Metrics zu aktivieren.

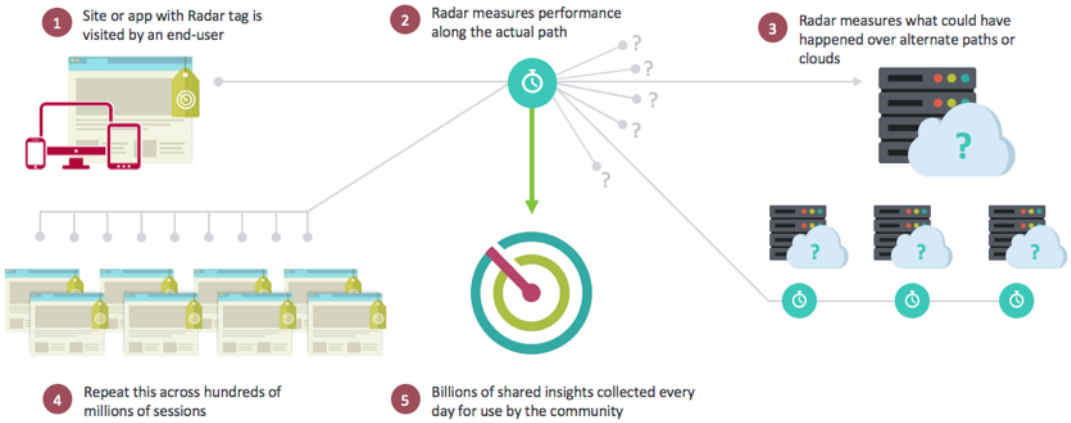
Der Radar-Client ist voll funktionsfähig, aber dennoch leicht und unauffällig. Der Client wartet, bis die meisten Seitenressourcen heruntergeladen wurden, bevor er den Großteil seiner Arbeit ausführt, und die gesamte Netzwerkkommunikation erfolgt, wo immer möglich, asynchron. Diese Anweisungen geben an, welche Plattform als Nächstes während der Sitzung gemessen werden soll. Dabei wird zwischen den Community-Plattformen und allen privaten Plattformen, die für dieses Community-Mitglied spezifisch sind, ausgewählt. Sie geben auch die Arten der durchzuführenden Messungen an, zu denen Verfügbarkeit, Hin- und Rückflugzeit, Durchsatz oder andere metrische Erfassung gehören können.

Um es so klein wie möglich zu halten, wird das JavaScript mit erweiterten Optimierungen mithilfe des Google Closure Compilers kompiliert. Erweiterte optionale Funktionen werden als Plug-ins für

Kunden bereitgestellt, die sich dafür entscheiden, sie zu verwenden.

Radar-Gemeinschaft

Mit einem einzigartigen, gemeinschaftsbasierten Ansatz sorgt Radar für beispiellose Transparenz in Bezug auf die globale Leistung und Verfügbarkeit der weltweit größten öffentlichen Infrastrukturen, von Cloud Computing und Storage bis hin zu Content und Application Delivery Networks. Mit Radar können Kunden schnell die Plattformen mit der besten und schlechtesten Leistung für jeden ihrer Besucher finden.



Radar ist die erste Cloud-Monitoring-Genossenschaft im Internet. Wenn Sie Community-Mitglied werden, haben Sie uneingeschränkten Zugriff auf unsere historische Berichtsdatenbank, einschließlich detaillierter Segmentierung nach Anbietern, Ländern und Netzwerken.

Als Mitglied der Radar-Community erhalten Sie außerdem eine Vielzahl von Tools zur Erfassung der Serviceniveaus, die sowohl von internen als auch von externen Infrastrukturen für die Bereitstellung von Inhalten bereitgestellt werden. Einzigartig an Radar ist die Möglichkeit, Ihre Website-Besucher dazu zu nutzen, das Erlebnis zu messen, das sie auf Plattformen erhalten würden, die derzeit nicht von einem Unternehmen genutzt werden. Dieselbe Methode ermöglicht objektive Bewertungen von Cloud-Plattformen während ihres gesamten Lebenszyklus, einschließlich der laufenden Bewertung der Leistung im Vergleich zu SLAs.

Durch Hinzufügen eines einfachen JavaScript-Tags zu Ihrer Webseite oder eines SDK zu mobilen Anwendungen können Kunden jeden ihrer Besucher in einen virtuellen „Testagenten“verwandeln. Radar löst gerätebasierte Messungen aus, indem Referenzobjekte heruntergeladen und interne und externe Infrastrukturen, Rechenzentren, Liefernetzwerke und Cloud-Plattformen aus Sicht der tatsächlichen Endnutzer von Websites oder Webanwendungen verglichen werden.

Hauptvorteile der Teilnahme

Radar bewältigt mit seinem Ansatz zur Überwachung und Datenerfassung mehrere Herausforderungen bei der Webbereitstellung. Die wichtigsten Vorteile der Teilnahme an der Radar-Community sind:

- Umfangreiche Testumgebung mit Endbenutzern in jedem Netzwerk an jedem Standort (bisher mehr als 42.000 anerkannte Netzwerke).
- Holen Sie sich vor dem Test wichtige Informationen über die Dienstleister, um eine fundiertere Entscheidung zu treffen.
- Transparenz über die Leistung aktueller Anbieter und deren Verhalten in Regionen, in denen Sie Nutzer haben und in denen es keine gibt.
- Konzentrieren Sie sich auf die Kennzahlen, die für Web- und Mobilnutzer einen echten Unterschied machen (Leistung, Verfügbarkeit und QoS).
- Globaler (über 190 Länder) uneingeschränkter Zugriff auf Informationen bis auf Länder-, Netzwerk-, Regions- und Bundesstaatsebene.
- Echte, unvoreingenommene Daten unter Verwendung von Endnutzern Radardaten sind Informationen aus der „realen Welt“und keine synthetischen Tests oder Schätzungen.
- Nicht alle Benutzer sind gleich: Verstehen Sie verschiedene Maschinen, Verbindungen und Geräte.
- Einblick in die Leistung der tatsächlichen Seiten.

Benchmarks

ITM Radar bietet 3 Hauptbenchmarks:

- Gemeinschaftliches Benchmarking
- Privates Benchmarking
- Benchmarking beim Laden von Seiten

Community-Benchmarking von CDN, Cloud und Rechenzentren

Community-Messungen werden im Rahmen eines Crowdsourcing-Modells durchgeführt, das dem Kunden einen Überblick über die Leistung und Verfügbarkeit eines Anbieters auf geografischer und logischer Ebene weltweit bietet. Die Community-Messungen ermöglichen Vergleiche zwischen der Erlebnisqualität eines Anbieters aus Sicht des Endnutzers und ermöglichen eine „Was-wäre-wenn “-Analyse bei der Bewertung von Anbietern und Anbietern für den Vertrieb von Inhalten und Anwendungen. Durch die Verwendung eines Crowdsourcing-Modells profitieren ITM-Kunden von einem höheren Maß an Granularität und Datenqualität bei der Bewertung und Überwachung der Lieferantenleistung, selbst an Standorten, an denen ein Kunde möglicherweise keine hohe Benutzerdichte oder gar keine Benutzer hat.

Die Messungen selbst verwenden einen Standardsatz von Objekten, die sich auf den verschiedenen Cloud- und CDN-Anbietern befinden und die Endbenutzer herunterladen, wenn sie den Radar-JavaScript-Client oder die mobile SDK-Logik auf der Website oder Anwendung eines Inhaltseigentümers ausführen.

Die folgenden Metriken werden dann an ITM zurückgemeldet und in den Portal- oder API-Berichtsschnittstellen dargestellt:

- Verfügbarkeit —ob das Objekt geladen wird oder nicht.
- Antwortzeit —wie lange es dauert, bis der Server auf eine nachfolgende Anfrage reagiert, sobald der gesamte Verbindungsaufbau abgeschlossen ist. Dies ist eine relativ genaue Annäherung an die TCP-Round-Time-Zeit (RTT) vom Browser zum Anbieter.
- Durchsatz —Dies ist die Datenrate der Verbindung in Kilobit pro Sekunde, gemessen beim Abrufen eines 100-KB-Objekts.

Privates Benchmarking

Im Rahmen der Implementierung von Radar Tag bietet ITM dem Kunden die Möglichkeit, seine eigenen „Benchmark"-Tests zu erstellen, die von den Besuchern des Kunden gemessen werden. Dies kann für Rechenzentren oder ihre eigenen CDN- und Cloud-Verträge sein. Wie bei den Community-Benchmark-Messungen werden dieselben Kennzahlen bereitgestellt —Verfügbarkeit, Reaktionszeit und Durchsatz, sodass der Kunde eine bestehende Strategie zur Inhaltsbereitstellung effektiv bewerten kann.

Diese privaten Informationen stehen nur dem Kunden zur Verfügung und werden nicht weitergegeben.
Zu den Anwendungsbeispielen gehören:

- Ihre eigene Rechenzentrumsarchitektur/en
- Verwenden eines eigenen Testobjekts oder einer eigenen Seite
- Nutzung eines eigenen Vertrags und Kontos bei einem bestimmten Anbieter oder einer Gruppe von Anbietern

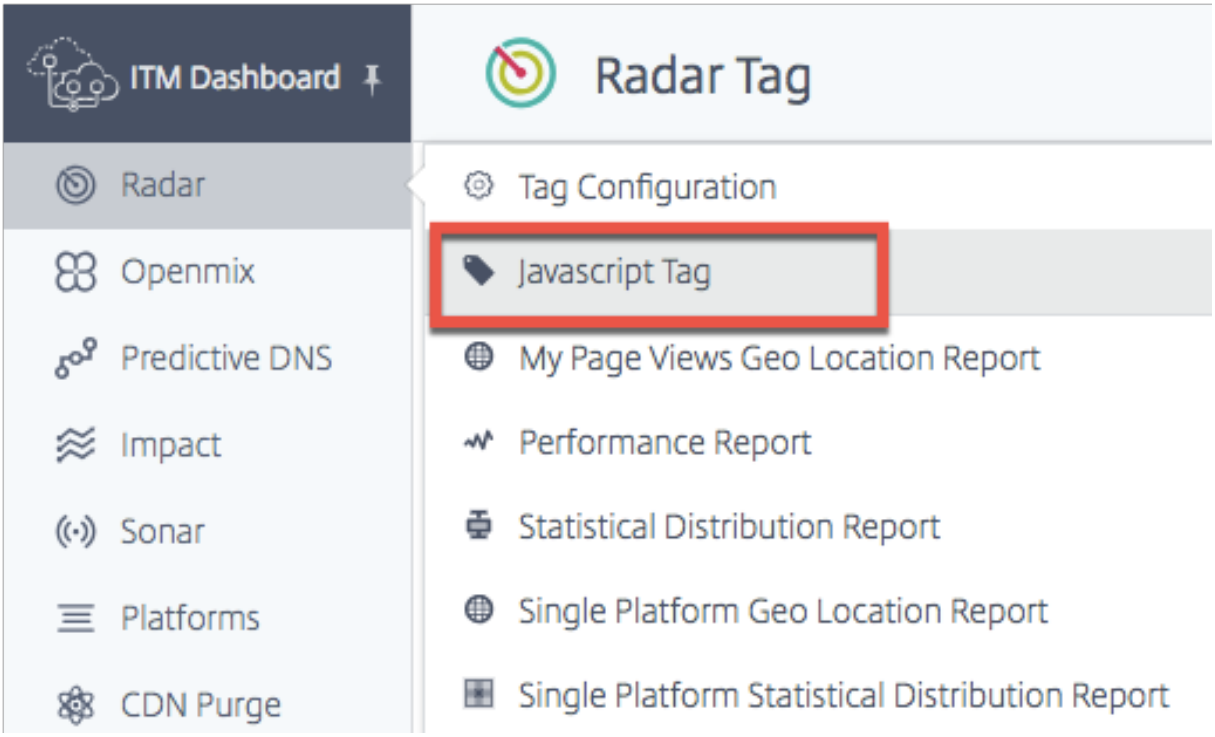
Benchmarking beim Laden von Seiten mit Radar

Innerhalb von Radar bietet ITM dem Kunden die Möglichkeit, detaillierte Informationen darüber einzusehen, wie die Seiten, auf denen das Tag implementiert ist, heruntergeladen werden. ITM bietet Informationen, anhand derer Sie die Leistung sehen können, die Endbenutzer bei der Interaktion mit Ihren Webseiten tatsächlich erleben. Die Daten werden über die Navigation Timing API bereitgestellt, die von vielen Browsern neuerer Versionen unterstützt wird.

Radar-Tag

Das Radar-Tag kann mithilfe eines JavaScript-Snippets integriert werden. Gehen Sie wie folgt vor, um zur **Radar-Tag-Seite** zu navigieren:

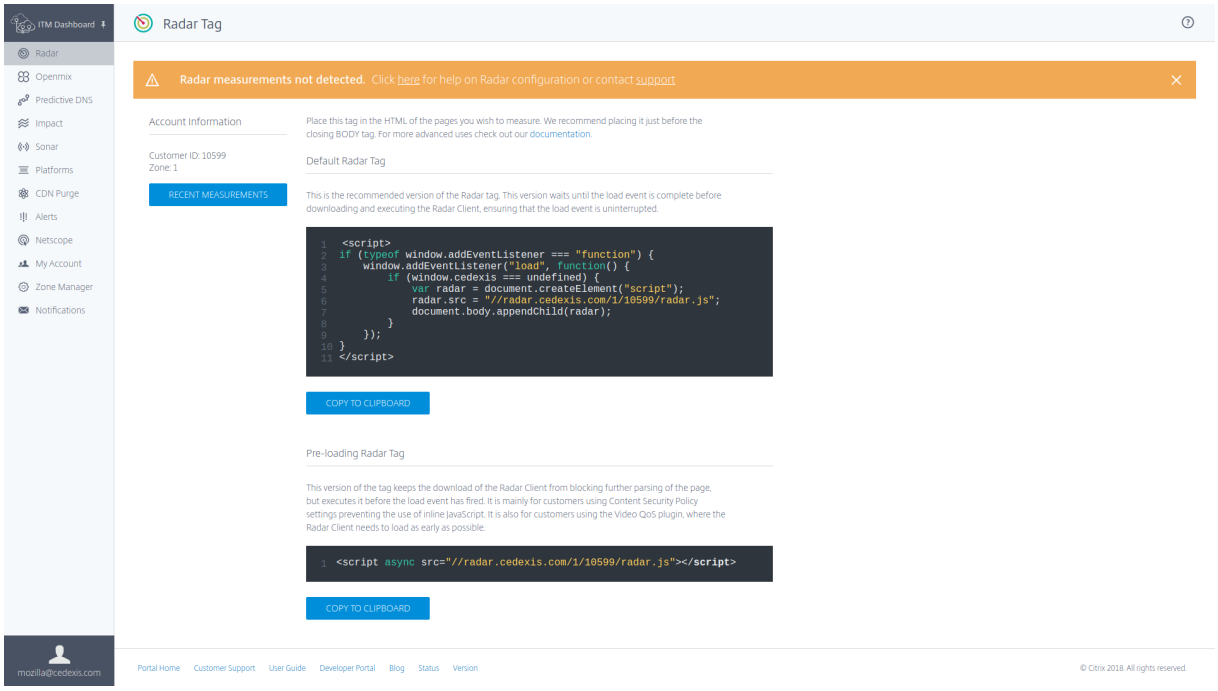
1. Melden Sie sich beim NetScaler Intelligent Traffic Management Portal an.
2. Wählen Sie im linken Navigationsmenü **Radar > Javascript-Tag**.



Die **Radar-Tag-Seite** wird geöffnet.

Wenn Sie das Radar-Tag noch nicht konfiguriert haben, sehen Sie oben auf dem Bildschirm eine orangefarbene horizontale Leiste, die Sie darüber informiert, dass keine Radarmessungen erkannt wurden.

Dieser orangefarbene Balken wird auch angezeigt, wenn das Tag nicht korrekt konfiguriert wurde.



Wenn das Radar-Tag wie erwartet funktioniert, sehen Sie alternativ einen grünen horizontalen Balken, der Sie darüber informiert, dass Radarmessungen erfolgreich durchgeführt wurden.

Auf dieser Seite können Sie die Tag-Version auswählen, die für Ihre Verwendung gilt, und sie in die Zwischenablage kopieren.

Hinweis: Es ist wichtig, dieses JavaScript-Snippet nicht zu ändern. Der Code enthält wichtige Informationen, die, wenn sie geändert werden, zu unerwartetem oder unzuverlässigem Verhalten führen können.

Integration des Radar-Tags

Die Integration des Radar-Tags ist relativ einfach. Sie müssen lediglich eines der folgenden JavaScript-Snippets zu Ihrem Site-Markup hinzufügen. Platzieren Sie es im HTML-Code der Seiten, die Sie messen möchten. Wir empfehlen, es am Ende der Seite vor dem schließenden Body-Tag zu platzieren `</body>`.

Standard-Radar-Tag

Dies ist die empfohlene Version des Radar-Tags. Diese Version wartet, bis das Ladeereignis abgeschlossen ist, bevor der Radar-Client heruntergeladen und ausgeführt wird, um sicherzustellen, dass das Ladeereignis nicht unterbrochen wird.

```
1 <script>
2 if (typeof window.addEventListener === "function") {
```



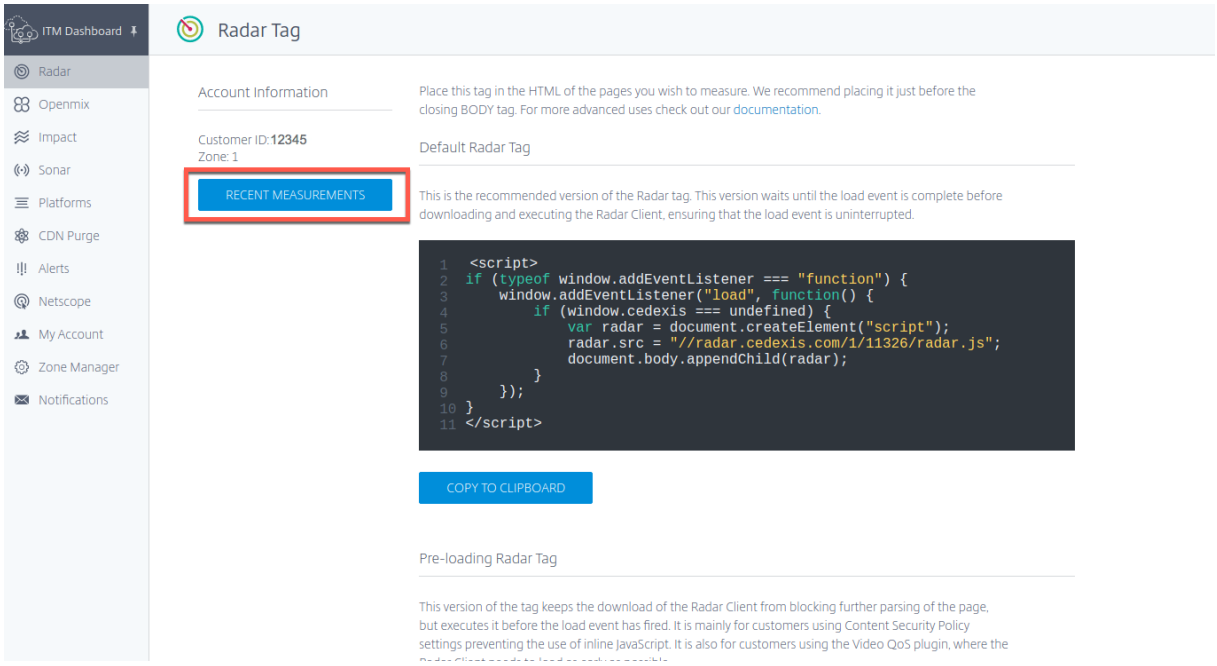
```
3
4       window.addEventListener("load", function() {
5
6           if (window.cedexis === undefined) {
7
8               var radar = document.createElement("script");
9               radar.src = "//radar.cedexis.com/1/54621/radar.js"; //
                    replace with user specific value
10              document.body.appendChild(radar);
11           }
12
13       }
14   );
15   }
16
17 </script>
18 <!--NeedCopy-->
```

Diese Version des Tags verhindert, dass der Download des Radar-Clients das weitere Parsen der Seite blockiert, führt ihn jedoch aus, bevor das Ladeereignis ausgelöst wird. Es ist hauptsächlich für Kunden gedacht, die Content Security Policy-Einstellungen verwenden, die die Verwendung von Inline-JavaScript verhindern. Es ist auch für Kunden gedacht, die das Video QoS-Plug-In verwenden, bei dem der Radar Client so früh wie möglich geladen werden muss.

```
1 <script src="//radar.cedexis.com/1/54621/radar.js" async></script>
2 <!--NeedCopy-->
```

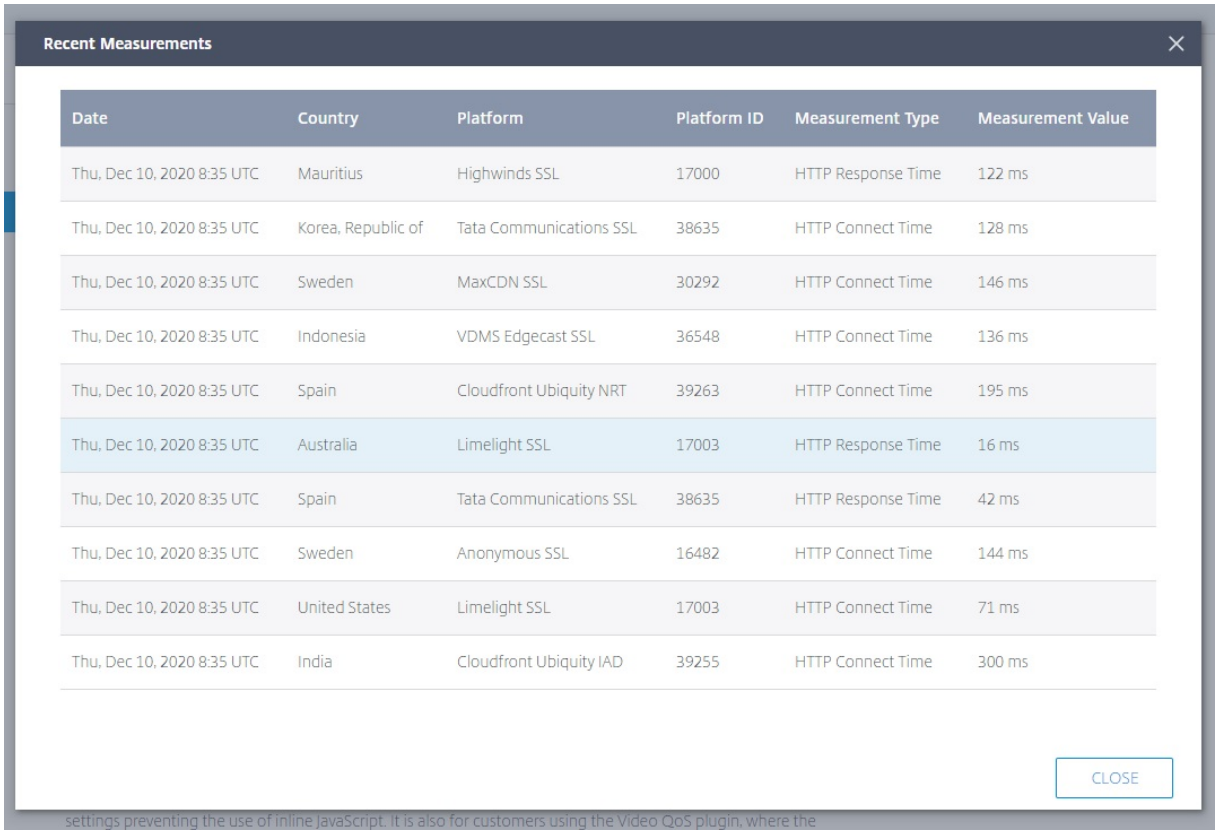
Aktuelle Messungen

In der Tabelle Aktuelle Messungen können Sie sich die neuesten Messungen ansehen, die mit Radar durchgeführt wurden.



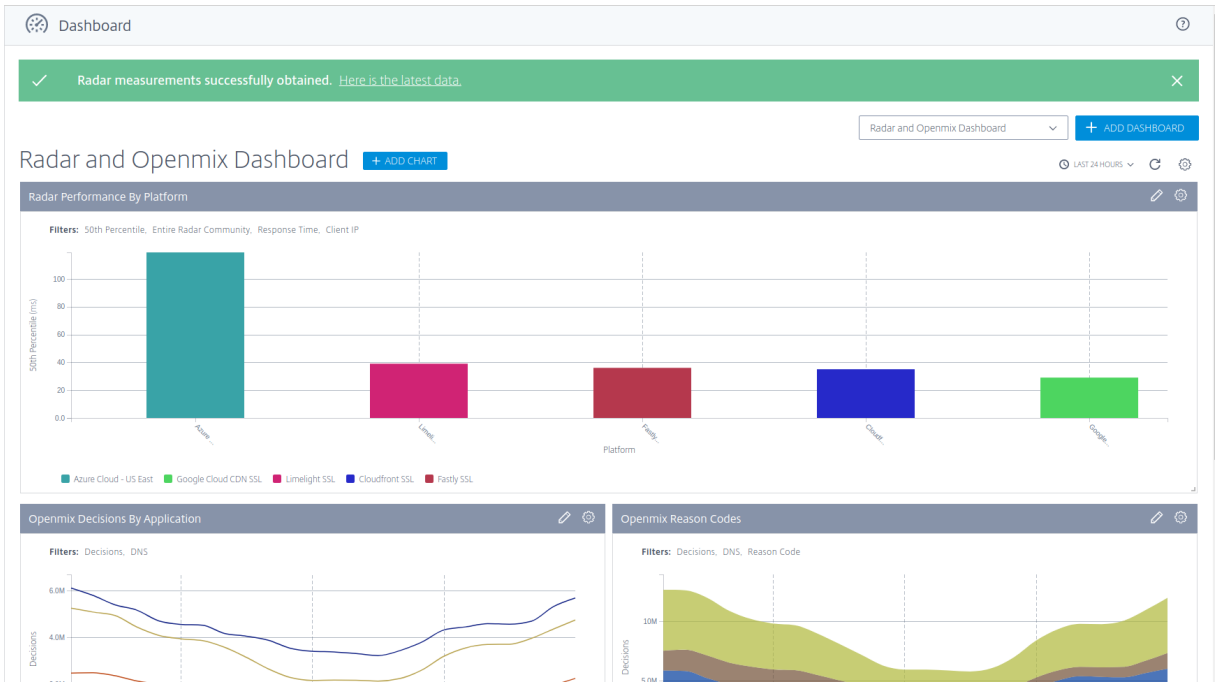
Klicken Sie auf die Schaltfläche **Letzte Messungen** . Es gibt Ihnen die folgenden Informationen:

- Datum und Uhrzeit der Messung in UTC.
- Land, in dem die Messung durchgeführt wurde.
- Die Plattform, die für die Messung verwendet wurde.
- Die ID der Plattform.
- Die Art der durchgeführten Messung, d. h. Verbindungszeit (in Millisekunden), Reaktionszeit (in Millisekunden) oder Durchsatz (in Kilobit pro Sekunde)
- Der tatsächliche Wert der Messung in Millisekunden (für Verbindungszeit und Reaktionszeit) oder Kilobit pro Sekunde (für Durchsatz).



Date	Country	Platform	Platform ID	Measurement Type	Measurement Value
Thu, Dec 10, 2020 8:35 UTC	Mauritius	Highwinds SSL	17000	HTTP Response Time	122 ms
Thu, Dec 10, 2020 8:35 UTC	Korea, Republic of	Tata Communications SSL	38635	HTTP Connect Time	128 ms
Thu, Dec 10, 2020 8:35 UTC	Sweden	MaxCDN SSL	30292	HTTP Connect Time	146 ms
Thu, Dec 10, 2020 8:35 UTC	Indonesia	VDMS Edgecast SSL	36548	HTTP Connect Time	136 ms
Thu, Dec 10, 2020 8:35 UTC	Spain	Cloudfront Ubiquity NRT	39263	HTTP Connect Time	195 ms
Thu, Dec 10, 2020 8:35 UTC	Australia	Limelight SSL	17003	HTTP Response Time	16 ms
Thu, Dec 10, 2020 8:35 UTC	Spain	Tata Communications SSL	38635	HTTP Response Time	42 ms
Thu, Dec 10, 2020 8:35 UTC	Sweden	Anonymous SSL	16482	HTTP Connect Time	144 ms
Thu, Dec 10, 2020 8:35 UTC	United States	Limelight SSL	17003	HTTP Connect Time	71 ms
Thu, Dec 10, 2020 8:35 UTC	India	Cloudfront Ubiquity IAD	39255	HTTP Connect Time	300 ms

Die Radarmessleiste wird auch auf der **Radar-Dashboard-Seite** angezeigt, wenn Sie sich zum ersten Mal im ITM-Portal anmelden.



Integration mit mobilen Apps

Die Integration mit mobilen Apps erfolgt über Wrapper für versteckte Webansichten, auf denen der JavaScript-Client ausgeführt wird. Dadurch wird sichergestellt, dass die in Browsern und mobilen Apps gesammelten Daten konsistent sind.

Anweisungen zur Integration von Radar mit der iOS-App
Dieses folgende GitHub-Repository enthält den Wrapper-Code und eine schrittweise Anleitung zur Integration von Radar mit der iOS-App:

Radar Runner für iOS

Anweisungen zur Integration von Radar in Android Android Radar ist eine Client-Bibliothek, mit der Radar einfach in Android-Apps integriert werden kann. Es ist hier zu finden:

Android-Radar-Bibliothek

Integration mit NetScaler

Das Radar-Tag ist wichtig, da es Openmix mit Messungen versorgt, die es Openmix ermöglichen, bessere Routing-Entscheidungen zu treffen. Je mehr Webseiten das Tag verwenden, desto besser sind die Routing-Entscheidungen.

Mit den folgenden Methoden können Sie das Radar-JavaScript-Tag mithilfe von NetScaler auf Ihrer Webseite platzieren. Sie können entweder die Befehlszeile oder das NetScaler Configuration Utility verwenden.

Mit diesen Methoden können Sie das Radar-Tag in Ihre Antworten einfügen. Um das Radar-Tag einzufügen, müssen Sie Rewrites verwenden. Umschreibungen sind in drei Schritte unterteilt: Aktionen erstellen, Richtlinien konfigurieren und Richtlinien binden.

Konfiguration über die Befehlszeile

Befehlszeile: Rewrite-Aktion konfigurieren Vorlage:

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-pattern <expression> | -search <expression>] [-refineSearch <string>] [-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add rewrite action radar_tag action insert_after HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).BEFORE_STR("</body>") '"<script async src=\\"//radar.cedexis.com/1/<customer_id>/radar.js\\"></script>"'
<!--NeedCopy-->
```


Hinweis: Geben Sie Ihre eigene Kundennummer dort ein, wo sie steht `<customer_id>`

Konfiguration der Rewrite-Richtlinie über die Befehlszeile Vorlage:

```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>]
<!--NeedCopy-->
```

Beispiel:

```
add rewrite policy radar_tag_policy HTTP.RES.HEADER("Content-Type").
    TO_LOWER.CONTAINS("text/html") radar_tag_action
<!--NeedCopy-->
```

Befehlszeilenbindung Rewrite-Richtlinie Vorlage 1:

```
bind vpn vserver <name> [-policy <string> [-priority <positive_integer
    >] [-secondary] [-groupExtraction] [-gotoPriorityExpression <
    expression>] [-type <type>]] [-intranetApplication <string>] [-
    nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <
    netmask> ] [-staServer <URL> [-staAddressType ( IPV4 | IPV6 )]] [-
    appController <URL>] [-sharefile <string>]
<!--NeedCopy-->
```

Beispiel 1:

```
bind vpn vserver <name_of_vserver> -policy radar_tag_policy -type
    RESPONSE -priority 10
<!--NeedCopy-->
```

Vorlage 2:

```
bind cs vserver <name> (-lbvserver <string> | -vServer <string> | (-
    policyName <string> [-targetLBVserver <string>] [-priority <
    positive_integer>] [-gotoPriorityExpression <expression>] [-type (
    REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>) ] ) | (-
    domainName <string> [-TTL <secs>] [-backupIP <ip_addr|ipv6_addr|*>]
    [-cookieDomain <string>] [-cookieTimeout <mins>] [-sitedomainTTL <
    secs>]))
<!--NeedCopy-->
```

Beispiel 2:

```
bind cs vserver <name_of_vserver> -policyName radar_tag_policy -type
    RESPONSE -priority 10
<!--NeedCopy-->
```

Vorlage 3:


```
bind lb vserver <name>@ (<serviceName>@ [- weight <positive_integer>])
    | <serviceGroupName>@ | (- policyName <string>@ [-priority <
    positive_integer>] [- gotoPriorityExpression <expression>] [-type (
    REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>) ] )
<!--NeedCopy-->
```

Beispiel 3:

```
bind lb vserver <name_of_vserver> -policyName radar_tag_policy -type
    RESPONSE -priority 10
<!--NeedCopy-->
```

Vorlage 4:

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression>]
    [-type <type>] [-invoke (<labelType> <labelName>) ]
<!--NeedCopy-->
```

Beispiel 4:

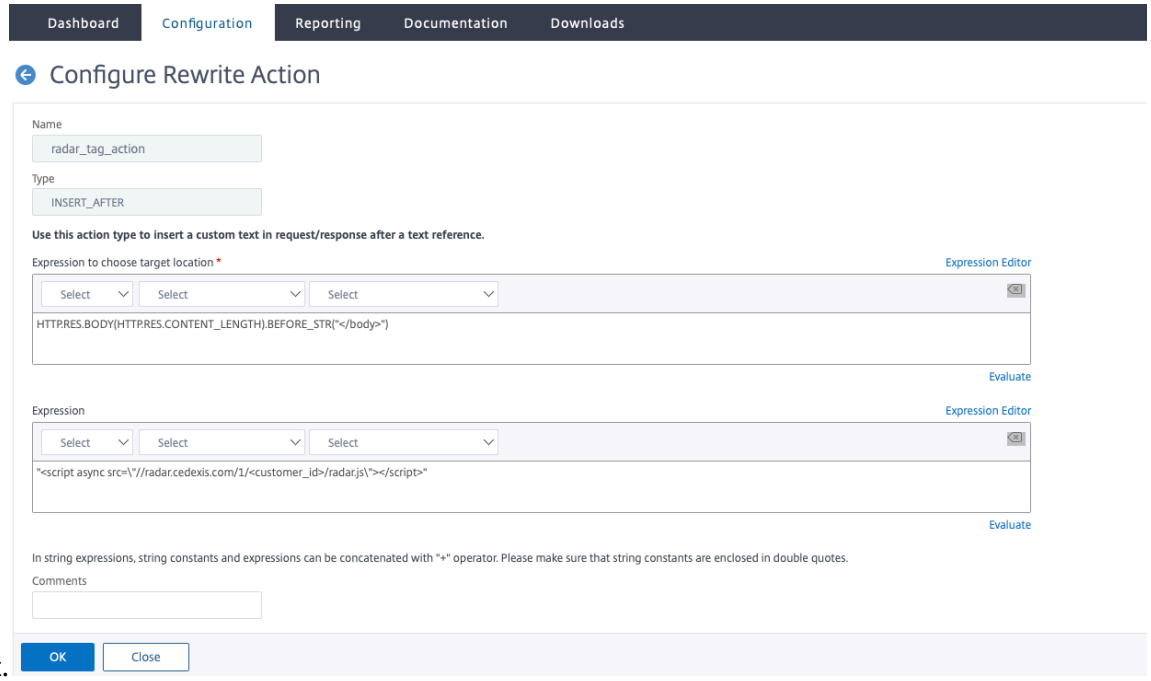
```
bind rewrite global radar_tag_policy 100 -type RES_DEFAULT
<!--NeedCopy-->
```

Konfiguration des GUI-Dienstprogramms

Aktion „GUI Rewrite“

1. **Navigieren Sie im linken Navigationsmenü auf der**NetScaler-Konfigurationsseite**zu**AppExpert**->**Rewrite -> Rewrite**Actions**
2. Wählen Sie die Schaltfläche **Hinzufügen** .
3. Geben Sie auf der Seite „ **Rewrite-Aktion konfigurieren** “den Ausdruck ein, wie im Beispiel

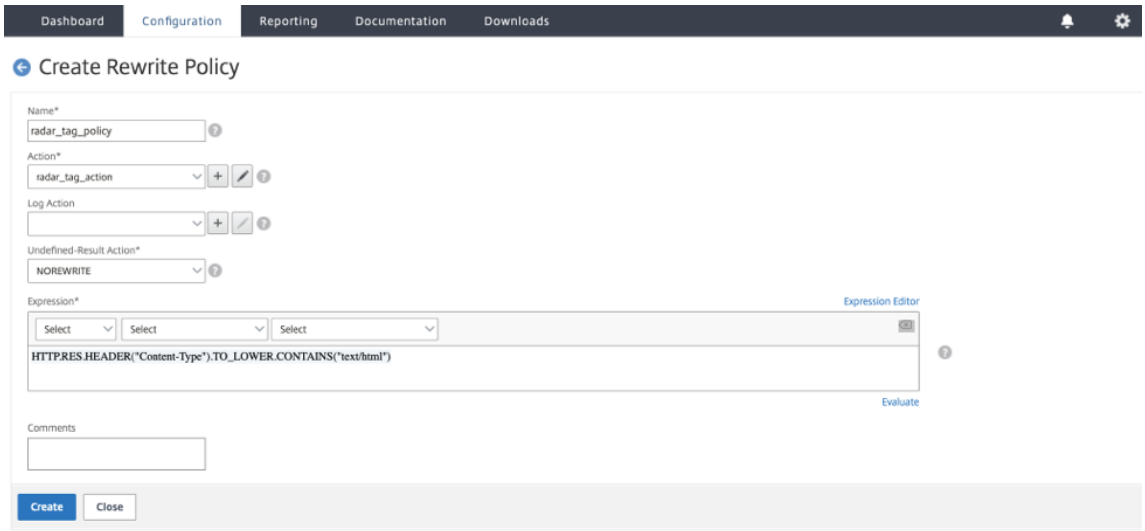
gezeigt.



4. Geben Sie im Radar-Skript Ihre Kunden-ID in das markierte Feld ein `<customer_id>`.
5. Wählen Sie **OK**. Sie haben die Erstellung Ihrer Rewrite-Aktion abgeschlossen.

Richtlinie zum Umschreiben der Benutzeroberfläche

1. **Gehen Sie im linken Navigationsmenü auf der**NetScaler-Konfigurationsseite**zu**AppExpert**->**Rewrite -> Rewrite Policies**
2. Wählen Sie die Schaltfläche **Hinzufügen** .
3. Geben Sie auf der Seite „ **Rewrite-Richtlinie konfigurieren** “den Ausdruck ein, wie im Beispiel gezeigt.

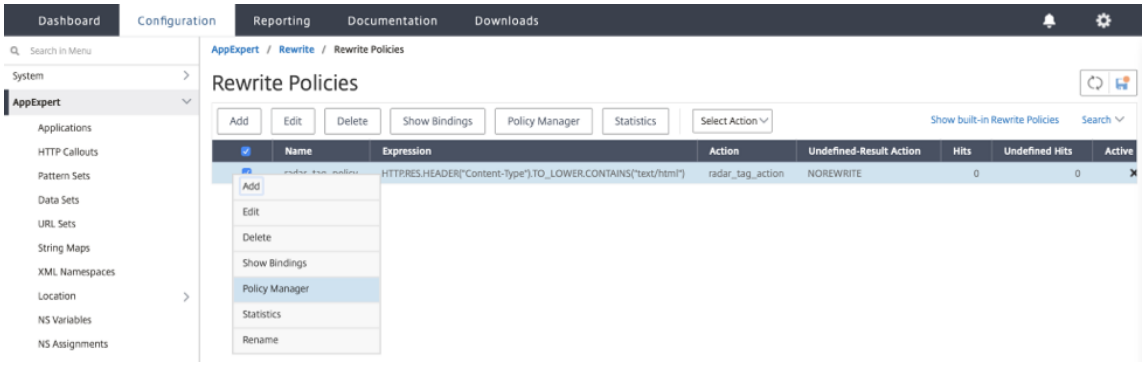


4. Klicken Sie auf **Erstellen**.

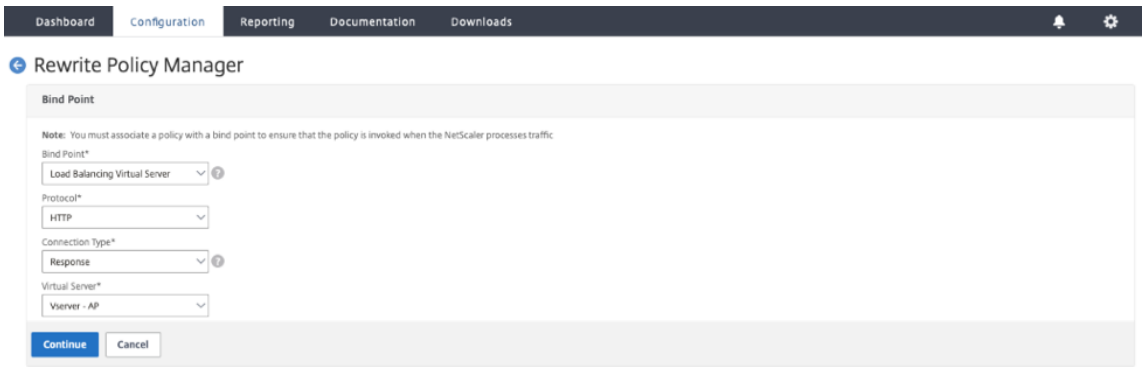
Sie haben die Konfiguration der Rewrite-Richtlinie abgeschlossen.

Richtlinie zum Umschreiben von GUI-Bindungen Sobald Sie mit der Konfiguration Ihrer Richtlinie fertig sind, besteht der letzte Schritt darin, die Richtlinie mithilfe des **Policy Managers**zu binden.

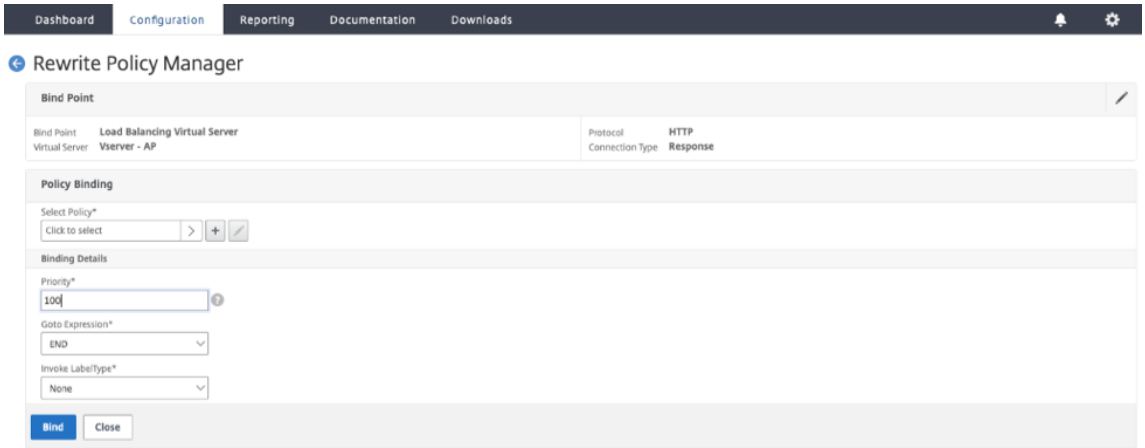
1. Rufen Sie die Seite **Rewrite Policies** auf.
2. Wählen Sie die Rewrite-Richtlinie aus, die Sie für das Radar-Tag erstellt haben.
3. Gehen Sie zum **Policy Manager**.



4. Auf der Seite **Policy Manager** können Sie die Richtlinie wie folgt binden.
   - Für **Bind Point** haben Sie die Möglichkeit, **Override Global**, **VPN Virtual Server**, **Content Switching Virtual Server**oder **Load Balancing Virtual Server**auszuwählen.
   - Wählen Sie als **ProtokollHTTP**aus.
   - Wählen Sie **als**Verbindungstyp**Antwort**aus.
   - Verwenden Sie für **Virtual Server** Ihren eigenen virtuellen Servernamen.



   - Klicken Sie auf **Weiter**.
   - Wählen Sie auf der nächsten Seite die **Rewrite-Richtlinie** aus, die Sie zuvor erstellt haben.
   - **Bindungsdetails**hinzufügen.
   - Klicken Sie auf **Bind**.

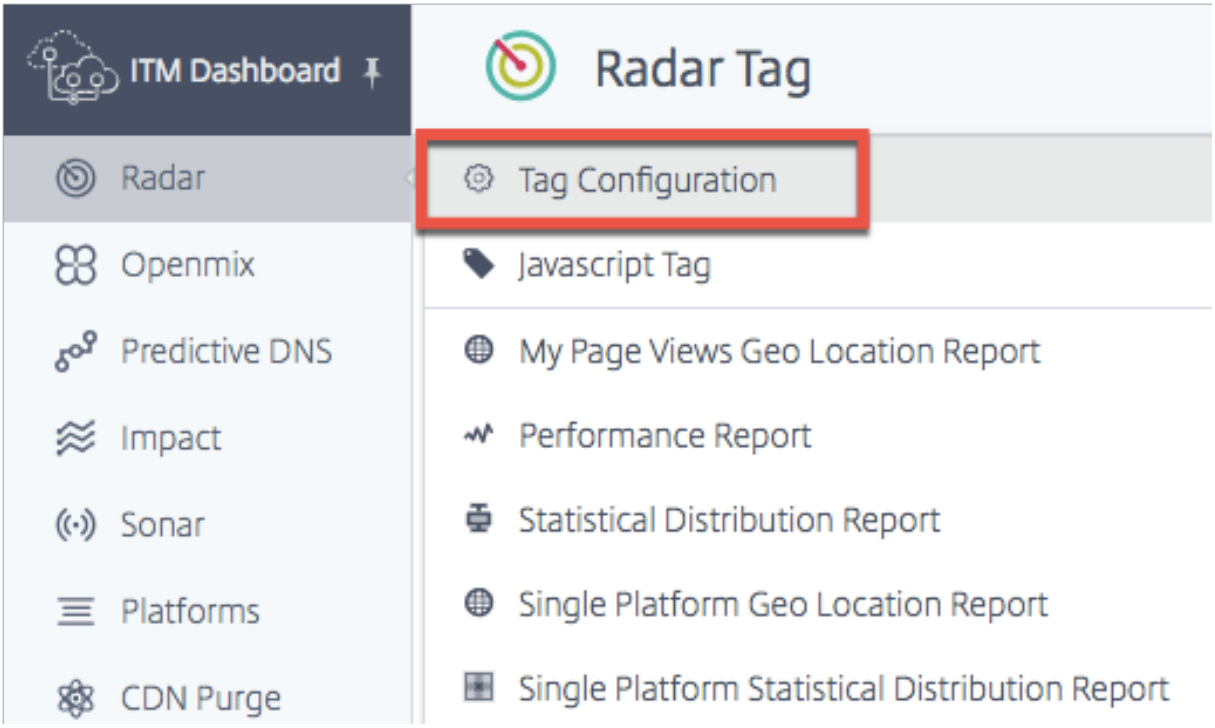


Mit den oben genannten Methoden können Sie das Radar-Tag in Ihre Webseiten einfügen. Es muss jedoch beachtet werden, dass dies eine grundlegende Implementierung ist. Weitere Filter können durchgeführt werden, um die Seiten, auf denen das Tag implementiert ist, besser kontrollieren zu können.

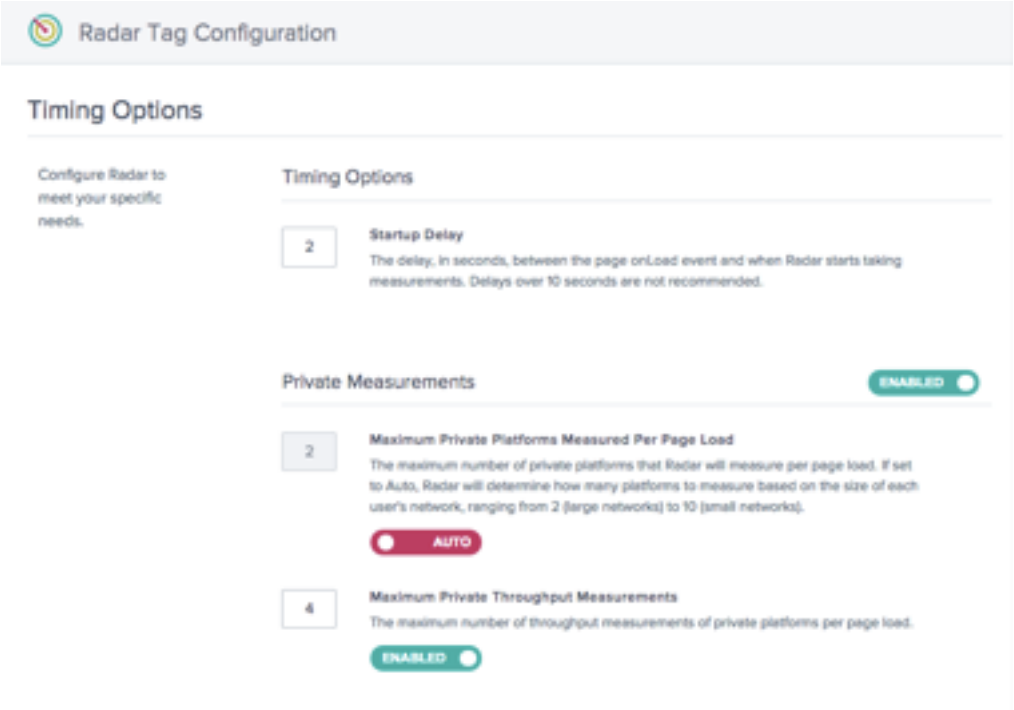
Radar-Tag-Konfiguration

Sie können Radar auf der Seite **Radar-Tag-Konfiguration** konfigurieren.

1. Melden Sie sich beim NetScaler Intelligent Traffic Management Portal an.
2. Wählen Sie im linken Navigationsmenü **Radar > Tag-Konfiguration**.



Die Seite Radar-Tag-Konfiguration wird geöffnet. Hier können Sie verschiedene Optionen einstellen, um Radarmessungen anzupassen. Das Radar-JavaScript verfügt über Parameter, die Sie anpassen können, um Timing- und Verzögerungselemente, die Anzahl der von Endbenutzern für Community- und Privatmessungen durchgeführten Tests sowie Timeout-Werte zur Messung der Verfügbarkeit usw. anzupassen.



Die folgende Tabelle enthält Informationen zu den Konfigurationsoptionen und den jeweiligen Standardeinstellungen. Wenn Sie Änderungen vornehmen, achten Sie darauf, unten auf dem Bildschirm auf **Radareinstellungen aktualisieren** zu klicken, um die Änderungen zu übernehmen.

Funktion	Parameter	Beschreibung	Standardeinstellung
Timing-Optionen	Startverzögerung	Die Verzögerung in Sekunden zwischen dem OnLoad-Ereignis der Seite und dem Zeitpunkt, zu dem Radar die Navigationszeit aufzeichnet.	2 Sekunden

Funktion	Parameter	Beschreibung	Standardeinstellung
	Verzögerung wiederholen	Die Verzögerung in Minuten zwischen den Messsitzungen. Wenn der Wert größer oder gleich 5 ist, führt das Radar-Tag nach jedem Wiederholungsverzögerungsintervall weitere Messungen durch. Wenn der Wert 0 ist, nimmt das Radar-Tag keine zusätzlichen Messungen vor.	5 Minuten
Protokolloptionen	Private HTTPS-Messungen immer zulassen	Ermöglicht dem Radar-Client, HTTPS-Messungen auch von einer HTTP-Website aus durchzuführen.	Messungen von Plattformen mit URL-Protokollen, die der Seite entsprechen, auf der der Radar-Client ausgeführt wird.
	Erlauben Sie private HTTP-Messungen auf HTTPS-Verbindungen.	Ermöglicht dem Radar-Client, HTTP-Messungen von einer HTTPS-Website aus durchzuführen.	Messungen von Plattformen mit URL-Protokollen, die der Seite entsprechen, auf der der Radar-Client ausgeführt wird.
Rate der Stichproben	Radar-Abtastrate	Der Prozentsatz der Seiten, auf denen das Radar-Tag aktiviert ist, um Messungen durchzuführen.	Disabled

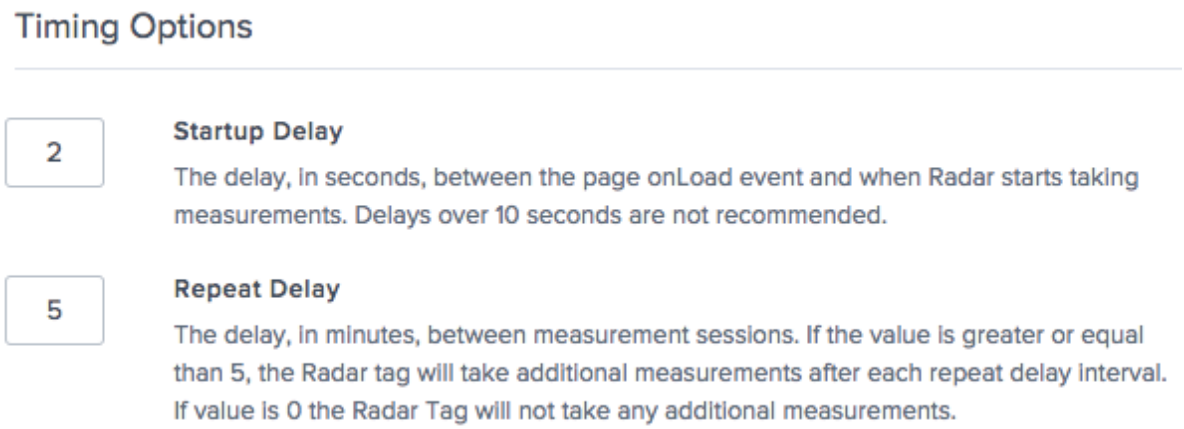
Funktion	Parameter	Beschreibung	Standardeinstellung
Private Messungen	Maximale Anzahl privater Messungen pro Seitenladevorgang	Die maximale Anzahl privater Plattformen, die Radar pro Seitenladevorgang misst.**	Auto*
	Maximale private Durchsatzmessungen	Die maximale Anzahl von Durchsatzmessungen privater Plattformen pro Seitenladevorgang.**	4
Messungen der Gemeinschaft	Maximale Community-Messungen pro Seitenladevorgang	Die maximale Anzahl von Community-Plattformen, die Radar pro Seitenladevorgang misst.**	Auto*
	Messungen des maximalen Gemeinschaftsdurchsatzes	Die maximale Anzahl von Durchsatzmessungen von Community-Plattformen pro Seitenladevorgang.**	4

*Automatisch bedeutet, dass NetScaler Intelligent Traffic Management anhand des Standorts des Endbenutzers bestimmt, wie viele Plattformen für eine bestimmte Sitzung gemessen werden müssen. Wir versuchen, mehr Plattformen pro Sitzung für kleine Netzwerke zu messen, in denen Daten spärlich sind, als für große Netzwerke, in denen sie dicht sind.

**Dies ist die maximale Anzahl von Messungen, die pro Sitzung versucht wurden. Radar kann beispielsweise 4 private Plattformen pro Sitzung messen, die alle so konfiguriert sind, dass sie sowohl RTT als auch den Durchsatz messen. Aber wenn Maximum Private Throughput Measurements auf 2 gesetzt ist, hört der Client nach der Messung der ersten beiden privaten Plattformen auf, die Durchsatzmessungen einzubeziehen. Für die letzten beiden Plattformen wird nur RTT gemessen.

Mit den Timing-Optionen können Sie festlegen, wie lange Radar warten muss, bevor es mit der Messung beginnt.

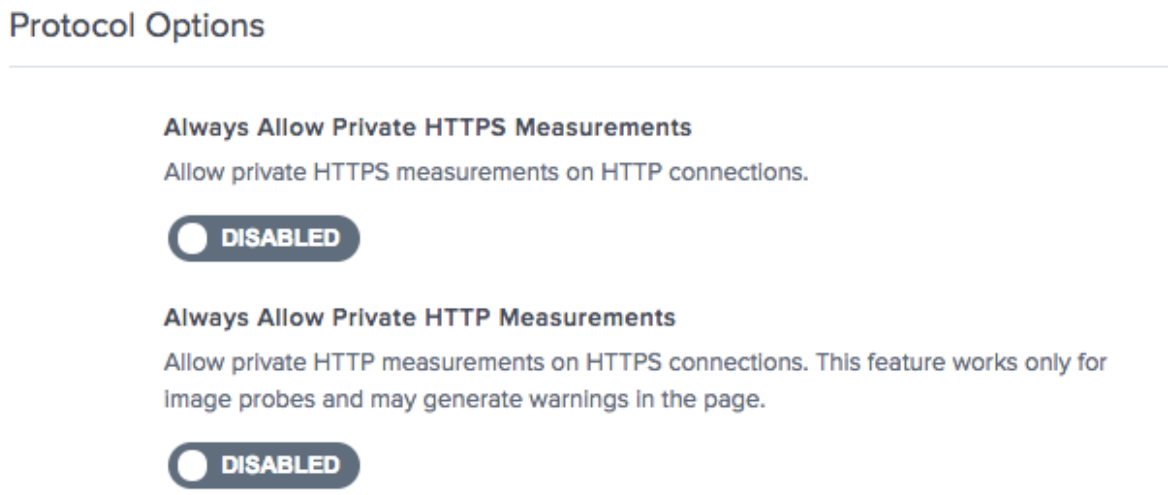
Hinweis: Die Startverzögerung wird in Sekunden und die **Wiederholungsverzögerung** in Minuten angegeben.



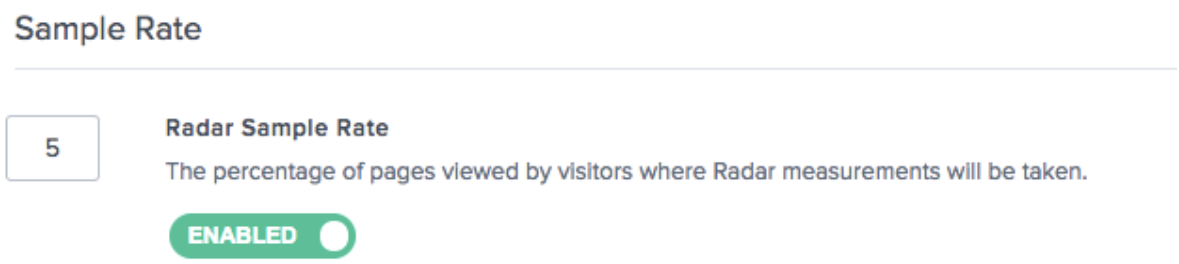
Protokolloptionen

Normalerweise misst der Radar-Client nur Plattformen mit URLs, deren Protokolle denen der Seite entsprechen, auf der er ausgeführt wird. Mit diesen Optionen können Sie dieses Verhalten für private Plattformen außer Kraft setzen. Wenn Sie beispielsweise „Private HTTPS-Messungen immer zulassen "aktivieren, kann der Client von dort `https://myprovider.com/r20.png` aus messen `http://example.com`, während „Private HTTP-Messungen immer zulassen"es dem Client ermöglicht, von dort `http://myprovider.com/r20.png` aus zu messen `https://example.com`.

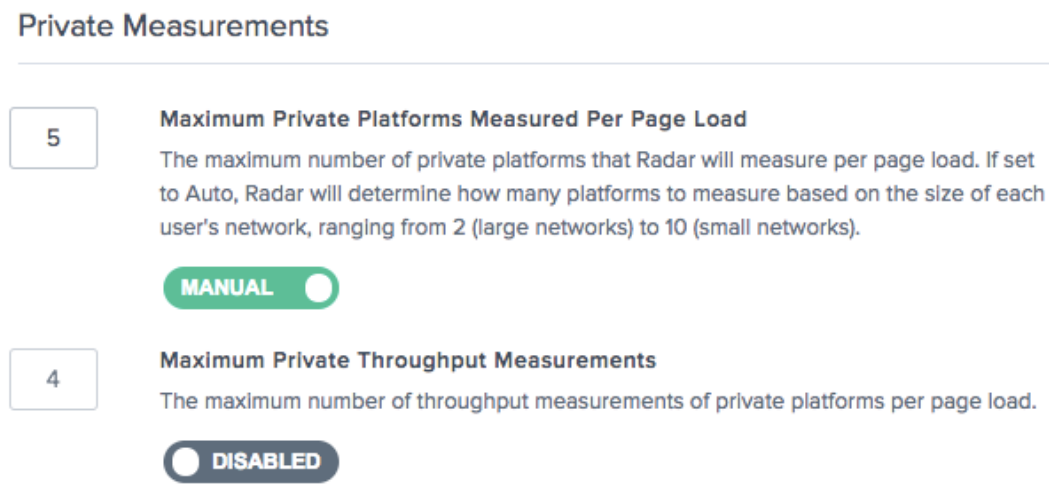
Diese Optionen müssen generell vermieden werden, außer in extremen Anwendungsfällen. Der beste Weg, um sicherzustellen, dass Sie eine angemessene private Messdichte erhalten, besteht darin, Ihre Plattformen so zu konfigurieren, dass sie die Plattformen und Protokolle messen, die Sie tatsächlich in der Produktion verwenden (und nicht mehr), und dass das Radar-Tag auf so vielen Produktionsseiten wie möglich bereitgestellt wird. Wir bezeichnen dies manchmal als „Radar dort einsetzen, wo es benötigt wird". „



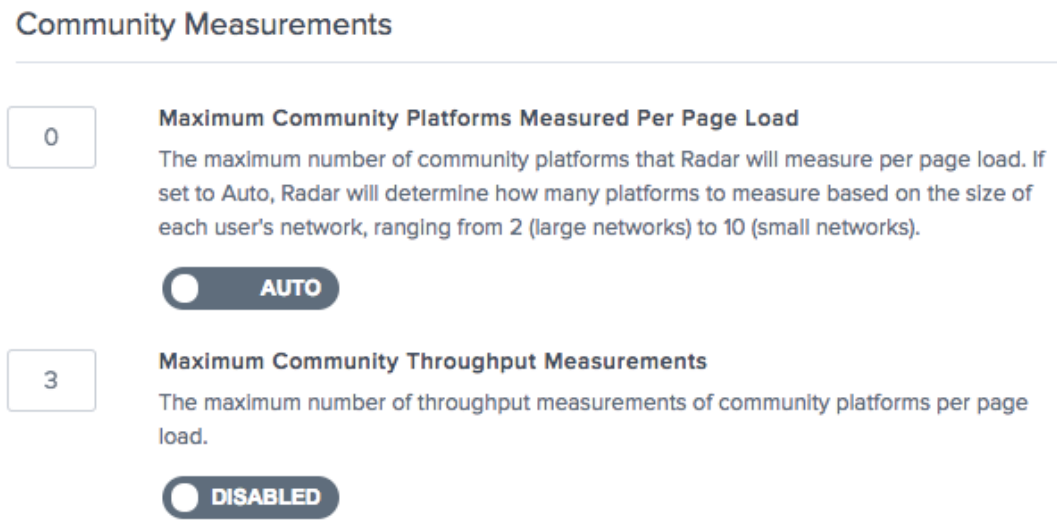
Mit der Samplerate können Sie einen Prozentsatz der (von Benutzern aufgerufenen) Webseiten festlegen, von denen Messungen erfasst werden sollen. Wenn Ihre Website beispielsweise 100.000 Seitenaufrufe pro Tag erhält und Sie eine Samplerate von 5% festlegen, erfasst Radar nur Messungen von 5% der 100.000 Seitenaufrufe.



Private Messungen Diese Einstellungen gelten für Messungen Ihrer privaten Plattformen. Private Plattformen sind solche, die Sie im Bereich **Plattformen** einrichten, um bestimmte CDNs, Cloud-Anbieter und andere Teile Ihrer Infrastruktur zu messen. Weitere Informationen finden Sie im Abschnitt Plattformen .



Mit dieser Option können Sie das Verhalten von Radar bei der Bereitstellung von Informationen an die Community konfigurieren.

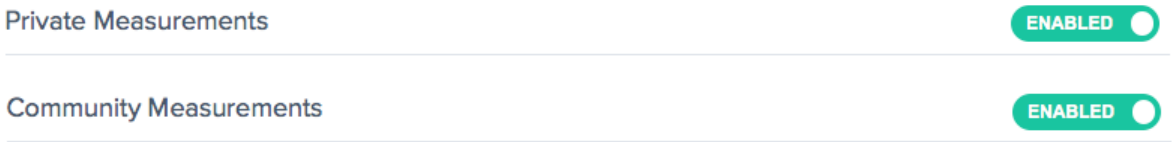


Radartests ausschalten

Wenn es erforderlich ist, die Radarmessungen schnell auszuschalten, falls etwas Unerwartetes passiert, können Sie dies im Portal tun, um Änderungen des Notfallcodes an Ihrer Site zu vermeiden.

Schalten Sie auf der Seite Radar-Tag-Konfiguration private Messungen, Community-Messungen oder beides aus, indem Sie auf die Umschaltfläche Aktiviert auf **Deaktiviert** klicken.

Klicken Sie auf **Radarkonfiguration speichern**, um die Änderungen zu bestätigen. Es kann ein oder zwei Minuten dauern, bis sich die Änderungen ausbreiten. Danach hören die Radarmessungen auf.



Methodologie für Radar-Kunden

Eine grundlegende Dimension des Kundenverhaltens ist die **Sitzung**. Alle Daten, die der Client sendet, sind einer Sitzung zugeordnet. Sitzungen werden durch einen Aufruf an NetScaler ITM-Server erstellt, der als Initialisierungsanforderung bezeichnet wird. Sitzungen laufen ziemlich schnell ab, wodurch sichergestellt wird, dass nur gültige Radardaten akzeptiert werden. Aufgrund dieser Funktion werden Radarmessungen immer in Stapeln geliefert, die mit ihrer Sitzungstransaktions-ID verknüpft sind, und wir sprechen oft von einer „Radarsitzung“, um die damit verbundenen Messungen zu beschreiben.

Radarsitzung

Eine Radarsitzung ist die Hauptarbeitseinheit, die der Kunde ausführt. Es besteht aus einer Anfrage an NetScaler ITM-Server, um die Kundenkonfiguration und eine Reihe von zu messenden Plattformen zu erhalten, gefolgt von Anfragen zur Messung dieser Plattformen und zur Meldung der Ergebnisse. Diese finden asynchron und serialisiert statt, sodass jeweils nur eine Anfrage erfolgt. Eine typische Sitzung ist in weniger als 10 Sekunden abgeschlossen.

Sondentypen

Jedem Bericht, den der Client sendet, ist ein Sondentyp zugeordnet, der dem System mitteilt, um welche Art von Messung es sich handelt und wie sie zu behandeln ist. Es gibt auch die Arten der durchzuführenden Messungen an, zu denen Verfügbarkeit, Hin- und Rückflugzeit, Durchsatz oder andere metrische Erfassung gehören können.“

Es besteht ein wichtiger Zusammenhang zwischen Verfügbarkeit und Leistungstests (z. B. Roundtrip-Zeit und Durchsatz). Die Verfügbarkeit einer bestimmten Ressource wird in einer bestimmten Messsitzung immer zuerst gemessen. Nur wenn die Verfügbarkeitsmessung erfolgreich ist, können zusätzliche Leistungsmessungen derselben Ressource in derselben Sitzung durchgeführt werden. „

Wenn in einem besonders langsamen Netzwerk ein Verfügbarkeitsausfall auftritt, kann dies dazu führen, dass sich die Gesamtleistung der Berichte, die dieses Netzwerk einbeziehen, tatsächlich verbessert. Dies ist nur ein Berichtsartefakt, da NetScaler Intelligent Traffic Management immer die detailliertesten, netzwerkspezifischen Leistungsdaten für Entscheidungen in Echtzeit verwendet.

Verfügbarkeit Verfügbarkeit, auch Kaltstart-Sonden genannt, sollen es Diensten ermöglichen, ihre Caches aufzuwärmen. Dieser Sonde ist zwar ein Messwert zugeordnet. Wir verwenden die Verfügbarkeitsprüfung, um festzustellen, ob der Anbieter verfügbar ist.

Wenn eine Plattform nicht für die Durchführung einer Kaltstartprüfung konfiguriert ist, verwenden wir die Ergebnisse der RTT-Prüfung anstelle eines Kaltstartberichts, um Verfügbarkeitsmetriken bereitzustellen.

In ähnlicher Weise lädt der Client bei dynamischen Objekten, die Standortbeschleunigungsdienste messen, das kleine Testobjekt einmal herunter und meldet den Messwert sowohl für den Kaltstart als auch für die Reaktionszeit.

Objekt testen	Definition
Standard	Verwendung von Resource Timing-Zeitstempeln: responseStart - requestStart
Dynamisch	Verwendung von Resource Timing-Zeitstempeln: ResponseEnd - DomainLookupStart

RTT

Objekt testen	Intervall	API	Beschreibung
Standard	ResponseStart - RequestStart	Zeitliche Planung der Ressourcen	Die Zeit, in der ein einzelnes Paket als Antwort auf eine HTTP-Anfrage zurückgegeben wird.
Dynamisch	Ende der Antwort — DomainLookupStart	Zeitliche Planung der Ressourcen	Die Zeit, in der eine Anfrage bearbeitet werden muss, einschließlich DNS-Suchzeit, Verbindungszeit und Antwortzeit.

Durchsatz

Objekt testen	Intervall	API	Beschreibung
Standard	Dateigröße (Kilobyte) * 8/(responseEnd - requestStart)	Zeitliche Planung der Ressourcen	Der gemessene Durchsatz (Kilobit pro Sekunde) für eine gesamte Anfrage und Antwort, basierend auf einem großen Testobjekt-Download.
Dynamisch	Dateigröße (Kilobyte) * 8/(ResponseEnd - DomainLookupStart)	Zeitliche Planung der Ressourcen	Der gemessene Durchsatz (Kilobit pro Sekunde) für eine gesamte Anfrage und Antwort, basierend auf einem großen Testobjekt-Download. Dies beinhaltet normalerweise nicht die Verbindungszeit oder die DNS-Suchzeit, falls ein RTT-Testobjekt bereits heruntergeladen wurde.

Objekte testen

Testobjekte sind Dateien, die auf Plattformen gehostet und vom Kunden heruntergeladen werden, um Messungen zu generieren. In diesem Abschnitt werden die verschiedenen Arten von Testobjekten beschrieben, die der Client unterstützt. Nicht alle Objekttypen gelten für jede Plattform.

Erforderlicher Header:

Der Timing-Allow-Origin-Antwortheader ist erforderlich, um JavaScript-Zugriff auf die von der Resource Timing-API bereitgestellten Low-Level-Timing-Daten zu ermöglichen. Die empfohlene Einstellung ist `Timing-Allow-Origin: *`, was bedeutet, dass JavaScript, das auf einer beliebigen Domain ausgeführt wird, die Erlaubnis zum Zugriff auf die Timing-Daten der Ressource erteilt werden muss.

Standard Die Standardtestobjekte sind Medien, die der Client herunterlädt, indem er das `src` Attribut für ein Image-Objekt festlegt. Nach dem Herunterladen verwendet der Client die Resource Timing API, um Leistungsdaten zu sammeln.
Diese Testobjekte müssen mit dem Timing-Allow-Origin-Antwortheader bedient werden. Weitere Informationen finden Sie im Abschnitt **Timing-Allow-Origin Header** .

Standard Klein Das standardmäßige kleine Testobjekt ist eine Einzelpixel-Bilddatei, die verwendet wird, wenn der Client eine einfache Netzwerkanfrage stellen muss.

Das kleine Standardtestobjekt wird in den folgenden Anwendungsfällen verwendet:

- Nichtdynamische Kaltstartsonden
- Nichtdynamische Roundtrip-Zeitsonden

Standard Groß Das standardmäßige große Testobjekt ist eine 100-KB-Bilddatei, mit der der Durchsatz einer Plattform gemessen wird.

Benennung großer Objekte: Um den Durchsatz zu berechnen, muss der Client die Größe des Testobjekts kennen. Der Client bestimmt den Dateinamen `r20-100KB.png`, indem er beispielsweise irgendwo im Dateinamen nach KB sucht. Kunden können beispielsweise Bilddateien unterschiedlicher Größe messen, sofern der Name die Dateigröße auf dieselbe Weise enthält `myimage-2048kb.jpg`
.

Dynamisch Dynamische Testobjekte werden verwendet, um die Leistung im Zusammenhang mit Site Acceleration Services zu messen.
Jede ist eine HTML-Datei, die JavaScript enthält, mit dem Zeitstempel von der Navigation Timing API erfasst und auf der übergeordneten Seite veröffentlicht werden können. Der Client lädt das Testobjekt mit einem Iframe herunter und erhält diese Zeitstempel, die er zur Berechnung der Messungen verwendet.

Sicherheit und Validierung Das Testobjekt ist ein 40-KB-Objekt. Eine neue Funktion des Testobjekts ist ein HMAC (Hash-based Message Authentication Code), den es auf der Grundlage von Abfrageparametern und einem geheimen Schlüssel bereitstellt, auf den der Server Zugriff hat. Dieser HMAC wird mit unserer Messung zurückgesendet, sodass wir überprüfen können, ob der Radar-Client auf das Testobjekt zugreifen konnte und nichts zwischengespeichert wurde.

Unterschied zwischen dynamischen und Standard-Testobjekten:

Bei standardmäßigen Radarmessungen versuchen wir, nur die primäre Anforderungsaktivität zu isolieren, die mit dem Herunterladen von Testobjekten verbunden ist, wohingegen unser Ziel bei Diensten zur Standortbeschleunigung darin besteht, einen größeren Teil der Aktivität zu messen.

Daher sind auch DNS-Suche und Verbindungszeit enthalten.
Außerdem sollen dynamische Messungen die Anforderungsleistung messen, wenn sie den Service-Ursprung erreichen, nicht nur einen Edge-Cache.

Im Portal können Sie diese Methode wie folgt wählen:

- Gehen Sie im linken Navigationsmenü zu **Plattformen**.
- Klicken Sie oben rechts auf der Seite auf das Symbol **Plattform hinzufügen** .
- Gehen Sie zu **Private Plattform > Kategorie > Dynamischer Inhalt**.
- Klicken Sie im Dialogfeld **Radartestobjekte** auf das Kontrollkästchen **Sonden anpassen** .
- Geben Sie die URL für die **Antwortzeit** ein und wählen Sie **Webpage Dynamic** aus der Dropdown-Liste **Objekttyp** aus.

Das dynamische kleine Testobjekt wird verwendet, um die Verfügbarkeit und die Roundtrip-Zeit zu messen, wobei dieselbe Sonde für Standortbeschleunigungsdienste verwendet wird.

iNAV Das iNav-Testobjekt ist eine statische HTML-Datei, die JavaScript enthält, das eine Reihe von Aufgaben ausführen kann. Der Client gibt an, welche Aufgabe er ausführen möchte, indem er Abfragezeichenfolgenparameter in die URL einfügt, die die HTML-Datei in einen Iframe lädt.
Das iNav-Testobjekt unterstützt die folgenden Anwendungsfälle: iNav-Kaltstart

iNav-Roundtrip-Zeit

Uni Das iUNI-Testobjekt wird verwendet, um den UNI-Wert zu ermitteln, der mit einer Reihe von Radarmessungen für eine Plattform verknüpft ist (die andere Methode ist CORS AJAX, für die kein separates Testobjekt erforderlich ist).

AJAX BEKOMMEN **Die AJAX GET-Methode kann im Allgemeinen mit jeder URL verwendet werden, die der Kunde messen möchte, vorausgesetzt, sie wird mit dem**Timing-Allow-Origin-Header und einem entsprechenden Access-Control-Allow-Origin-Header**bereitgestellt.**
Im Portal können Sie diese Methode wie folgt wählen:

- Gehen Sie im linken Navigationsmenü zu **Plattformen**.
- Klicken Sie oben rechts auf der Seite auf das Symbol **Plattform hinzufügen** .
- Gehen Sie zu **Private Plattform > Kategorie > Dynamischer Inhalt**.
- Klicken Sie im Dialogfeld **Radartestobjekte** auf das Kontrollkästchen **Sonden anpassen** .
- Geben Sie die **Antwortzeit** ein und wählen Sie **AJAX (GET)** aus der Dropdownliste **Objekttyp** aus.

Timing-Allow-Origin-Header Der Timing-Allow-Origin-Antwortheader ist erforderlich, um JavaScript-Zugriff auf die von der Resource Timing-API bereitgestellten Low-Level-Timing-Daten zu

ermöglichen.
Die empfohlene Einstellung ist `Timing-Allow-Origin: *`, dass die Berechtigung zum Zugriff auf die Zeitdaten der Ressource für JavaScript erteilt werden muss, das in einer beliebigen Domäne ausgeführt wird.

Radar-APIs

Radar bietet APIs sowohl für Betriebs- als auch für Datenabruffunktionen.

- Operations API —Radar-Konten hinzufügen/bearbeiten/löschen und die Kontrollmechanismen für den Betrieb Ihres Kontos über eine API
- Radardaten-API —Die ITM-Radardaten-API bietet Aggregate der öffentlichen Radar-Community und private Messdaten. Die Daten werden kontinuierlich aktualisiert und etwa alle 60 Sekunden gestapelt, um sie von der API abzurufen. Die Daten-API wird bereitgestellt, damit Kunden Radar-Daten in ihre eigenen Berichte und Dashboards integrieren können. Ein einziger Aufruf der API kann Radarquartil- oder Durchschnittswerte der Messwerte für alle Länder und bis zu 30 interessante ASNs für jede Plattform bereitstellen.

Radarberichte

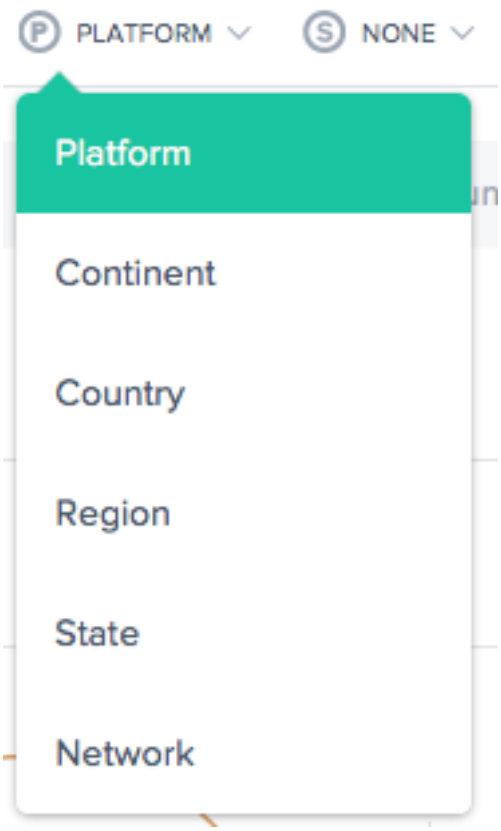
Radarberichte bieten einen umfassenden Einblick in die dynamischen Daten, die über das Radar-Tag gesammelt wurden.

Radar-Mitglieder erhalten Zugriff auf einen umfangreichen Datensatz, der in intuitiven interaktiven Diagrammen dargestellt wird. Der gesammelte Datensatz umfasst sowohl den vollständigen öffentlichen Datensatz mit Milliarden von Messungen als auch einen Kontext für private Daten, die aus dem Radar-Tag oder der mobilen SDK-Bereitstellung eines Kunden gesammelt wurden. Informationen zur Seitenladezeit werden mit dem eigenen Tag des Kunden erfasst und bieten so einen tiefen Einblick in die tatsächliche Leistungserfahrung der Endnutzer Ihrer Website und mobilen Anwendung.

Zusätzlich zu den Leistungskennzahlen bieten Radar-Berichte Einblicke in viele Facetten Ihrer Endnutzerschaft, darunter: Volumen, Regionen, Benutzeragenten, Betriebssystemtypen und den Zeitpunkt ihrer Nutzung Ihrer Website oder mobilen Anwendung.

Jeder Bericht ist unten definiert, aber hier sind wichtige Aspekte aller Berichte aufgeführt:

Primäre und sekundäre Dimensionen



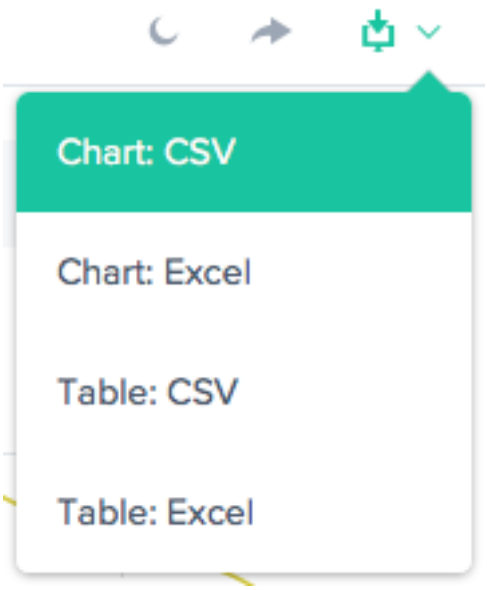
Die primäre Dimension des Diagramms wird über eine Listenauswahlliste über dem Diagramm ausgewählt. Verwenden Sie dies als wichtigen Dreh- und Angelpunkt für den Bericht. Eine sekundäre Dimension kann ebenfalls ausgewählt werden, um die Berichterstattung weiter zu verfeinern.

Visualisierungshintergrund


Umschalten

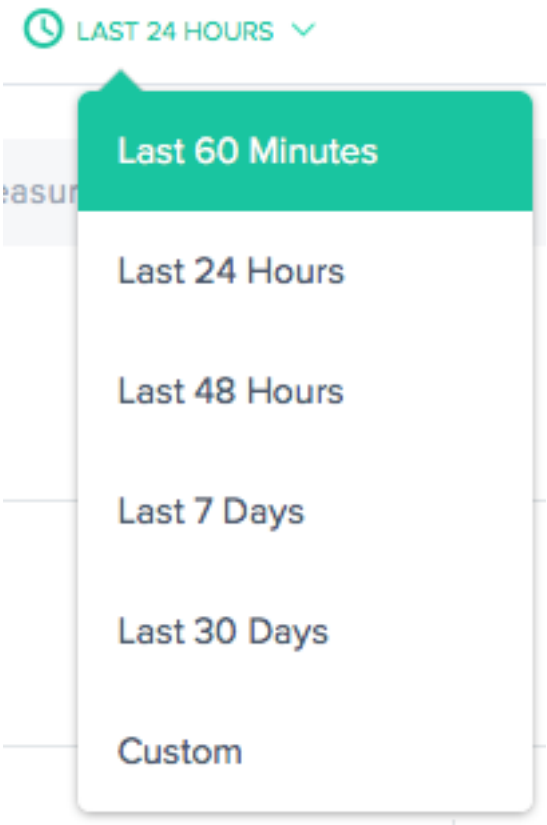
Diagramme sind standardmäßig auf einen weißen Hintergrund eingestellt. Schalten Sie den Hintergrund bei Monitoren mit hohem Kontrast mithilfe der Hintergrund-Umschalttaste auf eine dunkle Farbe um.

Daten-Export



Darüber hinaus kann der Endbenutzer die Diagramm- und Tabellendaten über den Download-Link oben im Bericht herunterladen.

Filter: Berichts-Zeitbereich



Die Radarberichte können mit einem Zeitraum von den letzten 60 Minuten, den letzten 24 Stunden, den letzten 48 Stunden, den letzten 7 Tagen, den letzten 30 Tagen oder einem benutzerdefinierten Bereich generiert werden. Die Standardansicht ist die Letzte 24 Stunden.

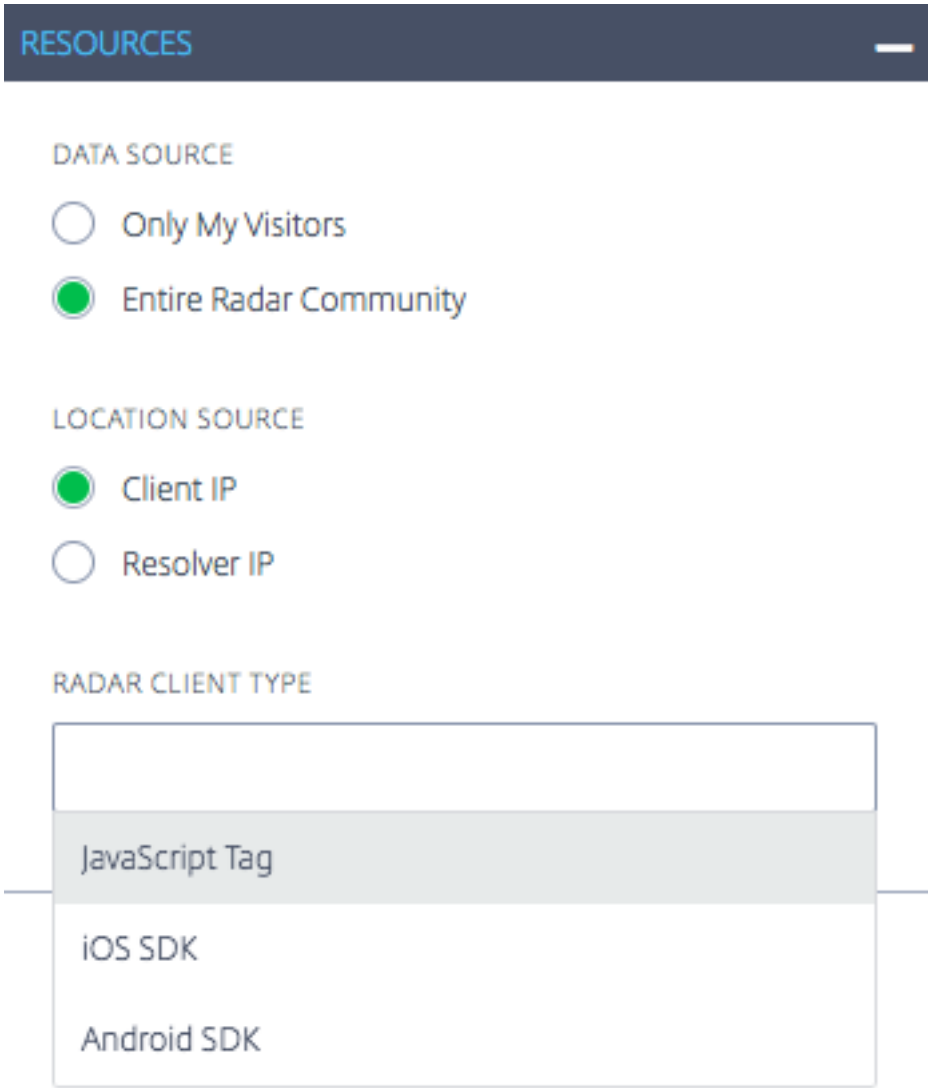
Filter: Plattform und Standort

Die Berichte unterscheiden sich geringfügig in Bezug darauf, welche Filter basierend auf den Daten geeignet sind. Die folgenden sind die häufigsten:

- **Plattform** —Wählen Sie eine oder mehrere Plattformen (Anbieter) aus, die einbezogen werden sollen.
- **Kontinent** —Wählen Sie einen oder mehrere Kontinente aus, die eingeschlossen werden sollen
- **Land** —Wählen Sie ein oder mehrere Länder aus, die einbezogen werden sollen.
- **Region** —Wählen Sie eine oder mehrere geografische Regionen (falls zutreffend), die einbezogen werden sollen.
- **Bundesstaat** —Wählen Sie einen oder mehrere geografische Staaten (falls zutreffend) aus, die eingeschlossen werden sollen.
- **Netzwerk** —Wählen Sie ein oder mehrere Netzwerke (ASN) aus, die eingeschlossen werden sollen.

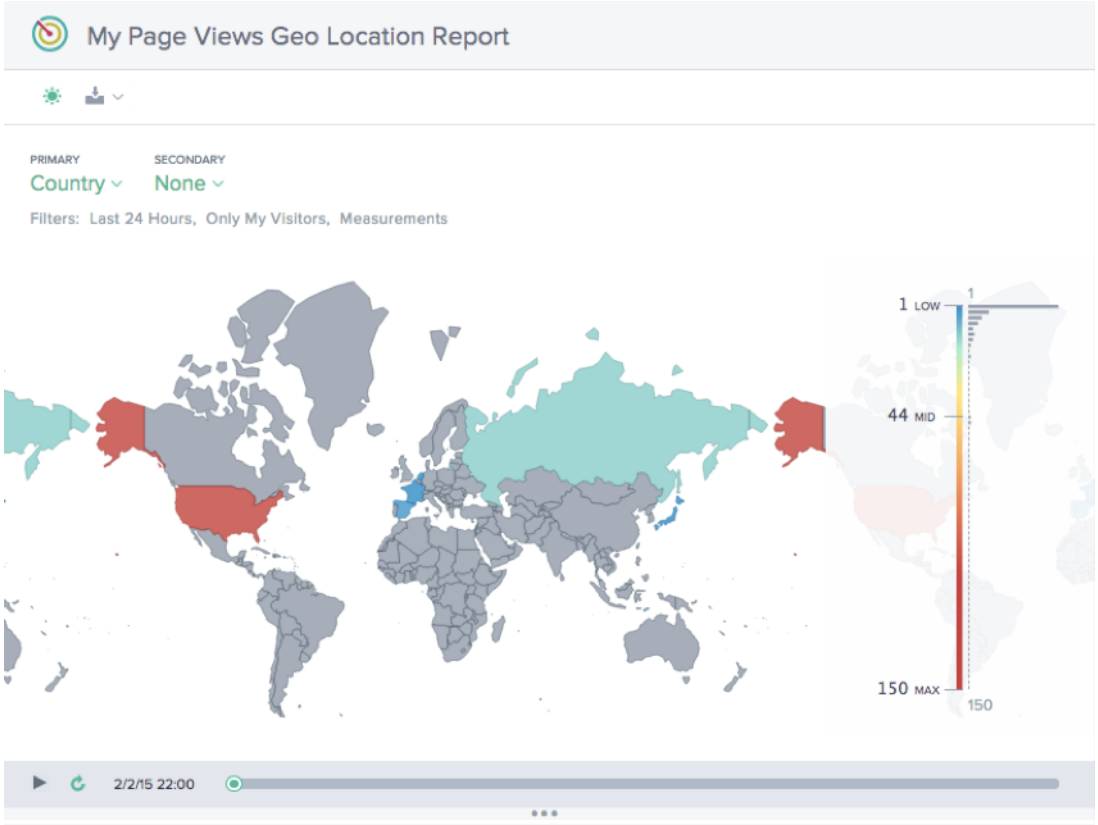
Filter: Ressourcen

- **Datenquelle** —Schließt Daten aus der gesamten Radar-Community oder nur von Besuchern Ihrer Website ein.
- **Standortquelle** —Wählen Sie die Client-IP oder die Resolver-IP als Ihre Standortquelle aus.
- **Radar-Clienttyp** —Wählen Sie den Radar-Clienttyp als JavaScript-Tag, iOS-SDK oder Android-SDK aus.



Meine Seitenaufrufe Geolokalisierungsbericht

Dieser Bericht zeigt die Anzahl der Seitenaufrufe für jedes Land. Diese Kartenansicht kann im Zeitverlauf (basierend auf dem für den Bericht ausgewählten Zeitraum) angezeigt werden, indem Sie unten im Diagramm auf die Schaltfläche **„Abspielen“** klicken.



Leistungsbericht

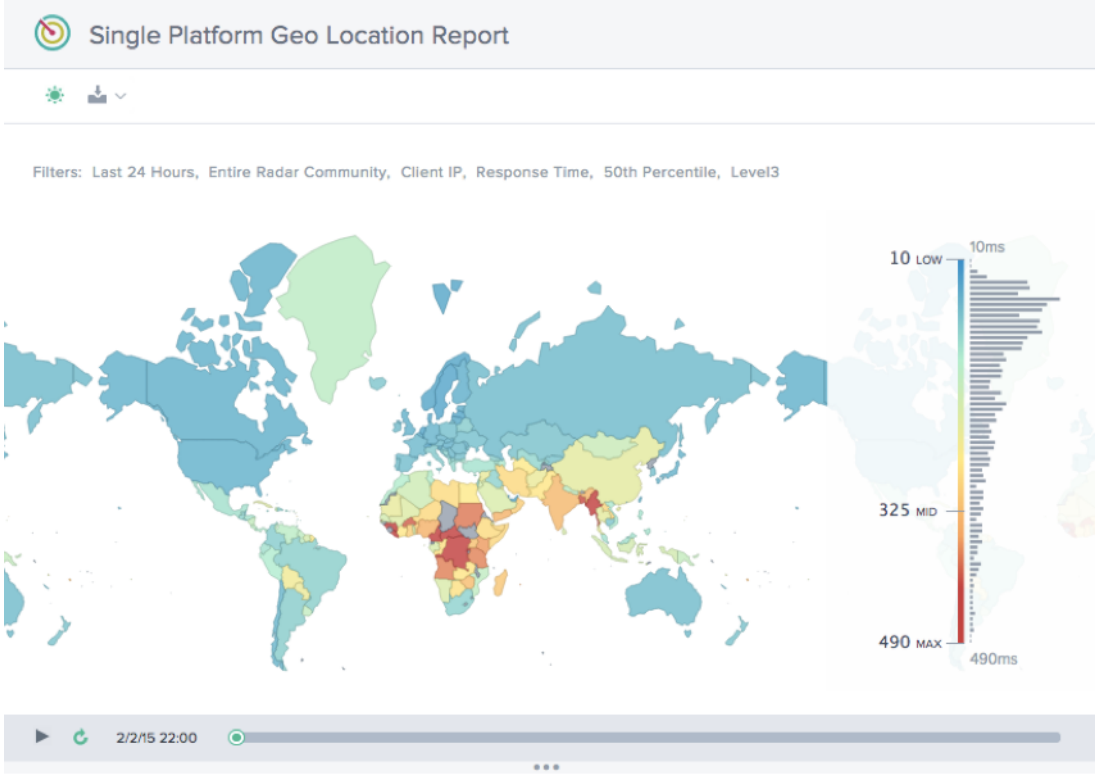
Dieser Bericht zeigt den Leistungstrend für jede der definierten Plattformen.

Statistischer Verteilungsbericht

Dieser Bericht zeigt die statistische Aufschlüsselung für jede der für das Konto definierten Plattformen.

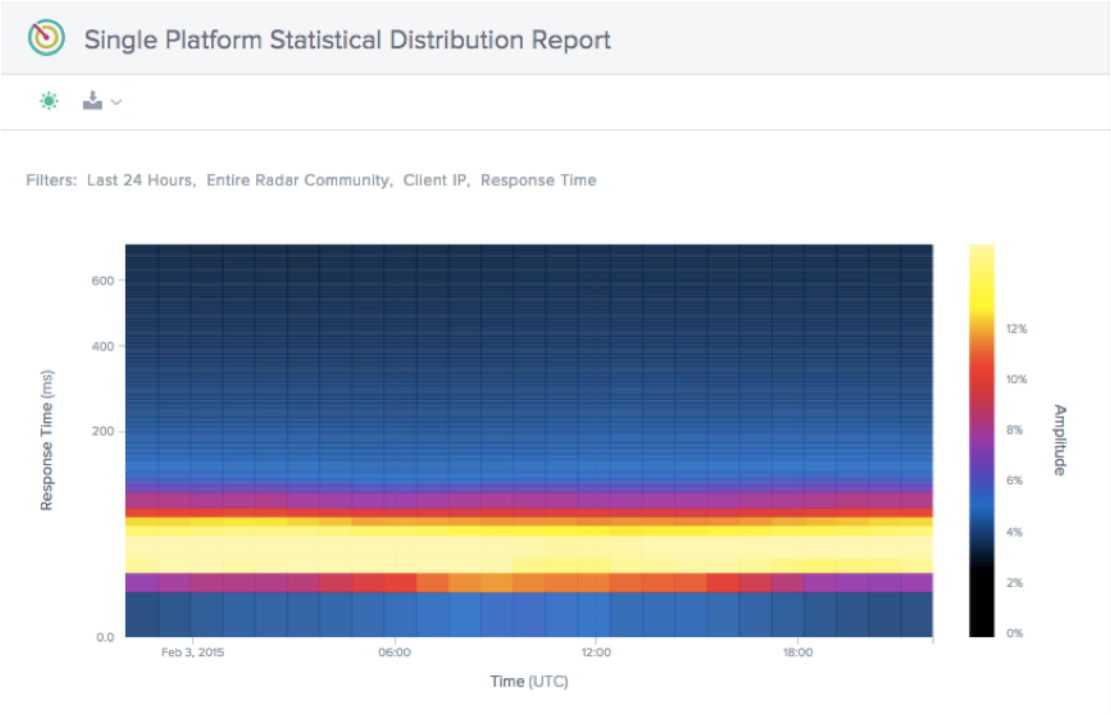
Geolokalisierungsbericht für eine einzige Plattform

Dieser Bericht zeigt die Verteilung des Radarverkehrs nach Ländern im Zeitverlauf für jeweils eine einzelne Plattform.



Statistischer Verteilungsbericht auf einer einzigen Plattform

Dieser Bericht zeigt die Verteilung des Radarverkehrs über die Zeit nach Reaktionszeit.

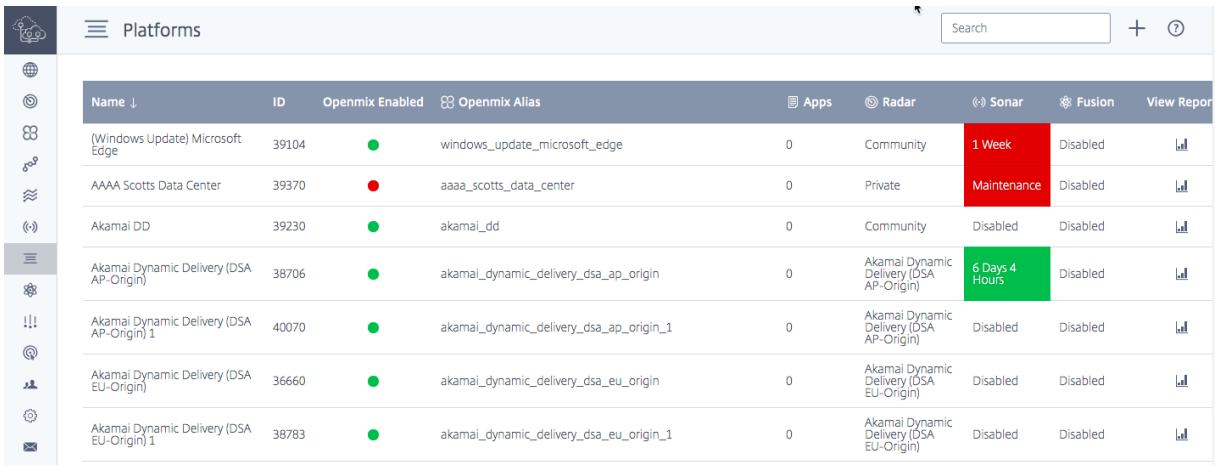


Plattformen

June 4, 2021

Auf der Seite **Plattformen** gibt der Kunde die CDNs, Clouds, Rechenzentren oder andere Endpunkte an, die überwacht und mit Openmix verwendet werden müssen. Für jeden Routing-Endpunkt, auf dem Sie Bericht erstellen möchten, muss eine Plattform eingerichtet werden. Meistens stellt eine Plattform einen CDN, eine Cloud-Region oder eine einzelne Instanz dar, wenn Openmix für GSLB verwendet wird.

Wenn Sie auf diesen Menüpunkt klicken, wird dem Kunden der folgende Bildschirm angezeigt.



Dieser Bildschirm zeigt eine vollständige Liste aller Plattformen, die für Reporting, Radarmessungen oder die Sonar- und Fusion-Services konfiguriert sind.

Die Tabelle zeigt:

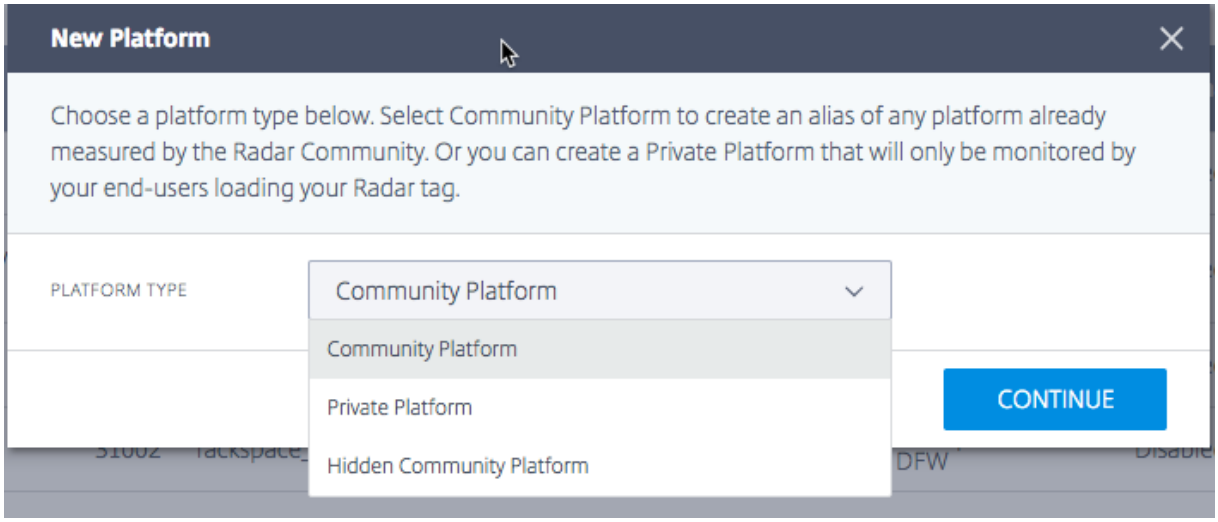
Überschrift	Beschreibung
Name	Der benutzerdefinierte Name der Plattform.
ID	Die für die Plattform generierte ID, die für den API-Zugriff und das Reporting nützlich ist.
Openmix-Alias	Der Alias, mit dem aus Openmix-Anwendungen auf die Plattform verwiesen werden soll.
Apps	Die Anzahl der Openmix-Anwendungen, die die Plattform verwenden.
Radar	Ob die Plattform für die Verwendung von Community- oder privaten Radarmessungen eingerichtet ist.
Sonar	Ob Sonar auf dieser Plattform aktiviert ist.
Fusion	Ob Fusion auf dieser Plattform aktiviert ist.

Erstellen einer Plattform

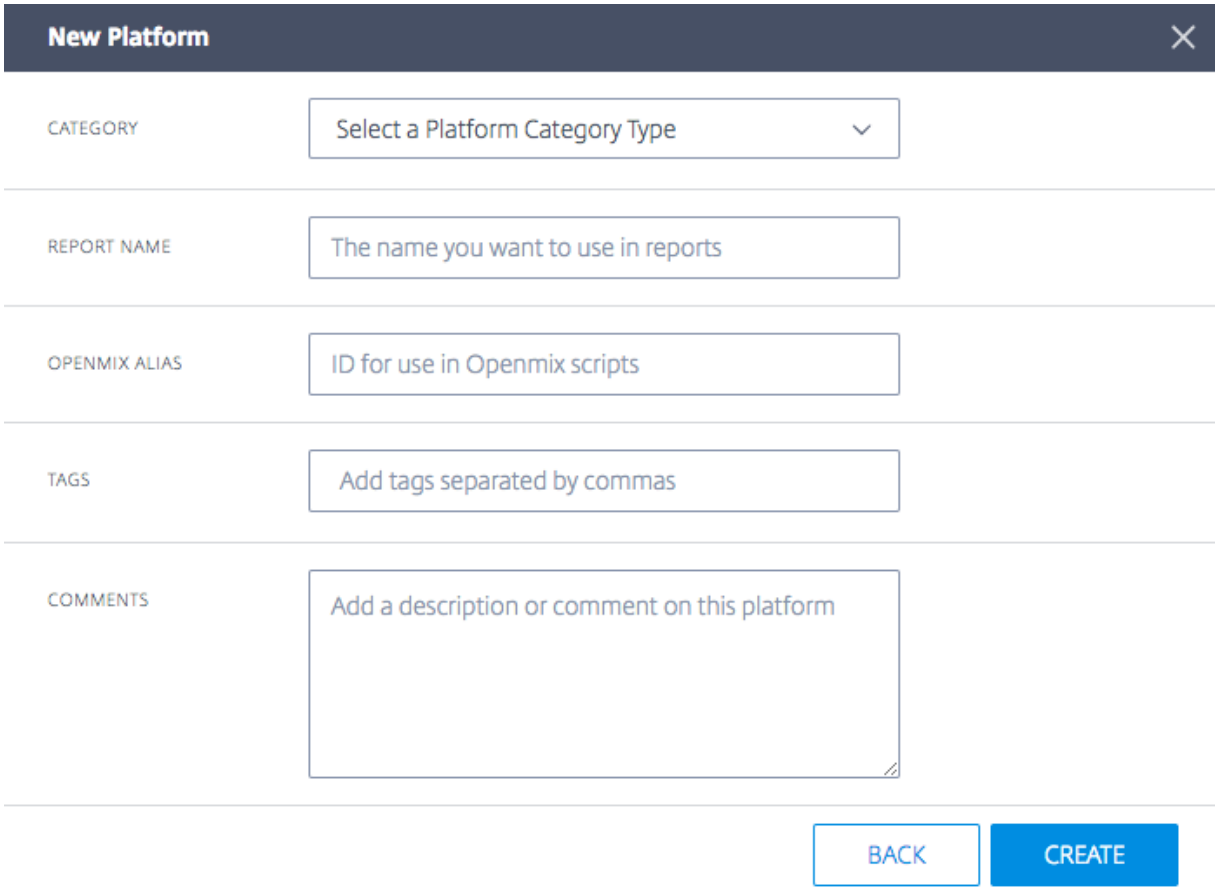
Um eine Plattform hinzuzufügen, klicken Sie oben auf der Seite Plattformen auf **+** .

Neue Plattformen

Nachdem Sie auf **Plattformen hinzufügen** geklickt haben, sehen Sie die folgende Seite, auf der Sie den Typ der Plattform auswählen können, den Sie konfigurieren möchten.



Nachdem Sie den **Plattformtyp**ausgewählt haben, können Sie einen Namen für die Plattform angeben, die zur Anzeige von Informationen verwendet und in anderen Diensten verwendet wird, die von ITM bereitgestellt werden, z. B. Openmix.

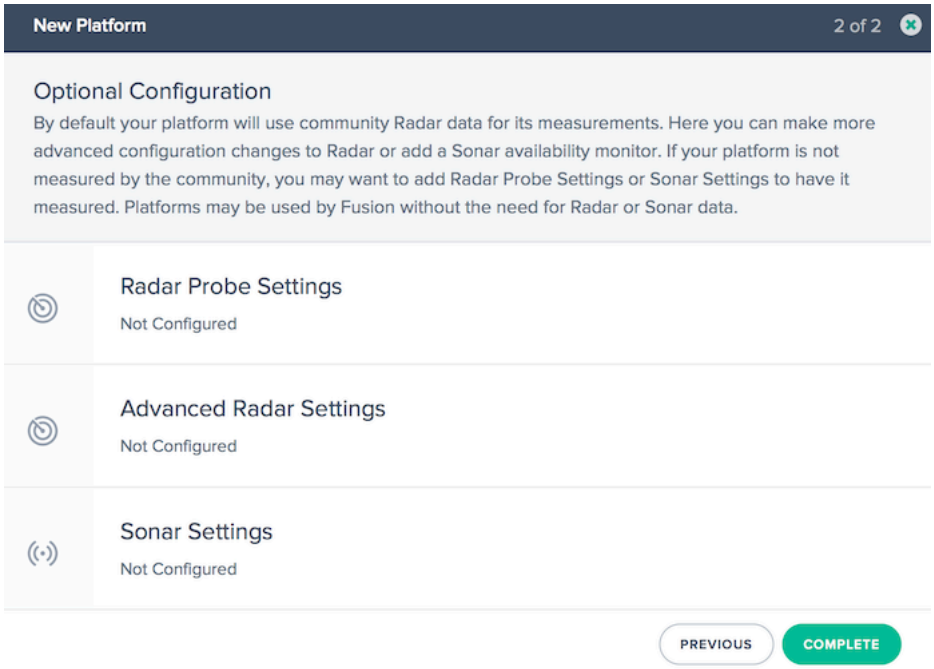


Geben Sie **unter Plattformeinstellungen**die folgenden Informationen ein:

Eingabeelement	Beschreibung
Kategorie	Die Art des Dienstes, den die Plattform darstellt. Plattformen werden je nach Typ in Radar und Openmix unterschiedlich gehandhabt. Die verfügbaren Plattformkategorien sind: Cloud Computing, Dynamic Content, Delivery Networks, Cloud Storage, Secure Object Delivery und Managed DNS. Für **private** Plattformen ist **Data Center** eine weitere Kategorie verfügbar. Hinweis: Alle importierten GSLBs werden als Rechenzentren erstellt.
Plattform	Wählen Sie die Plattform aus, die Sie testen möchten, z. B. Akamai, Amazon, Azure usw.
Name des Berichts	Name der Plattform, die in Anzeige und Berichterstellung verwendet wird.
Openmix-Alias	Der Alias, den Openmix-Anwendungen zur Identifizierung der Plattform verwenden.
Tags	Tags können Plattformen zugewiesen werden, so dass sie nach Bedarf organisiert werden können.

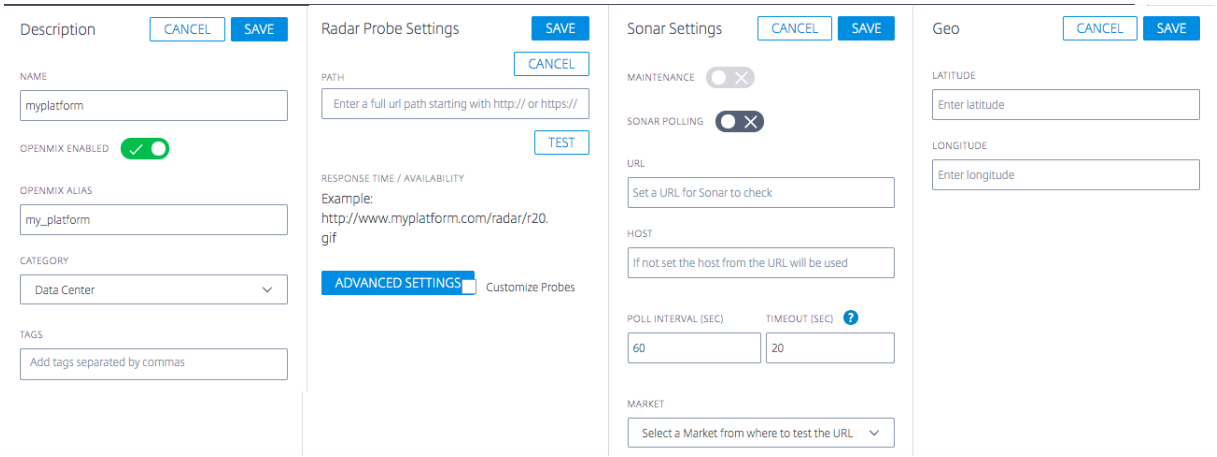
Wenn Sie eine vorhandene Plattform auswählen, werden die Felder **Report Name und Openmix Alias** ausgefüllt. Sie können diese Felder mit den Standardwerten belassen oder sie nach Belieben ändern.

Klicken Sie auf **Weiter**, um mit der optionalen Konfiguration fortzufahren. Wenn Sie mit der optionalen Konfiguration fertig sind, klicken Sie auf **Abschließen**, um die Plattform hinzuzufügen.



Bearbeiten einer Plattform

Das Bearbeiten einer Plattform ist so einfach wie das Klicken auf die Plattformzeile in der Tabelle und das Klicken auf die Schaltfläche **Bearbeiten** .



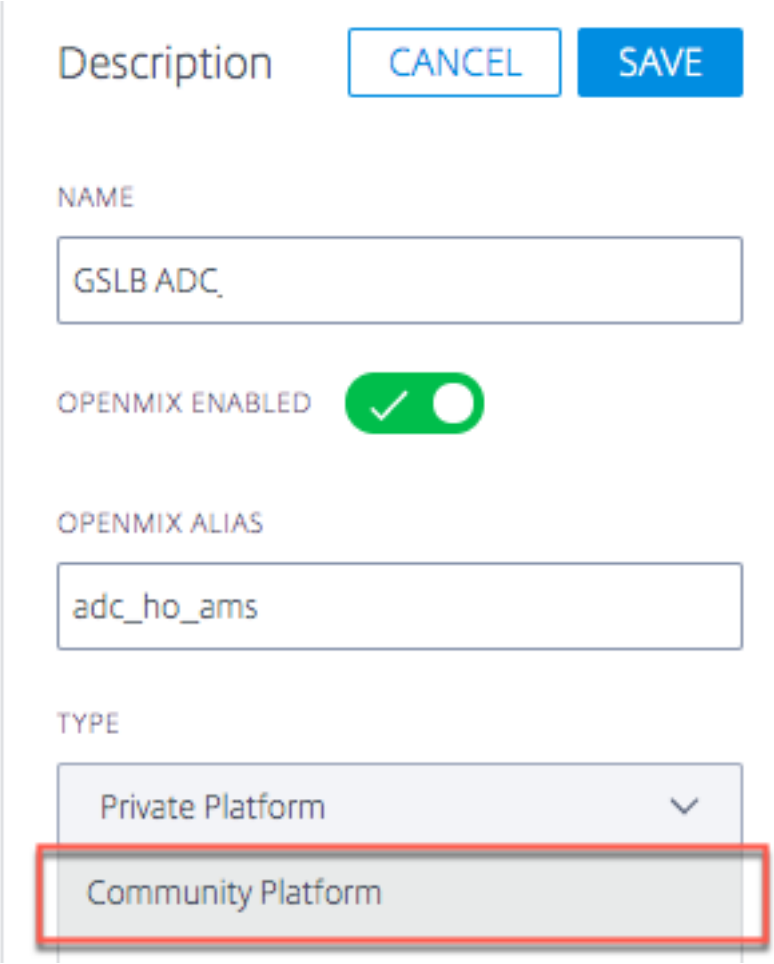
Sobald Sie die Konfiguration geändert haben, klicken Sie einfach auf **Speichern**, wie Sie es bei einer neuen Anwendung tun würden. Dadurch werden Sie wieder zum Plattformbildschirm mit den gespeicherten Änderungen zurückgeführt.

Plattformtyp ändern

Diese Funktion ist nützlich für Kunden, deren private Plattformen in einem öffentlichen Rechenzentrum oder einer Cloud-Region gehostet werden, die von der Radar-Community gemessen wird (z. B. AWS) und die Radar-Daten dieser Community-Plattform erben möchten. Wenn Kunden beispielsweise GSLBs in das ITM-Portal importieren, werden sie als private Rechenzentren importiert, können sich aber tatsächlich in einer Public Cloud-Region befinden. Um die Radar-Daten der Community-Plattform zu erben, können Kunden die aktuellen Einstellungen der privaten Plattform oder GSLB ändern, um stattdessen auf die Community-Plattform zu verweisen.

Gehen Sie wie folgt vor, um den Plattformtyp, z. B. eine GSLB oder ein privates Rechenzentrum, in eine öffentliche Community-Plattform (oder bei Bedarf von der Community zurück zu privat) zu ändern.

1. Klicken Sie in der Tabelle **Plattformen auf die Plattformzeile** .
2. Klicken Sie im Abschnitt **Plattformeinstellungen** auf die Schaltfläche **Bearbeiten** .
3. Gehen Sie zu **Typ**. Wählen Sie **Community-Plattform** aus der Liste, wenn Sie Ihre private Plattform in eine Community-Plattform ändern möchten.
4. Gehen Sie zu **Kategorie**. Wählen Sie eine Plattformkategorie aus der Liste aus.
5. Gehen Sie zu **Plattform**. Wählen Sie in der Dropdown-Liste Plattform die **Plattform** aus, zu der Sie wechseln möchten.
6. Klicken **Sie** oben rechts im Abschnitt **Plattformeinstellungen** auf Speichern. Sie erhalten eine Bestätigungsmeldung, die Ihnen mitteilt, dass die Radarsondeneinstellungen für Ihre private Plattform entfernt und durch die Einstellungen der Community-Plattform ersetzt werden.
7. Klicken Sie auf **Bestätigen**.

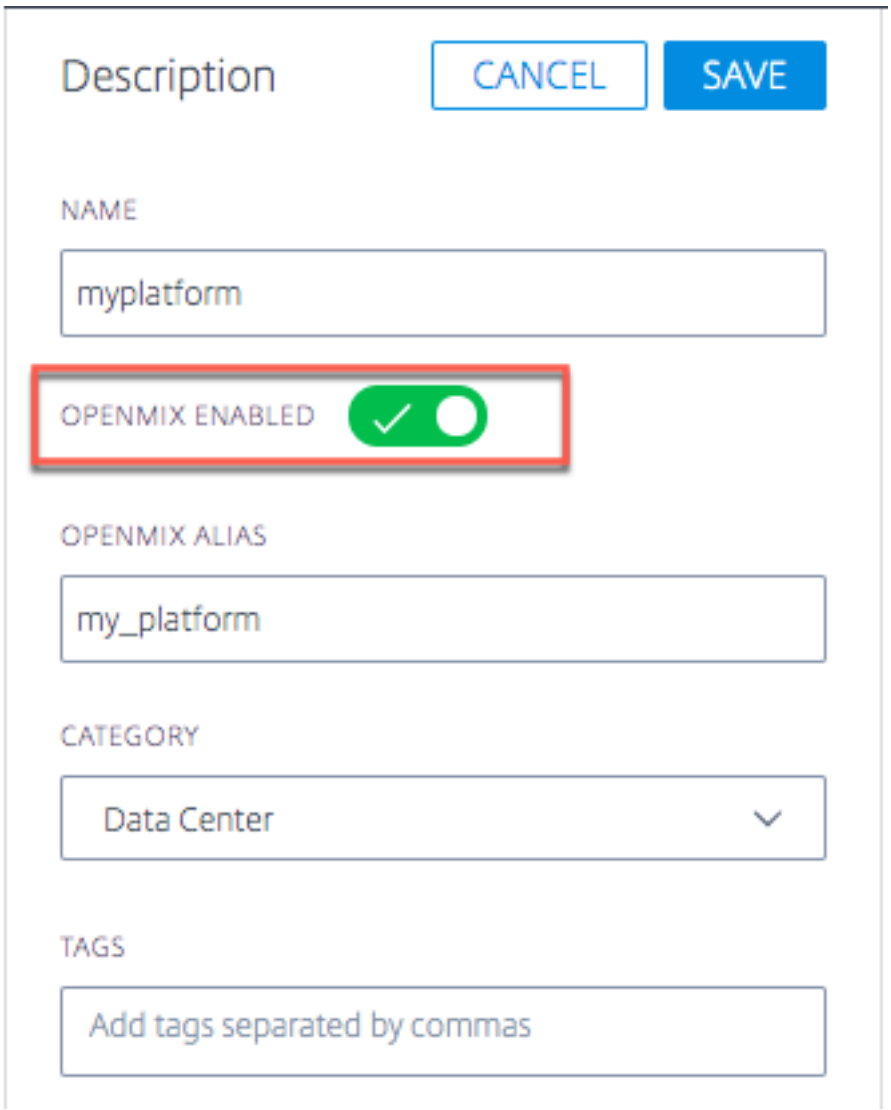


Hinweis: Wenn Sie sich entscheiden, von der Community zu Ihrer privaten Plattform zurückzukehren, müssen Sie die Einstellungen für die Radarsonde neu konfigurieren.

Plattform für Openmix aktivieren

Eine Plattform kann für Openmix aktiviert oder deaktiviert werden, indem die Schaltfläche "**Openmix Enabled**"in den **Plattformeinstellungen** aktiviert oder deaktiviert wird.

- Klicken Sie in den **Plattformeinstellungen** auf die **Schaltfläche Bearbeiten**
- Wählen Sie die Schaltfläche für **Openmix Enabled**, um sie einzuschalten.



Wenn eine bestimmte Plattform für Openmix deaktiviert ist, wird diese Plattform nicht mehr in Openmix-Entscheidungen berücksichtigt. Dies bedeutet, dass für die jeweilige Plattform kein Radarwert generiert wird.

In Quickstart-Apps wird die Plattform (wenn sie in der Benutzeroberfläche deaktiviert ist) nicht als Option angezeigt, die ausgewählt werden soll.

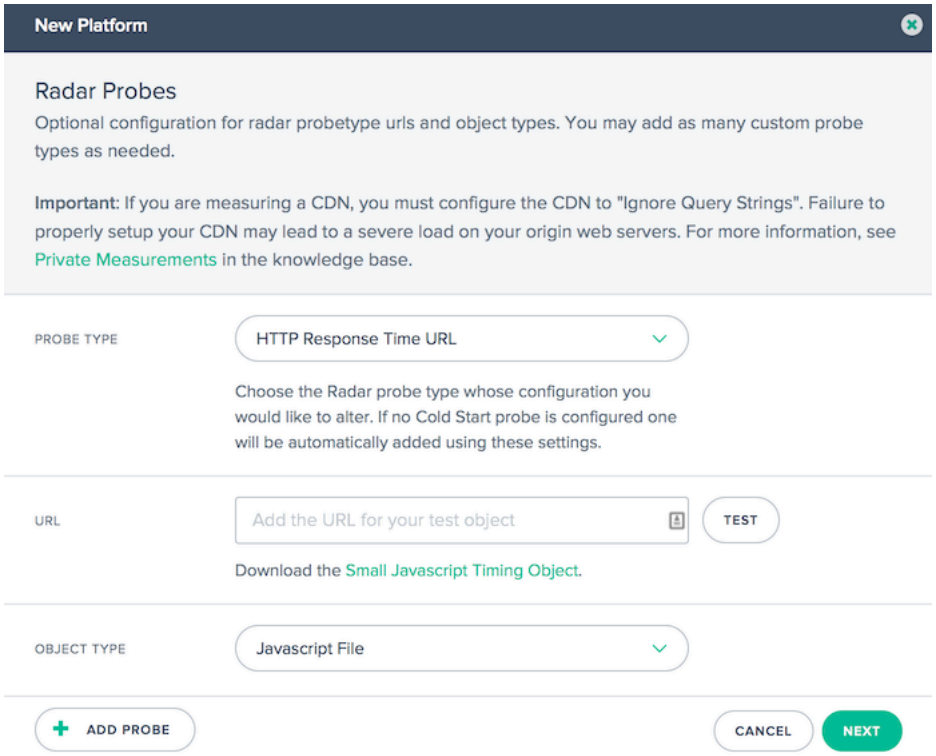
Wenn die Plattform jedoch fest in die App-Logik codiert ist, besteht die Möglichkeit, dass sie abgeholt wird (selbst wenn diese Plattform für Openmix in der Benutzeroberfläche deaktiviert ist). Um dies zu vermeiden, muss die benutzerdefinierte App so geschrieben werden, dass sie immer eine Logik enthält, um den Radarwert aufzunehmen. Wenn die Plattform für Openmix (in der Benutzeroberfläche) deaktiviert ist, wird keine Radarbewertung mehr generiert, und daher wird sie automatisch von der App ignoriert.

Dies kann als betrieblicher Ein-/Ausschalter verwendet werden, wenn ein Problem mit einer

bestimmten Plattform vorliegt und der Kunde diese während dieses Problems aus allen Apps herausziehen möchte.

Einstellungen für Radarsonden

Für jede Plattform können Radarsonden angegeben werden. Normalerweise ist dies nur notwendig, wenn Sie eine private Plattform für die Radarüberwachung einrichten. Öffentliche Plattformen stellen von der Community gesammelte Daten bereit und können für die meisten Anwendungen verwendet werden.



Es gibt einen Prüfpunkt für jeden erfassten Datentyp, z. B.: HTTPS-Antwortzeit, HTTP-Durchsatz, HTTPS-Kaltstart (für Verfügbarkeit) usw. Die meisten Radar-Setups verfügen über Prüfpunkte für mindestens Kaltstart- und Antwortzeit, wobei in einigen Fällen Durchsatz vorhanden ist.

Jeder Prüfpunkt hat die folgenden Einstellungen:

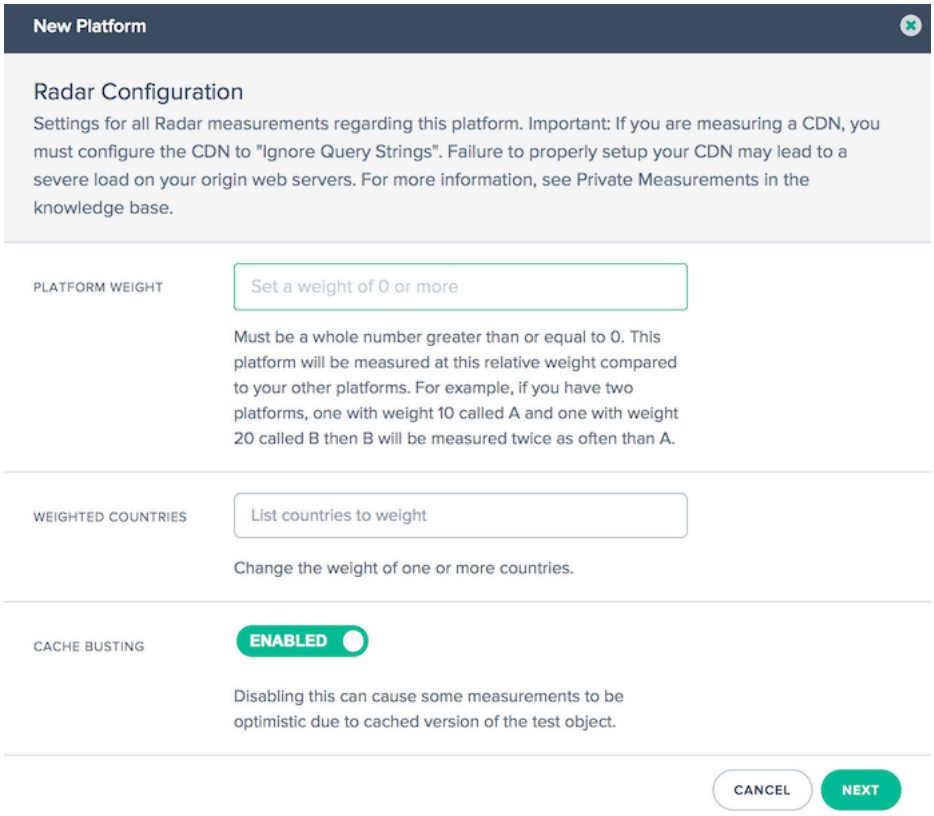
Eingabeelement	Beschreibung
Sondentyp	Der Wert, für den die Daten gemeldet werden sollen. Es gibt separate Prüfpunkte für jedes Protokoll (HTTP/HTTPS) und die Art der zu erfassten Daten (Kaltstart, Round Trip Time, Durchsatz usw.).

Eingabeelement	Beschreibung
URL	Die URL zum Prüfpunktobjekt.
Objekttyp	Der Dateityp, mit dem die Messung durchgeführt wird. In den meisten Fällen möchten Sie das “Timing-Objekt”über den Link im Dialog herunterladen und “Bilddatei”auswählen. Für Prüfpunkte von DSA-Diensten wählen Sie normalerweise “Webseite (dynamisch)”.

Klicken Sie unten links im Dialogfeld auf **Probe hinzufügen**, und fügen Sie Informationen für jeden Prüfpunkt hinzu. Klicken **Sie auf Speichern**, nachdem alle Prüfpunkte eingegeben wurden.

Erweiterte Radareinstellungen

Sie können das Verhalten der Radarprüfungen für die Plattform steuern. Diese sollten nur geändert werden, wenn Sie die Auswirkungen auf Ihre Openmix-Anwendung verstehen.



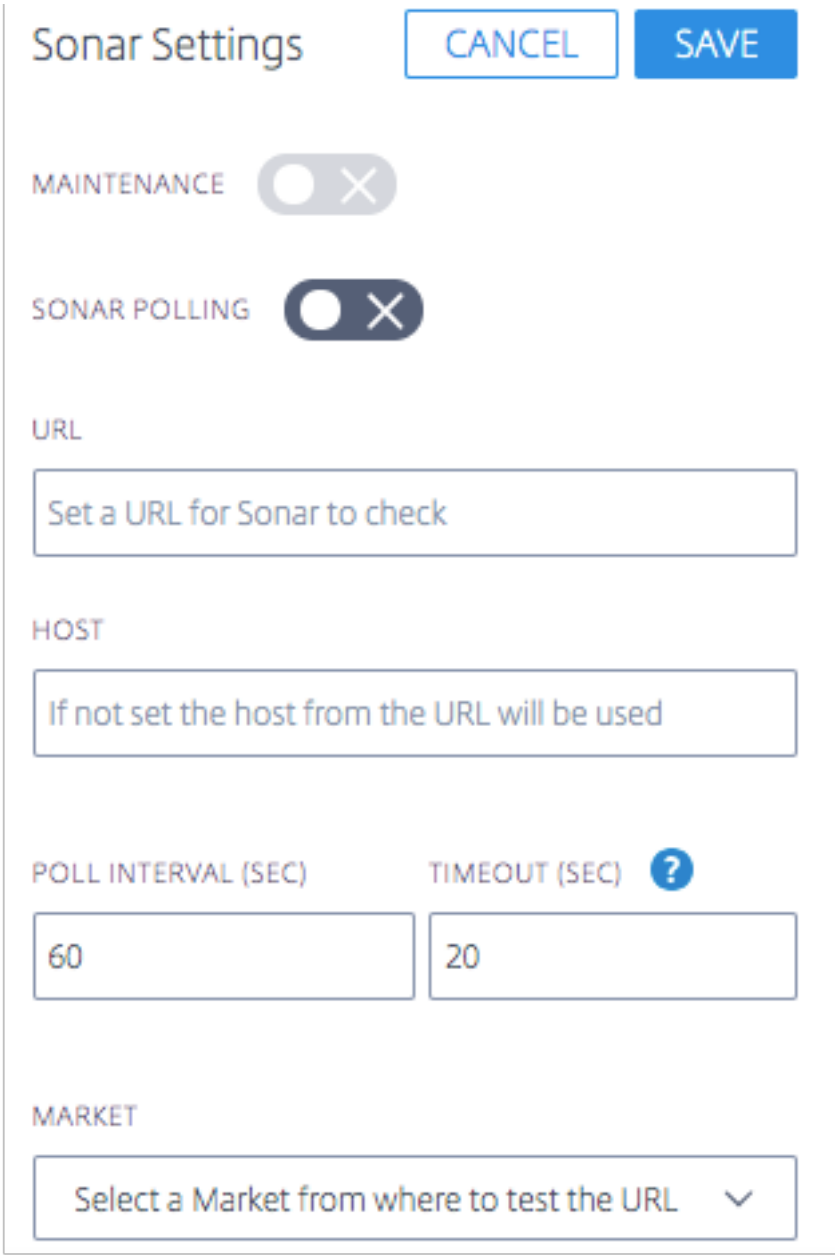
Folgende Optionen stehen zur Verfügung:

Eingabeelement	Beschreibung	Standard
Plattformgewicht	Radar verwendet ein Gewichtungssystem, um Kunden dabei zu helfen, ihre benutzerdefinierten Tests zu priorisieren, je höher die Zahl die höhere Priorität dieses privaten Tests. In der Regel wird dies verwendet, wenn Sie mehrere benutzerdefinierte Tests haben, wenn Sie nur einen als Standard konfigurieren.	10, keine Gewichtung
Gewichtete Länder	Sie können das Plattformgewicht für bestimmte Länder überschreiben, indem Sie die gewünschten Länder eingeben. Das Land wird mit den ISO-Ländercodes angegeben.	0, keine Gewichtung
Ländergewicht	Wenn gewichtete Länder angegeben werden, wird dieses Gewicht auf die Länder angewendet und überschreibt das Plattformgewicht. Wenn das Gewicht auf Null gesetzt ist, wird die Plattform in den angegebenen Ländern nicht gemessen.	
Cache-Busting	Das Deaktivieren dieser Einstellung kann dazu führen, dass einige der Messungen optimistisch sind, da zwischengespeicherte Versionen des Testobjekts gemeldet werden.	Aktiviert

Sonar-Einstellungen

Sonar ist ein Liveness Check Service, der verwendet werden kann, um webbasierte Dienste auf Verfügbarkeit zu überwachen. Sonar funktioniert, indem HTTP- oder HTTPS-Anfragen von mehreren Points of Presence auf der ganzen Welt zu einer URL, die Sie angeben.

Sonar ist in der Plattformkonfiguration aktiviert. Weitere Informationen finden Sie im Sonar Benutzerhandbuch.



Plattform Geo

Die Plattform **Geo** ist ein Standort (Breiten- und Längengrad), der einer Plattform zugewiesen ist. Geo-Informationen ermöglichen es Ihnen, Plattformen im **Visualizer-Tool** genau auf der Karte zu platzieren.

Hinweis: Der **Geo**gilt nur für Plattformen mit einem physischen Standort wie Rechenzentren oder Cloud-Regionen.

Für private Plattformen

Standardmäßig ist privaten Plattformen kein **Geo-Standort** zugewiesen. Wenn ein Benutzer eine private Plattform erstellt und einen **Radar-Prüfpunkt** konfiguriert, verwenden wir den Prüfpunkt, um ihn zu lokalisieren. Dies bedeutet, dass, wenn Sie eine URL zu den **Radareinstellungen** hinzufügen, wir Geolokalisieren die IP, die wir zurückbekommen, und weisen diese als **Geo** für die private Plattform zu. Sie können diesen **Geo** bei Bedarf bearbeiten. Alternativ können Sie Ihrer Plattform einen **Geo** manuell zuweisen, ohne sich auf den Radar-URL-Pfad zu verlassen.

Sobald der **Geo** eingestellt ist, wird er nicht von selbst zurückgesetzt. Auch wenn Sie die **Radar-URL** ändern, ändert dies nicht den **Geo** der Plattform. Sie müssen den **Geo** manuell bearbeiten, um ihn zu ändern.

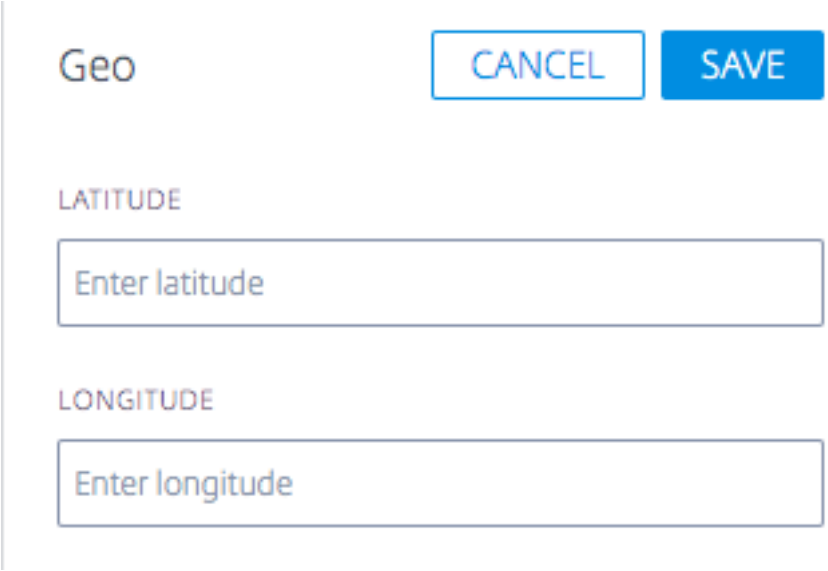
Hinweis: Nicht allen privaten Plattformen wird ein **Geo-Wert**zugewiesen. Geos gelten nur für Plattformen mit einem physischen Standort.

Für importierte Plattformen

Wenn Sie eine Plattform über eine GSLB- oder F5-Konfiguration importieren, suchen wir die öffentliche IP von dieser Konfiguration aus und verwenden diese als **Geo** der Plattform.

Für Community-Plattformen

Wenn ein Kunde seinem Konto eine Community-Plattform hinzufügt, erbt diese Plattform standardmäßig den ursprünglichen Geo der **Community-Plattform**. Der Geo dieser Plattform kann jedoch vom Kunden bearbeitet werden. Normalerweise muss ein Kunde es nicht bearbeiten. Wenn ein Kunde diesen **Geo** jedoch bearbeiten möchte und einen neuen Breiten- und Längengrad eingibt, würde die Einstellung des Kunden (für die Community-Plattform) das ursprüngliche **Geo** der **Community-Plattform** außer Kraft setzen.



Openmix

September 14, 2023

Übersicht

NetScaler Intelligent Traffic Management (ITM) Openmix bietet einen revolutionären Ansatz für Global Traffic Management/Global Server Load Balancing (GTM/GSLB). Für das herkömmliche globale Verkehrsmanagement bietet ITM einen DNS-basierten Ansatz für den Lastausgleich. ITM verwendet DNS CNAME oder Datensätze, in denen DNS-Antworten basierend auf der erforderlichen Geschäftslogik in Echtzeit geändert werden. Openmix kann auf verschiedene Arten in den Video-Workflow und die Bereitstellung integriert werden.

GTM- oder GSLB-Tools und -Dienste basieren auf proprietären, nicht erweiterbaren, statischen Regel-Engines, um einen engen Satz fester Richtlinien für Failover, Round-Robin und Geo-Targeting zu definieren und zu steuern. Die Mission von NetScaler ITM besteht darin, Cloud-Strategien der nächsten Generation auf der Grundlage von Echtzeit-Datenfeeds zu ermöglichen. Die Openmix-Plattform bietet ein äußerst robustes Mittel, um Echtzeitdaten aus verschiedenen Quellen aufzunehmen. Es stellt die Metadaten als Umgebungsvariablen zur Verfügung, die bei jeder Anforderung ausgewertet werden können.

Openmix: Hauptvorteile

- Eliminieren Sie Abhängigkeiten von einzelnen Anbietern und stellen Sie 100%ige Verfügbarkeit sicher
- Kontrollieren Sie Preis-/Leistungs-Kompromisse und beseitigen Sie Kopfschmerzen im Zusammenhang mit Multi-Sourcing
- Beseitigen Sie Unsicherheiten veralteter Performance-Tools und entlasten Sie den Datenverkehr selektiv und strategisch
- Anwenden bestimmter Anbieter auf einzelne Märkte

So funktioniert Openmix

Kunden melden sich beim Citrix ITM Portal an, um ihre erste Anwendung bereitzustellen. Eine Bibliothek mit Beispiel-Apps hilft Ihnen bei den ersten Schritten und ein schrittweises Assistenten-Tool, mit dem Sie Anwendungen mit der gängigsten Routing-Logik erstellen können. ITM Openmix-Anwendungen können zwei Protokolle zur Steuerung des Datenverkehrs unterstützen: DNS oder HTTP.

Anwendungsdefinierte Steuerung

Die weltweit verteilte Openmix-Plattform auf Abruf bringt die GTM/GSLB-Entscheidungsfindung nah an Ihre Anwendungszielgruppen heran. Jeder Host kann seine eigene benutzerdefinierte Openmix-Anwendung haben, die aktuelle Metriken und Variablen berücksichtigt, die die beste Optimierung für jede Routing-Anfrage bieten.

Openmix-Skripte sind in JavaScript programmiert, einer Sprache, die für die meisten Webprogrammierer und Netzwerkadministratoren zugänglich ist. Bei diesem skriptbasierten Ansatz kann praktisch jede Geschäftslogik mit minimaler Codierungskomplexität implementiert werden, um sie als Grundlage für wirklich dynamische Verkehrsmanagementrichtlinien zu verwenden. Dank des kollaborativen Charakters unserer Kundengemeinschaft bietet ITM auch “Schnellstart-Apps”an, bei denen es sich um Standardanwendungen handelt, die keinen Code benötigen.

Verwendung von HTTP- oder DNS-Diensten

ITM Openmix ermöglicht eine breite Palette von Optimierungen bei der Inhaltsbereitstellung. Welche Methode Sie verwenden, um Openmix zu aktivieren, hängt weitgehend von den Besonderheiten Ihres Anwendungsfalls ab. Die DNS-Methode ist einfach zu implementieren, für Kunden meist transparent und für eine Vielzahl von Inhalten nutzbar. Die Möglichkeit, den Anbieter zu wechseln, ist jedoch durch die in der DNS-Antwort festgelegte TTL eingeschränkt, und einige Inhalte können nicht mitten im Stream auf einen anderen Anbieter umgestellt werden. HTTP bietet mehr Integrationsflexibilität

und Optimierungsentscheidungen können getroffen werden, wenn es für den Client optimal ist. Diese größere Flexibilität erfordert mehr Arbeit für die Integration mit einem CMS oder Client.

Die folgende Tabelle fasst den Anwendungsfall des Kunden für die DNS- und HTTP-Schnittstellen zusammen.

	Openmix DNS	Openmix Web Services (HTTP)
Typical Use	Webpage Optimization Mobile App Optimization Player or Game Download Initial Video/Game Request Mid-Stream Requests (TTL expiration)	Initial Video Request Initial Game Server Selection Mid-Stream Requests Mid-Play Gaming Client Requests
Radar Tag / SDK & Fusion Data Collection	Cedexis Radar RUM CDN & Cloud Performance Monitoring CDN & Cloud Costs data, 3rd Party Monitoring Metrics: Player, Server or App Health, Synthetic Process Monitoring, etc.	
Client Data Collection	Video Player Performance Metrics	
Cedexis Billing	Per Millions of DNS Queries	Per Millions of HTTP Requests

Openmix: DNS

CNAME-Delegierung Die einfachste Integration für ITM-Kunden ist die Verwendung der DNS-CNAME-Delegierung. Die CNAME-Delegierung funktioniert, indem der Kunde seinen Endbenutzer-Hostnamen (im folgenden Beispiel `www.acme.com`) auf einen ITM-Hostnamen zeigt

```
www.acme.com  600  IN  CNAME  2-02-123d-000d.cdx.cedexis.net.
<!--NeedCopy-->
```

Beim Empfang einer DNS-Anfrage von einem Endbenutzer trifft das ITM-System eine Entscheidung in Echtzeit. Die Entscheidung basiert auf den Radar-Daten, der Geschäftslogik in der Anwendung und allen Informationen Dritter. Diese Entscheidung wird entweder als ein anderer CNAME-Eintrag (in unserem Beispiel unten acme.cdn1.net) oder als A-Datensatz wie 111.222.111.222 artikuliert.

Durch die Bereitstellung eines CNAME-Eintrags “verweist”ITM den Endbenutzer auf das CDN, die Cloud oder das Rechenzentrum seiner Wahl. Leitet den Endbenutzer an, diesen Anbieter im Vergleich zu einem anderen zu verwenden

```
2-02-123d-000d.cdx.cedexis.net.  19  IN  CNAME acme.cdn1.net.
<!--NeedCopy-->
```


Sobald das CDN oder der Cloud-CNAME bereitgestellt wurde, setzt der Computer des Endbenutzers die Auflösungskette fort. Es fordert einen CDN-Namensserver an, bis eine IP-Adresse des Knotens oder Servers empfangen wird. Wo beginnt der Prozess des Herunterladens von Inhalten.
Wenn ein Datensatz als Teil der Logik bereitgestellt wird, erhält der Computer des Endbenutzers die IP-Adresse. Es verbindet sich direkt mit dem Server und initiiert den Download von Inhalten.

```
acme.cdn1.net.  132  IN  A  111.222.222.111
<!--NeedCopy-->
```

Zonendelegierung Darüber hinaus ist autoritative DNS-Zonendelegierung eine Option zur Implementierung von Openmix. Der Kunde erstellt eine DNS-Zone und delegiert sie an eine im ITM-Portal erstellte Predictive DNS-Zone. Erstellen Sie einen Hostnamen in der delegierten Zone. Konfigurieren Sie es für die Verwendung einer Openmix-Anwendung oder eines dynamischen Predictive DNS-Eintrags zum Generieren einer Antwort.
Der Vorteil dieser Option besteht darin, dass es keine CNAME-Delegation zwischen dem Hostnamen und der dynamischen Antwort der ITM-Plattform geben muss. Im vorherigen Beispiel wird `www.acme.com`, der Hostname, direkt in den konfigurierten Wert für das optimale CDN, Cloud oder Data Center aufgelöst.

```
www.acme.com. 19 IN CNAME acme.cdn1.net.
```

A/AAAA-Datensätze können auch anstelle von CNAMEs verwendet werden, und der Hostname wird direkt in den Datensatz des optimalen Ziels aufgelöst.

```
www.acme.com. 19 IN A 111.222.222.111
```

DNS und Time To Live Implikationen Faktoren wie Time To Live (TTL) -Werte werden sorgfältig berücksichtigt, wobei eine angemessene Zeit für den Inhalt festgelegt wird und wie die Entscheidungsfindung für Benutzer sein muss. In den meisten Fällen empfiehlt ITM eine 20-Sekunden-TTL für Seiten- und Objektinhalte. Bei Videoinhalten arbeitet der ITM-Berater mit dem Kunden zusammen, um basierend auf der Chunk-Länge und der Integrationsmethode die am besten geeignete Balance zu finden.

Openmix: HTTP

Eine Alternative zu DNS ist die Verwendung der HTTP-API. Openmix verwendet HTTP-Anfragen, um einen Kunden wie einen Videoplayer oder ein CMS zu informieren, auf welcher Plattform er zu einem bestimmten Zeitpunkt verwendet werden soll.

```
http://hopx.cedexis.com/zones/1/customers/0/apps/1/decision
< HTTP/1.1 200 OK
< Content-Type: application/json
```



```
4  < Date: Mon, 22 Apr 2015 20:25:24 GMT
5  < Connection: keep-alive
6  < Content-Length: 177
7  <
8  {
9
10   "providers" : [
11     {
12
13     "provider" : "cdn2",
14     "host" : "foo.cdn2.net"
15      }
16  ,
17     {
18
19     "provider" : "cdn1",
20     "host" : "acme.cdn1.net"
21      }
22
23   ]
24  }
25
26 <!--NeedCopy-->
```

Der HTTP-Openmix-Dienst verwendet dieselbe Anwendungslogik wie sein DNS-basiertes Gegenstück. Es enthält auch einige zusätzliche Erweiterungen, die eine weitere Profilerstellung eines Client-Computers ermöglichen. Mit HTTP Openmix ist es beispielsweise möglich, die Header für User-Agent String, X-Forwarded-For und Referer zu betrachten. Stellen Sie IP-Außerkraftsetzungen mithilfe von Abfrage

Da die Nutzlast für HTTP Openmix erweiterbarer ist als DNS, ist es auch möglich, die CDN-, Cloud- oder Serverentscheidungsauswahl auf unterschiedliche Weise bereitzustellen. Die bisher gebräuchlichste war eine geordnete Liste von der am meisten bevorzugten Plattform zur wenigsten (wie oben). Eine vollständige Liste ermöglicht die Bereitstellung des Entscheidungsrangs an das CMS oder den Kunden, ermöglicht jedoch weiterhin die Verwendung interner Heuristiken bei der Auswahl des Anbieters.

CMS-Integration

Einige Kunden ziehen es vor, die Anbieterauswahl serverseitig zu handhaben, anstatt die Anbieterauswahl in jedem Client zu implementieren. Die HTTP-API kann verwendet werden, um eine Optimierungsentscheidung von Openmix zur Anforderungszeit vom Client abzurufen. Es kann verwendet werden, um eine Datei zu füllen, die vom CMS an den Client zurückgegeben wird.

Standardmäßig verwenden Openmix-HTTP-Endpunkte die IP des Aufrufers für Geolokalisierung und Entscheidungskriterien. Wenn Sie von einem CMS oder einem anderen System aus anrufen, das sich zwischen dem Endbenutzer-Client und Openmix befindet, können Sie IP als Parameter angeben, der

bei der Entscheidung verwendet werden soll.

```
http://hopx.cedexis.com/zones/1/customers/0/apps/1/decision?ip=1.2.3.4
< HTTP/1.1 200 OK
< Content-Type: application/json
< Date: Mon, 22 Apr 2015 20:25:24 GMT
< Connection: keep-alive
< Content-Length: 177
<
{

  "providers" : [
    {

    "provider" : "cd1",
    "host" : "acme.cdn1.net"
     }
 ,
    {

    "provider" : "cdn2",
    "host" : "foo.cdn2.net"
     }

  ]
 }

<!--NeedCopy-->
```

Mit dieser Methode können Sie eine CMS-Integration verwenden, um Entscheidungen aus Openmix abzurufen. Sie können auch die Vorteile der Geo- und ISP-Routenoptimierung für den Endbenutzer nutzen. Der von Openmix zurückgegebene Hostname wird dann in die Antwort gepackt, z. B. eine Video-Manifestdatei, und vom CMS an den Client zurückgegeben. Der Kunde verwendet die optimierte Entscheidung, ohne dass Änderungen erforderlich sind, um die Openmix-Optimierung zu unterstützen.

Openmix-Anwendungen

Openmix Quickstart-Anwendungen sind Load-Balancing- und Traffic-Management-Anwendungen. Diese Anwendungen bieten Datenverkehrsrouting in Echtzeit an den besten Anbieter basierend auf einer Reihe von Regeln.

Die Anwendungen werden für jede Anfrage an Openmix verarbeitet und eine Routing-Entscheidung wird basierend auf der angegebenen Logik getroffen. Ein Kunde kann eine Anwendung für Inhalte haben, die einen hohen Geschäftswert haben, und eine andere Anwendung für Inhalte mit geringerem Wert. Diese Anfragen werden separat weitergeleitet.

Wenn Sie eine Anwendung aufrufen, wird eine einzelne Anforderung an einen der Load-Balancer von

Citrix gesendet. Bei DNS handelt es sich um eine einzelne DNS-Anfrage an die DNS-Load-Balancer. Bei HTTP handelt es sich um eine GET- oder HEAD-Anfrage an den Openmix HTTP-Endpunkt.

Die folgenden Apps sind derzeit über das NetScaler Intelligent Traffic Management Portal verfügbar.

- Statisches Routing
- Failover
- Runde Robin
- Optimale Hin- und Rückflugzeit (ORTT)
- Durchsatz
- Statische Nähe

Openmix Custom JavaScript-Anwendungen werden von speziellen Openmix-Servern verwendet, um auf DNS- oder HTTP-Anfragen basierend auf der Logik in den Skripten zu antworten. Die Bereitstellung der Skripte erfolgt über das Kundenportal, in dem die App konfiguriert und veröffentlicht wird. Weitere Informationen zur Möglichkeit, eigene JavaScript-Skripts zu erstellen, finden Sie in den Informationen in unserer Developer Exchange.

Bevor Sie mit der Einrichtung der Apps fortfahren, ist es wichtig, die folgenden Konzepte zu verstehen:

Schwellenwert für Verfügbarkeit

Der Verfügbarkeitsgrenzwert ist der Mindestverfügbarkeitswert, den eine Plattform erfüllen muss, um für das Routing berücksichtigt zu werden. Der standardmäßige Mindestverfügbarkeitsschwellenwert für alle Anwendungen liegt bei 80%. Sie können diesen Prozentsatz jedoch ändern und auf einen Wert festlegen, der für Ihren Standort, die Netzwerkverfügbarkeit und die Zuverlässigkeit angemessen ist.

Hinweis: Wenn keine Plattform diesen Mindestverfügbarkeitsschwellenwert erreicht (der Standardwert ist 80% oder der von Ihnen festgelegte Wert), wird für Round-Robin-, ORTT- und Durchsatzanwendungen ein zufälliges Routing durchgeführt.

Fallback

Die Fallback-Antwort wird zurückgegeben, wenn die Openmix-Anwendung aus irgendeinem Grund nicht erfolgreich ausgeführt wird. Oder wenn Sonar bestätigt, dass keine verfügbaren Plattformen verfügbar sind. Daher muss ein gültiger Fallback-CNAME/A/AAAA-Record oder eine gültige IP (oder ein Pfad in HTTP) angegeben werden, mit dem Openmix antworten kann. Diese Fallback-URL oder CNAME-Eintrag kann für eine Plattform verwendet werden, die in Openmix vorkonfiguriert ist.
Fallback tritt manchmal auch in den folgenden Szenarien auf:

- Wenn Sie zwischen Versionen Ihrer Anwendung wechseln, laden Sie ein neues Skript hoch und veröffentlichen es. Es gibt einen kurzen Fallbackzeitraum von Millisekunden, bis das neue Skript initialisiert und das alte entfernt wird.
- Sollte es jemals zu einer Überlastung kommen (was selten vorkommt), reagiert Openmix mit dem Fallback CNAME/A/AAAA, da der Fallback die Last des Dienstes ausgleicht.

Für den Fallback müssen Sie einen gültigen Hostnamen (CNAME/A/AAAA-Eintrag) oder eine IP-Adresse in DNS und einen gültigen URI (er kann das Format `scheme:[//host[:port]][/path][?query][#fragment])` in HTTP haben) eingeben.

TTL

In Openmix teilt die DNS Time to Live (TTL) für die Anwendung Resolvern mit, wie lange sie die Entscheidung behalten müssen, bevor sie Openmix erneut fragen.
Die TTL wird verwendet, um das Verkehrsaufkommen zu kontrollieren, das eine Openmix-App erhält. Es steuert auch, wie empfindlich eine App auf Änderungen der Daten reagieren muss, auf die sie reagiert.
Die Standard-TTL ist 20 Sekunden. Sie können diesen Wert zwar ändern, es wird jedoch nicht empfohlen, dies zu tun. Wenn Sie die TTL senken, erhalten Sie mehr Volumen und mehr Echtzeit-DNS-Abfragen. Dies kann zu zusätzlichen Kosten und geringerer Leistung führen, da DNS-Abfragen auf dem Client Zeit in Anspruch nehmen. Daher ist es am besten, den Standardwert von TTL nicht zu ändern.

> **Hinweis:** Die Zeit bis zum Leben gilt für Schnellstart-Apps, benutzerdefinierte JS-Apps, wenn im Code keine TTL angegeben ist, und für alle Fallback-Antworten

Gewichte (für Round Robin verwendet)

Sie können Gewichtungen für die Priorisierung und Auswahl jeder Plattform global und/oder nach Markt oder Land zuweisen.

Angenommen, Sie haben drei Plattformen für Ihre Anwendung ausgewählt - P1, P2 und P3. Sie geben ihnen die Gewichte: 60, 50 und 10. Die Round-Robin-App wandelt diese Werte in Prozentsätze wie P1= 50%, P2= 42% und P3= 8% um, was 100% ergibt. Diese Prozentsätze bedeuten, dass Benutzer in 50% der Fälle über P1, in 42% der Fälle durch P2 und in 8% der Fälle durch P3 geleitet werden.

Die Gewichte, die Sie den Plattformen geben, müssen sich nicht auf 100 summieren. Sie können eine beliebige ganze Zahl zwischen 0 und 1.000.000 sein. Die Gewichte, die den Plattformen bei der Umrechnung in Prozentsatz (von der App im Backend) gegeben werden, summieren sich auf 100%. Wenn alle ausgewählten Plattformen das gleiche Gewicht erhalten, wird der Verkehr im Laufe der Zeit gleichmäßig auf sie verteilt. Wenn Sie eine Plattform haben, wird diese Plattform zu 100% genutzt, unabhängig vom Gewicht, das Sie ihr geben.

Gewichte werden nur für Plattformen verwendet, die gemäß Radar- und Sonar-Verfügbarkeitsprüfungen als verfügbar gelten, abhängig von der Konfiguration der Anwendung. Nicht verfügbare Plattformen führen dazu, dass die Verteilung nicht den konfigurierten Gewichtungen entspricht. Wenn P1 beispielsweise 100 und P2 0 wiegt, P1 jedoch die Radarverfügbarkeitsprüfung nicht besteht, wird der gesamte Verkehr an P2 weitergeleitet.

Handicap (wird für ORTT und Durchsatz verwendet)

Das **Handicap** ist ein Prozentwert, der auf eine Plattform angewendet werden kann, um die Radarwerte für RTT und Durchsatz zu ändern, dh die Reaktionszeit (in Millisekunden) künstlich zu erhöhen oder den Durchsatz (in kbps) zu verringern. Durch Erhöhen oder Verringern dieser Werte wird die Leistung der Plattform beeinträchtigt, sodass die Wahrscheinlichkeit, dass sie ausgewählt wird, gering wird. Handicaps können auf Plattformen weltweit oder separat für bestimmte Märkte oder Länder hinzugefügt werden.
In Fällen, in denen eine Plattform in einem bestimmten Markt oder Land teuer ist und Sie die Wahrscheinlichkeit verringern möchten, ausgewählt zu werden, wenn ein gleichwertiger Anbieter in Bezug auf die Leistung nahe beieinander liegt. Sie setzen einen Handicap-Wert als Multiplikator ein, um den Wert der Reaktionszeit zu erhöhen oder den Wert des Durchsatzes zu verringern. Infolgedessen verringert es die Wahrscheinlichkeit, dass eine Plattform ausgewählt wird.

Im Folgenden wird grob beschrieben, wie **Handicap** im Backend funktioniert:

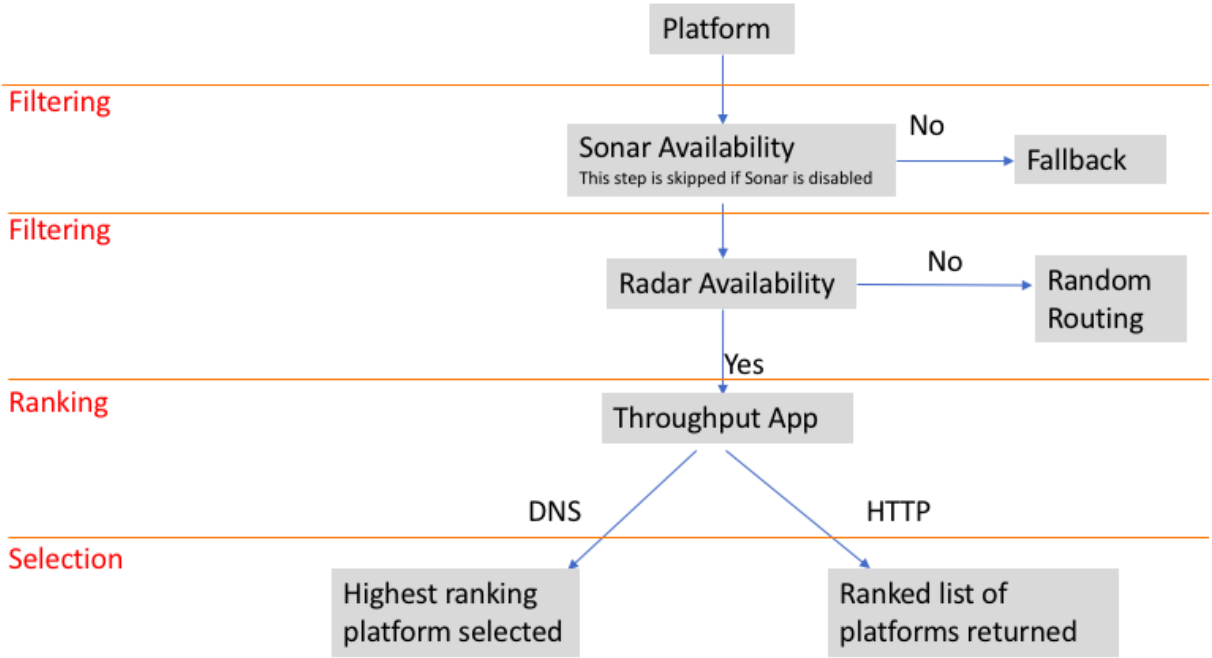
- Plattform-RTT mit angewendetem Handicap = RTT (Roundtrip Time in Millisekunden) * (1+ Handicap) oder
- Plattformdurchsatz mit angewendetem Handicap = (Durchsatz in kbps) * (1 —Handicap)

Hinweis: Die RTT- und Durchsatzwerte für die Plattform sind Werte aus Radardaten.
Die folgende Tabelle zeigt, wie sich Handicap auf die beiden Plattformen P1 und P2 auswirkt. Und wie das Handicap die Wahrscheinlichkeit verringert, dass P1 ausgewählt wird.

	P1	P2
RTT ohne Handicap	50 Millisekunden	60 Millisekunden
RTT mit 50% (0,5) Handicap für P1 und 0% (0) für P2	50 (1+0,5) = 75 Millisekunden	60 (1+0) = 60 Millisekunden
Durchsatz ohne Handicap	3000 kBit/s	2800 kbps
Durchsatz mit 50% (0,5) Handicap für P1 und 0% (0) für P2	3000 (1-0,5) = 1500 kbps	2800 (1- 0) = 2800 kbps

Arbeitsablauf für Filter, Rangfolge und Auswahl

Beispielflussdiagramm für die Durchsatz-App



Auswahlkriterien für Plattformen

Openmix Quickstart-Apps verwenden die folgenden Kriterien als Filter der 1., 2. und 3. Ebene, um die beste Plattform zu bewerten und auszuwählen.

Filtrationsgrad	Auswahlkriterium	CRTT	Durchsatz	Runde Robin	Failover	Statisches Routing	Statische Nähe
1. Ebene	Sonar-Verfügbarkeitsprüfung (falls aktiviert)	X	X	X	X	X	X
1. Ebene	Radar-Verfügbarkeitsprüfung (falls aktiviert)	X	X	X	X	X	Nicht verfügbar
1. Ebene	Gewichte (benutzerdefiniert)	Nicht verfügbar	Nicht verfügbar	X	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar

Filtrationsgrad	Auswahlkriterium	OPTT	Durchsatz	Runde Robin	Failover	Statisches Routing	Statische Nähe
1. Ebene	Umlaufzeit (in Millisekunden)	X	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
1. Ebene	Durchsatz (in kbit/s)	Nicht verfügbar	X	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar

Ursachencode-

Ursachencodes geben Aufschluss darüber, warum die Entscheidung getroffen wurde, und erfahren auch, welcher Teil des Codes der App ausgeführt wird. Während der Ausführung kann eine App dem Feld für den Ursachencode jederzeit etwas hinzufügen.
Ursachencodes bedeuten für jede Schnellstart-App unterschiedliche Dinge. Es gibt einige Gemeinsamkeiten zwischen den Ursachencodes für jede App, die jedoch nicht umfassend ist.

Hinweis: Damit Ursachencodes korrekt angezeigt werden, dürfen sie die maximale Zeichenbegrenzung von 200 Zeichen nicht überschreiten. Wenn dieser Grenzwert überschritten wird, wird der Ursachencode als **Unbekannt**angezeigt. Wenn der Benutzer keinen Ursachencode hinzugefügt hat, wird **Unbekannt**angezeigt.

Im Folgenden sind die Ursachencodes für Schnellstart-Apps aufgeführt:

Ursachencode	Beschreibung	Optimaler RTT	Runde Robin	Statisches Routing	Durchsatz	Statische Nähe	Failover
Optimaler Nutzen	Der Anbieter mit der besten Leistung ist verfügbar und wurde ausgewählt.	X	–	–	X	–	X

Ursachencode	Beschreibung	Optimaler RTT	Runde Robin	Statisches Routing	Durchsatz	Statische Nähe	Failover
Optimales nicht verfügbares Radar	Der Anbieter mit der besten Leistung ist nicht verfügbar; ein anderer berechtigter Anbieter wurde ausgewählt, der laut Radar verfügbar ist	X	–	–	X	–	X
Optimales nicht verfügbares Radar+Sonar	Der Anbieter mit der besten Leistung ist aufgrund von Radar und/oder Sonar nicht verfügbar.	X	–	–	X	–	X

Ursachencode	Beschreibung	Optimaler RTT	Runde Robin	Statisches Routing	Durchsatz	Statische Nähe	Failover
All Unavail-Radar	Alle in Frage kommenden Plattformen sind laut Radar nicht verfügbar. Anfrage an Fallback weitergeleitet	X	X	–	X	–	X
All Unavail-Sonar	Alle geeigneten Plattformen sind laut Sonar nicht verfügbar. Anfrage wurde an Fallback weitergeleitet.	X	X	–	X	–	X

Ursachencode	Beschreibung	Optimaler RTT	Runde Robin	Statisches Routing	Durchsatz	Statische Nähe	Failover
Datenproblem	Bezeichnet fehlende Radarmessungen für eine oder mehrere Plattformen. Die Plattform wird als Ergebnis zufällig ausgewählt	X	X	–	X	–	X
Geo-Standard	Die standardmäßigen Geo-Einstellungen sind in Kraft	X	X	–	X	X	X
Geo Override-Land	Für diese Entscheidung ist eine Länderüberschreibung in Kraft	X	X	–	X	X	X

Ursachencode	Beschreibung	Optimaler RTT	Runde Robin	Statisches Routing	Durchsatz	Statische Nähe	Failover
Geo Override-Markt	Für diese Entscheidung ist eine Marktüberschreibung in Kraft.	X	X	–	X	X	X
Alles verfügbar	Alle geeigneten Plattformen sind über Sonar und Radar verfügbar	X	X	–	X	–	–
Proximal Avail	Die geografisch nächstgelegene Plattform ist verfügbar und wurde ausgewählt	X	–	–	–	X	–

Ursachencode	Beschreibung	Optimaler RTT	Runde Robin	Statisches Routing	Durchsatz	Statische Nähe	Failover
Berechtigtes Unavail-Radar	Für Round Robin ist der berechtigte Anbieter laut Radar nicht verfügbar	–	X	–	–	–	–
Persistente App	Die Entscheidung diente einer zwischengespeicherten Antwort, es wurde keine Logik ausgeführt	X	X	X	X	X	X
Anfrage Geo nicht verfügbar	Das Geo der Anfrage kann nicht ermittelt werden. Anfrage an Fallback weitergeleitet	X	–	–	–	X	–

Ursachencode	Beschreibung	Optimaler RTT	Runde Robin	Statisches Routing	Durchsatz	Statische Nähe	Failover
Alle nicht verfügbaren Anbieter	Alle Anbieter sind nicht verfügbar. Anfrage an Fallback weitergeleitet	X	–	–	–	X	–
Nicht verfügbarer Provider-Dist	Für keinen Anbieter wurden Proximity Scores gefunden. Anfrage an Fallback weitergeleitet	X	–	–	–	X	–

Openmix Quickstart-Anwendungen

1. Melden Sie sich beim NetScaler Intelligent Traffic Management Portal an.
2. Navigieren Sie im linken Navigationsmenü zu **Openmix > Anwendungskonfiguration**.
3. Wenn Sie Ihre Openmix-App zum ersten Mal konfigurieren, wird die Seite **Erste Schritte** angezeigt, wenn Sie auf **Openmix > Anwendungskonfiguration**klicken.
4. Um eine neue App zu konfigurieren, klicken Sie entweder auf die Schaltfläche **Erste Schritte** oder auf die Schaltfläche **Hinzufügen** in der oberen rechten Ecke der Seite. Wenn Openmix-Apps zuvor konfiguriert wurden, wird auf dieser Seite eine Liste der Apps angezeigt.

Die folgenden Abschnitte führen Sie durch den Prozess der Konfiguration von Openmix-Apps im Portal.

Statisches Routing

Diese Art von Anwendung verwendet keine Auswertungslogik, um zu entscheiden, welche DNS-Antwort dem Endbenutzer bereitgestellt werden muss. Die App wählt hier immer eine einzige Plattform aus, die vom Benutzer angegeben wird. Daher verwendet die App nur eine einzige DNS-CNAME- oder IP-Adressantwort. Die Anwendung Static Routing kann über das Portal auf der Seite **Anwendungskonfiguration** konfiguriert werden.

Hinweis: Bevor Sie Ihre Anwendung konfigurieren, stellen Sie sicher, dass Ihre Plattformen zuerst konfiguriert sind. Informationen zur Plattformkonfiguration finden Sie auf der Seite Plattformen .

Navigation

1. Navigieren Sie zu **Openmix > Anwendungskonfiguration**.
2. Klicken Sie oben rechts auf die Schaltfläche **Hinzufügen**

Das Dialogfenster **Grundlegende Informationen** wird geöffnet.

Grundlegende Informationen Gehen Sie folgendermaßen vor, um **Basisinformationen** einzugeben:

1. Wählen Sie für **Protokoll** DNS oder HTTP aus der Liste aus.
2. Wählen Sie für **Anwendungstyp** “Statisches Routing”. Oder wenn Sie einen anderen App-Typ konfigurieren, wählen Sie ihn aus der Liste aus.
3. Geben Sie Ihrer Anwendung einen **Namen** (Pflichtfeld), fügen Sie eine **Beschreibung** (optionales Feld) und ein **Tag** (optionales Feld) hinzu.
4. Klicken Sie für **Konfiguration** auf **Weiter**.

Konfiguration Gehen Sie wie folgt vor, um die App zu konfigurieren:

1. Wählen Sie die zugehörige Plattform aus der Liste **Plattform** aus. Es ist die Plattform, die Sie auf der Seite Plattformen einrichten und die das CDN, die Cloud oder das Rechenzentrum darstellt.
2. Geben Sie einen **CNAME/A/AAAA-Eintrag** (für DNS) oder eine **URL** (für HTTP) ein. Der DNS-CNAME oder die HTTP-URL für die ausgewählte Plattform muss auf eine gültige IP-Adresse oder einen gültigen Hostnamen verweisen.
3. Wählen Sie für **CORS**in einem HTTP-Protokoll die Option Keine, Alle oder Benutzerdefiniert für CORS aus. Mit CORS können Sie den Zugriff auf Ihre Website von anderen Websites aus steuern. Sie können entweder den Zugriff auf Ihre Website von anderen Websites vollständig einschränken (indem Sie auf **Keine**klicken), den Zugriff von allen anderen Websites zulassen (durch Klicken auf **Alle**) oder den Zugriff nur von bestimmten Websites zulassen (indem Sie auf **Benutzerdefiniert**klicken).

4. Geben Sie eine **TTL** (Time-To-Live) für die Antwort ein. Die Standardeinstellung ist 20 Sekunden, kann aber außer Kraft gesetzt werden.
5. Klicken Sie auf **Vollständig**
6. Klicken Sie im Bestätigungs-Popup auf **Fertig** oder **Veröffentlichen**, um Ihre App auf der Openmix-Anwendungsseite anzuzeigen. Wenn Sie auf **Veröffentlichen**klicken, wird Ihre App sofort live geschaltet und hat einen grünen Status. Dies bedeutet, dass die Anwendung in Produktion ist. Wenn Sie auf **Fertig**klicken, wird Ihre App weiterhin auf der Anwendungsseite aufgeführt, sie ist jedoch nicht veröffentlicht und der Status ist rot.

Failover

Die Failover-Anwendung unterstützt eine einfache Routing-Logik, bei der eine Plattform basierend auf ihrer Position in der Leitung und ihrer Verfügbarkeit ausgewählt wird. Der Kunde kann eine Failoverkette erstellen, die entscheidet, welche Plattform zuerst, zweite usw. ausgewählt werden soll. Diese Failover-Kette kann geschaffen werden, um entweder global oder für einzelne Märkte und Länder zu funktionieren.

Die **Failoveranwendung** kann im Portal auf der Seite **Anwendungskonfiguration** konfiguriert werden.

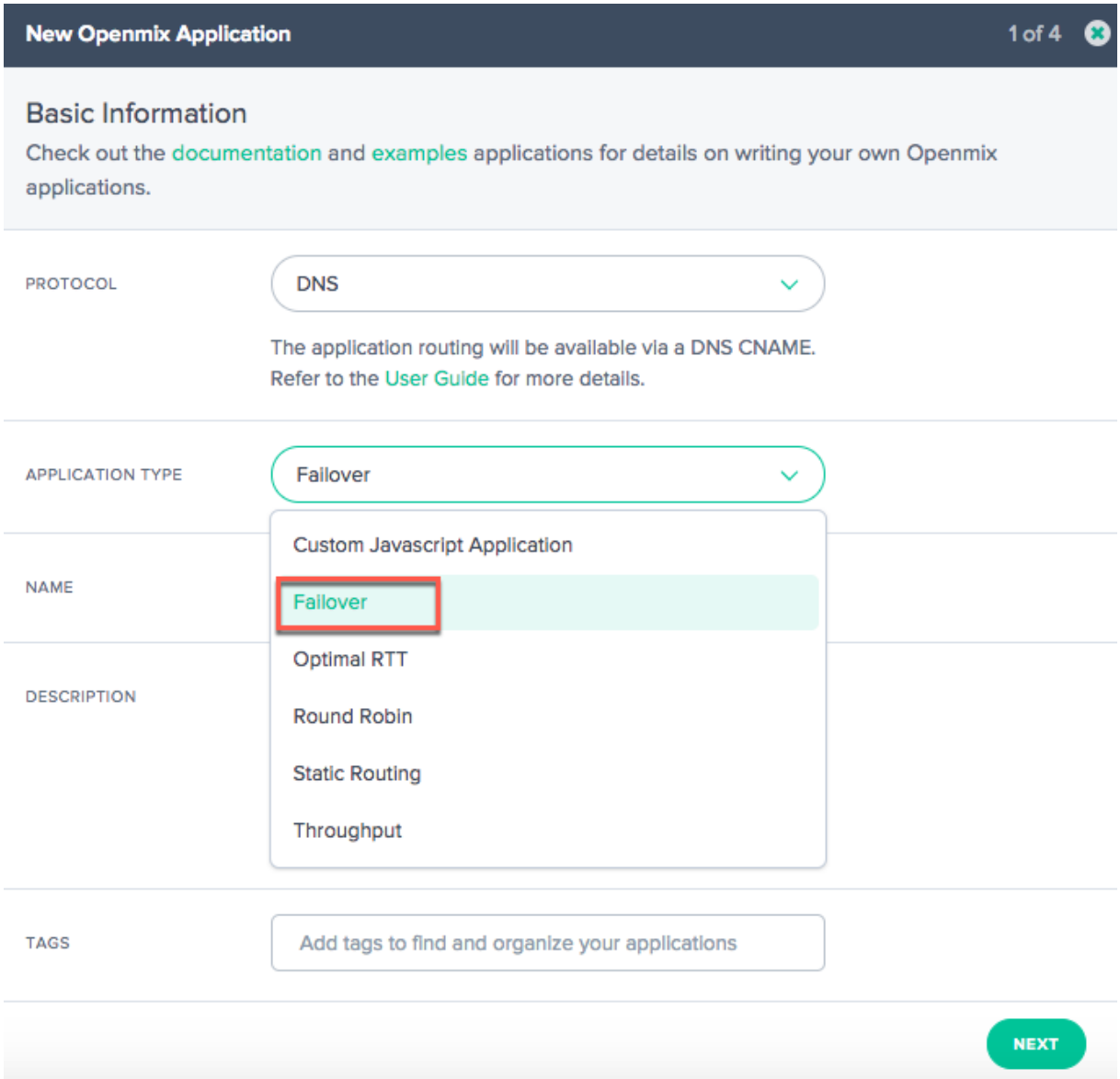
Hinweis: Bevor Sie Ihre Anwendung konfigurieren, stellen Sie sicher, dass Ihre Plattformen zuerst konfiguriert sind. Informationen zur Plattformkonfiguration finden Sie auf der Seite Plattformen .

Navigation

1. Loggen Sie sich im Portal ein.
2. Navigieren Sie im linken Navigationsmenü zu **Openmix > Anwendungskonfiguration**.
3. Klicken Sie oben rechts auf die Schaltfläche Hinzufügen, um zum Dialogfeld Neue Openmix-Anwendung, **Basisinformationen**, zu gelangen.

Grundlegende Informationen

1. Wählen Sie **DNS** aus der **Protokollliste** aus.
2. Wählen Sie in der Liste **Anwendungstyp** die Option **Failover**aus.
3. Geben Sie Ihrer Anwendung einen **Namen** (Pflichtfeld), fügen Sie eine **Beschreibung** (optionales Feld) und ein **Tag** (optionales Feld) hinzu.
4. Klicken Sie anschließend auf **Weiter**.



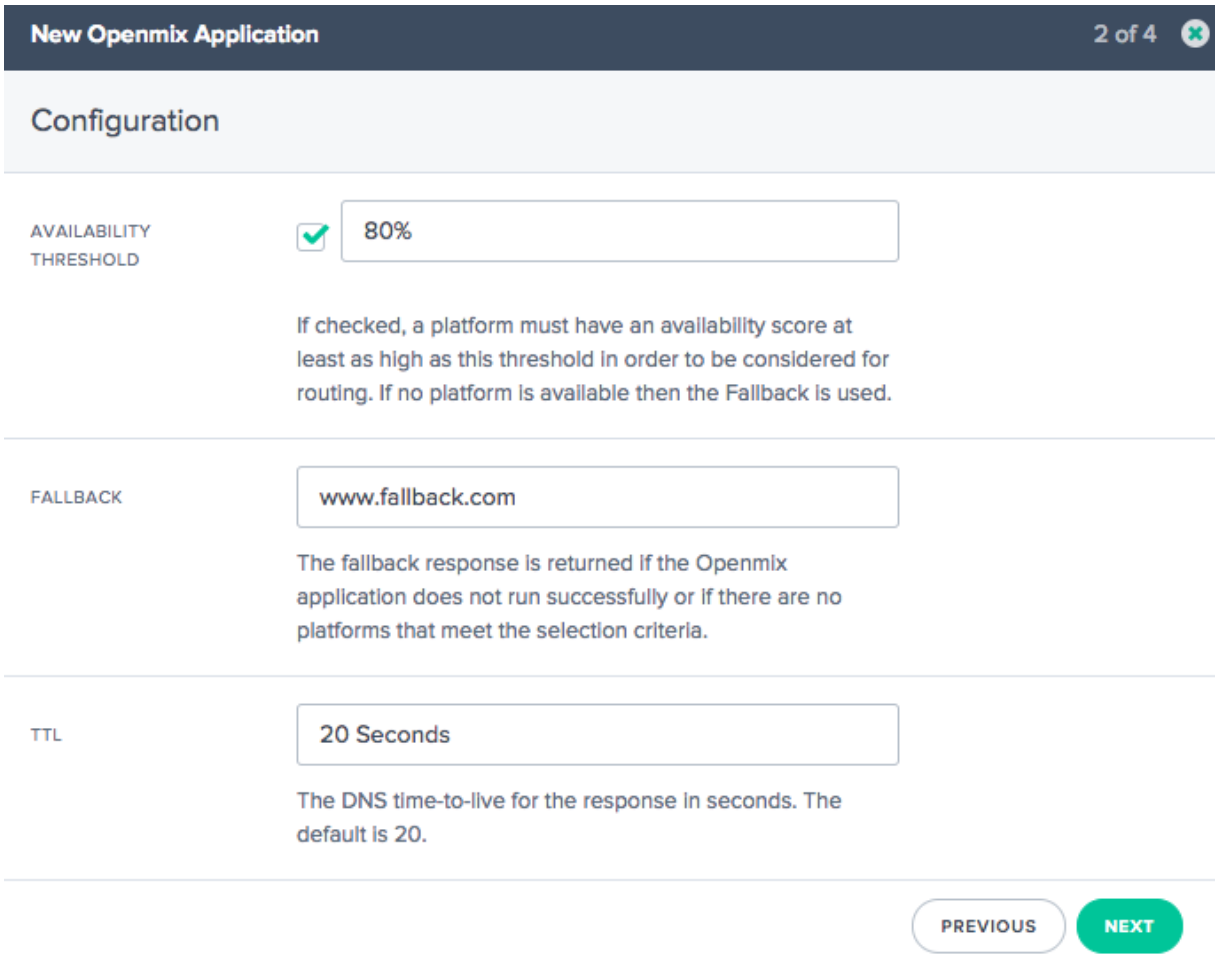
Konfiguration

1. Aktivieren Sie im Dialogfeld Konfiguration das Kontrollkästchen **Verfügbarkeitsschwellenwert** . Der Verfügbarkeitsschwellenwert hat einen Standardwert von 80%. Eine Plattform muss einen Verfügbarkeitswert haben, der mindestens so hoch ist wie dieser Schwellenwert, um für das Routing berücksichtigt zu werden.

    - Wenn Sie den Standardverfügbarkeitsschwellenwert ändern möchten, geben Sie einfach einen neuen Wert ein, um den Standardwert zu ersetzen.
    - Wenn keine Plattform einen Verfügbarkeitswert aufweist, der gleich oder größer als der angegebene Schwellenwert ist, wird die Fallback-CNAME oder A- oder AAAA- oder IP-Adresse verwendet.

- Wenn das Kontrollkästchen nicht aktiviert ist, geht die Plattform von einem Nullverfügbarkeitsschwellenwert aus. Dies bedeutet, dass auf dieser Plattform keine Radar-Verfügbarkeitsprüfung durchgeführt wird.

2. **Geben Sie eine CNAME/A/AAAA- oder IP-Adresse für Fallback ein.** Der Fallback-CNAME/A/AAAA oder IP wird normalerweise verwendet, wenn die Anwendung auf Probleme oder Fehler stößt.
3. Geben Sie eine **TTL** (Time-To-Live) für die Antwort ein. Der Standardwert ist 20 Sekunden. Sie können diesen Wert bei Bedarf überschreiben.



Informationen zur Plattform

1. Wählen Sie im Dialogfeld **Plattforminformationen** eine **Plattform** aus der Liste aus.
   - Mit der Schaltfläche Plattformen **hinzufügen können Sie mehrere Plattformen** auswählen. Die Idee ist, alle verfügbaren Plattformen für globale und geo- (Märkte und Länder) Routing auszuwählen.
   - Die Plattformen in dieser Liste sind diejenigen, die Sie auf der Seite Plattformen innerhalb des Portals eingerichtet haben und die Ihr CDN, Ihre Cloud oder Ihr Rechenzentrum darstellen.

- Für alle Openmix-Apps muss vorher eine zugehörige Plattform eingerichtet werden. Wenn Sie in der Liste keine Plattform finden, können Sie sie auf der Seite Plattformen im Portal einrichten.

2. Geben Sie den **CNAME/A/AAAA-Datensatz** für die Plattform ein.
3. Stellen Sie sicher, dass das Kontrollkästchen **Aktiviert** (das zeigt an, dass die Plattform aktiviert ist) aktiviert ist, bevor Sie zum nächsten Schritt wechseln.
4. Wenn **Sonar** konfiguriert ist und Sie Sonar-Daten verwenden möchten, um den anfänglichen Entscheidungsprozess zu unterstützen, stellen Sie sicher, dass Sie das Kontrollkästchen **Sonar für Plattformverfügbarkeit verwenden** aktivieren. **Hinweis**: Das Kontrollkästchen Sonar wird nur angezeigt, wenn Sonar für diese Plattform aktiviert ist.
5. Klicken Sie auf **Weiter** für die **Standortkonfiguration**.

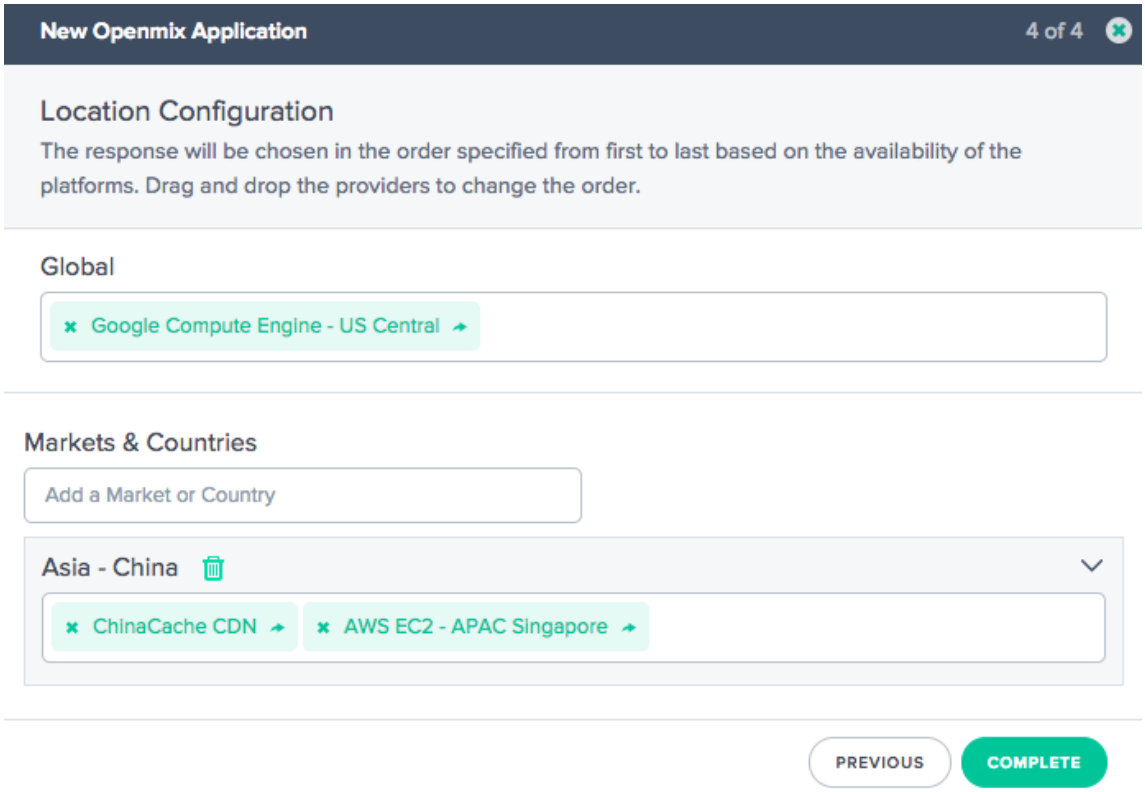
Standort-Konfiguration

1. Wählen Sie im Dialogfeld **Standortkonfiguration** die erforderlichen Plattformen für **globales** Routing aus.

   - **Global** gibt an, dass Sie eine Kette von Plattformen für globales Routing einrichten.
   - Wenn Sie in das Feld **Global** klicken, werden in einer Liste alle Plattformen angezeigt, die Sie im Schritt **Plattforminformationen** ausgewählt haben.
   - Wählen Sie die erforderlichen Plattformen aus der Liste für verfügbarkeitsbasiertes globales Routing aus.
   - Die Reihenfolge, in der Sie die Plattformnamen in dieses Feld eingeben, bestimmt die Priorität für ihre Auswahl. Wenn beispielsweise die erste Plattform auf Ihrer Liste nicht verfügbar ist, wird die zweite ausgewählt. Wenn keine der Plattformen in der Liste verfügbar ist, wird ein Fallback verwendet.
   - Sie können die Plattformnamen ziehen, um ihre Prioritätsreihenfolge zu ändern.

2. Klicken Sie auf **Märkte & Länder**, wenn Sie Plattformen für lokales Geo-Routing einrichten möchten.

   - Wenn Sie in das Feld **Märkte und Länder** klicken, werden in der Liste alle Plattformen angezeigt, die Sie im Schritt **Plattforminformationen** ausgewählt haben.
   - Wählen Sie Plattformen für das lokale Geo-Routing, getrennt für jedes Geo (Markt/Land).
   - Die Reihenfolge, in der Sie die Plattformnamen in dieses Feld eingeben, bestimmt die Priorität für ihre Auswahl. In China möchten Sie beispielsweise zuerst den China POP verwenden, und nur wenn dieser nicht verfügbar ist, möchten Sie, dass Ihr Singapur-POP verwendet wird, den Sie als nächstes in der Reihe platzieren würden usw.
   - Sie können die Plattformnamen ziehen, um ihre Prioritätsreihenfolge zu ändern.



3. Klicken Sie auf **Vollständig**, um die Konfiguration Ihrer App abzuschließen.
4. Klicken Sie im Bestätigungs-Popup auf **Fertig** oder **Veröffentlichen**, um Ihre App auf der **Openmix-Seite** aufgeführt zu sehen.
   - Wenn Sie auf **Veröffentlichen**klicken, wird Ihre App sofort live geschaltet und hat einen grünen Status. Ihre Anwendung ist in Produktion.
   - Wenn Sie auf **Fertig**klicken, wird Ihre App weiterhin auf der Openmix-Seite aufgeführt, sie ist jedoch nicht veröffentlicht und der Status ist rot.

Runde Robin

Diese Anwendung folgt einer typischen Global Server Load-Balancing-Methode von Round Robin, bei der jeder CNAME-Wechsel an Endbenutzer zurückgegeben wird, wenn DNS-Anforderungen gestellt werden. Es verwendet Sonar-Daten (wenn Sonar aktiviert ist) und den Schwellenwert für die **Plattformverfügbarkeit**, um die beste Plattform für den anfragenden Benutzer zu bewerten. Jede Plattform wird basierend auf der Round-Robin-Verteilungsmethode ausgewählt. Wenn beispielsweise die Plattformen P1, P2 und P3 den Verfügbarkeitsschwellenwert erreichen, wird die erste Anforderung an P1, die zweite an P2 und die dritte an P3 weitergeleitet. Die vierte Anforderung wird erneut an P1 weitergeleitet und so weiter.

Um eine neue Round Robin-App zu konfigurieren, klicken Sie auf die Schaltfläche **Hinzufügen** in

der oberen rechten Ecke der Openmix-Seite. Das Dialogfeld **Grundlegende Informationen** wird geöffnet.

Navigation

1. Loggen Sie sich im Portal ein.
2. Navigieren Sie im linken Navigationsmenü zu Openmix > Anwendungskonfiguration.
3. Klicken Sie oben rechts auf die Schaltfläche Hinzufügen, um zum Dialogfeld Neue Openmix-Anwendung, Basisinformationen, zu gelangen.

Grundlegende Informationen

1. Wählen Sie im Dialogfeld Grundinformationen DNS als Protokoll für Round Robin aus.**Hinweis**: Für die Round-Robin-App ist das Routing nur über einen DNS-CNAME verfügbar.
2. Wählen Sie den **Anwendungstyp** aus der Liste aus. Geben Sie der App einen **Namen** (Pflichtfeld), eine **Beschreibung** (optionales Feld) und ein **Tag** (optionales Feld).
3. Klicken Sie für Konfiguration auf **Weiter**.

Konfiguration

1. Der **Verfügbarkeitsschwellenwert** hat einen Standardwert von 80%. Um diesen Wert zu ändern, geben Sie einfach einen neuen Wert ein, um den Standardwert zu ersetzen.
2. Geben Sie einen CNAME/A/AAAA oder eine IP-Adresse für das Fallback ein. Der Fallback-CNAME/A/AAAA oder IP wird normalerweise verwendet, wenn die Anwendung auf Probleme oder Fehler stößt.
3. Geben Sie eine TTL (Time-To-Live) für die Antwort ein. Die Standardeinstellung ist 20 Sekunden, aber dieser Wert kann bei Bedarf außer Kraft gesetzt werden.
4. Klicken Sie auf **Weiter** für Plattforminformationen.

Informationen zur Plattform

1. Wählen Sie eine Plattform aus der **Plattformliste** aus. **Hinweis**: Alle Openmix-Apps benötigen vorher eine zugehörige Plattform. Wenn Sie in der Liste keine Plattform finden, können Sie sie auf der Seite Plattformen im Portal einrichten.
2. Wählen Sie weitere Plattformen aus, indem Sie auf die Schaltfläche **Plattform hinzufügen** klicken.
3. Geben Sie einen CNAME- oder A/AAAA-Record oder eine IP (in DNS) oder eine URL (in HTTP) für diese Plattform ein. Es muss eine gültige URL, Hostname oder IP-Adresse sein. Es kann die Form haben: `scheme:[//host[:port]][/path][?query][#fragment]`.
4. Stellen Sie sicher, dass das Kontrollkästchen **Aktiviert** (das zeigt an, dass die Plattform aktiviert ist) aktiviert ist, bevor Sie zum nächsten Schritt wechseln.

5. Wenn Sonar verfügbar ist und Sie Sonar-Daten als Hilfe bei der anfänglichen Entscheidungsfindung verwenden möchten, müssen Sie das Kontrollkästchen **Sonar für Plattformverfügbarkeit verwenden** aktivieren.
6. Klicken Sie auf **Speichern**, um zu Schritt 4 zu gelangen und für jede Plattform geeignete Gewichte zuzuweisen.

Standort-Konfiguration

1. Weisen Sie **Gewichte** für die Priorisierung und Auswahl jeder Plattform weltweit und/oder nach Markt oder Land zu.
2. Um Plattformgewichte für Markt oder Land separat zuzuweisen, geben Sie den Namen in das Suchfeld Märkte & Länder ein und wählen Sie aus der Liste aus.
3. Klicken Sie auf **Abschließen**, um Ihre Anwendung zu erstellen.
4. Klicken Sie im Bestätigungs-Popup auf **Fertig** oder **Veröffentlichen**, um Ihre App auf der Openmix-Seite anzuzeigen. Wenn Sie auf **Veröffentlichen**klicken, wird Ihre App sofort live geschaltet und hat einen grünen Status. Ihre Anwendung ist in Produktion. Wenn Sie auf **Fertig**klicken, wird Ihre App weiterhin auf der Openmix-Seite aufgeführt, sie ist jedoch nicht veröffentlicht und ihr Status ist rot.

App für optimale Hin- und Rückflugzeit (ORTT)

Die ORTT-App verwendet die Radarreaktionszeit, Sonardaten, falls Sonar aktiviert ist, und den Schwellenwert für die Plattformverfügbarkeit, um die beste Plattform für den anfordernden Benutzer zu bewerten. Der Verfügbarkeitsschwellenwert ist die Mindestverfügbarkeit (80% ist der Standardwert), die die Plattform erfüllen muss, um ausgewählt zu werden. Darüber hinaus nutzt die ORTT-App auch einen Handicap-Wert, der es Kunden global oder lokal ermöglicht, die Weiterleitung von Endbenutzern zu beeinflussen.

Die ersten drei Schritte —Basisinformationen, Konfiguration und Plattforminformationen —werden auf dieselbe Weise wie bei den anderen Apps eingegeben.

Folgen Sie diesen Schritten, um Standortinformationen zu konfigurieren und Werte für **Handicap** für jede Plattform, global oder nach Standort/Markt, einzugeben.

Standort-Konfiguration

1. Geben Sie im Dialogfeld **Standortkonfiguration** einen Wert für **Handicap** für eine oder alle ausgewählten Plattformen ein. Sie können einen Handicap-Wert zwischen 0 und 6000 eingeben. Die Verwendung des Handicaps besteht darin, die Wahrscheinlichkeit, dass eine bestimmte Plattform für das Routing ausgewählt wird, manuell zu verringern, wenn bessere Plattformen verfügbar sind, in Bezug auf Kosten oder Komfort. Je höher der Handicap-Wert ist,

desto geringer ist die Wahrscheinlichkeit, dass die Plattform ausgewählt wird. Sie können bei Bedarf die Auswahl einer Plattform aufheben, indem Sie die Schaltfläche **Plattformauswahl** deaktivieren.

2. Klicken Sie auf **Märkte & Länder**, um einen bestimmten Markt oder ein bestimmtes Land aus der Liste auszuwählen, und geben Sie die **Handicap-Werte** für jede der zugehörigen Plattformen separat ein.
3. Klicken Sie auf **Vollständig**, um die Konfiguration Ihrer App abzuschließen.
4. Klicken Sie im Bestätigungs-Popup auf **Fertig** oder **Veröffentlichen**, um Ihre App auf der Listenseite der Openmix-Anwendungen anzuzeigen. Wenn Sie auf **Veröffentlichen**klicken, wird Ihre App sofort live geschaltet und hat einen grünen Status. Ihre Anwendung ist in Produktion. Wenn Sie auf **Fertig**klicken, wird Ihre App weiterhin auf der Seite Anwendungen aufgeführt, sie ist jedoch nicht veröffentlicht und ihr Status ist rot.

Durchsatz

Die **Durchsatz-App** wählt die Plattform basierend auf Sonardaten (wenn Sonar aktiviert ist), dem höchsten Durchsatz (unter Verwendung von Radardaten) und dem Schwellenwert für die Plattformverfügbarkeit (standardmäßig 80%) aus. Darüber hinaus können Sie mit dieser App einen Handicap-Wert hinzufügen, um den Durchsatz für bestimmte Plattformen zu verringern und zu beeinflussen, wie Endbenutzer weitergeleitet werden. Dieser optionale Handicap-Wert kann global und/oder lokal (für bestimmte Märkte oder Länder) zugewiesen werden.

Die ersten drei Schritte —**Basisinformationen, Konfiguration und Plattforminformationen** —werden auf dieselbe Weise wie bei den anderen Apps eingegeben. Die **Standortkonfiguration** wird auf dieselbe Weise wie in der ORTT-App eingegeben.

Wenn Sie fertig sind, klicken Sie auf **Fertig stellen**, um zur Listenseite der Openmix-Anwendungen zurückzukehren. Klicken Sie abschließend auf Veröffentlichen, um Ihre Anwendung zu **veröffentlichen**, wenn Sie bereit sind, live zu gehen.

Status des Antrags

Der Status der App zeigt ihre aktuelle Konfiguration an.

- Rot steht für unveröffentlicht. Wenn Sie nach Abschluss der Konfiguration auf **Fertig** klicken, wird Ihre Anwendung auf der Anwendungsseite mit einem roten Punkt angezeigt, der darauf hinweist, dass sie noch nicht veröffentlicht wurde.
- Grün steht für veröffentlicht. Wenn Sie auf **Veröffentlichen** klicken, wird Ihre App sofort live geschaltet und mit einem grünen Punkt gekennzeichnet, was bedeutet, dass die Anwendung in Produktion ist.

- Gelb steht für die neueste Version, die unveröffentlicht ist. Der gelbe Punkt zeigt an, dass die Anwendung erstellt und bearbeitet wurde und die zuletzt geänderten Einstellungen noch nicht veröffentlicht wurden.

Statische Nähe

Die Static Proximity-Anwendung reagiert auf die Plattform, die sich in der Nähe des Breiten- und Längengrads des anfragenden Benutzers befindet.

> **Hinweis:**
>
> Für alle Openmix-Apps müssen zuvor eine Reihe zugehöriger Plattformen eingerichtet werden. Wenn Sie in der Liste keine Plattform finden, können Sie sie auf der Seite Plattformen innerhalb des Portals einrichten.

Navigation

1. Melden Sie sich beim NetScaler Intelligent Traffic Management-Portal an.
2. Navigieren Sie im linken Navigationsmenü zu **Openmix > Anwendungskonfiguration**.
3. Klicken Sie oben rechts auf die Schaltfläche mit dem Pluszeichen **Openmix App hinzufügen** .
4. Wählen Sie **Schnellstart-App**aus.

Grundlegende Informationen

1. Wählen Sie im Dialogfeld **GrundinformationenDNS** als Protokoll aus.
2. Wählen Sie **Statische Nähe** als Anwendungstyp aus. Geben Sie der App einen Namen (Pflichtfeld), eine Beschreibung (optionales Feld) und ein Tag (optionales Feld).
3. Klicken Sie für Konfiguration auf **Weiter**.

Konfiguration

1. Wenn diese Option aktiviert ist, hat der **Verfügbarkeitsschwellenwert** einen Standardwert von 80%. Geben Sie einen neuen Wert ein, der den Standardwert ersetzt.
2. **Geben Sie eine CNAME/A/AAAA- oder IP-Adresse für Fallback ein.** Der Fallback-CNAME/A/AAAA oder IP wird normalerweise verwendet, wenn die Anwendung auf Probleme oder Fehler stößt. Dieses Feld darf nicht leer sein.
3. Geben Sie **TTL (Time-To-Live)** für die Antwort ein. Die Standardeinstellung ist 20 Sekunden, aber dieser Wert kann bei Bedarf außer Kraft gesetzt werden.
4. Klicken Sie auf **Weiter** für Persistenzsteuerungen.

Persistenz-Steuerung Richten Sie **Lokale Persistenz**ein. Weitere Informationen finden Sie unter Lokale Persistenz. Klicken Sie auf **Weiter** für Plattforminformationen.

Informationen zur Plattform Für jede Plattform muss der Breiten- und Längengrad auf der Seite **Plattformen** eingerichtet sein. Aliase für Community-Plattformen erben zunächst Geoinformationen von der Community-Plattform, obwohl Sie sie nach dem Erstellen eines Alias ändern können. Private Plattformen müssen beim Erstellen oder danach über ihren Konfigurationsbereich eingerichtet werden. Um den Konfigurationsbereich anzuzeigen, klicken Sie einfach auf den Plattformeintrag der Tabelle.

Nur Plattformen, die zu den folgenden Kategorien gehören, können Geoinformationen haben und Teil der Antwortliste einer opx-App sein:

- Cloud-Computing
- Cloud-Speicher
- Rechenzentrum

1. Wählen Sie eine Plattform aus der **Plattformliste** aus.
2. Geben Sie einen CNAME oder einen A/AAAA-Eintrag oder eine IP (in DNS) oder eine URL (in HTTP) für die Plattform ein. Es muss eine gültige URL, Hostname oder IP-Adresse sein. Es kann folgende Form haben:

   ```
   scheme:[//host[:port]][/path][?query][#fragment]
   ```

3. Stellen Sie sicher, dass das Kontrollkästchen **Aktiviert aktiviert** ist, um anzuzeigen, dass die Plattform aktiviert ist, bevor Sie mit dem nächsten Schritt fortfahren.
4. Wenn Sonar für diese Plattform verfügbar ist und Sie Sonardaten verwenden möchten, die bei der DNS-Auflösung berücksichtigt werden sollen, stellen Sie sicher, dass Sie das Kontrollkästchen **Sonar für Plattformverfügbarkeit verwenden** aktivieren.
5. Sie können weitere Plattformen hinzufügen, indem Sie auf **Plattform hinzufügen**klicken.
6. Klicken Sie auf **Weiter** für die **Standortkonfiguration**.

Standort-Konfiguration

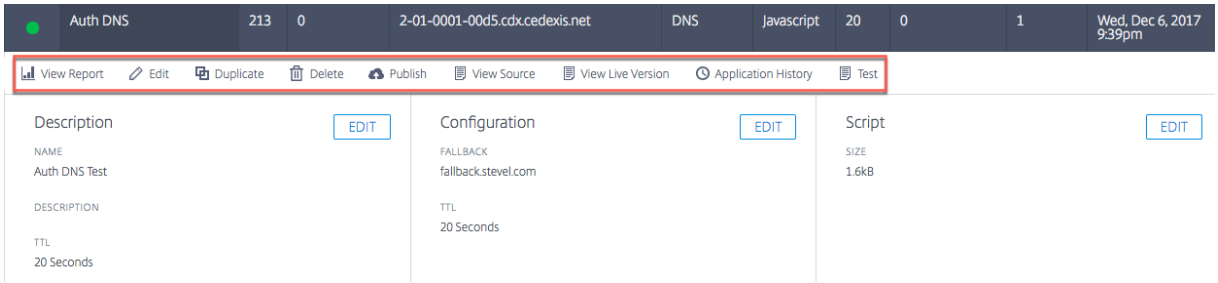
1. Im Bereich Global des Dialogfelds Standortkonfiguration können Sie eine Kette von Plattformen für das globale Routing einrichten. Sie können die Auswahl jeder Plattform global aktivieren oder deaktivieren.
2. In den Märkten und Ländern können Sie verschiedene Setups pro Markt oder Land erstellen, wobei Sie effektiv Geo-Fencing-Regeln für diese festlegen.
3. Klicken Sie auf **Abschließen**, um Ihre Anwendung zu erstellen.

Klicken Sie im Bestätigungs-Popup auf **Veröffentlichen, Weitere hinzufügen** oder **Fertig**:

- Wenn Sie auf **Veröffentlichen**klicken, wird Ihre App sofort live geschaltet und der Status ist grün. Dies bedeutet, dass die Anwendung in Produktion ist.
- Wenn Sie auf **Fertig**klicken, wird Ihre App auf der Openmix-Seite aufgeführt, sie ist jedoch nicht veröffentlicht und der Status ist rot.
- Wenn Sie auf **Weitere hinzufügen**klicken, ist der Status der App derselbe wie **Fertig**, aber Sie starten denselben Vorgang erneut, um eine neue App zu erstellen.

Schnellstart-Anwendungen verwalten

Verwenden Sie die oberen Registerkarten im Anwendungsmanager-Panel, um Berichte zu bearbeiten, zu duplizieren, zu löschen, zu testen, Berichte anzuzeigen, die Quelle anzuzeigen und den Versionsverlauf der Anwendung anzuzeigen Klicken Sie auf der Openmix-Anwendungslistenseite auf Ihre Anwendung, um den Anwendungsmanager zu erweitern.



Bericht ansehen

Bericht anzeigen führt Sie zur Seite Openmix-Entscheidungsberichte, auf der Sie den Trend der Openmix-Entscheidungen für jede Ihrer Anwendungen, Plattformen und Regionen anzeigen können.

Bearbeiten

Um Ihre Openmix-App zu bearbeiten, klicken Sie einfach auf das Symbol **Bearbeiten** oben im Anwendungsmanager-Panel. Sie können einzelne Änderungen auch separat für grundlegende Informationen, Konfiguration, Plattform oder Standortinformationen vornehmen, indem Sie auf die Schaltflächen **Bearbeiten** innerhalb des Bedienfelds klicken, wie in der Abbildung gezeigt. Wenn Sie die Bearbeitung abgeschlossen haben, klicken Sie auf **Fertig**, um die App mit dem Status "Nicht veröffentlicht"aufzulisten (weitere Änderungen später), oder klicken Sie auf **Veröffentlichen**, um sofort live zu gehen.

Duplicate

Klicken Sie auf **Duplizieren**, um die Konfiguration der aktuellen Anwendung zu replizieren und unter einem neuen Namen zu speichern.

Löschen

Klicken Sie auf **Löschen**, um Anwendungen zu entfernen, die Sie nicht mehr benötigen.

Veröffentlichen

Klicken Sie auf **Veröffentlichen**, um die Anwendung direkt über den Openmix-Anwendungsmanager zu veröffentlichen. Diese Option ist nur sichtbar, wenn die App noch nicht veröffentlicht ist.

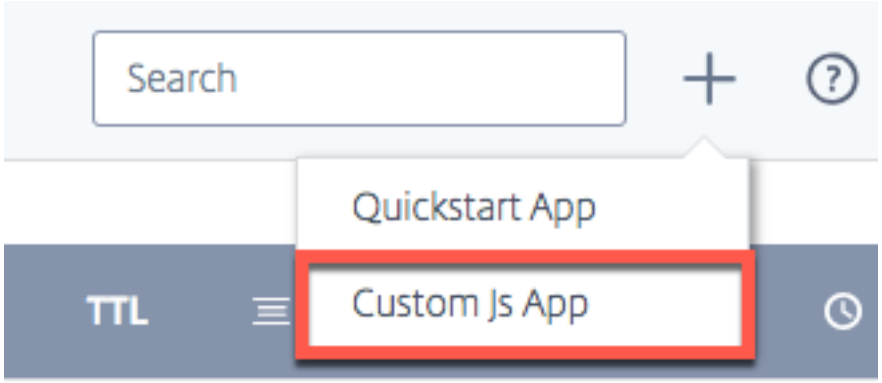
Benutzerdefinierte Openmix JavaScript-Anwendungen

Openmix JavaScript-Anwendungen sind Apps mit anpassbaren Java-Skripts. Sie können mithilfe der Benutzeroberfläche im ITM-Portal erstellen, konfigurieren, testen und veröffentlichen.

Hinweis: Diese Anleitung bezieht sich nicht auf die tatsächliche Erstellung des benutzerdefinierten Skripts (Syntaxen, Variablen usw.). Weitere Informationen zum Erstellen von benutzerdefiniertem JavaScript finden Sie in Developer Exchange.

Navigation

1. Melden Sie sich beim ITM-Portal an.
2. Gehen Sie im linken Navigationsmenü zu **Openmix**.
3. Wählen Sie **Anwendungskonfiguration**.
4. Um eine neue Openmix-App zu konfigurieren, klicken Sie auf das Hinzufügen-Symbol in der oberen rechten Ecke.
5. Wählen Sie **Benutzerdefinierte JS-App**.
6. Die Seite “**Openmix-Anwendungskonfiguration** “wird geöffnet.



Grundlegende Informationen

1. **Anwendungsname**: Geben Sie Ihrer App einen Namen.
2. **Beschreibung**: Geben Sie der App eine Beschreibung oder fügen Sie hier einen Versionshinweis hinzu. Es ist ein optionales Feld.
3. **Tags**: Geben Sie bei Bedarf ein geeignetes Tag ein. Tags helfen dabei, Ihre App zu identifizieren und zu organisieren. Es ist ein optionales Feld.
4. **Protokoll**: Wählen Sie DNS oder HTTP als Protokoll.
   - **DNS**: Wenn Sie DNS auswählen, muss ein TTL-Wert eingegeben werden.
   - **HTTP**: Wenn Sie HTTP auswählen, können Sie **Secure Access**aktivieren.
5. **TTL**: Geben Sie eine DNS-Laufzeit für die Anwendung ein. Der empfohlene Wert ist 20 Sekunden. Hinweis: Diese TTL gilt, wenn von der benutzerdefinierten JS-App kein TTL festgelegt wurde oder wenn es sich bei der Antwort um einen Fallback-Wert handelt.
6. **Fallback**: Geben Sie einen CNAME/A/AAAA oder eine IP-Adresse für **Fallback**ein. Der Fallback-CNAME/A/AAAA oder IP wird normalerweise verwendet, wenn die Anwendung auf Probleme oder Fehler stößt.
7. **Sicherer Zugriff**: Wenn **Secure Access**aktiviert ist, muss die HTTP-API beim Aufruf einen Oauth-Zugriffsschlüssel vom Client benötigen. Weitere Informationen finden Sie unter Openmix HTTP API sichern .

   Hinweis: Wenn Sie den sicheren Zugriff aktivieren, wird in der Liste der Apps auf der Openmix-Startseite neben dem App-Namen ein Schlosssymbol angezeigt.

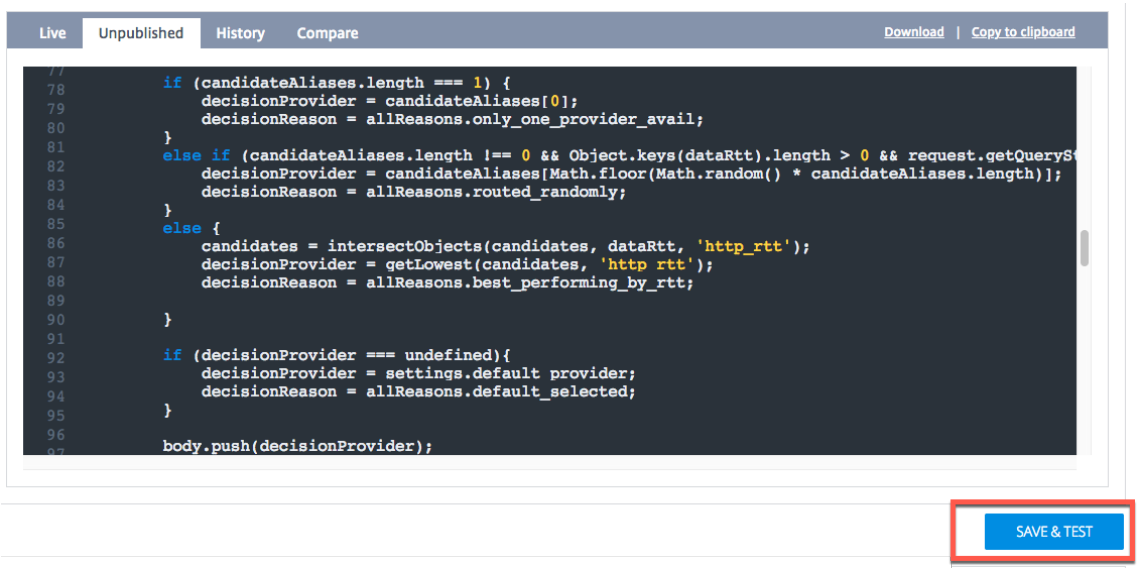
Benutzerdefiniertes JavaScript

Sobald Sie die Konfigurationsinformationen eingegeben haben, können Sie Ihr benutzerdefiniertes JavaScript hochladen.

1. Klicken Sie auf die Schaltfläche **Datei auswählen** und wählen Sie die JavaScript-Datei aus, die Sie hochladen möchten. Sie können jederzeit eine neue Datei hochladen, um eine vorhandene Datei zu überschreiben.

2. Klicken Sie auf **Speichern und testen**, um Ihre Anwendung zu speichern.

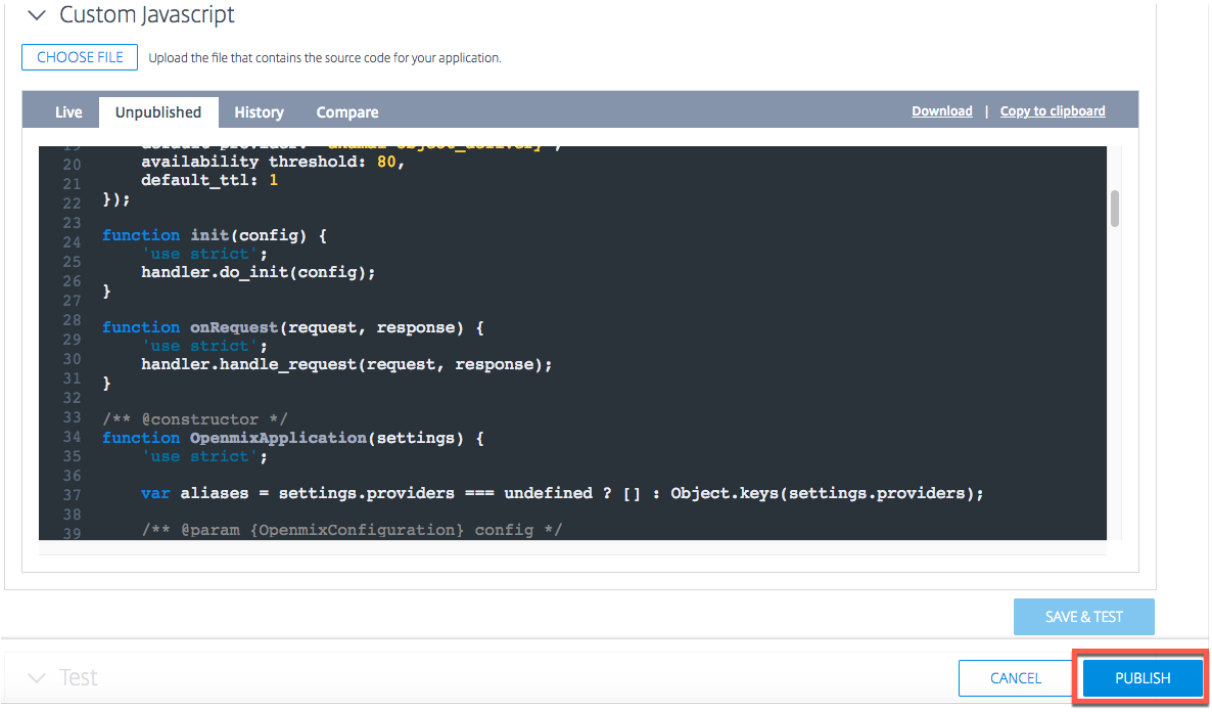
   Hinweis: Die Anwendung wird automatisch mit einem Application Checker getestet, wenn sie hochgeladen und gespeichert wird. Wenn Fehler vorliegen, zeigt die Anwendungsprüfung die Fehlerinformationen und den Speicherort des Fehlers an. Weitere Informationen zu den im Application Checker verfügbaren Daten finden Sie im Abschnitt Anwendungsüberprüfung .



3. Klicken Sie auf **Abbrechen**, um zur Seite Openmix-Anwendungen zurückzukehren, oder klicken Sie auf **Veröffentlichen**, wenn Sie bereit sind, die Anwendung live zu schalten.

   Hinweis: Wenn Sie auf **Veröffentlichen**klicken, wird Ihre App sofort live geschaltet und hat einen grünen Status. Ihre Anwendung ist in Produktion.

Wenn Sie auf **Abbrechen**klicken, wird Ihre App auf der Anwendungsseite aufgeführt, ist aber nicht veröffentlicht, und der Status ist rot. Weitere Informationen zum Status finden Sie im Abschnitt Status der Anwendung.



Anwendungsrollout in Phasen

Sie können den Rollout Ihrer Anwendung verwalten, indem Sie einen kleinen Prozentsatz Ihres Web-Traffics über eine neue Version senden, die manchmal als Canary Deployment bezeichnet wird. Mit ITM können Sie einen bestimmten Prozentsatz des Datenverkehrs an die neue Version einer App senden, um sicherzustellen, dass sich die Anwendungslogik wie erwartet verhält. Sie können über das Verhalten der vorhandenen und neuen Versionen berichten, um die Änderungen an Ihrer App in einer Live-Umgebung auszuwerten. Mit dieser Option können Sie alle Probleme oder Anomalien beheben, die auftreten, bevor Sie 100% Ihres Webverkehrs durch die neu bearbeitete App leiten. Nachdem Sie das gewünschte Verhalten überprüft haben, können Sie den Prozentsatz des Datenverkehrs auf die neueste Version erhöhen oder die Anwendung für alle Benutzer bereitstellen.

Gehen Sie wie folgt vor, um den Rollout der Anwendung durchzuführen und eine Testversion Ihrer neu geänderten App freizugeben:

- Klicken Sie auf den Namen der App (auf der Listenseite der Openmix-Anwendungen). Das Anwendungsmanager-Panel wird geöffnet.
- Klicken Sie auf das Symbol **Bearbeiten**, um Ihre App zu bearbeiten.
- Ändern Sie Ihre bestehende App mit allen notwendigen Änderungen.

- Wenn Sie mit den Änderungen fertig sind, klicken Sie auf **Speichern und testen**.
- Scrollen Sie unten auf der Seite mit den Schaltflächen **Abbrechen** und **Veröffentlichen** nach unten. Geben Sie den Prozentsatz des Web-Traffics (1% bis 99%) ein, den Sie durch diese neu geänderte Version fließen möchten.
- Aktivieren Sie das Kontrollkästchen für die teilweise Verteilung des Datenverkehrs durch diese neue Version der Anwendung. Der verbleibende Datenverkehr wird an die vorherige Live-Version gesendet.
- Klicken Sie auf **Veröffentlichen**. Diese neue Testversion der App wird nun in der Liste der Apps auf der **Openmix-Konfigurationsseite** mit einem neuen **Statussymbol** angezeigt. Das neue **Statussymbol** zeigt an, dass nur ein Teil des Webverkehrs live durch diese Version fließt.

Sie können den Verkehrsfluss auf die Testversion ändern und den Prozentsatz des Verkehrsflusses ändern, um die Leistung anzuzeigen.

```
1 ![Canary](/en-us/citrix-intelligent-traffic-management/media/openmix-
    jsapp-edit-canary.png)
```

Um die Leistung Ihrer App zu überprüfen, rufen Sie den Openmix Decision Report auf. Wählen Sie **Anwendung** als primäre Dimension und **Version** als sekundäre Dimension aus. Klicken Sie dann auf **Filter anwenden**, nachdem Sie Ihre Anwendung aus der Liste ausgewählt haben. Das Diagramm zeigt die Leistung verschiedener Versionen Ihrer Anwendung.

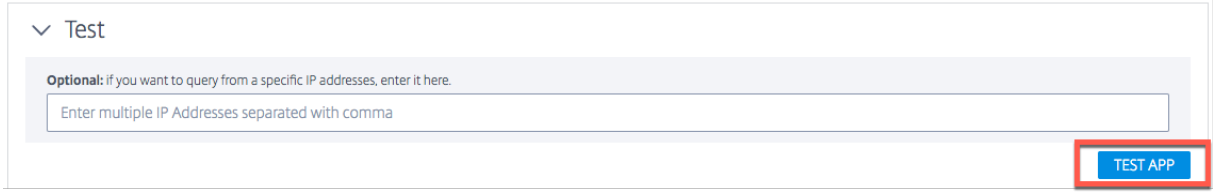
Sobald Sie mit der Leistung dieser Version der App zufrieden sind, können Sie 100% Ihres Webverkehrs durch die App leiten, indem Sie auf die Schaltfläche **Go Live** klicken.

Diese Version ersetzt die aktuelle Live-Version durch die neu bearbeitete Version.

Wenn Sie mit dieser Version nicht live gehen möchten, klicken Sie auf **Veröffentlichung rückgängig**machen. Ihre Änderungen werden gespeichert und als unveröffentlichte App in der Liste der Apps auf der **Openmix-Konfigurationsseite** angezeigt. Jetzt fließt 100% Ihres Webverkehrs durch die aktuelle Live-Version Ihrer App.

Testen

Sie können Ihre JavaScript-Anwendung vor oder nach der Veröffentlichung mit der Schaltfläche **App testen** .

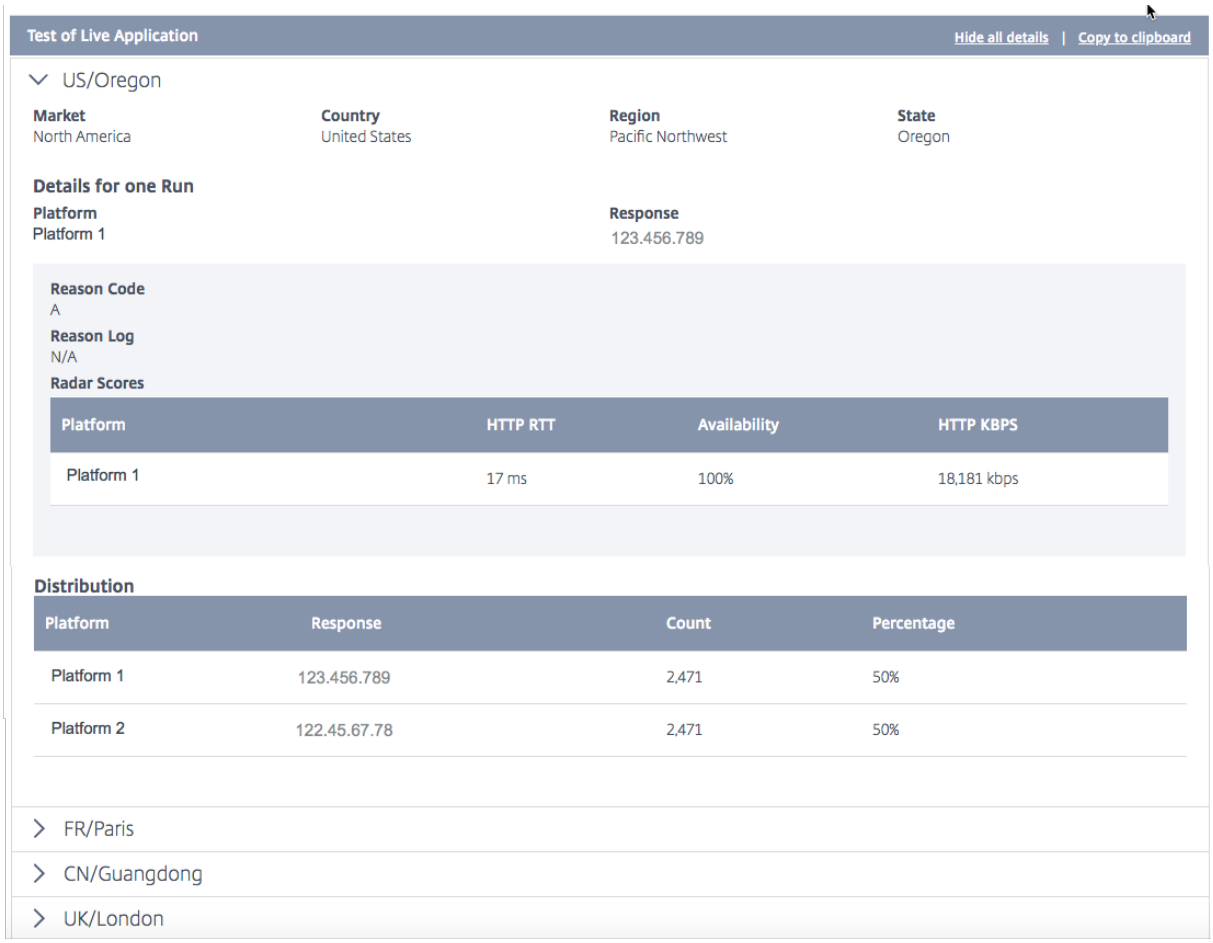


Es ermöglicht Ihnen, Testergebnisse für bestimmte Gruppen von Märkten, Ländern, Regionen und Bundesstaaten anzuzeigen. Sie können die App von bestimmten IP-Adressen aus abfragen.

Zu den Testergebnissen gehören: Von der App ausgewählte **Plattform**, erhaltene **Antwort**, **Ursachencode, Ursachenprotokoll**,**Radarwerte**,**Verteilung** usw.

Mit dieser Funktion können Sie auch die Verteilung von Entscheidungen auf verschiedene Plattformen anzeigen. Wenn beispielsweise zwei Plattformen für das Routing verwendet werden, können Sie die Anzahl der Entscheidungen und die für jede von ihnen empfangene Antwort anzeigen.

Klicken Sie auf den Link **Alle Details anzeigen**, um die Testergebnisse Ihrer App anzuzeigen.



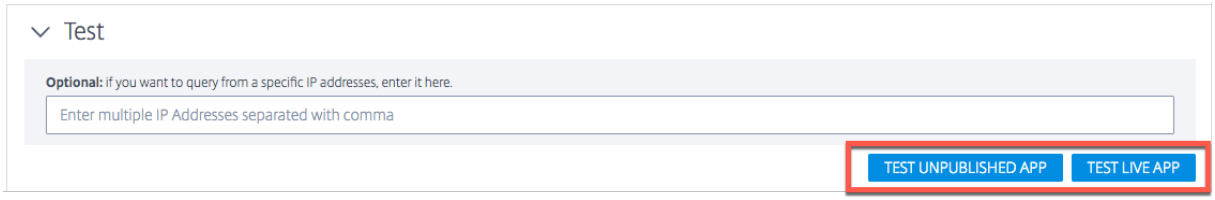
Die folgenden Werte werden als Testergebnisse angezeigt:

Feld	Beschreibung
Markt, Land, Region und Bundesland	Der Ort, an dem die App getestet wurde.
Plattform	Die von der App ausgewählte Plattform.
Antwort	Der CNAME oder die IP-Adresse der von der App ausgewählten Plattform.
Ursachencode	Beschreibt den Grund für die Entscheidung.

Feld	Beschreibung
Ursache-Protokoll	Kundendefinierter Output aus der App. Ermöglicht es Kunden, Informationen über die App-Entscheidungen zu protokollieren.
Radar-Score	Die für die Plattform aufgezeichneten Messungen von **Reaktionszeit (RTT)**, **Verfügbarkeit**und **Durchsatz** .
Distribution	Die Verteilung der Plattformen, die eine App für jeden getesteten Standort auswählt. Die **Anzahl** gibt an, wie oft die Plattform ausgewählt wurde. Und der **Prozentsatz** ist der Prozentsatz der Gesamtanzahl für die Plattformauswahl.

Hinweis: Sie können diesen Test für die Live-App oder die unveröffentlichte Version ausführen, das heißt, wenn die App noch nicht veröffentlicht ist.

Sobald Ihre App veröffentlicht ist, haben Sie die Möglichkeit, die Live-App zu testen, indem Sie auf die Option **Live-App testen** klicken. Wenn Sie Ihre App bearbeiten oder eine neue Version hochladen, können Sie sie vor der Veröffentlichung testen, indem Sie auf die Schaltfläche **Unveröffentlichte App testen** klicken.



Anwendungsverifizierung

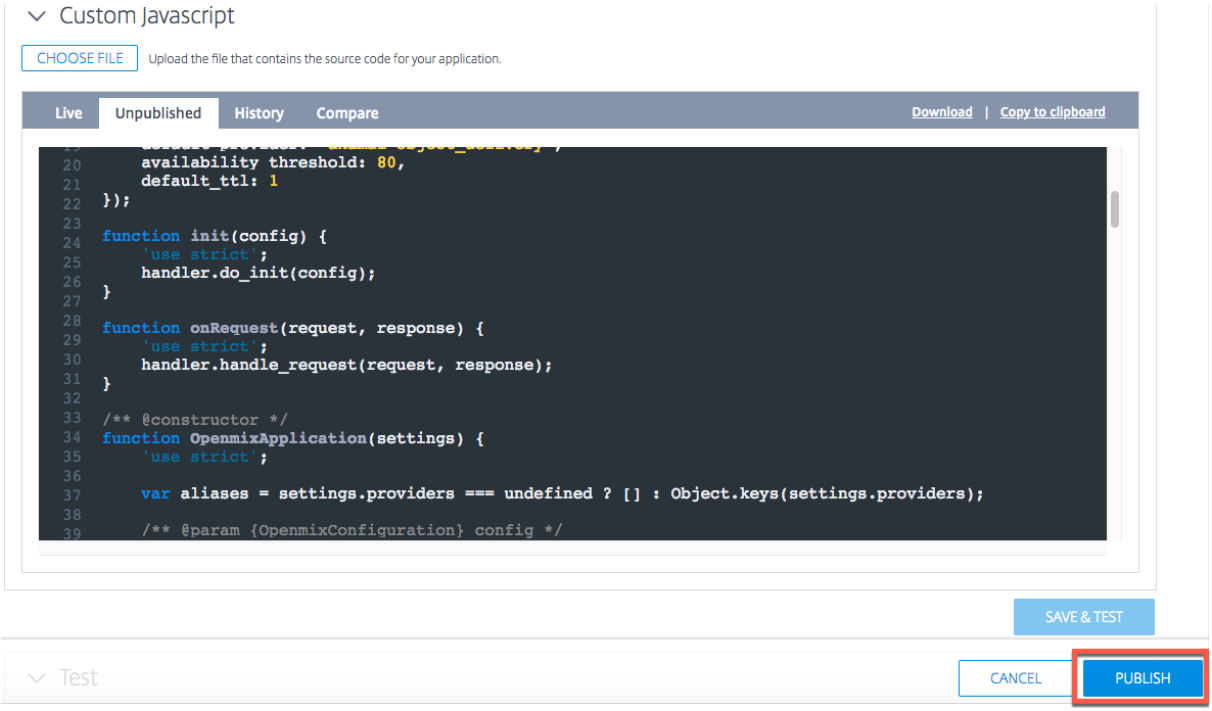
Um sicherzustellen, dass sich benutzerdefinierte JavaScript-Apps wie erwartet verhalten, führen Sie die App durch eine Code- und Logiküberprüfung aus, wenn Sie sie in das ITM-Portal hochladen. Der Application Verifier führt die App über einen Entscheidungsserver mit synthetischem Datenverkehr aus, um zu testen, ob die Anwendung erfolgreich kompiliert und ausgeführt wird.

Wenn die Anwendung ohne Fehler ausgeführt wird, liefert der Verifizierer Informationen über die Entscheidungsverteilung und die Ausführungsmerkmale. Wenn der Entscheidungsserver dagegen beim Ausführen der App auf einen Fehler stößt, liefert der Verifizierer Informationen über den Fehler. Wir empfehlen, dass die Anwendung vor der Veröffentlichung fehlerfrei sein muss.

Bei Fehlern können Sie die JavaScript-Datei in Ihrem lokalen Verzeichnis reparieren und erneut in das Portal hochladen, indem Sie auf die Schaltfläche **Datei auswählen** klicken.

Veröffentlichen

Um Ihre App zu veröffentlichen und live zu schalten, klicken Sie auf die Schaltfläche **Veröffentlichen** . Diese Option ist ausgegraut, wenn die App noch nicht gespeichert oder bereits veröffentlicht ist. Wenn die App live geht, wird sie auf der Openmix Application Manager-Seite mit einem grünen Status angezeigt. Weitere Informationen zum Status der App finden Sie im Abschnitt Status der Anwendung.

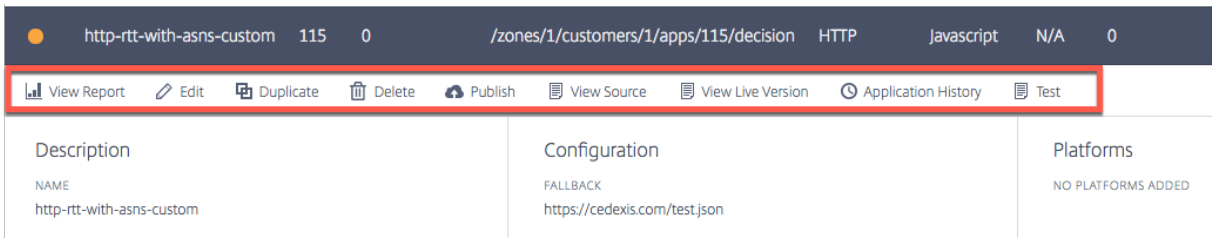


Hinweis: Die App wird bei Bedarf mit Fehlern veröffentlicht.

Benutzerdefinierte JavaScript-Anwendungen

Verwenden Sie die oberen Registerkarten im Anwendungs-Manager-Bereich, um Berichte anzuzeigen, zu bearbeiten, zu duplizieren, zu löschen, zu veröffentlichen, Quelle anzuzeigen, Live-Version anzuzeigen und den Verlauf anzuzeigen.

Klicken Sie auf der Openmix-Anwendungslistenseite auf Ihre App, um das Anwendungsmanager-Panel zu erweitern.

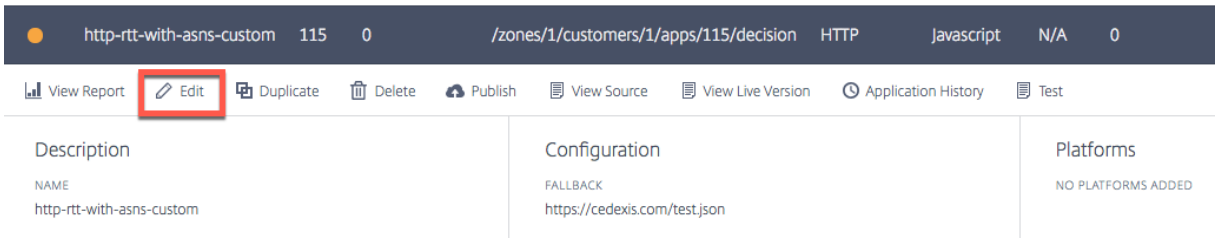


Bericht ansehen

Bericht anzeigen führt Sie zur Seite **Openmix-Entscheidungsberichte**, auf der Sie den Trend der Openmix-Entscheidungen für jede Ihrer Apps, Plattformen und Regionen anzeigen können.

Bearbeiten

Um eine benutzerdefinierte Openmix-Javascript-App zu bearbeiten, klicken Sie auf den App-Namen (auf der Listenseite der Openmix-Anwendungen). Das Anwendungsmanager-Panel wird geöffnet. Änderungen und Aktualisierungen können an der Konfiguration vorgenommen werden, indem Sie auf das Symbol **Bearbeiten** klicken.



Quelltext ansehen

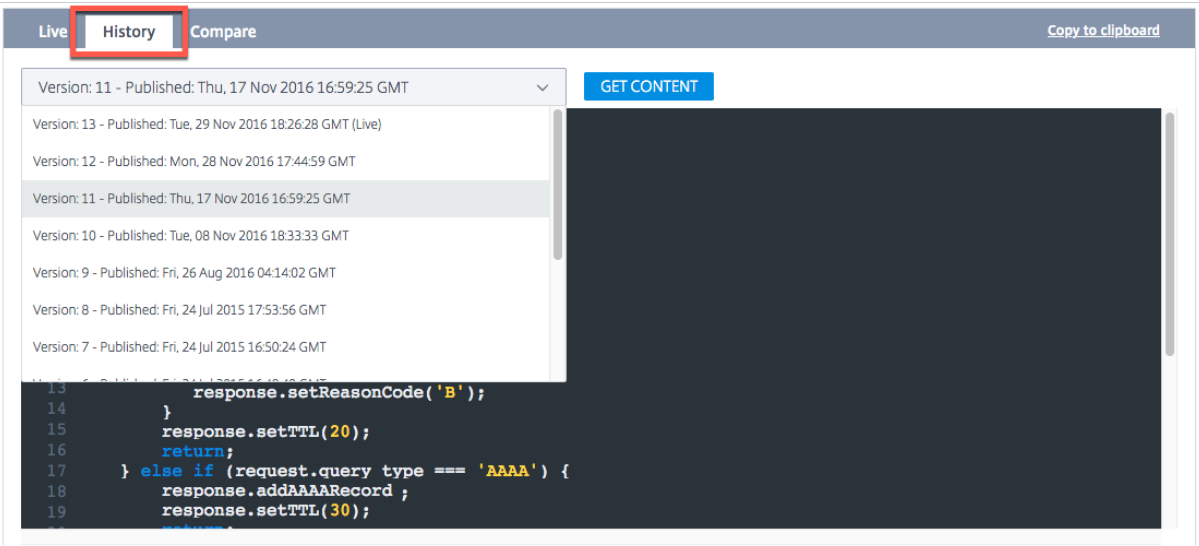
Quelle anzeigen ermöglicht es Ihnen, die JavaScript-Quelle der App anzuzeigen, d. h. die neueste Version der App, unabhängig davon, ob sie veröffentlicht wurde. Diese Option ist nur für benutzerdefinierte JavaScript-Apps verfügbar.

Live-Version anzeigen

Sie können die neueste veröffentlichte Version der App anzeigen, kopieren und herunterladen. Diese Option ist nur für benutzerdefinierte JavaScript-Apps verfügbar.

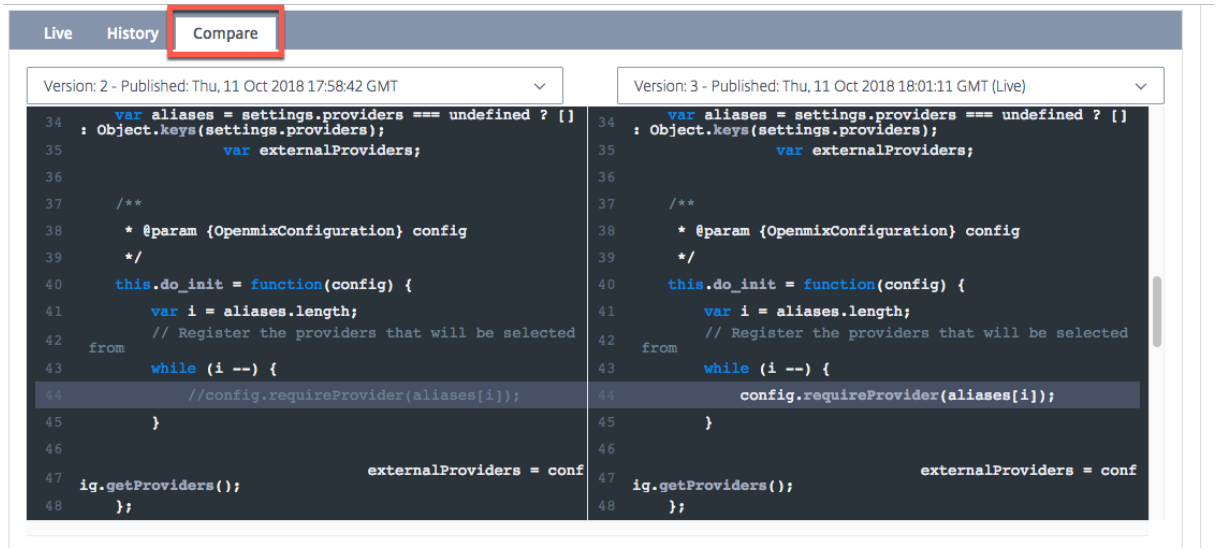
Verlauf der Anwendung

Mit dem**Anwendungsverlauf** können Sie verschiedene Versionen der App anzeigen. Sie können die Liste **Version auswählen** verwenden, um von einer Live-Version zu einer älteren Version zu wechseln. Klicken Sie auf **Inhalt abrufen**, um zur älteren Version zu wechseln. Diese Option ist nur für benutzerdefinierte JavaScript-Apps verfügbar.



Vergleichen

Mit der Funktion **Vergleichen** können Sie verschiedene Versionen Ihrer JavaScript-Datei vergleichen. Sie können die Unterschiede zwischen den beiden Versionen Ihrer App deutlich mit hervorgehobenen Skriptzeilen sehen.



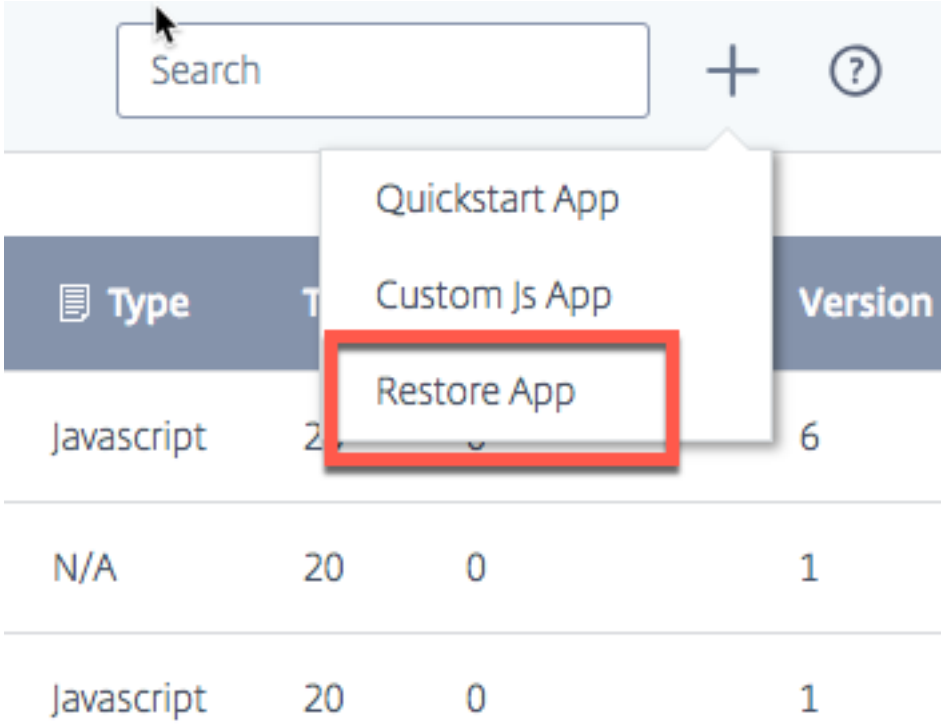
Löschen

Um eine Openmix-App zu löschen, klicken Sie auf den Namen der App (auf der Listenseite der Openmix-Anwendungen). Das Anwendungsmanager-Panel wird geöffnet. Klicken Sie auf das Symbol "**Löschen** "und wählen Sie dann im Bestätigungsdialogfeld die Schaltfläche "**Löschen**". Die App verschwindet aus der Liste.

App wiederherstellen

Mit der Funktion **App wiederherstellen** können Sie eine App wieder aktivieren, nachdem sie gelöscht wurde.
Gehen Sie wie folgt vor, um eine App wiederherzustellen:

1. Klicken Sie oben rechts auf der Seite auf das Symbol **Hinzufügen +** .
2. Wählen Sie **App wiederherstellen** aus dem Dropdown-Menü. Das Fenster **Anwendung wiederherstellen** wird geöffnet.



3. Suchen Sie in der Liste nach der App, die Sie erneut aktivieren möchten, und klicken Sie auf die entsprechende Schaltfläche **Wiederherstellen** .

Die App wird mit demselben Status wieder in die Liste auf der Openmix-Seite gesetzt.

Lokale Persistenz

Die Funktion **Local Persistence** bietet die Möglichkeit zur Entscheidungsfähigkeit, wenn sie für eine Openmix-Anwendung aktiviert ist. Die Anforderungen werden mithilfe der IP-Subnetzmaske identifiziert, deren Länge konfigurierbar ist. Wenn ein Kunde beispielsweise innerhalb eines bestimmten Zeitraums eine Anfrage an dieselbe Anwendung wiederholt, wird die ursprüngliche Entscheidung zurückgestellt. Dies kann ein wesentliches Merkmal sein, wenn ein Kunde während einer bestimmten Sitzung nicht zwischen verschiedenen Entscheidungen wechseln muss. Es ist sowohl für DNS- als auch für HTTP-Openmix-Anwendungen verfügbar.

Aufgrund der zugrunde liegenden natürlichen Einschränkungen des Mechanismus ist die Persistenz für 100% der Anfragen nicht garantiert. Stattdessen wird ein Best Effort-Ansatz angewendet. Tests haben gezeigt, dass die erwartete Persistenzgenauigkeit im Bereich von 95-97% liegt.

> **Hinweis:**
>
> Um die Funktion Local Persistence für Ihr Konto zu aktivieren, öffnen Sie ein Support-Ticket oder wenden Sie sich an Ihren Kundenerfolgsmanager Darüber hinaus ist eine prädiktive DNS-Zone

> erforderlich, die mit Namenservern `ns5.cedexis.net` und `ns6.cedexis.net` konfiguriert ist. Bedenken Sie, wie viel Zeit die DNS-Zonenaktualisierungen möglicherweise benötigen, um im Internet verbreitet zu werden.

Konfiguration

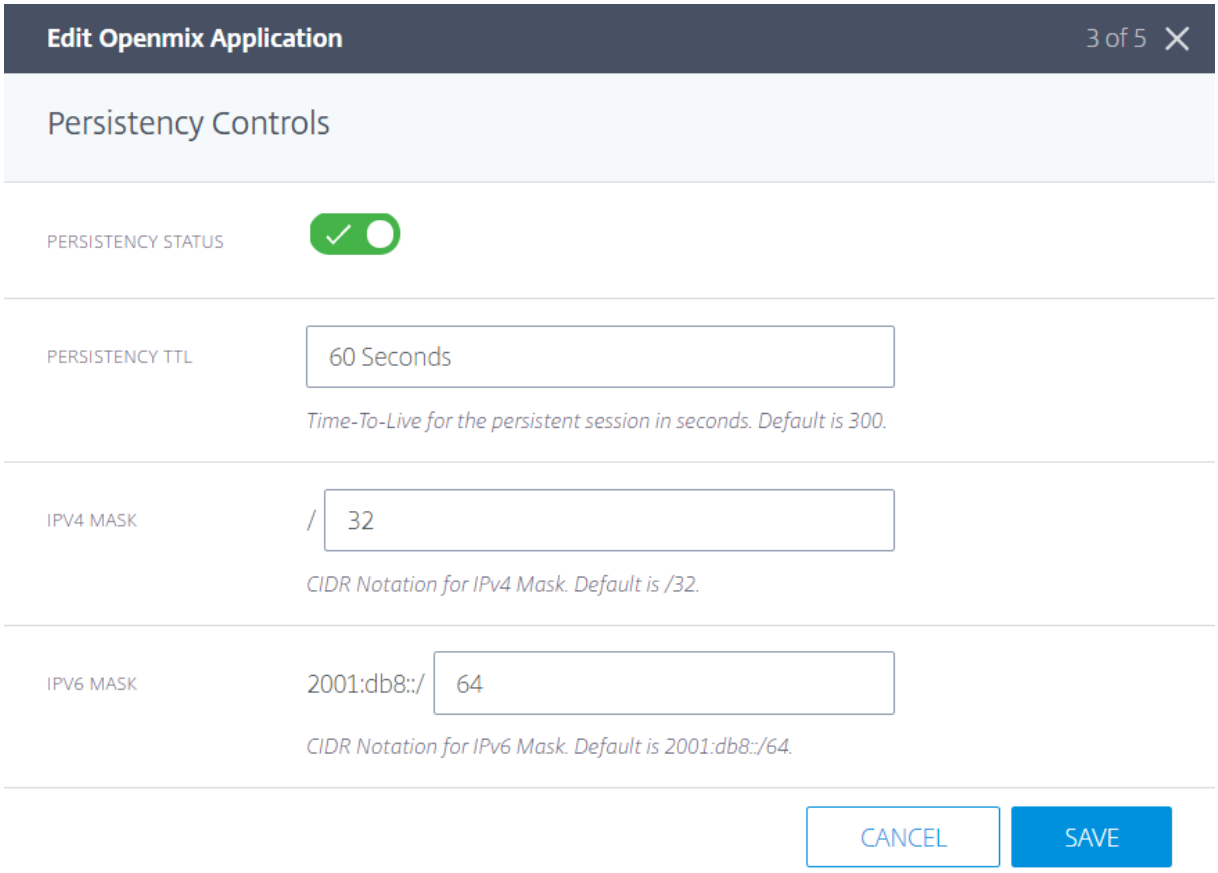
Um Local Persistence zu aktivieren, wählen Sie **Persistency Controls > Edit**unter den Openmix-Anwendungsoptionen aus.

Die verfügbaren Einstellungen lauten wie folgt:

1. Geben Sie im Dialogfeld “Konfiguration”die **Persistency TTL**ein. Die Standardoption ist 300 Sekunden. Werte zwischen 60 und 1440 sind zulässig. Nach einer ersten Anfrage wird die bereitgestellte DNS-Entscheidung maximal 300 Sekunden lang aufbewahrt. Wenn vor dem Ablauf eine weitere Anfrage aus demselben IP-Subnetzbereich im System stammt, dient sie derselben Entscheidung.
2. Sowohl IPv4- als auch IPv6-Masken werden zur Einstellung der Granularität der Persistenz bereitgestellt. Die Standardeinstellung ist “/32”und “/64”für IPv4 bzw. IPv6. Zulässige Werte sind:

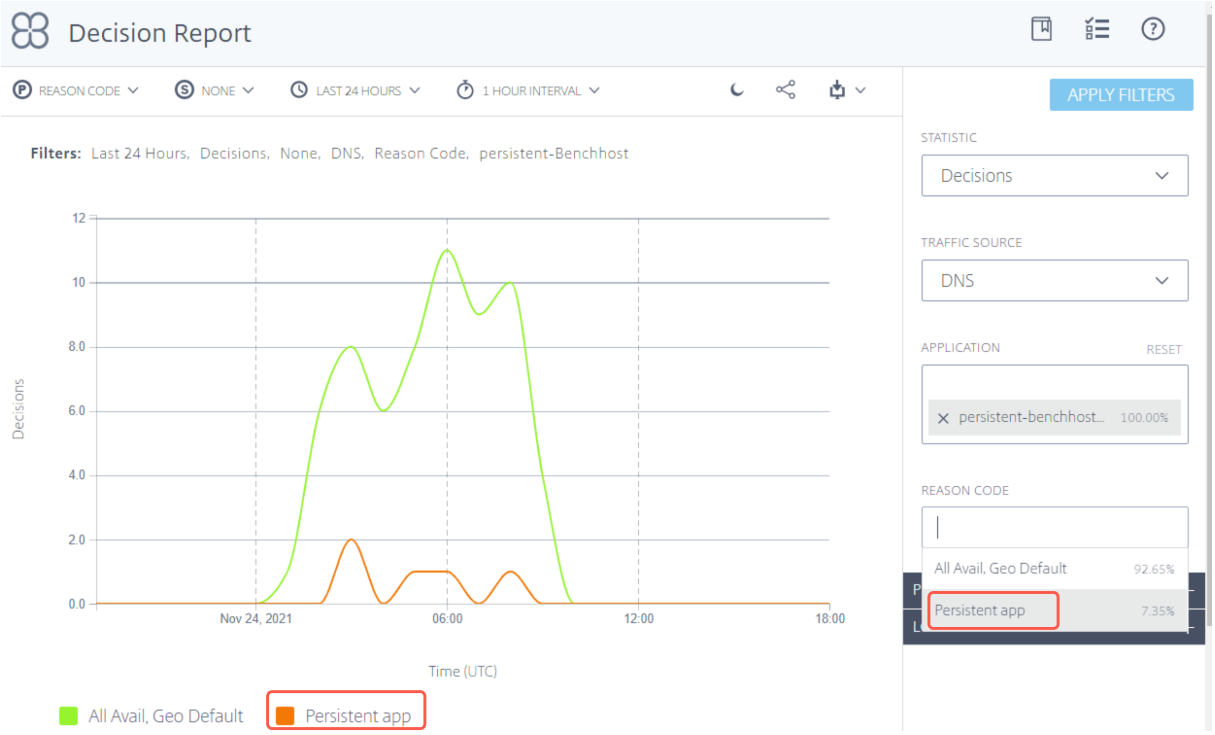
   - /8 bis zu /32, für IPv4
   - /32 bis zu /64, für IPv6

   Diese Maskierung der IP-Adresse des Clients bestimmt den im internen Datenspeicher verwendeten Persistenzschlüssel. Wenn beispielsweise zwei (oder mehr) Client-IPs derselben maskierten IP-Adresse zugeordnet sind, werden sie mit derselben dauerhaften Entscheidung bedient.



Dieselben Einstellungen sind auch unter den Einstellungen für die prädiktive Anwendung verfügbar.

Die Openmix-Entscheidungen, die über den internen Datenspeicher bereitgestellt werden, werden mit dem Ursachencode **Persistent App** im Decision Report gemeldet.



Integritätsprüfungen

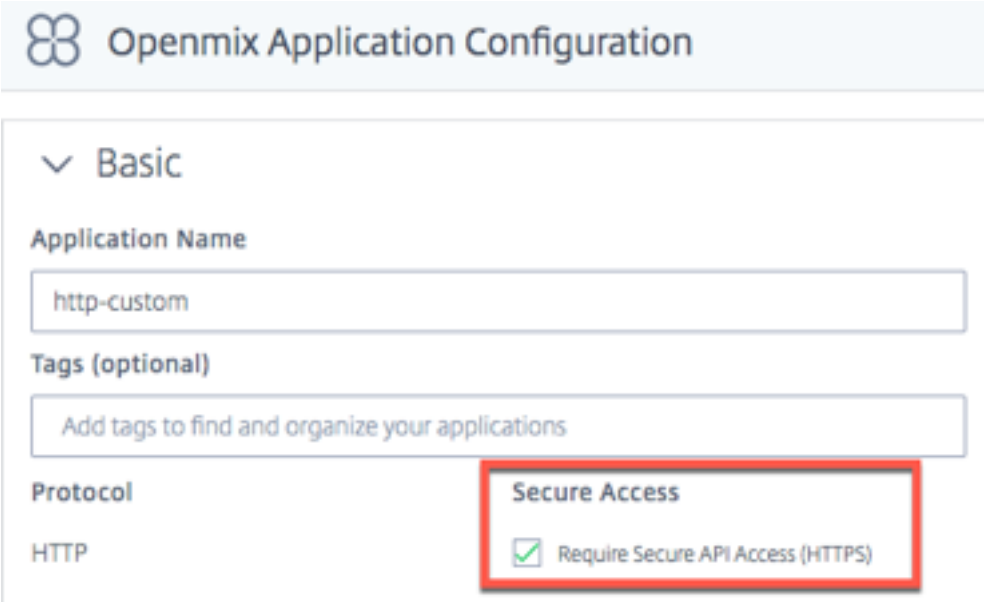
Entscheidungen, die aus dem Persistenz-Cache bedient werden, werden zusätzlichen Integritätsprüfungen unterzogen, bevor sie bedient werden:

1. Wenn die Anwendung mit **Sonar Availability Check**konfiguriert ist, wird der Zustand der Sonar-Verfügbarkeit überprüft, bevor eine zwischengespeicherte Entscheidung zugestellt wird. Wenn Sonar meldet, dass die Plattform “ausgefallen”ist, wird die zwischengespeicherte Entscheidung ignoriert und die OpenMix-Anwendung wird erneut ausgeführt.
2. Wenn die Anwendung mit **Radar Availability Check**konfiguriert ist, wird der Zustand der Radar-Verfügbarkeit überprüft, bevor eine zwischengespeicherte Entscheidung zugestellt wird. Wenn die Verfügbarkeit der Plattform unter dem konfigurierten Schwellenwert liegt, wird die zwischengespeicherte Entscheidung ignoriert.

> **Hinweis:**
>
> Für die Persistenz wird der maximale Schwellenwert für die Gesundheit der Radar-Verfügbarkeit auf feste 10% festgelegt.

Sicherung der Openmix-HTTP-API

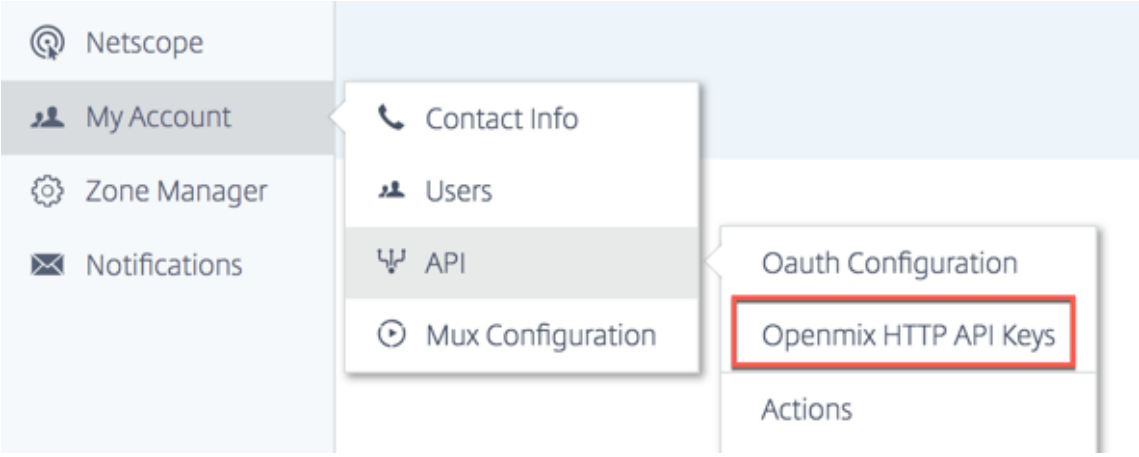
Openmix ist über DNS oder eine HTTP-API zur Integration in Nicht-DNS-Workflows verfügbar. Standardmäßig wird die HTTP-API über einfaches HTTP aufgerufen. Die API kann auch über TLS und Schlüsselauthentifizierung gesichert werden. Dies erfolgt über die Benutzeroberfläche, indem Sie das Kontrollkästchen für **Sicheren API-Zugriff (HTTPS) benötigen**aktivieren.



API-Schlüssel erstellen

Gehen Sie wie folgt vor, um die Schlüsselauthentifizierung zu aktivieren

1. Wählen Sie auf der Seite **Openmix-Anwendungskonfiguration** das Feld **Secure API Access (HTTPS) erforderlich** aus, um den sicheren Zugriff für jede Anwendung zu aktivieren.
2. Um einen sicheren Zugriffsschlüssel zu generieren, navigieren Sie zu **Mein Konto** -> **API** -> **Openmix HTTP API Keys**



3. Wenn Sie zum ersten Mal Benutzer sind, werden Sie durch Eingabe Ihrer Kunden-ID aufgefordert, loszulegen. Geben Sie Ihre **Client-ID** im Dialogfeld **Neuer Client** ein, und klicken Sie auf **Abgeschlossen** .
4. Der Schlüssel **Client Secret** wird neben der **Client ID** auf der Seite **Openmix HTTP API Authentication Configuration** angezeigt.
5. Sie können jetzt eine Anfrage an die Openmix-App mit der grundlegenden Authentifizierung stellen. Verwenden Sie Ihre **Kunden-ID** als Benutzernamen und das **Client Secret** als Kennwort, um die App im Browser aufzurufen.

   Verwenden Sie den folgenden cURL-Befehl, um die App über die Befehlszeile aufzurufen:

```
curl https://hopx.cedexis.com/zones/<zone>/customers/<customer_id
   >/apps/<app_id>/decision --user <client_key>:<client_secret>
<!--NeedCopy-->
```

Hinweis: Mit den von Ihnen erstellten Schlüsseln haben Sie Zugriff auf alle Ihre Openmix-Anwendungen.

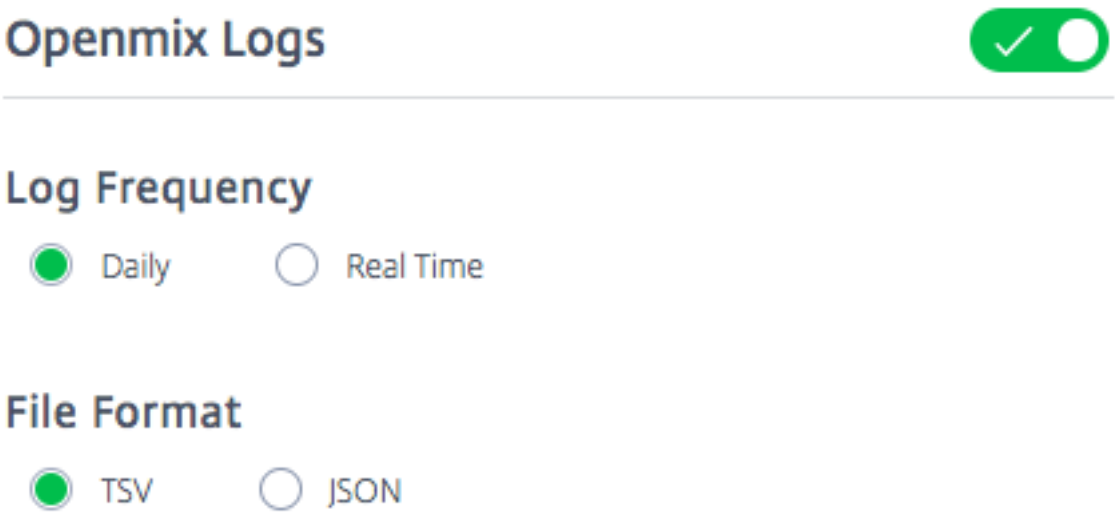
Weitere Informationen zum Aufrufen der Openmix HTTP API finden Sie in der Dokumentation zur Verwendung der Openmix HTTP API.

Löschen von API-Schlüsseln

1. Um einen Schlüssel zu löschen, navigieren Sie zur Seite **Openmix HTTP API Authentication Configuration** .
2. Klicken Sie auf die **Kunden-ID**.
3. Wählen Sie **Löschen** in der Liste. Der Schlüssel wird aus dem System entfernt. Es ist nicht gültig für die Authentifizierung oder den sicheren Zugriff auf die Openmix-Anwendung.

Zugriff auf Protokolle

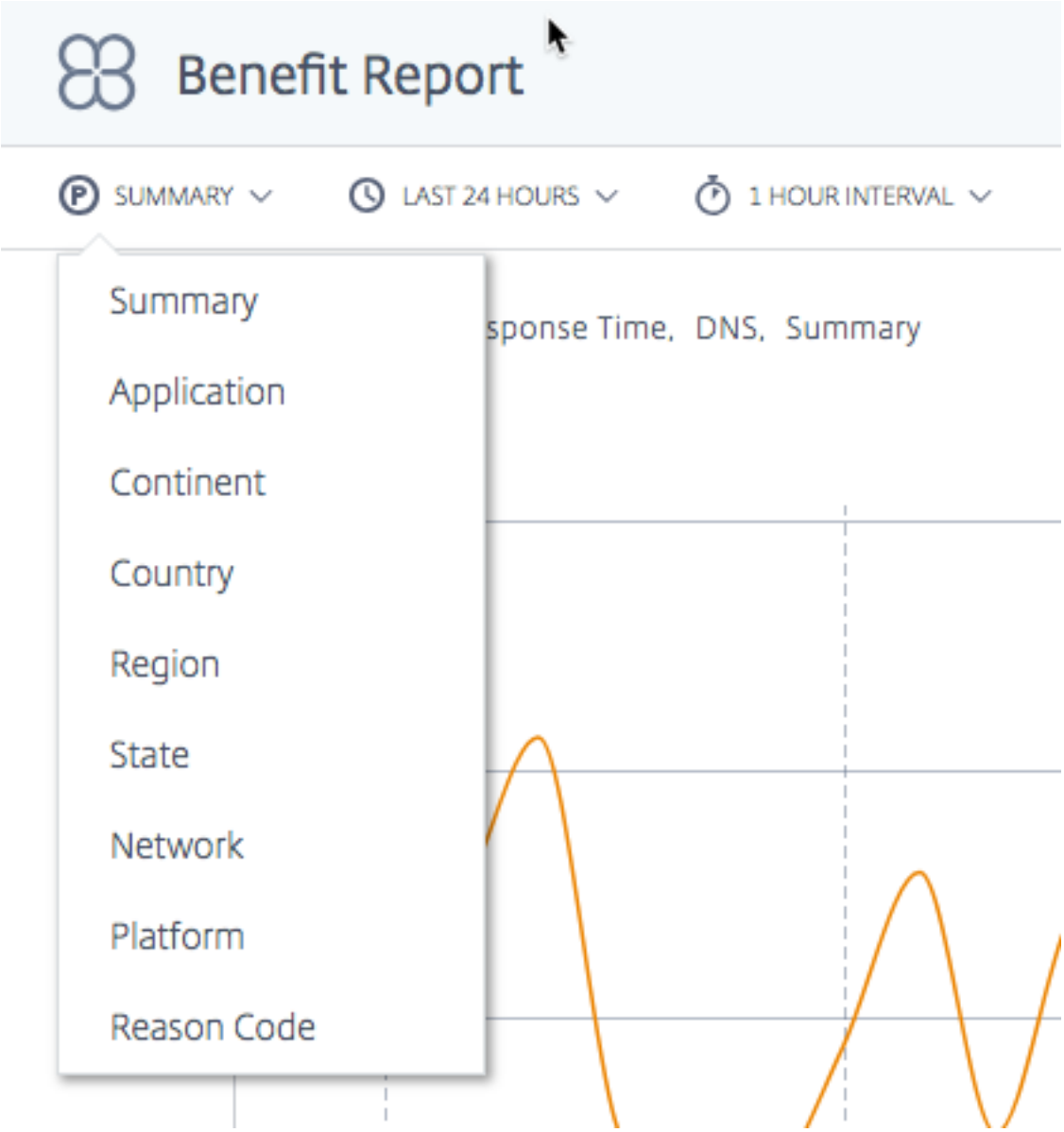
Das von Openmix erstellte Entscheidungsprotokoll kann gesammelt und zum sicheren Download zur Verfügung gestellt werden. Diese Protokolle können Ihnen helfen, die von Ihrer Openmix-Anwendung getroffenen Entscheidungen zu analysieren und das Verhalten von Anfragen zu debuggen. Die Protokolle können auf Kontoebene ein- und ausgeschaltet werden. Einzelheiten zum Aktivieren und Herunterladen von Openmix-Protokollen sowie zu diesen Protokollbeschreibungen finden Sie unter Netscope.



Openmix-Berichte

Openmix-Berichte bieten einen starken Einblick in die Openmix-Entscheidungen, die für Ihren DNS- oder HTTP-Datenverkehr getroffen wurden. Jeder Bericht wird im folgenden Abschnitt definiert, aber hier sind einige wichtige Aspekte der Berichte:

Primäre und sekundäre Dimensionen



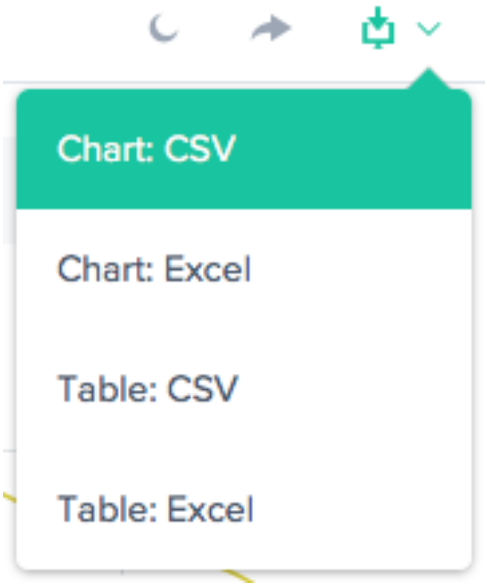
Die primäre Dimension des Diagramms wird über eine Liste oberhalb des Diagramms ausgewählt. Verwenden Sie diese Liste als leistungsfähigen Drehpunkt für den Bericht. Eine sekundäre Dimension kann ebenfalls gewählt werden, um das Reporting weiter zu verfeinern.

Visualisierungshintergrund

Diagramme sind standardmäßig auf einen weißen Hintergrund eingestellt. Schalten Sie den Hintergrund bei Monitoren mit hohem Kontrast mithilfe der Hintergrund-Umschalttaste auf eine dunkle

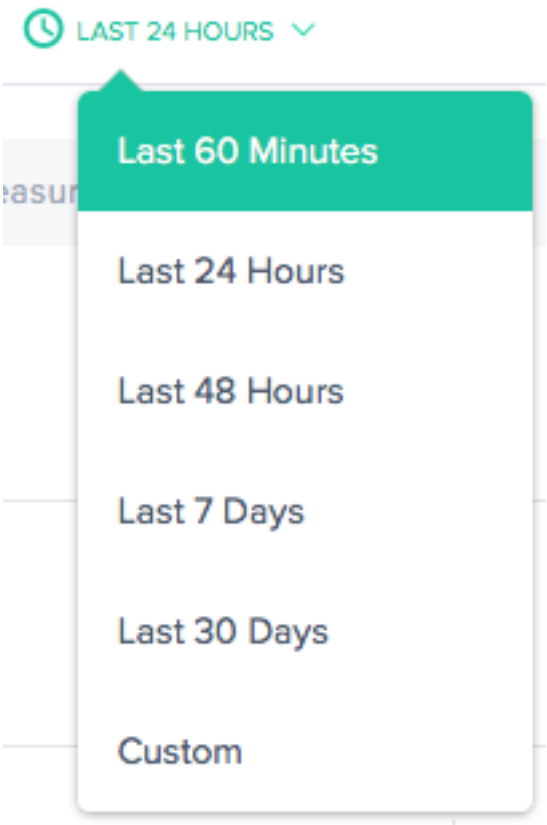
Farbe um.

Daten-Export



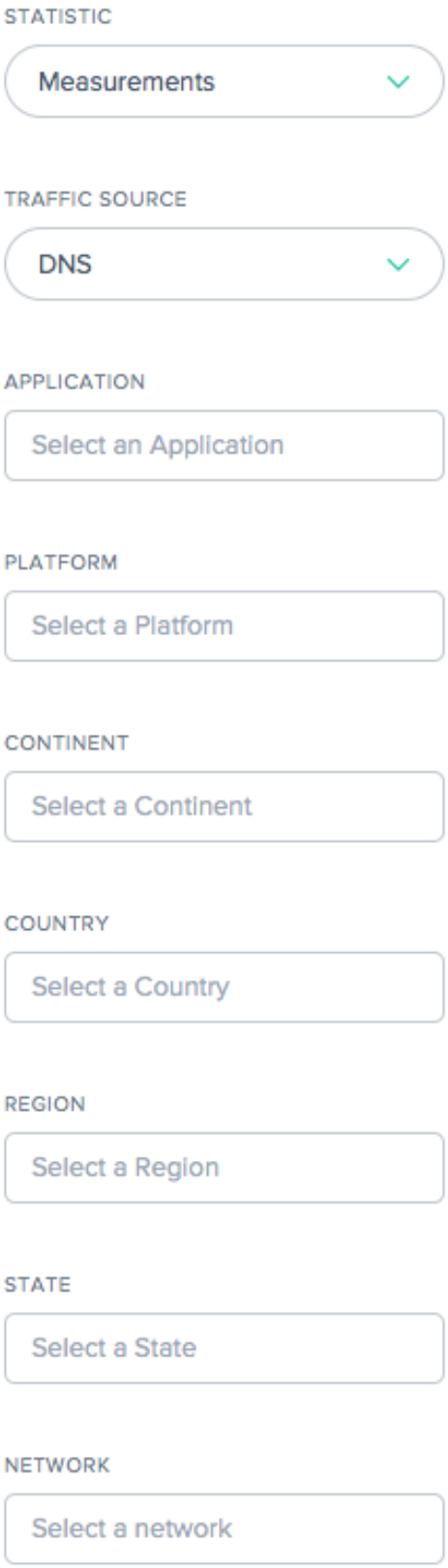
Darüber hinaus kann der Endbenutzer die Diagramm- und Tabellendaten über den Download-Link oben im Bericht herunterladen.

Filter: Berichts-Zeitbereich



Sie können einen Bericht mit einem Zeitraum von 60 Minuten, 24 Stunden, 48 Stunden, 7 Tagen, 30 Tagen oder einem benutzerdefinierten Bereich erstellen. Die Standardansicht ist die Letzte 24 Stunden.

Filter: Leistungsstarke Drilldown-Funktionen



Die Berichte unterscheiden sich geringfügig in Bezug darauf, welche Filter basierend auf den Daten geeignet sind. Die folgenden sind die häufigsten:

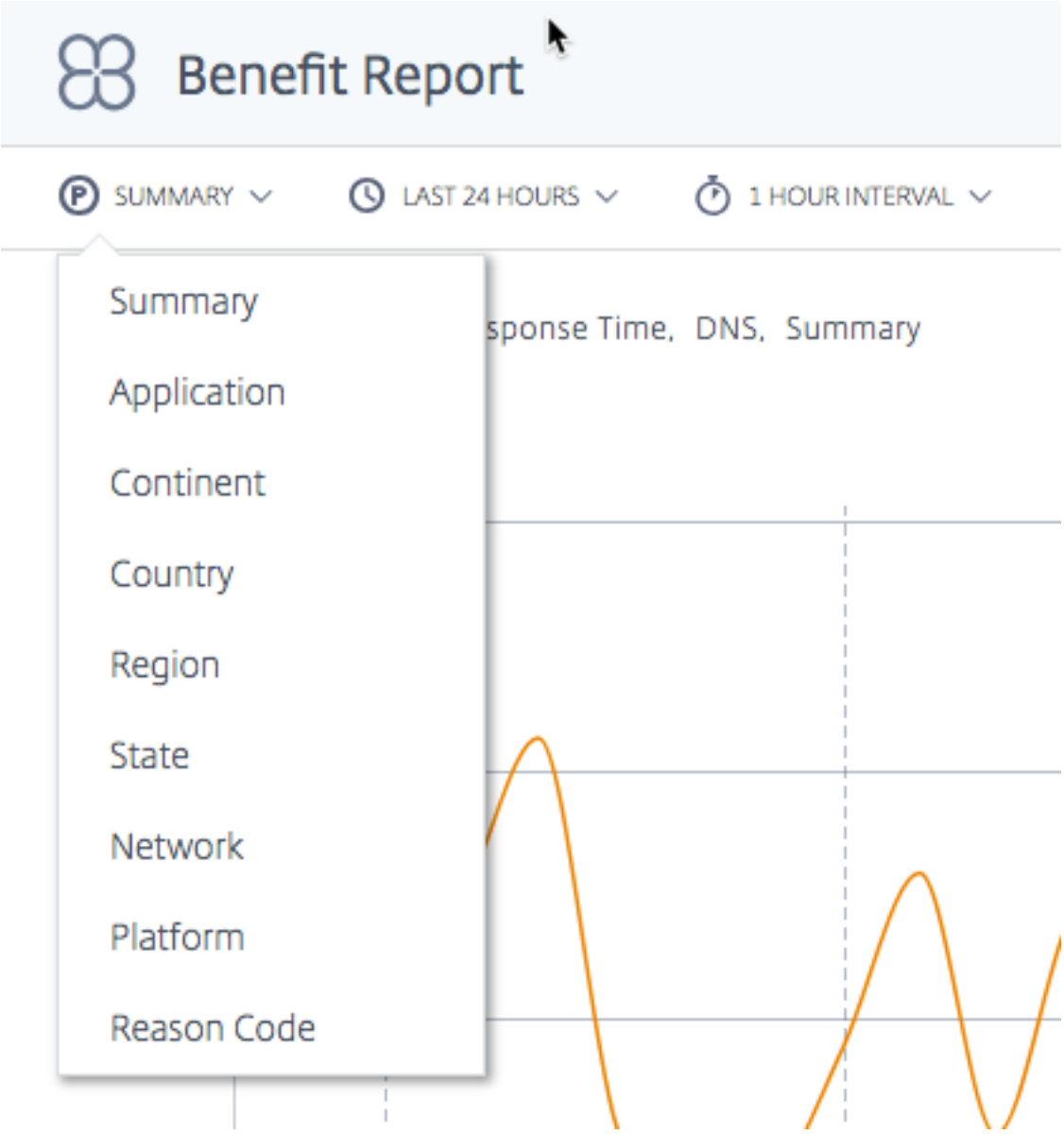
- **Statistik** - Wählen Sie den im Diagramm angezeigten Wert aus, meistens die Anzahl der Entscheidungen.
- **Traffic-Quelle** —Wählen Sie die Art des anzuzeigenden Datenverkehrs aus: DNS oder HTTP.
- **Anwendung** —Wählen Sie eine oder mehrere Openmix-Anwendungen zur Anzeige aus.
- **Plattform** —Wählen Sie eine oder mehrere Plattformen (Anbieter) aus, die einbezogen werden sollen.
- **Kontinent** —Wählen Sie einen oder mehrere Kontinente aus, die eingeschlossen werden sollen
- **Land** —Wählen Sie ein oder mehrere Länder aus, die einbezogen werden sollen.
- **Region** —Wählen Sie eine oder mehrere geografische Regionen (falls zutreffend), die einbezogen werden sollen.
- **Bundesstaat** —Wählen Sie einen oder mehrere geografische Staaten (falls zutreffend) aus, die eingeschlossen werden sollen.
- **Netzwerk** —Wählen Sie ein oder mehrere Netzwerke (ASN) aus, die eingeschlossen werden sollen.

Bericht über Leistungen

Der Benefit-Bericht zeigt Ihnen die allgemeine Verbesserung der Leistung Ihrer Anwendungsbereitstellung, wenn Sie den NetScaler Intelligent Traffic Management (ITM) -Service verwenden. Der Vorteil zeigt sich in einer prozentualen Verbesserung der Reaktionszeit und des Durchsatzes. Wählen Sie eine bestimmte Plattform aus dem Pool der Kandidatenplattformen aus, um den Bericht zu erstellen.

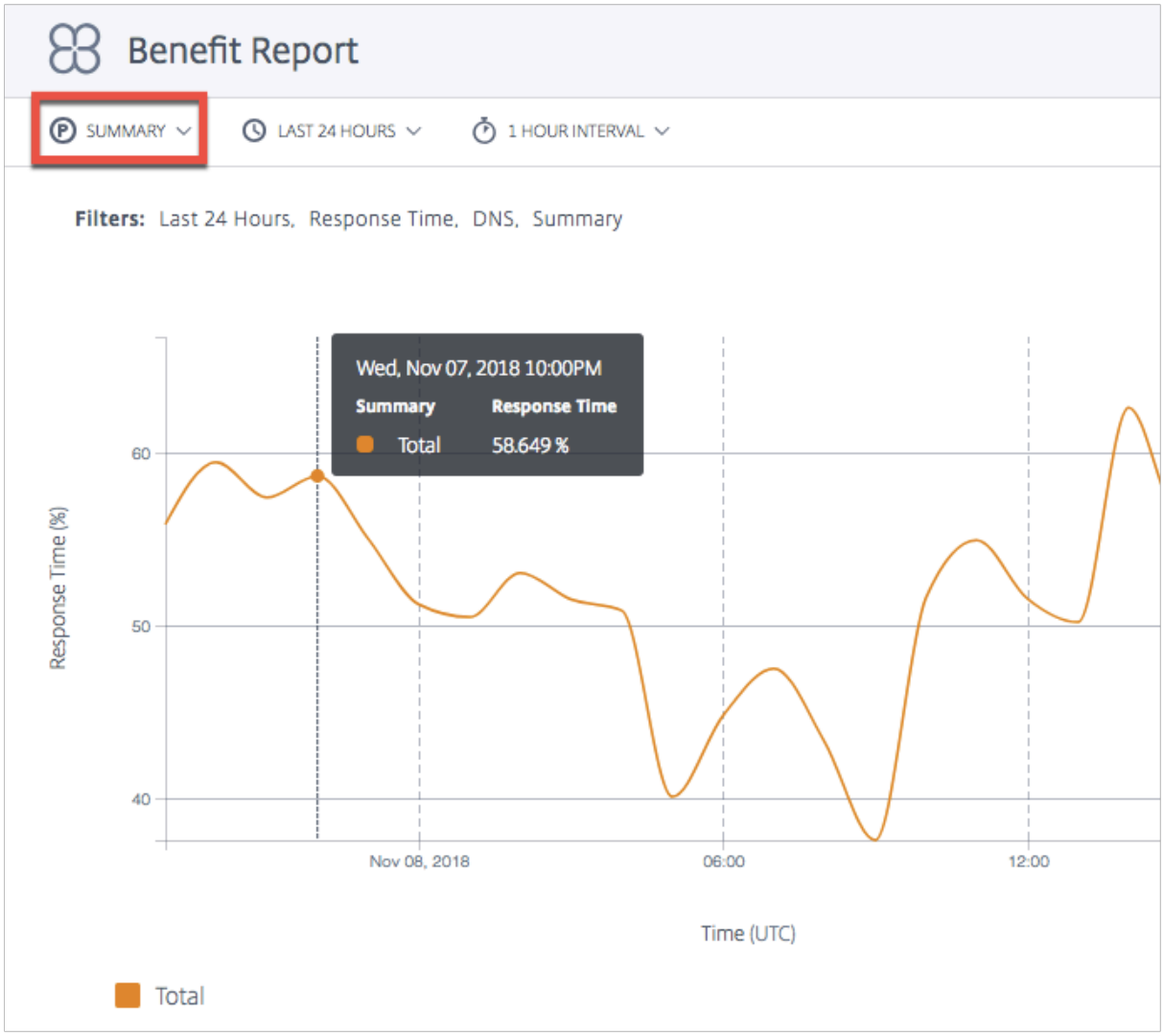
Primäre Dimensionen für den Leistungsbericht

Primäre Dimensionen sind unabhängige Kennzahlen, auf deren Grundlage der Nutzenbericht angezeigt wird. In den folgenden Abschnitten wird jede dieser primären Dimensionen detailliert beschrieben.



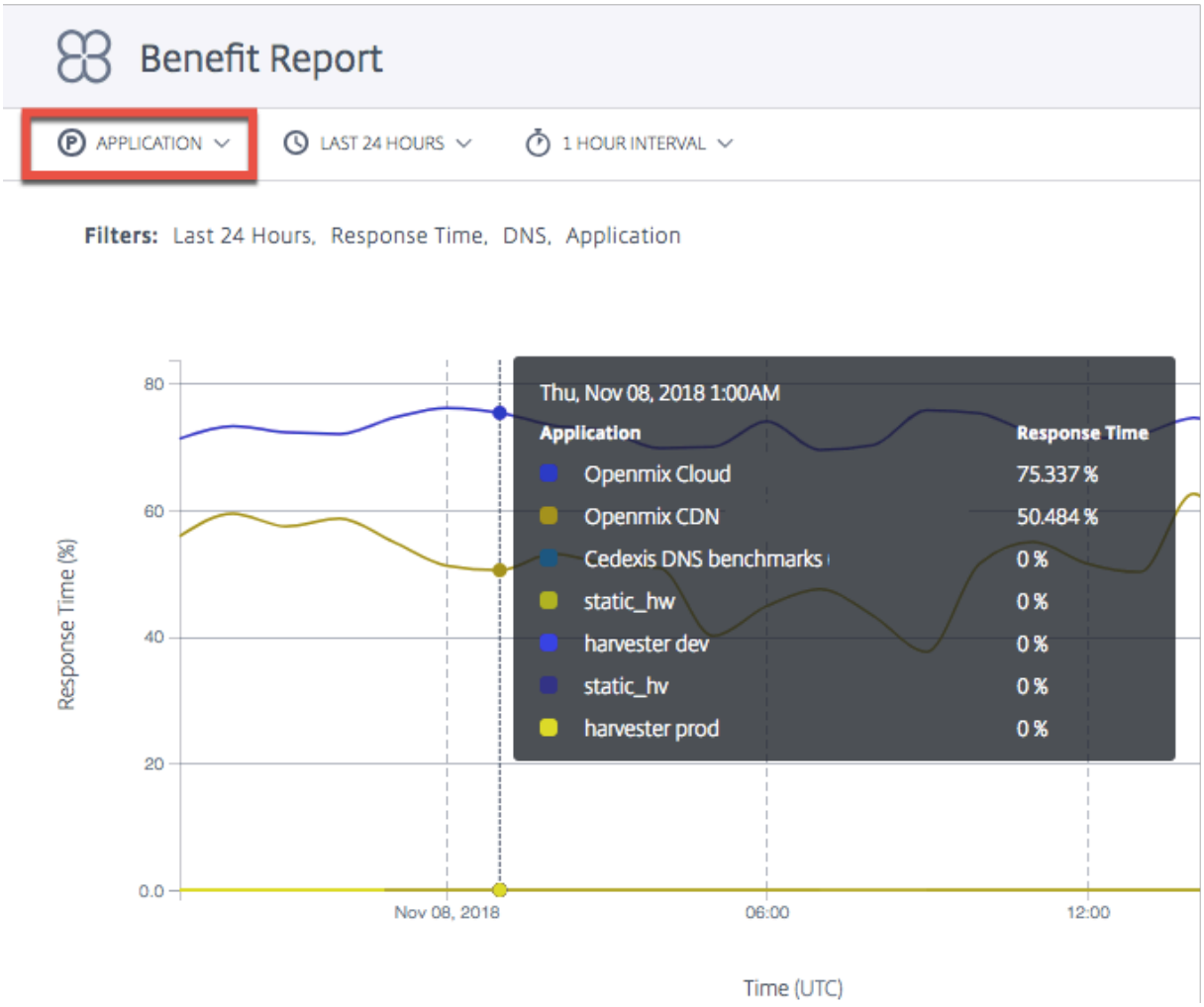
Zusammenfassung **Zusammenfassung** ist die standardmäßige primäre Dimension. Das Übersichtsdiagramm zeigt den Durchschnitt des gesamten prozentualen Nutzens (in Bezug auf Reaktionszeit oder Durchsatz), der von allen Anwendungen erhalten wurde.

Hinweis: Mithilfe des **Statistikfilters** können Sie zwischen dem in Bezug **auf Reaktionszeit** oder **Durchsatz** angezeigten Vorteil wechseln.



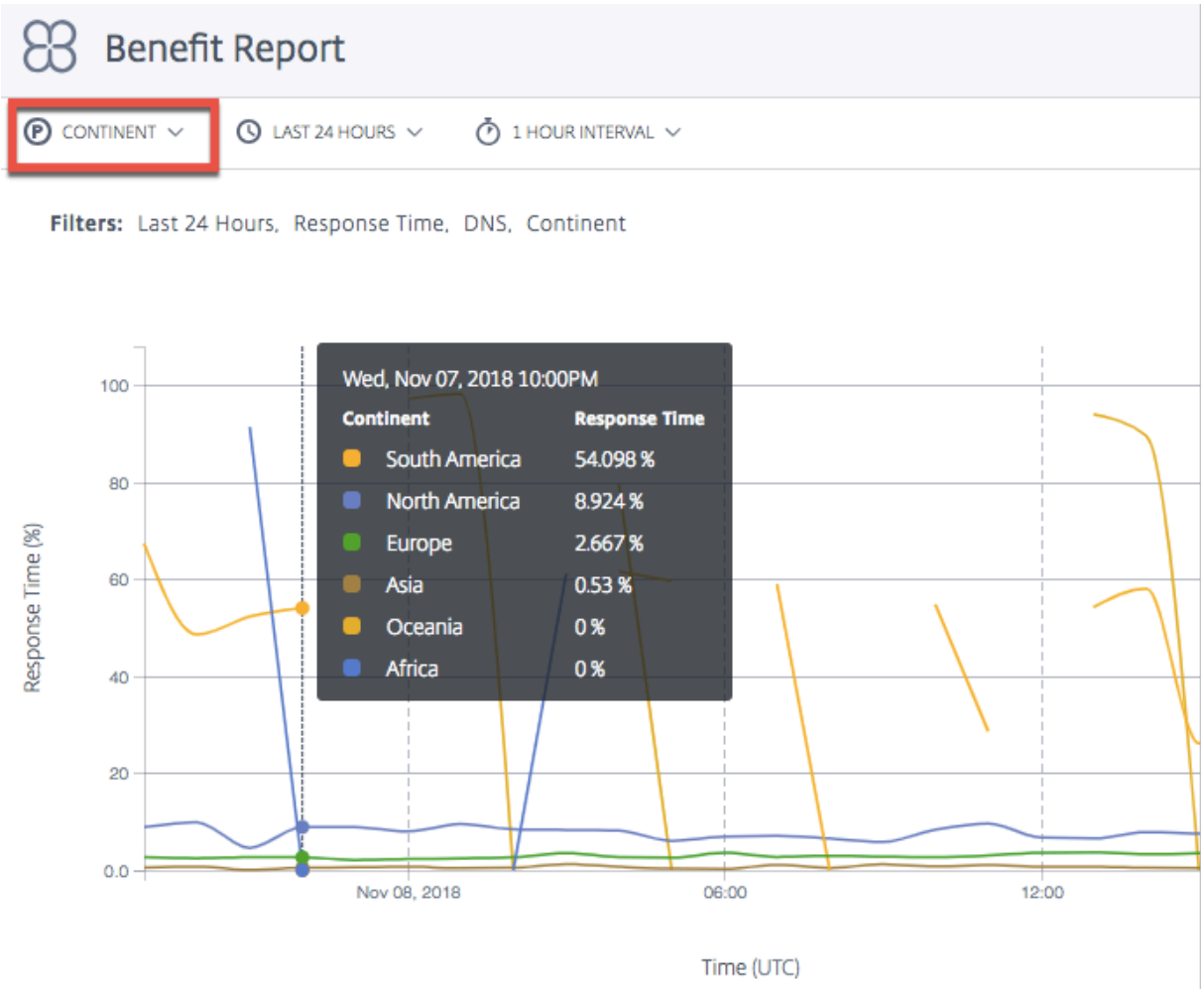
Anwendung Wenn **Anwendung** als primäre Dimension ausgewählt wird, zeigt das Diagramm jede der Anwendungen und die entsprechende Leistung (in Bezug auf Reaktionszeit oder Durchsatz) als prozentualen Vorteil bei der Auswahl einer bestimmten Plattform gegenüber anderen Kandidatenplattformen.

Hinweis: 0% bedeutet, dass es keinen zusätzlichen Nutzen oder keine Verbesserung bei der Auswahl einer bestimmten Plattform gegenüber einer anderen gab.

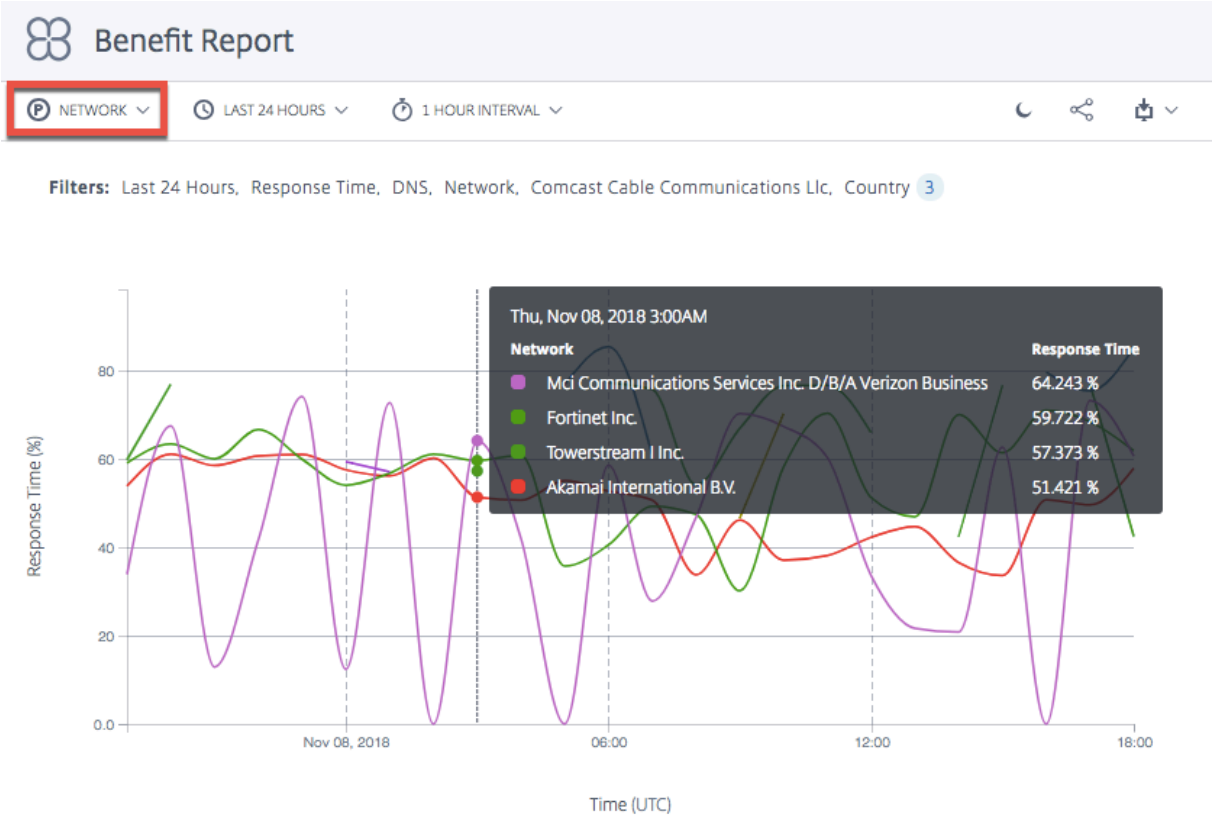


Standort (Kontinent, Land, Region, Bundesland) Wenn Standort (**Kontinent**, **Land**, **Region**oder **Bundesland**) als primäre Dimension ausgewählt wird, zeigt der Nutzenbericht den Durchschnitt der gesamten prozentualen Leistungsverbesserung (in Bezug auf Reaktionszeit oder Durchsatz) für jeden Standort an. Sie können den Standort nach Kontinent, Land, Region oder Bundesstaat auswählen.

Hinweis: Plattformen, die aufgrund von Georegeln oder aus anderen Gründen nicht ausgewählt werden können, werden bei der Berechnung nicht berücksichtigt. Plattformen, die für den betreffenden Standort geografisch eingezäunt sind, werden jedoch gezählt.

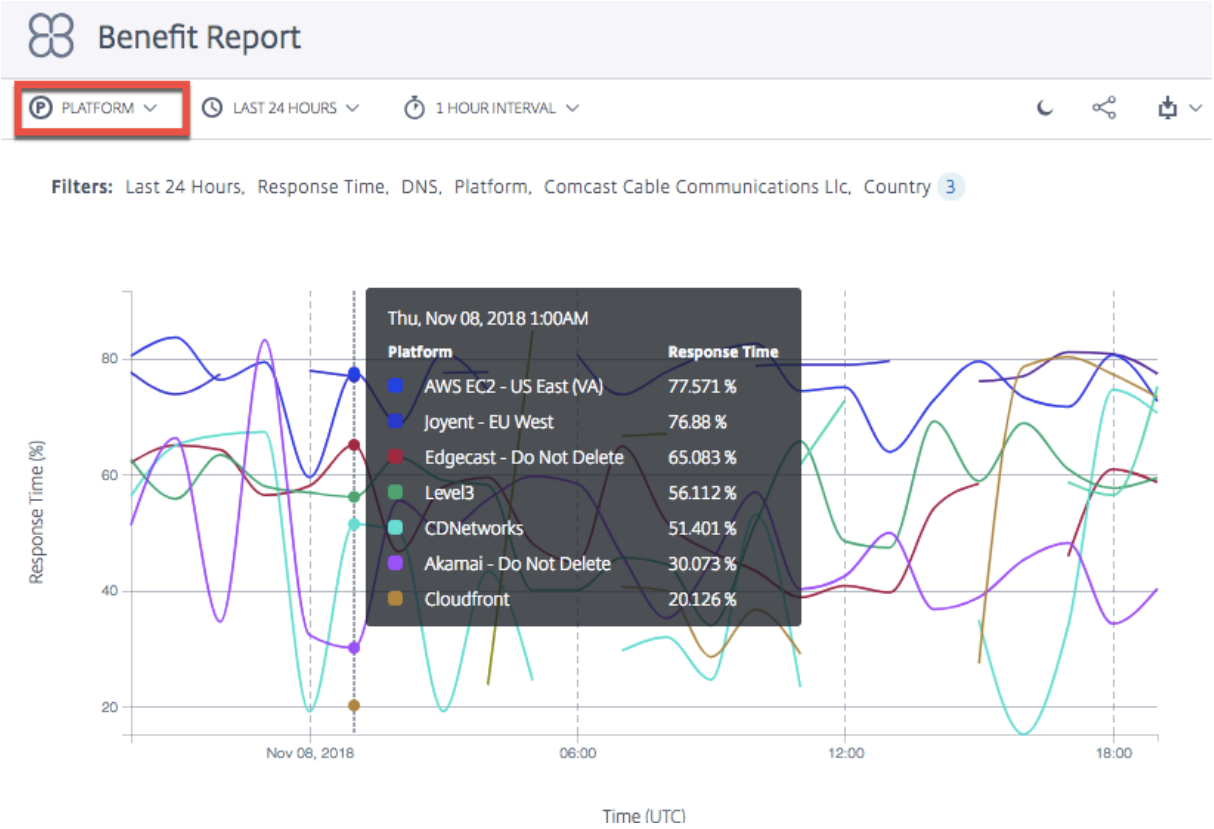


Netzwerk Wenn Sie **Netzwerk** als primäre Dimension auswählen, sehen Sie die prozentuale Verbesserung der Leistung für Benutzer, die in den spezifischen Netzwerken (oder Dienstanbietern) gruppiert sind, von denen aus Benutzer auf ITM zugreifen. Es hilft Ihnen zu erkennen, welche Benutzergruppen den Leistungsvorteil sehen, wenn sie aus diesen spezifischen Netzwerken kommen.

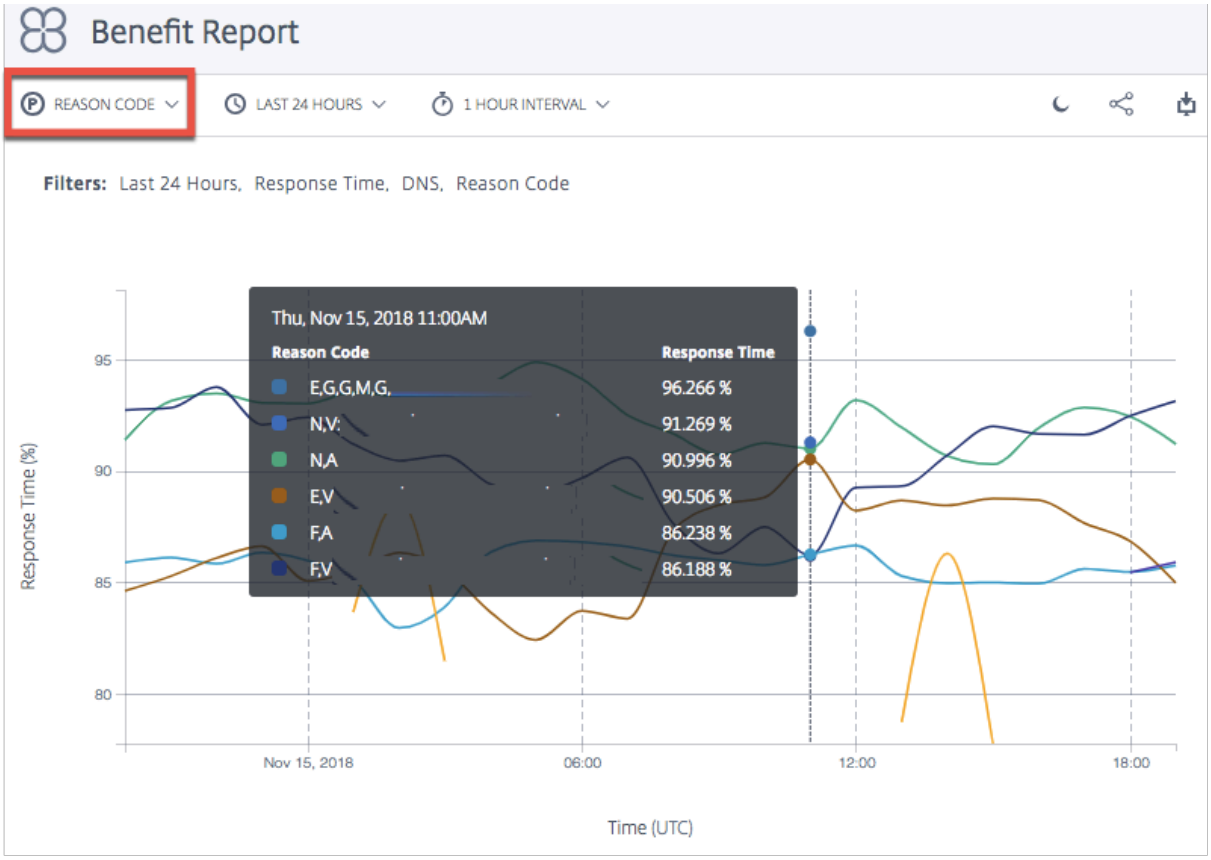


Plattform Wenn Sie **Plattform** als primäre Dimension auswählen, sehen Sie einzelne Plattformen, die von verschiedenen Apps ausgewählt wurden, und die entsprechend verbesserte Leistung, wenn sie ausgewählt werden. Die verbesserte Leistung oder der Nutzen ergibt sich aus der Reaktionszeit oder dem Durchsatz (in Prozent).

Hinweis: Die prozentuale Leistungssteigerung, die angezeigt wird, wenn eine App diese Plattform auswählt. Die Liste in der Tabelle zeigt nicht unbedingt ein Leistungsranking zwischen diesen Plattformen an.



Ursachencode Wenn Sie **Ursachencode** als primäre Dimension auswählen, entspricht der im Diagramm angezeigte Prozentsatz dem durchschnittlichen Gesamtnutzen, wenn Entscheidungen für einen bestimmten Ursachencode getroffen werden.



Plattformen im Leistungsbericht ignorieren

Um die Genauigkeit der **Openmix-Entscheidungen** für Ihren Nutzungsbericht zu verbessern, können Sie bestimmte Plattformen ignorieren und die App so einstellen, dass nur Plattformen ausgewählt werden, die für den Vergleich am besten geeignet sind.

Beispielsweise verfügt Ihre Anwendung über fünf Plattformen, die zum Vergleich berücksichtigt werden müssen - drei in Europa für den europäischen Verkehr und zwei in den USA für den US-Verkehr. Geo-Regeln legen fest, dass der europäische Verkehr über die europäischen Plattformen und der US-Verkehr über die US-Plattformen erfolgen muss.

Um sicherzustellen, dass die Berechnung über die drei europäischen Plattformen erfolgt, können Sie die App so einstellen, dass die anderen beiden außereuropäischen Plattformen ignoriert werden. Verwenden Sie die Methode `ignoredProvider()` in Ihrem JavaScript.

Die Methode verwendet den Alias des Anbieters (z. B. `provider-1`, `provider-2`) als Eingabeargument (ähnlich wie die requireProvider()-Methode). Die API muss einmal pro Alias aufgerufen werden.

Verwenden Sie diesen Beispielcode in Ihrer JavaScript-Datei innerhalb der Funktion `onRequest`:

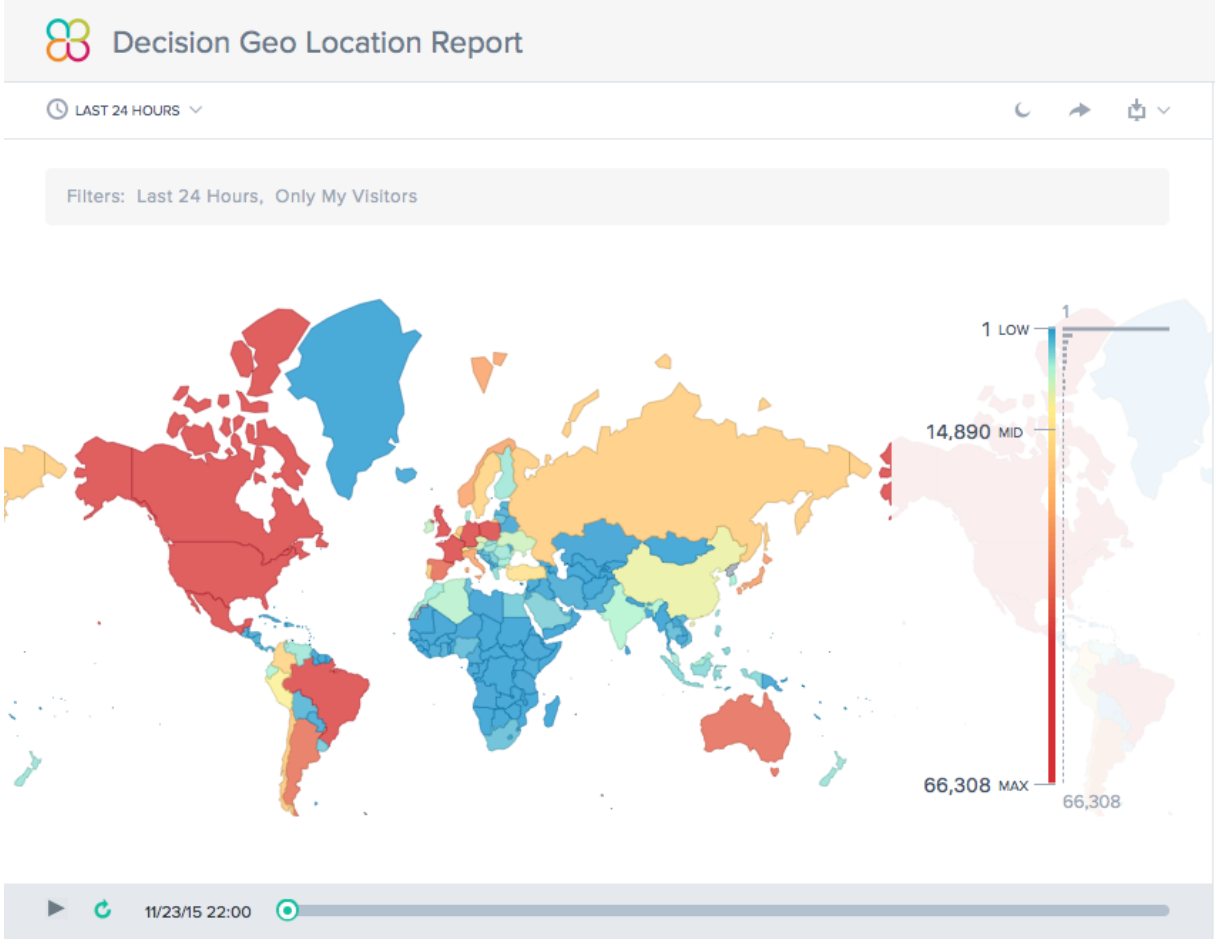

```
function onRequest(request, response) {

  response.ignoredProvider('provider-1');
  response.ignoredProvider('provider-2');
  response.setReasonCode('Ignoring provider-1 and provider-2');
  response.setTTL(this.__defaultTTL);
  response.respond('provider-3', 'cmg.test.fake.cname');
 }

<!--NeedCopy-->
```

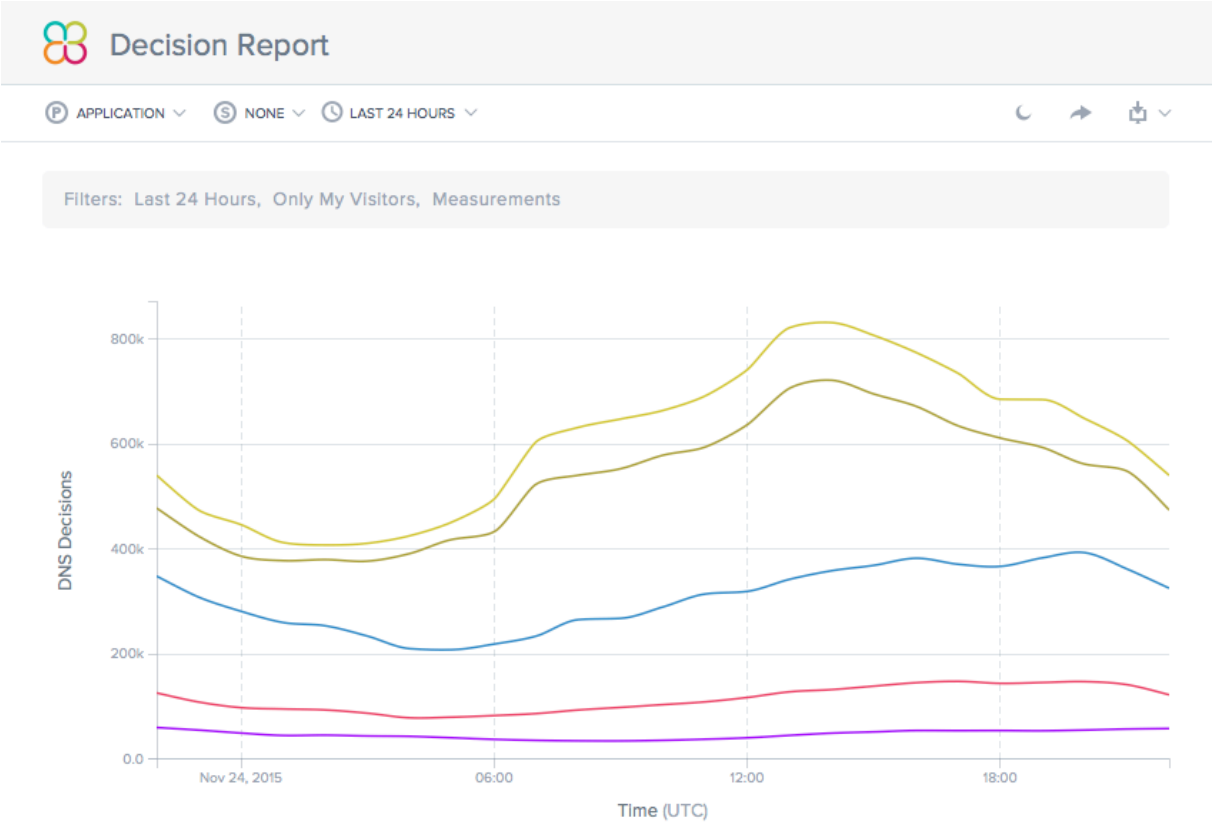
Geolokalisierungsbericht zur Entscheidung

Dieser Bericht zeigt das Volumen der Openmix-Entscheidungen für jedes Land. Diese Kartenansicht kann im Laufe der Zeit (basierend auf dem für den Bericht ausgewählten Zeitraum) angezeigt werden, indem Sie unten im Diagramm auf die Schaltfläche **Abspielen** klicken.



Entscheidungsbericht

Dieser Bericht zeigt den Trend der Openmix-Entscheidungen für jede der Anwendungen, Plattformen und Regionen.



Predictive DNS

September 14, 2023

Übersicht

Predictive DNS ist eine autoritative DNS-Plattform, die auf maschinellem Lernen basiert und Ihre Zonen verwaltet und Routing-Entscheidungen auf der Grundlage der Dienstverfügbarkeit in Echtzeit trifft. Es ist hochverfügbar und verfügt über mehrere Anycast-Netzwerke, die flexible und zuverlässige Routing-Regeln bieten. Es handelt sich um ein Unternehmensangebot für anspruchsvolle DNS-Kunden, die Wert auf die Qualität ihres DNS-Entscheidungsprozesses legen. Es richtet sich an Kunden, die eine datengesteuerte, intelligente, globale Verkehrsmanagementrichtlinie auf einer robusten und leistungsstarken Infrastruktur anwenden müssen.

Predictive DNS unterstützt die Erstellung primärer und sekundärer Zonen. Der Zonenimport wird auch mit den am häufigsten verwendeten Datensatztypen wie A (IPV4-Version), AAAA (IPV6-Version), NS, SOA, CNAME, MX, PTR, SRV, SPF und TXT unterstützt. Wir unterstützen Openmix-Kunden auch mit einer nahtlosen Integration über Openmix App Records. Eine beliebige Anzahl von A/AAAA/CNAME-Datensätzen in einer Zone kann zu jedem Zeitpunkt vollständig OpenMix-intelligent gemacht werden. Kunden können Predictive DNS auch in einer dualen primären Umgebung ausführen, indem sie unsere API verwenden, um die Konfiguration voranzutreiben.

Höhepunkte der Integration von Predictive DNS und Openmix

1. Reibungsloser Übergang zwischen statischen Aufzeichnungen und ausgeklügelten, datengesteuerten Verkehrsmanagement-Richtlinien ohne Ausfallzeiten.
2. Vollständig konfigurierbare Richtlinien für das Verkehrsmanagement (Round-Robin, verteilt, geografisch, netzwerkbasiert usw.).
3. Es wurde ein Echtzeit-Datenbewusstsein für den globalen Internetverkehr, den Zustand der Endgeräte, den Status der Infrastruktur, den Status von Drittanbietern usw. hinzugefügt
4. Einfache Bereitstellung oder Änderung des Verkehrsmanagements.
5. Umfassende Analysen und Berichterstattung über Aktivitäten auf Anfrage.

Schritte zum Einrichten und Delegieren einer Zone

Bevor Sie sich beim NetScaler Intelligent Traffic Management Portal anmelden, finden Sie hier einige allgemeine Schritte, die Ihnen helfen sollen, zu verstehen, wie Sie eine Zone einrichten und delegieren.

Schritt 1: Definieren und erstellen Sie Ihre Zone

Erstellen Sie zunächst eine Zone mit demselben Namen wie der Domainname Ihres Unternehmens. Eine Zone steht für eine einzige übergeordnete Domain mit einer Sammlung von Datensätzen darin. Es enthält Informationen darüber, wie Sie den Verkehr für Ihre Domain und ihre Subdomains weiterleiten möchten. Wenn Sie eine Zonendatei von Ihrem aktuellen DNS-Anbieter haben, importieren Sie sie. Mit einer importierten Zonendatei können Sie schnell alle Datensätze für Ihre Zone erstellen.

Schritt 2: Fügen Sie Ihre Datensätze hinzu und testen Sie sie

Sie können entweder manuell Datensätze auf der Predictive DNS-Konsole im NetScaler Intelligent Traffic Management Portal erstellen, oder Sie können eine Zonendatei mit all ihren Einträgen importieren. Wenn Sie eine Zonendatei importieren, repliziert Predictive DNS Ihre ursprüngliche Zonendefinition und migriert alle vorhandenen Einträge darin.

Sie können Zonen und Datensätze auch programmgesteuert mithilfe der Predictive DNS-API erstellen. Die API finden Sie im Portal unter **Meine Konten > API > Konfiguration > authdns**.

Openmix-Kunden können eine bestehende Openmix-Anwendung über den Openmix-App-Datensatztyp einem CNAME- oder A/AAAA-Datensatz zuordnen. Eine beliebige Anzahl von A/AAAA/CNAME-Datensätzen in einer Zone kann zu jedem Zeitpunkt vollständig OpenMix-intelligent gemacht werden.

Um die Einträge in Ihrer Zone zu testen, können Sie ein Tool namens dig verwenden, das DNS-Server direkt abfragt. Führen Sie dig mit Ihrem Zonennamen als Parameter aus.Zum Beispiel:

```
dig @ns1.ourdomain.net NS mydomain.com
```

```
dig @ns1.ourdomain.net A host.mydomain.com
```

Der `@ns1.ourdomain.net` weist dig an, eine Anfrage an die DNS-Infrastruktur von NetScaler Intelligent Traffic Management zu stellen, und der Eintragstyp (NS oder A) gibt an, nach welchem Datensatz gefragt werden soll. Der NS-Befehl würde nach den NS-Datensätzen für die `mydomain.com` Zone fragen, und der zweite Befehl `@ns1.ourdomain.net A host.mydomain.com` wäre ein A-Eintrag für den Host in der `mydomain.com` Zone.

Schritt 4: Weisen Sie NetScaler Intelligent Traffic Management als autorisierendes DNS zu, indem Sie Ihre Nameserver aktualisieren

Um uns als autoritatives DNS für die Verwaltung Ihres Domainnamens zuzuweisen, aktualisieren Sie die Nameserver, die für die Beantwortung Ihrer DNS-Anfragen an unsere Nameserver verantwortlich sind. Der neue NetScaler ITM-Nameserver antwortet dann autoritativ für Ihr Unternehmen.

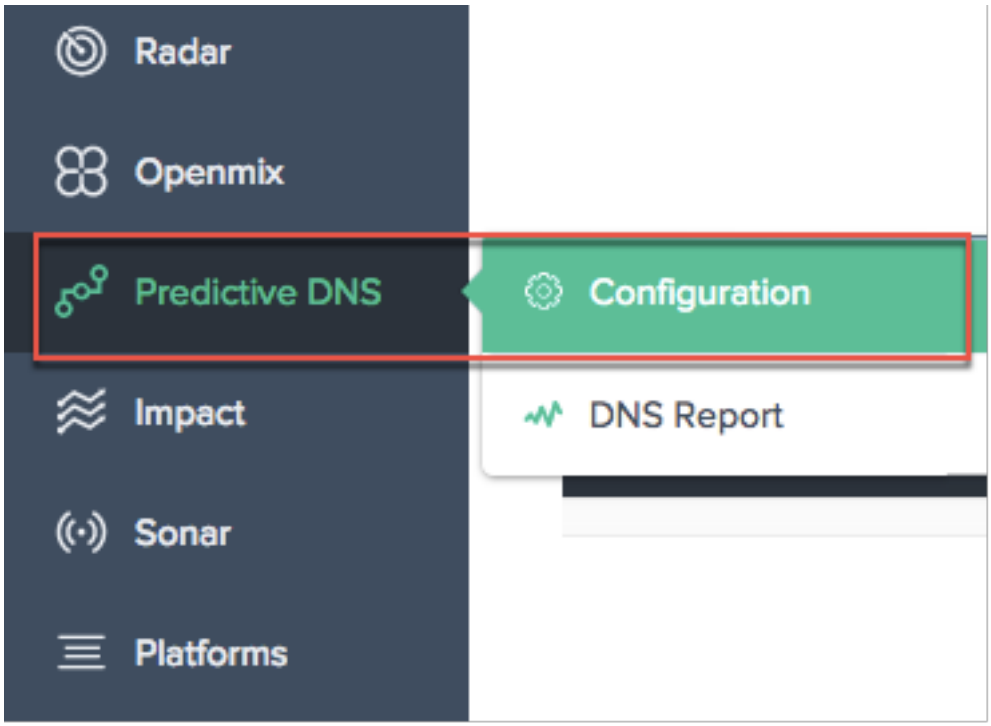
Schritt 5: Überprüfen Sie den Verkehrsfluss angemessen

Anfänglich wird je nach Länge der TTL im vorherigen System Datenverkehr zwischen beiden Systemen (Ihrem vorherigen DNS-Dienst und Citrix Predictive DNS) ausgeführt. Es kann eine Weile dauern, bis der Verkehr vollständig migriert ist. Wenn bei der Migration Fehler auftreten, kehren Sie zu den Nameservern zurück, die von Ihrem vorherigen DNS-Dienst bereitgestellt wurden, und ermitteln Sie dann, was schief gelaufen ist. Wenn Sie sehen, dass der Datenverkehr wie erwartet fließt, haben Sie erfolgreich zu Citrix Predictive DNS migriert. Die Standard-TTL ist hier 3600 Sekunden. Möglicherweise möchten Sie die TTL zunächst verringern, bis Sie sichergestellt haben, dass die Migration erfolgreich ist. Sobald Sie mit dem Verkehrsfluss zufrieden sind, können Sie die TTL gegebenenfalls auf eine längere Dauer erhöhen.

Navigation

Gehen Sie wie folgt vor, um zur Predictive DNS-Konsole zu navigieren:

1. Melden Sie sich beim NetScaler Intelligent Traffic Management Portal an.
2. Wählen Sie im linken Navigationsmenü **Predictive DNS > Konfiguration**.



Dadurch gelangen Sie zur Seite **Zone hinzufügen**, auf der Sie mit der Erstellung Ihrer Zone beginnen können.

Primäre und sekundäre Zonen

Eine Zone stellt eine einzelne übergeordnete Domäne mit einer Sammlung von Datensätzen dar. Sie können Ihre Zone in Predictive DNS entweder als primäre oder als sekundäre Zone einrichten. Primäres und sekundäres DNS sind eine Möglichkeit, Redundanz im DNS zu schaffen. Primary wird manchmal Master genannt, während Secondary Slave genannt wird. Dies liegt daran, dass die Primärkopie über die Masterkopie der Zonendaten verfügt, während die Sekundärseite diese Daten nur durch Zonenübertragungen in regelmäßigen Intervallen oder auf Aufforderung durch die Primärseite klont.

Dieser Vorgang wird oft auch als Zonenübertragung oder AXFR-Übertragung bezeichnet. Wenn Sie Ihre primäre Zone mit aktivierten Zonenübertragungen einrichten, werden alle an der Zone vorgenommenen Änderungen automatisch auf alle Ihre sekundären Server übertragen. Jede IP, die als sekundärer Server eingegeben wird, erhält dieses Update. In ähnlicher Weise können Sie auch eine sekundäre Zone einrichten.

Wenn Sie eine Zone erstellen, werden automatisch ein Nameserver-Datensatz (NS) und ein SOA-Eintrag (Start of Authority) für die Zone erstellt. Sie können die Predictive DNS-Benutzeroberfläche

verwenden, um Zonen hinzuzufügen, zu bearbeiten, zu duplizieren oder zu löschen.

Hinweis: Diese Operationen (Bearbeiten, Duplizieren oder Löschen) wirken sich auf die gesamte Zone aus, einschließlich aller Antworten für jeden Datensatz innerhalb der Zone. Sie müssen mit äußerster Vorsicht durchgeführt werden.

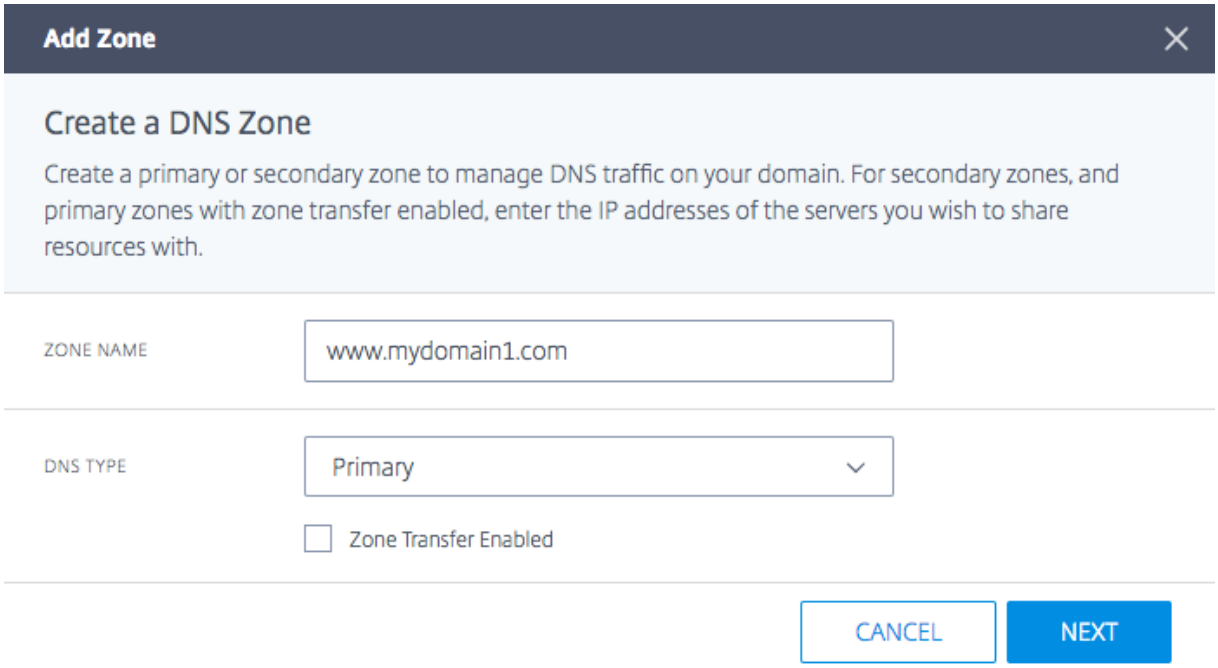
Zone hinzufügen

Um eine Zone hinzuzufügen oder zu erstellen:

1. Wenn dies Ihr erstes Mal ist, wird der Startbildschirm angezeigt, auf dem Sie auf **Zone hinzufügen** klicken können, um loszulegen.
2. Dadurch gelangen Sie zum Dialogfeld **Zone hinzufügen**, in dem Sie eine Zone für Ihre Domain erstellen können.

Wenn dies nicht Ihr erstes Mal ist, sehen Sie eine Liste der vorhandenen Zonen (Domainnamen), die für die Domänen in Ihrem Unternehmen erstellt wurden, sowie die Anzahl der Datensätze, die mit jeder dieser Zonen verknüpft sind.

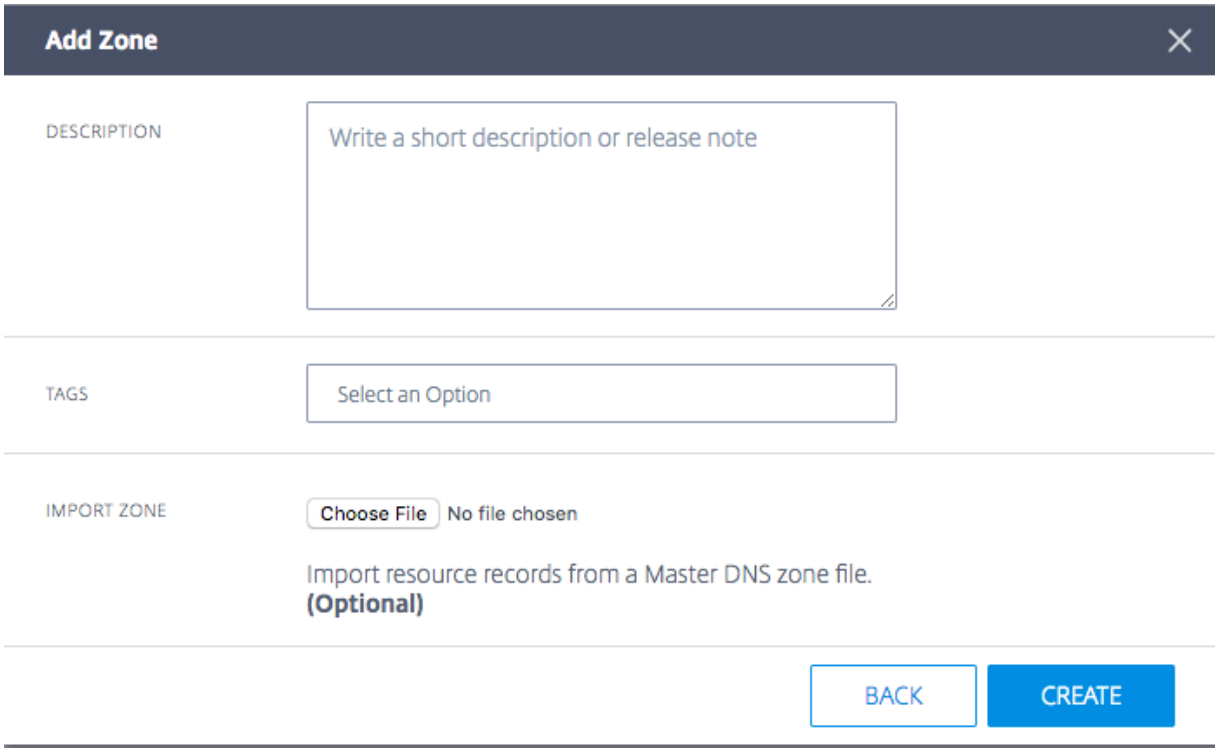
1. Klicken Sie oben rechts auf der Seite auf das Symbol Hinzufügen, um mit der Erstellung einer Zone zu beginnen.
2. Das Dialogfeld **Zone hinzufügen** wird geöffnet.



1. Geben Sie Ihren Domainnamen als **Zonennamen ein**. Zum Beispiel `www.mydomain.com`. Der Zonenname muss global eindeutig sein, was bedeutet, dass Sie keinen Zonennamen erstellen

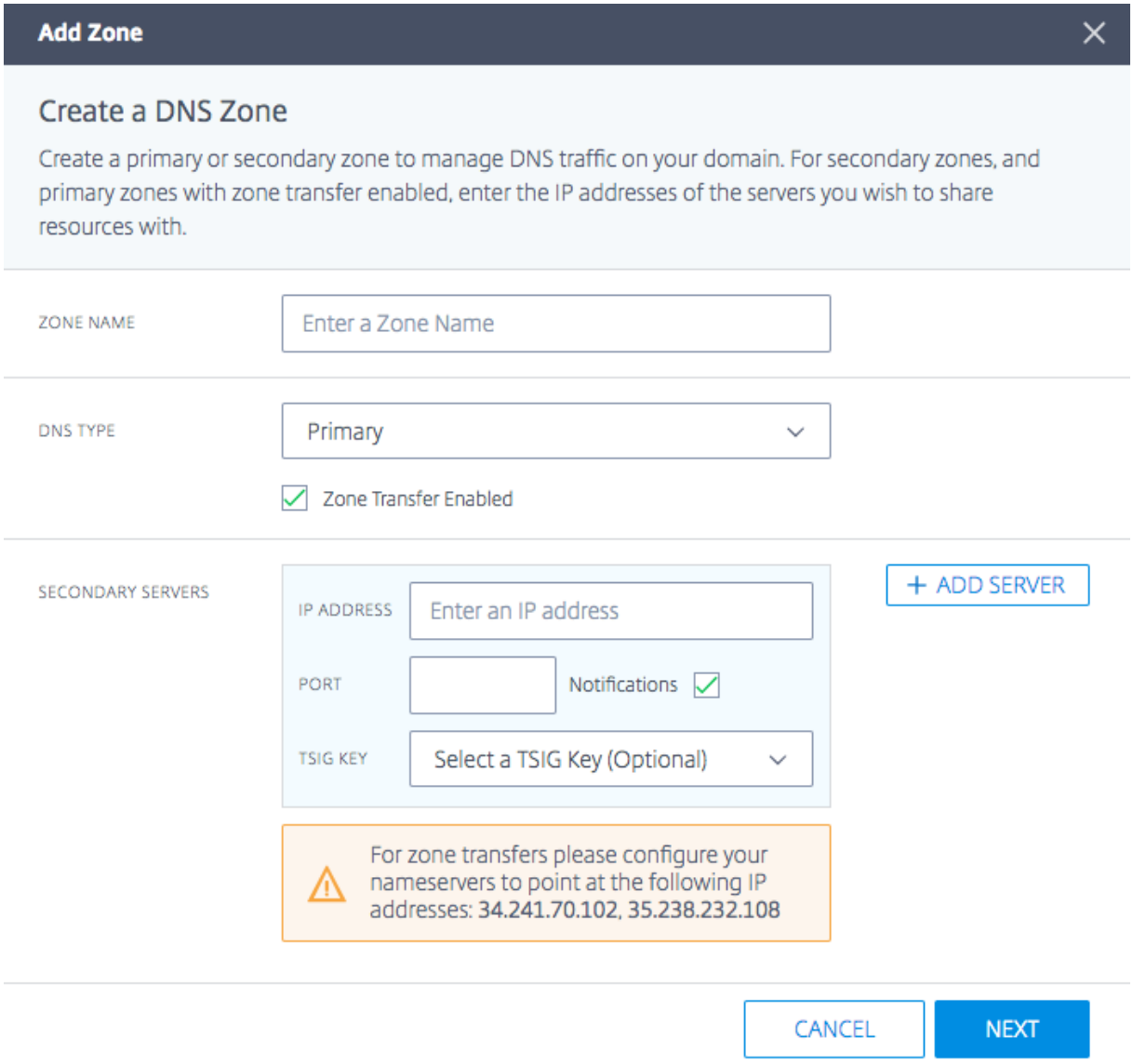
können, der bereits vorhanden ist oder sich auch nur teilweise mit einem vorhandenen Zonennamen überschneidet. Wenn es jedoch ein gültiges Szenario gibt, in dem Sie einen Zonennamen erstellen müssen, der sich möglicherweise mit einem vorhandenen überschneidet, oder wenn Sie keine Zone für eine Domain erstellen können, die Sie besitzen, wenden Sie sich an den Support.

2. Wählen Sie den **DNS-Typ** als **Primär** oder **Sekundär**aus.
3. Klicken Sie auf das Kontrollkästchen **Zonenübertragung aktiviert**, um die Zonenübertragung zu aktivieren, und geben Sie Informationen für den **Primär** - oder **Sekundärserver** ein. Einzelheiten finden Sie unter Serverinformationen .
4. Klicken Sie auf **Weiter**, um Zoneninformationen wie eine **Beschreibung** und **Tags**einzugeben.
5. **Wählen Sie Datei auswählen**, um eine Zonendatei von Ihrem Computer zu importieren (falls verfügbar).
6. Klicken Sie auf **Erstellen**, um das Hinzufügen einer neuen Zone abzuschließen.



Wenn neue Zonen erstellt werden, werden sie in der Liste auf der Seite **Zonen** angezeigt.

Informationen zum Server



IP-Adresse Geben Sie die IP des primären oder sekundären Servers ein.

Port Geben Sie die dem Server zugeordnete Portnummer ein. Dies ist ein optionales Feld. Es ist nur für sekundäre Server konfigurierbar. Wenn das Feld leer gelassen wird, ist es standardmäßig 53.

Benachrichtigungen Aktivieren Sie Benachrichtigungen, indem Sie das Kontrollkästchen **Benachrichtigungen** aktivieren, wenn Sie möchten, dass Ihr primärer DNS den sekundären DNS benachrichtigt, wenn Updates erfolgen. Wenn das Kontrollkästchen deaktiviert ist, werden Updates von der Primärseite in regelmäßigen Zeitintervallen von 60 Minuten an die Sekundärseite gesendet.

Server hinzufügen Mit der Schaltfläche **Server hinzufügen** können Sie mehrere Server für Zonenübertragungen konfigurieren.

TSIG-Schlüssel Sie können einen **TSIG-Schlüssel** aus der Liste auswählen. Diese Liste enthält Schlüssel, die Sie im Abschnitt TSIG-Schlüssel erstellen und verwalten. Dies ist ein optionales Feld für mehr Sicherheit. Weitere Informationen finden Sie unter TSIG Keys .

Beschreibung Fügen Sie eine kurze Beschreibung oder einen Kommentar zu der Zone hinzu, die Sie erstellen möchten. Dies ist ein optionales Feld, das ausschließlich Ihren eigenen Anforderungen entspricht. Es hat keinerlei Auswirkungen auf die tatsächlichen DNS-Antworten.

Tags Mithilfe von Tags können Sie Ihre Zonen in einer Liste sortieren und filtern. Dies ist auch ein optionales Feld.

Zone importieren Wenn Sie eine Zonenimportdatei haben, die die Konfiguration für Ihre Zone enthält, kann sie hier importiert werden. Um eine Zonendatei zu importieren, erstellen Sie zunächst eine Zone mit demselben Namen wie die Datei, die Sie importieren. Die folgenden Anforderungen gelten für den Import:

- Der Name der Zone in der Zonendatei muss mit dem Namen der Zone übereinstimmen, die Sie erstellen.
- Die Zonendatei verwendet ein Standard-BIND-Format für Datensätze.
- Die importierte Datei muss ein RFC-definiertes Zonendateiformat haben.
- Sie können maximal 5000 Datensätze importieren. Wenn Sie mehr als die 5000 Datensätze importieren müssen, wenden Sie sich an den Support.

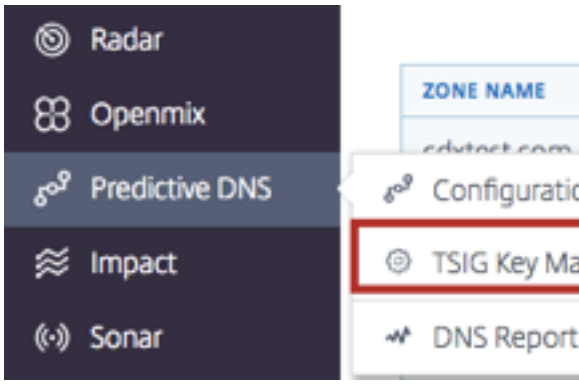
Gehen Sie wie folgt vor, um eine Zonendatei zu importieren:

1. Gehen **Sie im Dialogfeld Zone hinzufügen** zu **Zone importieren**.
2. Klicken Sie auf **„Datei auswählen**“.
3. Wählen Sie die Zonendatei aus, die Sie zum Füllen der Zone verwenden möchten.
4. Klicken Sie auf **Erstellen**, um den Vorgang abzuschließen.

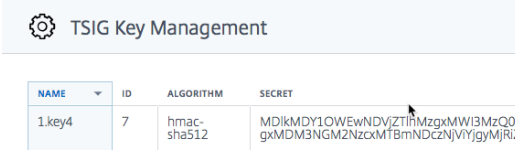
TSIG-Schlüssel

TSIG-Schlüssel bieten ein zusätzliches Maß an Sicherheit für den Informationsaustausch zwischen einem primären und einem sekundären Server. Das Geheimnis des Schlüssels muss auf beiden Servern (primär und sekundär) verfügbar sein, damit ein erfolgreicher Handshake stattfinden kann.

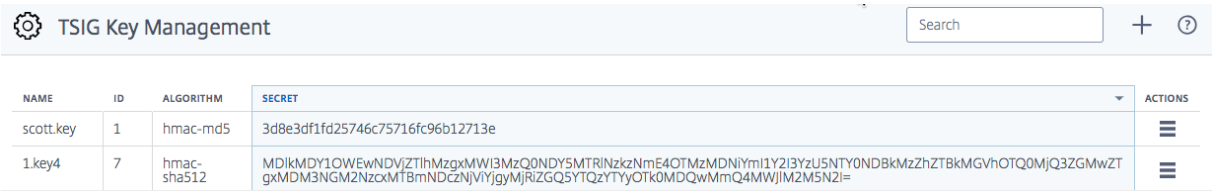
Gehen Sie wie folgt vor, um TSIG-Schlüssel zu generieren und zu verwalten:



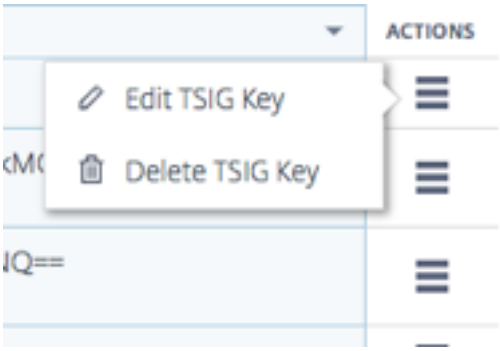
1. Wählen Sie im linken Navigationsmenü **Predictive DNS**aus.
2. Klicken Sie auf **TSIG Key Management**.
3. Die Seite TSIG Key Management wird geöffnet.



4. Klicken Sie oben rechts auf der Seite auf das Hinzufügen-Symbol.
5. Das Dialogfeld **TSIG-Schlüssel hinzufügen** wird geöffnet.
6. Geben Sie einen **Namen** für das TSIG ein.
7. Wählen Sie einen Algorithmus aus der Liste aus.
8. Für **Secret**haben Sie die Möglichkeit, ein beliebiges Wort oder einen Satz in das Feld einzugeben. Solange das, was Sie eingeben, 32 Zeichen (ohne Leerzeichen) lang und Base64-kodiert ist, wird es als solches akzeptiert. Andernfalls wird es gemäß dem von Ihnen ausgewählten Algorithmus gehasht. **Hinweis**: Die geheimen Werte und die Algorithmuswerte müssen zwischen dem primären und dem sekundären System übereinstimmen. Der Wert des Geheimnisses muss Base64-kodiert sein und eine Zeichenlänge von 32 Zeichen haben. Die Schaltfläche „Hash generieren“dient nur dazu, einen Hash zu generieren, falls noch keiner existiert.
9. Klicken Sie auf **Erstellen**, um die Generierung des Schlüssels abzuschließen. Das neu erstellte TSIG ist auf der Seite **TSIG Key Management** aufgeführt.

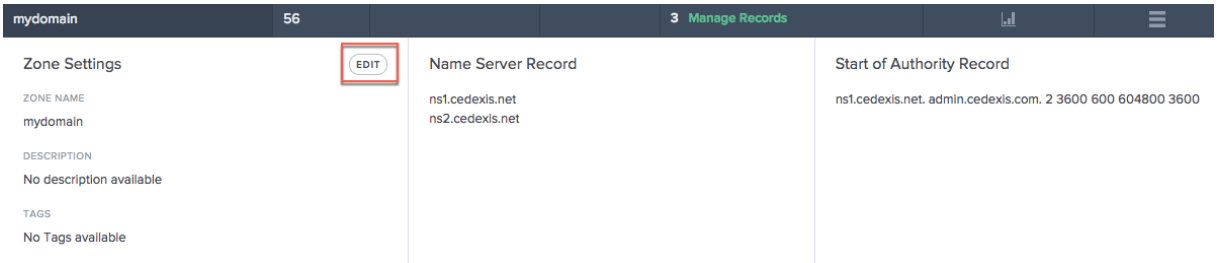


Um den **TSIG-Schlüssel** zu bearbeiten oder zu löschen, klicken Sie auf die Spalte **Aktionen** . Wählen Sie **Bearbeiten**, um den Schlüssel zu ändern, oder **Löschen**, um den Schlüssel zu entfernen.



Zone bearbeiten

1. Klicken Sie auf den Namen der Zone, die Sie bearbeiten möchten.
2. Die Bearbeitungsschublade wird geöffnet.
3. Klicken Sie auf die Schaltfläche **Bearbeiten**, um den Namen, die Beschreibung und die Tags der Zone zu ändern.
4. Klicken Sie auf **Save**, um die Änderungen zu speichern.

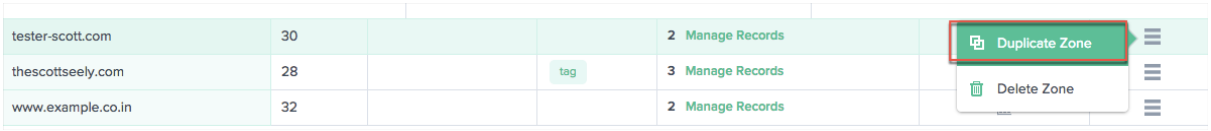


Wichtig: Seien Sie vorsichtig, wenn Sie einen Zonennamen bearbeiten. Da alle Datensätze in der Zone effektiv mit dem Zonennamen als Suffix versehen sind, ändert das Umbenennen einer Zone jede Anfrage.

Zone duplizieren

Beim Duplizieren einer Zone wird einfach eine weitere Zone mit Informationen aus einer vorhandenen Zone erstellt, jedoch mit einem anderen Zonennamen.

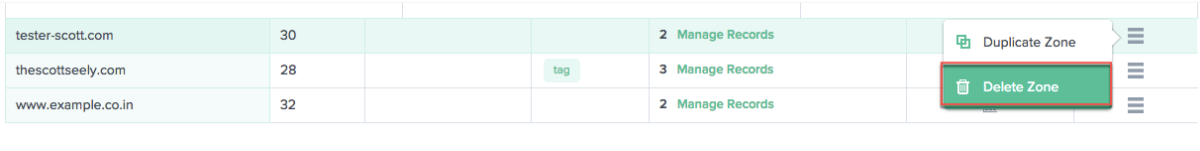
1. Um eine Zone zu duplizieren, klicken Sie auf das Symbol in der Spalte **Aktionen** .
2. Wählen Sie **Zone duplizieren**.
3. Das Dialogfeld **Zone hinzufügen** wird mit Informationen aus der ursprünglichen Zone geöffnet.
4. Geben Sie der Zone einen neuen Namen und ändern Sie alle Informationen, die Sie benötigen.
5. Klicken Sie auf **Erstellen**, um den Vorgang abzuschließen.
6. Eine neue Zone wird mit den Datensätzen und Informationen aus der ursprünglichen Zone erstellt.



Hinweis: Sie können alle Informationen innerhalb der neuen Zone nach eigenem Ermessen ändern. Sie müssen jedoch mindestens den **Zonennamen** ändern, um eine doppelte Zone zu erstellen. Doppelte Zonennamen sind nicht zulässig.

Zone löschen

1. Um eine Zone zu löschen, klicken Sie auf das Symbol in der Spalte **Aktionen** .
2. Wählen Sie **Zone löschen**.
3. Klicken Sie auf **Bestätigen**.



: Dieser Vorgang wirkt sich auf die gesamte Zone aus, einschließlich aller Antworten für jeden Datensatz innerhalb der Zone. Dies muss mit äußerster Vorsicht geschehen.

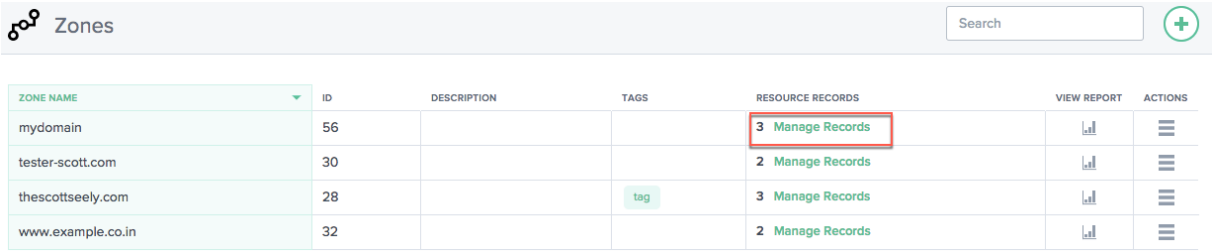
Rekorde

Nachdem Sie beispielsweise eine Zone für Ihre Domain erstellt `mydomain.com`haben, können Sie der Zone Datensätze hinzufügen. Jeder Datensatz, den Sie hinzufügen, enthält einen Namen, einen Datensatztyp und andere Informationen, die für den Datensatztyp gelten.
Alle Datensätze innerhalb einer Zone müssen den Domänennamen der Zone als Suffix haben. Wenn es sich beispielsweise um die Zone `mydomain.com` handelt, kann sie Datensätze mit dem Namen enthalten `www.mydomain.comwww.portal.mydomain.com`, und kann keinen Datensatz mit dem `www.mydomain.co.in` Namen der Zone enthalten, d. h., dem Namen jedes Datensatzes wird der Name der Zone angehängt.
Hinweis: Wenn eine Zone erstellt wird, werden die Eintragstypen Name Server (NS) und Start Of Authority (SOA) automatisch für diese Zone erstellt.

Aufzeichnungen verwalten

Um zur Seite Datensätze zu gelangen und Ihre Datensätze zu verwalten, klicken Sie in der Spalte **Ressourceneinträge Ihrer Zone auf Datensätzeverwalten**. Die Seite**Datensätze** wird mit einer Liste von Datensätzen unter der ausgewählten Zone geöffnet. Auch wenn Sie noch keine Datensätze erstellt

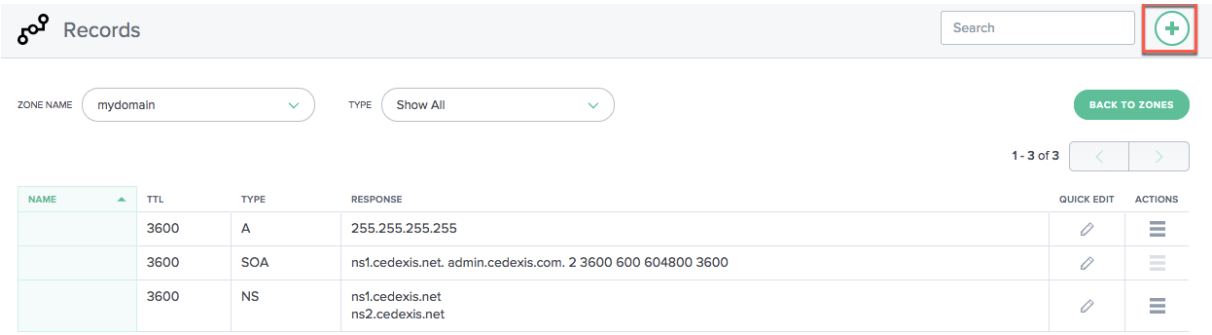
haben, werden unter Ressourceneinträge mindestens zwei Datensatztypen für eine oder mehrere Zonen angezeigt, die Sie erstellt haben. Dies sind die NS- und SOA-Einträge, die standardmäßig erstellt werden, wenn Sie Ihre Zone zum ersten Mal erstellen.



Auf dieser Seite können Sie Datensätze hinzufügen, bearbeiten, löschen oder duplizieren. Außerdem werden TTL, Datensatztyp und Antwort für jede Subdomain oder jeden Datensatz aufgeführt.

Datensatz hinzufügen

1. Klicken Sie auf der Seite **Zonen** auf **Datensätze verwalten**. Dadurch gelangen Sie zur **Seite Aufzeichnungen**.
2. Um einen neuen Datensatz hinzuzufügen, klicken Sie auf die Schaltfläche Hinzufügen in der oberen rechten Ecke der **Datensatzseite** .
3. Das Dialogfeld **Datensatz hinzufügen** wird geöffnet.



Name Geben Sie den Namen des Datensatzes ein. Wenn Sie dieses Feld leer lassen, wird ein Datensatz am Scheitelpunkt der Zone erstellt. Wenn es sich bei Ihrer Zone beispielsweise um einen A-Eintrag im Stamm dieser Domain handelt `mydomain.com` und Sie einen A-Eintrag im Stamm dieser Domain haben möchten, würden Sie diesen als namenlosen Datensatz in der Zone angeben. `mydomain.com` Einige andere Spezifikationen und Anbieter bezeichnen dies als den @-Record.

TTL Geben Sie einen Wert für TTL ein. TTL ist die Zeitspanne in Sekunden, für die rekursive DNS-Resolver Informationen zu diesem Datensatz zwischenspeichern sollen. Wenn Sie einen längeren Wert angeben (z. B. 172.800 Sekunden oder zwei Tage), verwenden Resolver eine frühere Antwort

wieder und senden seltener Anfragen an den autorisierenden DNS-Server. Dies bedeutet jedoch, dass es länger dauert, bis Änderungen am Datensatz wirksam werden, da rekursive Resolver die Werte in ihrem Cache für längere Zeiträume verwenden, anstatt nach den neuesten Informationen zu fragen.

Typ Wählen Sie den Datensatztyp aus, den Sie erstellen möchten. Weitere Informationen zu den verschiedenen Datensatztypen finden Sie im Abschnitt Datensatztypen .

Response-Typ Geben Sie eine Antwort ein, die dem Wert des Datensatztyps entspricht. Für alle Typen außer CNAME können Sie mehr als einen Antwortwert eingeben. Geben Sie mehrere Antwortwerte ein, indem Sie auf das Symbol „Hinzufügen“klicken. Wenn mehrere Werte eingegeben werden, werden alle angegebenen Antworten für jede Anfrage dieses Typs und Namens zurückgegeben.

Klicken Sie auf **Erstellen**, um den Datensatz hinzuzufügen. Der neu hinzugefügte Datensatz wird an die DNS-Server weitergegeben und live bereitgestellt, wenn die Änderung vorgenommen wird.

Datensätze auflisten

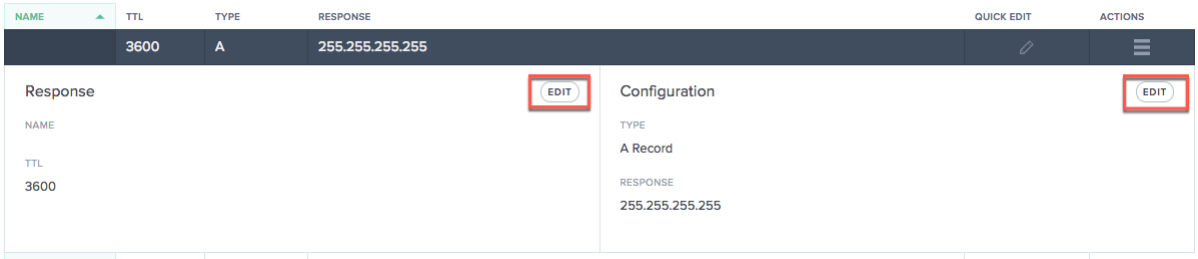
Wenn Sie einen neuen Datensatz hinzufügen, wird er auf der Seite Datensätze aufgeführt. Auf dieser Seite werden alle Datensätze aufgeführt, die Sie unter einem bestimmten **Zonennamen** erstellt haben, zusammen mit **TTL**, **Datensatztyp**und **Antwort** für diesen Datensatz.

Alle Datensätze auf dieser Seite gehören zu einer bestimmten Zone, die in der Liste **Zonenname** oben links auf der Seite **Datensätze** angezeigt wird. Diese Liste enthält eine Liste der Zonen, die bereits für Ihr Unternehmen erstellt wurden. Sie können zu einer anderen Zone wechseln (und ihre eigenen Datensätze anzeigen), indem Sie sie aus der Liste auswählen.

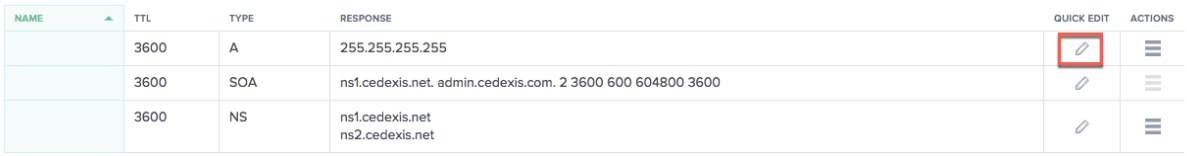
Sie können die Liste „ **Datensatztyp** “auch verwenden, um diese Liste nach dem Datensatztyp zu filtern.

Datensatz bearbeiten

Es gibt zwei Möglichkeiten, Datensätze zu bearbeiten: detaillierte Bearbeitung und schnelle Bearbeitung. Um eine detaillierte Bearbeitung durchzuführen, klicken Sie in der Liste (auf der Seite **Datensätze**) auf Datensatz. Es wird geöffnet, um die Datensatzdetails mit Schaltflächen zum Bearbeiten anzuzeigen. Klicken Sie auf die Schaltfläche **Bearbeiten**, um die Datensatzinformationen anzuzeigen. Wenn Sie mit der Bearbeitung fertig sind, klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

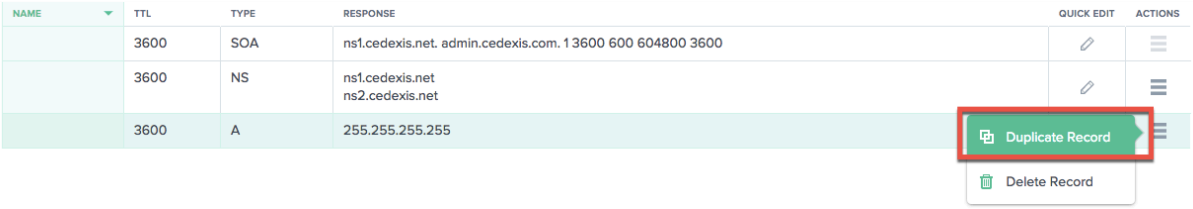


Um **Quick Edit**zu verwenden, klicken Sie einfach auf das Bearbeitungssymbol (in der Spalte **Schnellbearbeitung**) für den Datensatz, den Sie bearbeiten möchten. Sie können die TTL und die Antwort für den Datensatz bearbeiten. Wenn Sie mit der Bearbeitung fertig sind, klicken Sie auf das Speichersymbol (Häkchen), um Ihre Änderungen zu speichern, oder auf Abbrechen, um die Änderungen rückgängig zu machen.



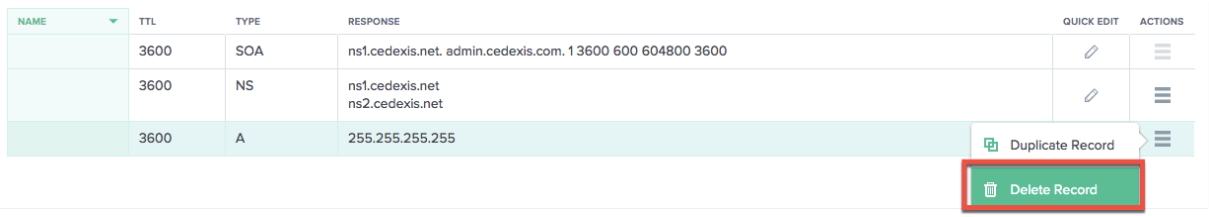
Datensatz duplizieren

Um einen Datensatz zu duplizieren, klicken Sie auf das Symbol in der Spalte **Aktionen** . Wählen Sie Datensatz duplizieren. Das Dialogfeld Datensatz hinzufügen wird mit Informationen aus dem Datensatz geöffnet, den Sie duplizieren möchten. Klicken Sie auf Erstellen, um einen Datensatz mit Informationen aus dem ursprünglichen Datensatz zu erstellen. Bitte beachten Sie, dass mindestens der Datensatzname oder -typ geändert werden muss, damit der neue Datensatz erstellt werden kann. Hinweis: SOA-Datensätze können nicht dupliziert werden.



Datensatz löschen

Um einen Datensatz zu löschen, klicken Sie auf das Symbol in der Spalte **Aktionen** . Wählen Sie Datensatz löschen. Diese Aktion löscht den Datensatz und Predictive DNS reagiert nicht mehr auf Abfragen für den Datensatz. Um bestimmte Antworten innerhalb eines Datensatzes zu entfernen, verwenden Sie die Option Schnellbearbeitung



Hinweis: NS- und SOA-Datensätze sind Standarddatensatztypen und können nicht gelöscht werden. Diese Datensätze werden nur entfernt, wenn die Zone selbst gelöscht wird.

Arten von Datensätzen

NS-Rekord

NS- oder Nameserver-Einträge sind dafür verantwortlich, eine DNS-Zone an einen autoritativen Server zu delegieren. Wir erstellen einen Nameservereintrag (NS), der automatisch zugewiesen wird, wenn Sie eine Zone erstellen, z. B. ns1.ourdomain.net und ns2.ourdomain.net. Dies sind die Nameserver, die Sie in Ihrem Registrar so konfigurieren würden, dass DNS-Anfragen an Ihre Zone weitergeleitet werden können.
Diese Nameserver dienen dazu, die Servergruppe zu bestätigen, die für die Bearbeitung von Anfragen für die Zone verfügbar ist, und stellen sicher, dass die in der Delegierungsanfrage zurückgegebenen Nameserver und der vom delegierten Server zurückgegeben wurden, übereinstimmen. Sie können die Nameserver auch bearbeiten, um sicherzustellen, dass sie übereinstimmen.

Wir ermöglichen es Ihnen auch, von Ihnen erstellte Nameserver zu bearbeiten, sodass Sie jede Ihrer Domains auf die Nameserver eines anderen Unternehmens verweisen können, die Ihre DNS-Zone enthalten und Ihre Einträge dort verwalten können.

Hinweis: NS-Datensätze können bearbeitet, aber nicht gelöscht werden.

SOA-Rekord

Der SOA-Datensatz (Start of Authority) identifiziert die maßgeblichen Informationen über die Zone. Ein SOA-Ressourceneintrag wird standardmäßig erstellt, wenn Sie Ihre Zone erstellen. Sie können den Datensatz nach Bedarf ändern.

Hinweis: SOA-Datensätze können nicht vom Benutzer erstellt werden, aber bestimmte Parameter können bearbeitet werden.

Das Format eines SOA-Datensatzes sieht wie folgt aus: `[MNAME] [RNAME] [Serial Number] [Refresh Time] [Retry Interval] [Expire Time] [Minimum TTL]`

Hier ist ein Beispiel: `ns1.ourdomain.net admin.mydomain.com.314 3600 600 604800 10`

Zu den Elementen des SOA-Datensatzes gehören:

- **MNAME**: Der Domainname des primären Nameservers, wie `ns1.ourdomain.net` im obigen Beispiel.
- **RNAME**: Die E-Mail-Adresse des Administrators in einem Format, bei dem das @-Symbol durch einen Punkt ersetzt wird, wie `admin.mydomain.com` im obigen Beispiel.
- **Seriennummer**: Eine Revisionsnummer, die erhöht wird, wenn Sie die Zonendatei ändern und Änderungen an die DNS-Server verteilen. Eine 32-Bit-Ganzzahl ohne Vorzeichen, wie 314 im obigen Beispiel.
- **Aktualisierungszeit**: Aktualisierungszeit in Sekunden, die die DNS-Server warten, bevor sie den SOA-Eintrag abfragen, um nach Änderungen zu suchen. Ein 32-Bit-Ganzzahl-Zeitintervall ohne Vorzeichen in Sekunden, z. B. 3600 im obigen Beispiel.
- **Wiederholungsintervall**: Das Wiederholungsintervall in Sekunden, das ein sekundärer Server wartet, bevor er eine fehlgeschlagene Zonenübertragung erneut versucht, z. B. 600 (10 Minuten) im obigen Beispiel. Normalerweise ist die Wiederholungszeit kürzer als die Aktualisierungszeit.
- **Ablaufzeit**: Die Ablaufzeit in Sekunden, die ein sekundärer Server immer wieder versucht, eine Zonenübertragung abzuschließen, z. B. 604800 (eine Woche) im obigen Beispiel.
- **Minimale TTL**: Die Mindestlebensdauer (TTL) in Sekunden, z. B. 10 Sekunden im obigen Beispiel.

A —IPv4-Adresse

Eine IP-Adresse im IPv4-Format, z. B. `192.0.2.235`.Der Wert für einen A-Datensatz ist eine IPv4-Adresse in punktierter Dezimalschreibweise.

AAAA —IPv6-Adresse

Eine IP-Adresse im IPv6-Format, zum Beispiel. `2001:0db8:85a3:0:0:8a2e:0370:7334`Der Wert für einen AAAA-Datensatz ist eine IPv6-Adresse im durch Doppelpunkte getrennten Hexadezimalformat, wie in RFC 4291/5952-Darstellungen angegeben.

CNAME —Kanonischer Name

Das ist der vollqualifizierte Domainname (z. B. `www.mydomain.com`), den Predictive DNS als Antwort auf DNS-Abfragen für diesen Eintrag zurückgeben soll. Ein CNAME-Wertelement hat dasselbe Format wie ein Domainname.

Wichtig: Das DNS-Protokoll erlaubt es Ihnen nicht, einen CNAME-Eintrag für das Stammverzeichnis der Zone zu erstellen, d. h. wir lassen keine namenlosen CNAME-Einträge zu. Wenn Ihre Zone beispielsweise ist `mydomain.com`, können Sie keinen CNAME-Eintrag für `mydomain.com`erstellen.

Sie können jedoch CNAME-Einträge für `www.mydomain.comportal.mydomain.com`, usw. erstellen.
Wenn Sie einen CNAME-Eintrag für eine Subdomain erstellen, können Sie außerdem keine anderen Datensätze für diese Subdomain erstellen. Wenn Sie beispielsweise einen CNAME-Eintrag für erstellen, können Sie keine anderen Datensatztypen `www.mydomain.com`mit dem Namen erstellen. `www.mydomain.com`
Hinweis: Wenn eine Subdomain einen Openmix-App-Record hat, können Sie keine A-, AAAA- oder CNAME-Einträge in derselben Subdomain haben.

MX —E-Mail-Austausch

Dieser Datensatz wird beim Routing von Anfragen an Mailserver verwendet. Beispiel: `1 mail.mydomain.com`

Jeder Wert für einen MX-Datensatz enthält zwei Werte:

1. Die Priorität für den Mailserver, die eine beliebige 16-Bit-Ganzzahl größer als 0 sein kann.
2. Der Domainname des Mailservers.

Wenn Sie mehrere Server angeben, gibt der Wert, den Sie für die Priorität angeben, an welchen E-Mail-Server die E-Mail zuerst, an den zweiten usw. weitergeleitet werden soll. Wenn Sie beispielsweise zwei Mailserver haben und die Werte 1 und 2 für die Priorität angeben, werden E-Mails immer an den Server mit der Priorität 1 gesendet, sofern dieser nicht verfügbar ist. Wenn Sie die Werte 1 und 1 angeben, werden E-Mails ungefähr gleichmäßig an die beiden Server weitergeleitet.

Openmix (A/AAAA/CNAME)

Kunden von Openmix Application können jetzt ihren gesamten Datensatz in der Zone (einschließlich statischer Datensätze) von denselben Diensten verwalten und bedienen lassen. Auf diese Weise können Kunden jeden ihrer Hosts Openmix intelligent machen. Wenn also ein CNAME an eine Openmix-App angehängt wird, wird er mit den gleichen datengesteuerten, dynamischen und vollständig programmierbaren Funktionen wie Openmix bedient.

Sie können beispielsweise mehrere Web-App-Server hinter einer Openmix-App für Ihren WWW-Datensatz haben, und die Openmix-App würde anhand ihrer integrierten intelligenten Logik entscheiden, mit welchem CNAME sie antworten soll.

Hinweis: Eine Openmix-App kann einen CNAME-, A- oder AAAA-Datensatz zurückgeben. Daher können Sie nicht gleichzeitig eine Openmix-App mit einem dieser Datensatztypen haben, der denselben Namen verwendet.

PTR —Zeigerdatensatz

PTR-Einträge werden verwendet, um eine IP einem Domainnamen zuzuordnen, hauptsächlich für Reverse-DNS. Richtig konfigurierte PTR-Einträge können für Sicherheitsszenarien wichtig sein, z. B. für die Überprüfung der Glaubwürdigkeit von E-Mail-Absendern oder die umgekehrte DNS-Suche, die beim Aufbau einer SSH-Sitzung durchgeführt wird. Ein PTR-Recordwert hat dasselbe Format wie ein Domainname. Beispiel: `hostname.mydomain.com`.

SPF —Sender Policy Framework

Ein SPF-Eintrag identifiziert, welche Mailserver E-Mails im Namen Ihrer Domain versenden dürfen. Es beginnt mit v=spf, zum Beispiel v=spf1 ip 4:192.168 .0.1/16-all.

SRV —Service-Locator

Ein SRV-Datensatz wird von Voice over IP, Instant Messaging-Protokollen, Service Discovery und anderen Anwendungen verwendet. Ein SRV-Datensatzwertelement besteht aus vier durch Leerzeichen getrennten Werten. Die ersten drei Werte sind Dezimalzahlen, die für Priorität, Gewicht und Port stehen. Der vierte Wert ist ein Domainname.

Das Format eines SRV-Datensatzes ist:

```
[priority] [weight] [port] [domain name]
```

Beispiel:

```
1 10 5269 xmpp-server.example.com
```

TXT —Text

Ein Textdatensatz kann beliebigen Text enthalten und auch zur Definition maschinenlesbarer Daten verwendet werden, z. B. Informationen zur Sicherheit oder zur Missbrauchsprävention. Es wird auch häufig zur Überprüfung des Domainbesitzes verwendet (Sie können beispielsweise ein Zertifikat erhalten, Tools von Drittanbietern registrieren, die im Namen Ihrer Domain arbeiten, usw.).
Es muss nur Text enthalten, zum Beispiel Sample Text Entry.

Prädiktiver Datensatz (A/AAAA/CNAME)

Predictive Records bieten verschiedene Konfigurationsoptionen für das globale Verkehrsmanagement auf der Grundlage der Verfügbarkeit von Diensten in Echtzeit. Mit Predictive Records können

Sie die Routing-Konfiguration auf Adresspools anwenden und das Verhalten individuell für verschiedene Standorte, Netzwerke oder IPs/CIDR-Blöcke definieren. Dieser Service kombiniert Failover- und Round-Robin-Routing-Logik, um höchste Verfügbarkeit, keine Ausfallzeiten und ein nahtloses datengesteuertes Verkehrsmanagement auf allen Plattformen zu gewährleisten.

Predictive DNS-Kunden können den Predictive-Eintragstyp für die Antworttypen CNAME, A oder AAAA verwenden.

Wenn Sie als Predictive DNS-Kunde Datensätze zu Ihrer Zone hinzufügen, wählen Sie Predictive (A/AAAA/CNAME)**aus der Liste der Eintragstypen aus.**

Navigation

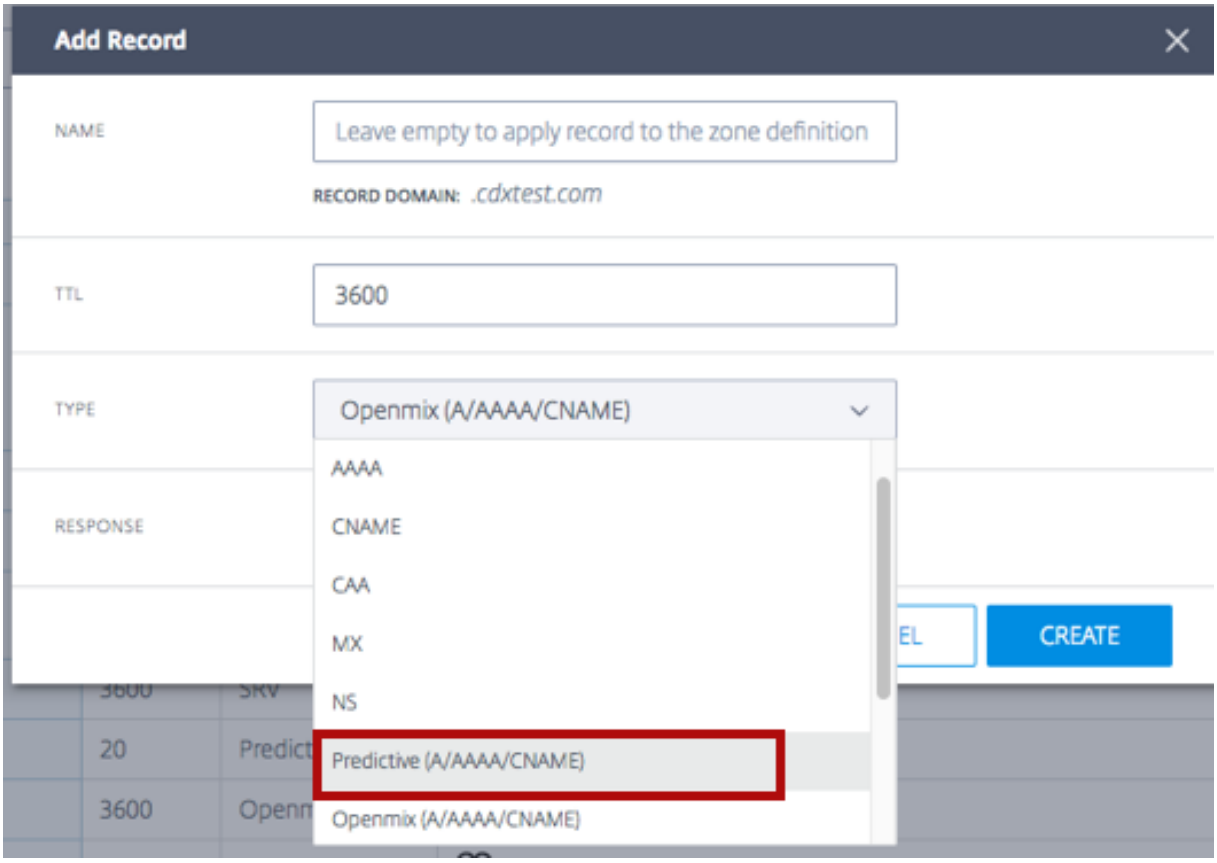
1. Gehen Sie zur **Datensatzseite** Ihrer Zone.
2. Klicken Sie auf der **Datensatzseite auf die Schaltfläche Datensatz hinzufügen** . Weitere Informationen zum Hinzufügen von Datensätzen finden Sie im Abschnitt Datensatz hinzufügen .
3. Das Dialogfeld **Datensatz hinzufügen** wird geöffnet.

Prädiktive Datensätze hinzufügen

Geben **Sie im Dialogfeld „Datensatz hinzufügen** "Folgendes ein:

1. **Name**: Geben Sie einen Namen für den Datensatz ein. Wenn das Feld leer gelassen wird, enthält der Datensatz automatisch die Zonendefinition. Sie können auch ein einzelnes Sternchen `*` als Platzhalter ganz links im Namen verwenden, um Anfragen für alle nicht existierenden Subdomains abzugleichen. Sie können beispielsweise, `**.example.com`, oder verwenden `*.something.example.com`. `*.` ist jedoch ungültig, d. h. ein Sternchen, gefolgt von nur einem Punkt, ist nicht zulässig. Wir unterstützen die Wildcard-Funktionalität, wie sie in den RFCs definiert ist.
2. **TTL**: Sie können die Standard-TTL unverändert lassen oder sie nach Bedarf ändern. **Hinweis:** DNS Time to Live (TTL) teilt Resolvern mit, wie lange sie die Entscheidung behalten müssen, bevor sie erneut nach Updates fragen. Die TTL wird zur Steuerung des Verkehrsaufkommens und auch zur Steuerung der Empfindlichkeit gegenüber Änderungen der Daten verwendet, auf die sie reagiert. Die Standard-TTL ist 20 Sekunden. Wenn Sie die TTL senken, erhalten Sie mehr Volumen und mehr Echtzeit-DNS-Abfragen. Dies kann jedoch zu zusätzlichen Kosten und geringerer Leistung führen (da DNS-Abfragen auf dem Client einige Zeit in Anspruch nehmen). Daher wird empfohlen, den Standardwert von 20 Sekunden nicht zu ändern.
3. **Typ**: Klicken Sie auf die **Typliste** und wählen Sie Prädiktiv (A/AAAA/CNAME) aus.

4. **Antworttyp**: Klicken Sie auf die Liste **Antworttyp** und wählen Sie als Antworttyp A, AAAA oder CNAME aus.
5. **Fallback**: Geben Sie die **Fallback-Antwort** ein. **Für Fallback muss ein gültiger CNAME, A, AAAA angegeben werden.** Der Fallback wird verwendet, falls bei der Bearbeitung der Anwendung ein Fehler auftritt. **Hinweis**: Die **Fallback-Antwort** muss ein gültiger CNAME sein, wenn der **Antworttyp**, den Sie im vorherigen Schritt ausgewählt haben, CNAME ist. Wenn der gewählte **Antworttyp** A ist, muss die Fallback-Antwort eine CNAME- oder eine IPv4-Adresse sein. Wenn **als Antworttyp** AAAA ausgewählt wurde, muss die Fallback-Antwort alternativ eine CNAME- oder eine IPv6-Adresse sein.
6. Klicken Sie auf **Routing erstellen und definieren**.
7. Die Seite **Predictive Configuration** wird geöffnet.



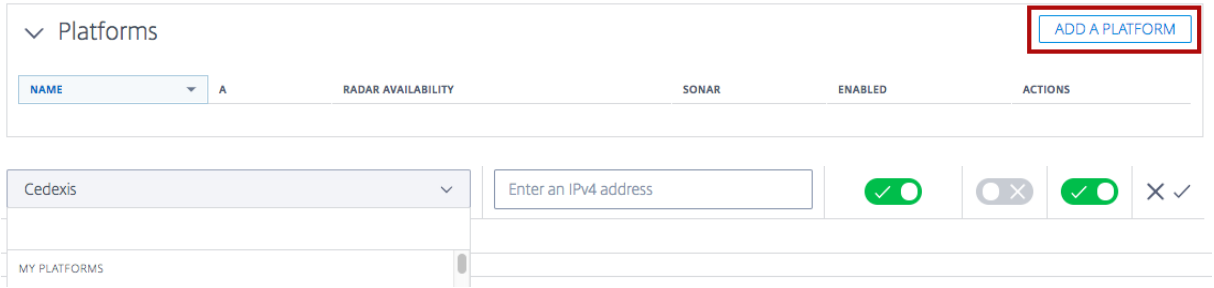
Konfigurationsschritte

Oben auf dieser Seite befindet sich der Abschnitt **Allgemein**, in dem angezeigt wird, was Sie im Dialogfeld **Datensatz hinzufügen** eingerichtet haben. Es hat auch optionale Felder, mit denen Sie Ihren Predictive-Datensätzen **Tags** oder eine **Beschreibung** hinzufügen können.

Gehen Sie wie folgt vor, um den Datensatz zu konfigurieren.

Schritt 1: Wählen Sie alle verfügbaren Plattformen Der erste Schritt zur Konfiguration des Predictive Record besteht darin, alle Plattformen auszuwählen, die für verschiedene Standorte, Netzwerke oder IPs/CIDR-Blöcke verfügbar sein sollen. Wenn Sie Ihre Plattform nicht in der Liste finden, können Sie sie auf der Seite Plattformen hinzufügen.

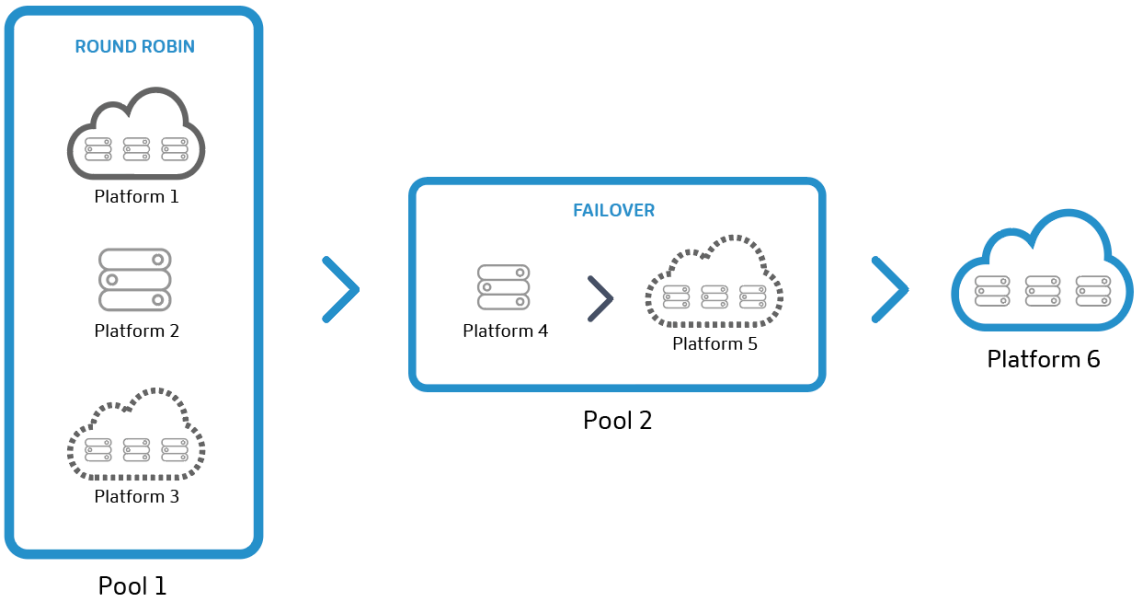
1. Klicken **Sie oben rechts in diesem Abschnitt auf Plattform hinzufügen** .
2. Fügen Sie alle Plattformen hinzu, die für das Routing verfügbar sein sollen, einschließlich der Plattformen, die zu Adresspools hinzugefügt werden müssen. Sie können dies tun, indem **Sie auf das Feld Plattform** auswählen klicken und Plattformen einzeln aus der Liste auswählen.
3. Geben Sie je nach **Antworttyp** (A, AAAA oder CNAME), den Sie in der Liste **Datensatz hinzufügen** ausgewählt haben, eine IPv4-Adresse, IPv6-Adresse oder CNAME für die Plattform ein. Sie können zum Abschnitt **Allgemein** zurückkehren, um den **Antworttyp**bei Bedarf zu bearbeiten.
4. Sobald die Plattform ausgewählt und der **Antworttyp** eingegeben wurde, können Sie die Plattform aktivieren oder deaktivieren, indem Sie auf die Umschaltfläche **Aktiviert** klicken. Sie können **Radar Availability und Sonar auch mit ähnlichen Umschalttasten ein- und** ausschalten.
5. Wählen Sie in der Spalte **Aktionen** das Häkchensymbol aus, um Ihre Änderungen zu speichern, oder das Kreuzmarkensymbol, um abzubrechen.



Schritt 2: Adresspools hinzufügen und definieren

Adresspools Adresspools sind eine Sammlung von Plattformen, die einer vom Benutzer angegebenen Routing-Methode folgen. Der Zweck eines Adresspools besteht darin, Ihnen die Definition logischer Gruppen von Plattformen zu ermöglichen, die mit jeder bestimmten Routing-Methode verwendet werden können. Sie können **Round-Robin-** oder **Failover-Routing-Methoden** angeben, denen die Plattformen innerhalb eines Pools folgen sollen.

Sie können jedem Pool eine beliebige Anzahl von Plattformen und für jeden Ihrer geografischen Standorte eine beliebige Anzahl von Pools hinzufügen. Sie können beispielsweise einen EU-Pool (bestehend aus Plattformen, die überwiegend die EU-Region bedienen), einen Asien-Pool (mit Plattformen in China, Indien und Singapur) und einen US-Pool (mit Plattformen in den Vereinigten Staaten) einrichten.



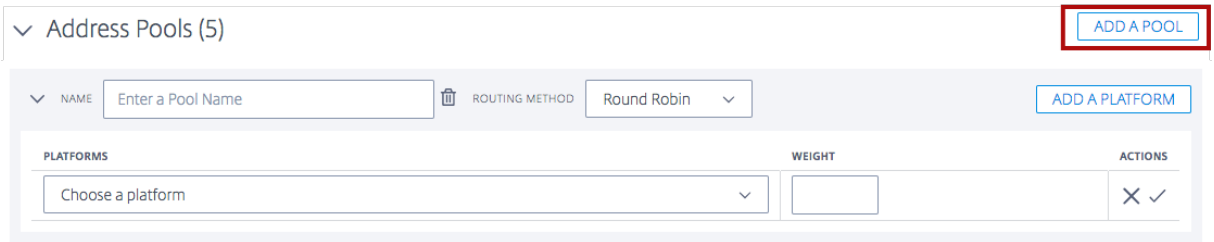
Hinweis: Adresspoolssind optional. Sie können stattdessen einzelne Plattformen verwenden und diese zur Routing-Konfiguration hinzufügen.

Round-Robin-Routing-Methode Diese Art von Routing folgt einer typischen Methode des globalen Serverlastenausgleichs nach dem Round-Robin-Verfahren, bei dem jeder CNAME/A/AAAA abwechselnd an die Endbenutzer zurückgegeben wird, wenn DNS-Anfragen gestellt werden. Wenn beispielsweise die Plattformen P1, P2 und P3 den Verfügbarkeitsschwellenwert erfüllen, wird die erste Anforderung an P1 weitergeleitet, die zweite an P2, die dritte nach P3, die vierte nach P1 erneut usw. Sie können auch Gewichtungen für die Priorisierung und Auswahl jeder Plattform global und/oder nach Markt oder Land zuweisen.

Failover-Routing-Methode Diese Routing-Methode unterstützt eine einfache Routing-Logik, bei der eine Plattform auf der Grundlage ihrer Position in der Leitung und ihres Verfügbarkeitsschwellen-

werts ausgewählt wird. Sie können eine Failover-Kette erstellen, die entscheidet, welche Plattform zuerst, welche zweite usw. ausgewählt werden soll. Diese Failover-Kette kann so eingerichtet werden, dass sie global und/oder für einzelne Märkte und Länder funktioniert.

Einen Adresspool hinzufügen Gehen Sie wie folgt vor, um einen Adresspool hinzuzufügen:



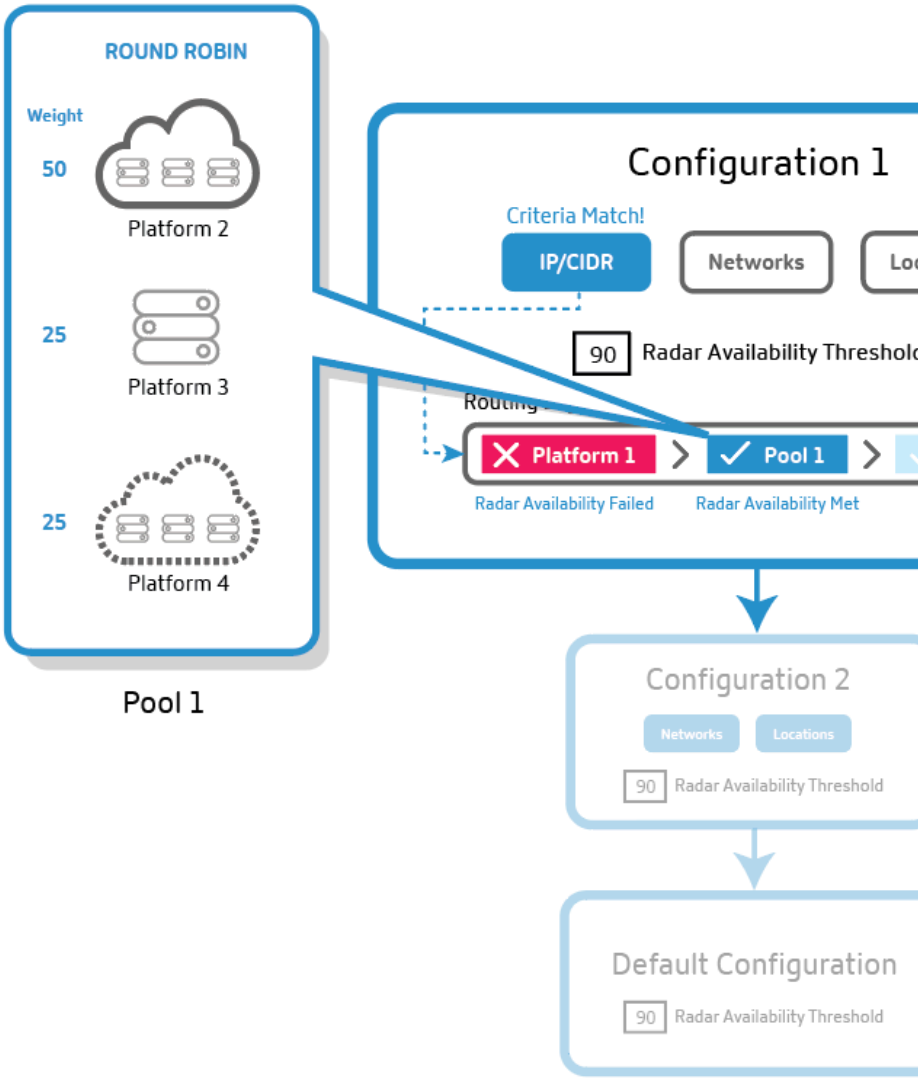
1. Klicken Sie oben rechts im Abschnitt auf die Schaltfläche **Pool hinzufügen** .
2. Geben Sie einen **Namen** für den Pool ein. Der Name kann verwendet werden, um den Zweck des Pools zu identifizieren.
3. Wählen Sie eine **Routing-Methode**aus. Sie können entweder **Round Robin** oder **Failover**wählen.
4. Wählen Sie eine **Plattform** aus der Liste aus, die Sie im vorherigen Schritt erstellt haben.
5. Sie können diesem Pool beliebig viele Plattformen hinzufügen, indem Sie auf die Schaltfläche **Plattform hinzufügen** klicken.
6. Geben Sie für jede Plattform, die Sie auswählen, ein entsprechendes **Gewicht**ein. Der Zweck von Gewichten besteht darin, Plattformen für die Verkehrsverteilung zu priorisieren und auszuwählen. Die Gewichte, die Sie den Plattformen zuweisen, müssen sich nicht auf 100 summieren. Sie können eine beliebige ganze Zahl zwischen 0 und 1.000.000 sein. Wenn diese Gewichte (im Backend) in Prozent umgerechnet werden, ergeben sie zusammen 100%. Wenn alle ausgewählten Plattformen das gleiche Gewicht erhalten, wird der Verkehr im Laufe der Zeit gleichmäßig auf sie verteilt. Wenn Sie nur eine Plattform haben, wird diese zu 100% genutzt, unabhängig davon, wie viel Gewicht Sie ihr geben.
7. Wenn Sie fertig sind, wählen Sie das Häkchensymbol, um Ihre Änderungen zu speichern, oder das Kreuzmarkensymbol, um abzubrechen.
8. Anschließend können Sie Ihre Plattformauswahl bearbeiten oder löschen, indem Sie die entsprechenden Symbole in der Spalte **Aktionen** auswählen.

Schritt 3: Failover konfigurieren Failover gilt für den gesamten Satz von Adresspools und/oder einzelnen Plattformen. Es unterstützt eine einfache Validierungsmethode, bei der eine einzelne Plattform oder ein Pool anhand der folgenden Kriterien für das Routing bewertet wird:

- Standort, Netzwerk und/oder IP/CIDR. Mindestens eines dieser Kriterien muss angegeben werden.

  > **Hinweis:**
  >
  > Standortkriterien für Failover sollten keine Mischung aus Kontinenten und Ländern enthalten, aber Sie können die Routinglogik verwenden, um mehrere Failovers zu erstellen.

- Sonar- und Radarverfügbarkeit, falls konfiguriert, und
- In der Reihe platzieren



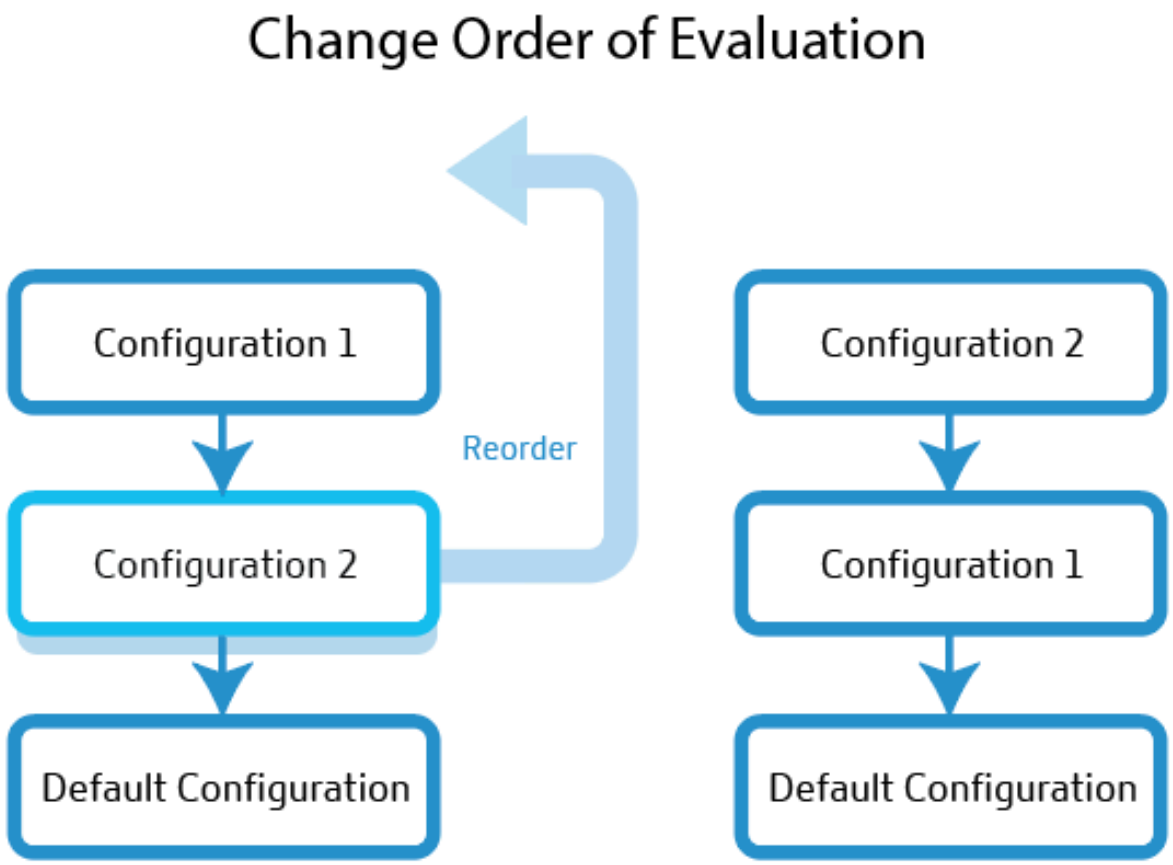
Failover für Predictive Records

1. Der Predictive Record bewertet den ersten Konfigurationsblock nach den erforderlichen Kriterien (Standort, Netzwerk und/oder IPs). Wenn der erste Routing-Konfigurationsblock die erforderlichen Kriterien nicht erfüllt, geht er zum zweiten Block in der Reihe über und so weiter.

2. Der Konfigurationsblock, der alle erforderlichen Kriterien erfüllt, wird für die Verkehrsverteilung ausgewählt.
3. Innerhalb des ausgewählten Konfigurationsblocks werden die Adresspools oder Plattformen anhand ihrer Position in der Leitung und ihres Verfügbarkeitsschwellenwerts (Radar und Sonar) bewertet.
4. Die erste Plattform innerhalb des Adresspools (oder außerhalb davon), die den Verfügbarkeitsschwellenwert erreicht, wird für die Verteilung des Datenverkehrs ausgewählt. Dann kommt die Round-Robin- oder Failover-Routing-Logik ins Spiel.

Hinweis: Wenn der Pool nur eine Plattform enthält, wird diese Plattform zu 100% ausgewählt, und die Round-Robin-Logik gilt nicht für sie.

Als Benutzer können Sie die Routing-Konfigurationsblöcke so anordnen, dass derjenige mit der höchsten Priorität an erster Stelle steht usw. Die Neuordnung kann manuell vorgenommen werden, indem jeder Pool oder jede Plattform an die gewünschte Stelle in der Zeile gezogen wird.



Standardkonfiguration Sie müssen mindestens eine Plattform oder einen Pool im Standard-Routing-Konfigurationsblock haben. Es muss eine oder mehrere Plattformen oder Pools enthalten,

die der Predictive-Datensatz verwendet, wenn alle anderen Optionen die angegebenen Kriterien nicht erfüllen. In der Standardeinstellung müssen keine Kriterien angegeben werden und sie entspricht allen Anfragen. Wenn die Plattformverfügbarkeit den Schwellenwert für die Radarverfügbarkeit nicht erreicht, gibt die Antwort Fallback zurück.

Schritte zur Konfiguration von Failover Gehen Sie wie folgt vor, um die Konfiguration zu definieren:

1. Geben Sie einen **Namen**ein. Dieser Name hilft bei der Identifizierung Ihres Routing-Konfigurationsblocks.
2. Sie können die Standard-TTL unverändert lassen oder sie nach Bedarf ändern.
3. Vergewissern Sie sich, dass die **Radarverfügbarkeit** aktiviert ist. Sie können den Schwellenwert für die Radarverfügbarkeit auf das gewünschte Niveau einstellen. Wenn Sie diese Option deaktivieren, wird Radar für die Gruppe von Pools oder Plattformen deaktiviert.
4. Wählen Sie **Standorte, Netzwerke und/oder IP/CIDR**aus. Wenn Ihre Routing-Konfiguration beispielsweise für die Region Ozeanien gilt, können Sie Standorte, Netzwerke und/oder IP-Adressen von Plattformen oder Pools in dieser Region angeben.
5. Im Feld **Failover-Konfiguration** können Sie die Auswahlpriorität für alle Pools und Plattformen festlegen. Die Reihenfolge, in der Sie diese Pools oder Plattformen platzieren, bestimmt ihre Auswahl für das Routing. Und der Verkehr wird auf der Grundlage der im vorherigen Schritt angegebenen Methode (Round-Robin oder Failover) weitergeleitet.
6. Um einen Konfigurationsblock zu löschen, klicken Sie auf das Papierkorbsymbol neben dem Feld **Name** .

DNS-Berichte

DNS-Berichte bieten einen umfassenden Einblick in das Volumen der DNS-Anfragen auf der Grundlage verschiedener Kriterien für eine bestimmte Domain oder einen bestimmten Hostnamen. Sie zeigen, wie oft bestimmte Eintragstypen abgefragt werden, und bieten eine völlig unterschiedliche Aufschlüsselung. Dieser Grad an Granularität ermöglicht es Predictive DNS-Benutzern, Trends und Abfragevolumen für bestimmte Zonen, Hostnamen, Anfragetypen, Märkte, Länder, Regionen, Bundesstaaten und Netzwerke zu verstehen.

Diese Berichte dienen in erster Linie der besseren Sichtbarkeit und Analyse. Sie geben Aufschluss über den Verkehrsfluss für jede Zone oder jeden Hostnamen und helfen bei der Diagnose von DNS-Problemen. Sie decken auch Anomalien wie Anforderungsspitzen oder andere Unregelmäßigkeiten auf, indem sie das Volumen der Anfragen nach Datensatztypen und geografischen Standorten aufschlüsseln.

Sie können auch unnötiges Rauschen filtern, indem Sie wissen, in welchen Zonen der meiste Verkehr herrscht, und sich nur auf die Zonen oder Datensatztypen konzentrieren, die Ihnen wichtig sind.

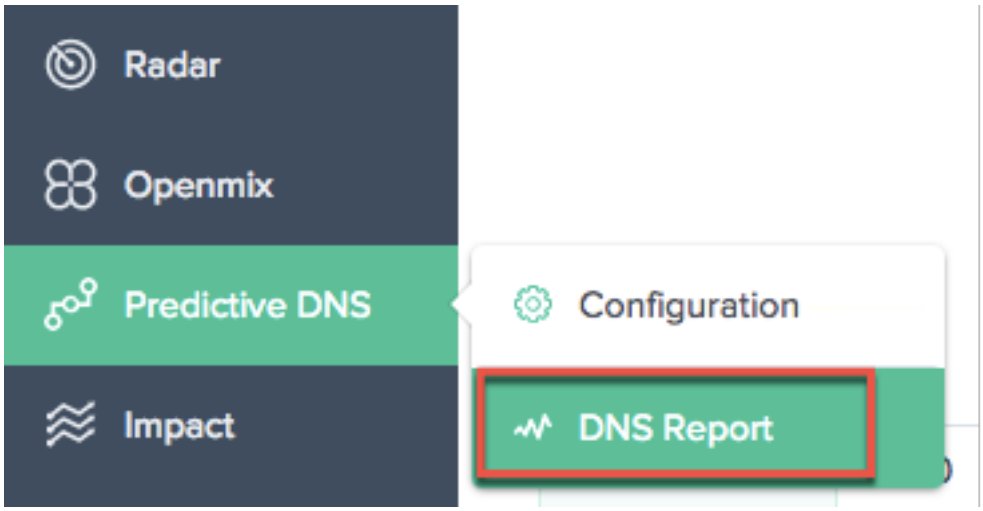
DNS im Vergleich Openmix-Berichterstattung

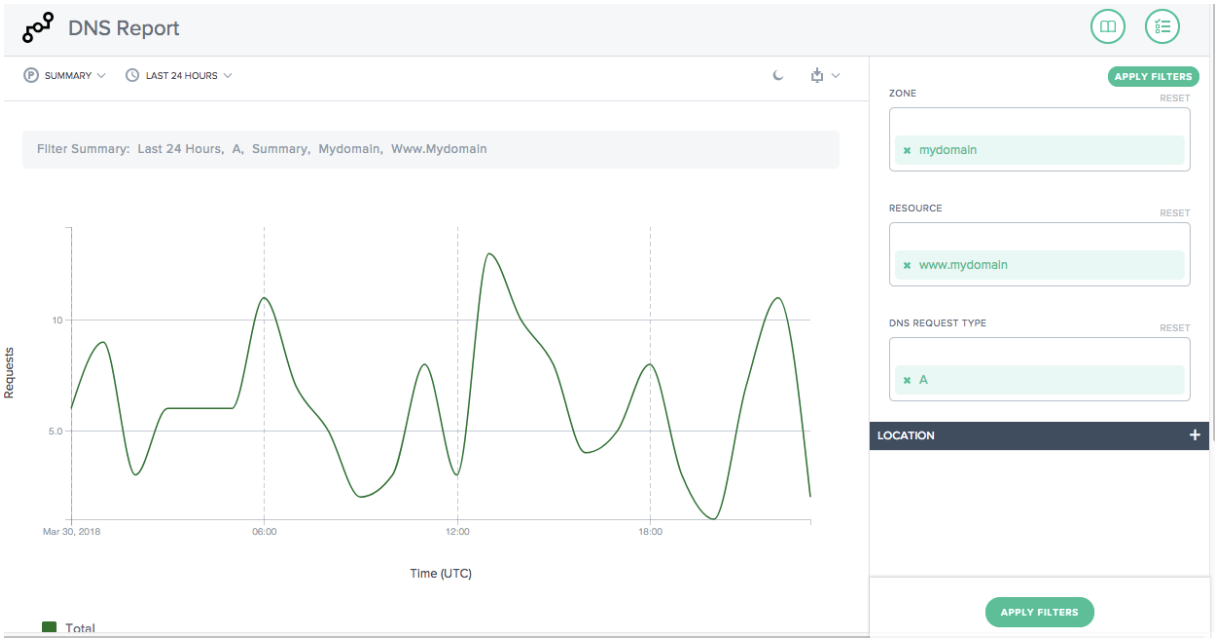
Für Openmix-Kunden erscheinen Berichte in den DNS-Berichten und in den Openmix-Entscheidungsberichten. DNS-Berichte liefern Informationen über Anfragen an unsere autoritativen Zonen, während Openmix Berichte darüber bereitstellt, wann die intelligente Openmix-Plattform zur Erfüllung einer Anfrage verwendet wurde, entweder über einen Openmix-Anwendungsdatensatz oder direkt an einen Openmix-CNAME.

Navigation

So navigieren Sie zum Abschnitt **DNS-Bericht** :

1. Klicken Sie im linken Navigationsmenü auf **Predictive DNS** .
2. Navigieren Sie zu **DNS-Bericht**.
3. Die Seite **DNS-Bericht** wird geöffnet.

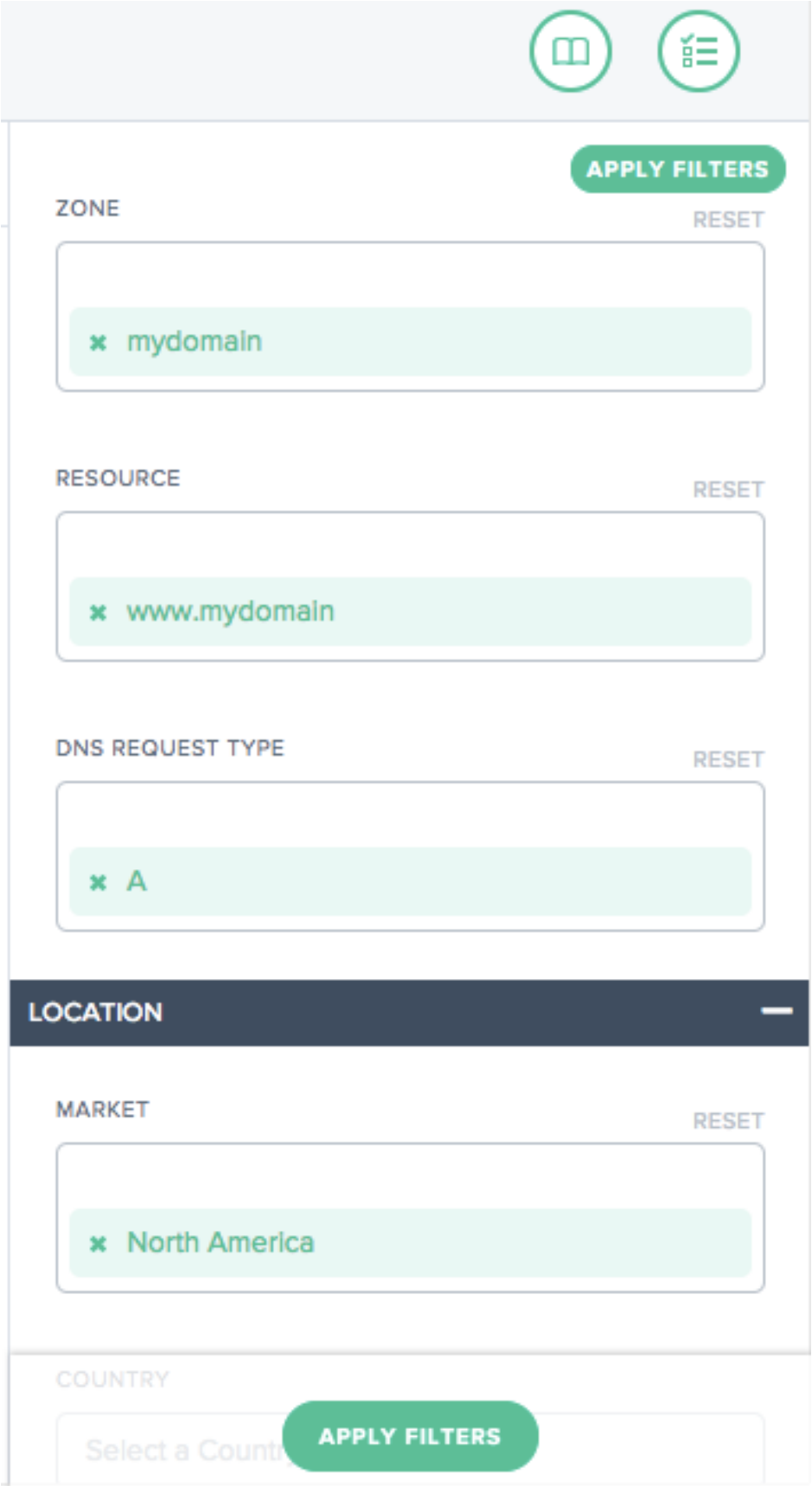




Filter anwenden

Im Bereich **Filter anwenden** auf der rechten Seite können Sie nur die Daten auswählen und anzeigen, die im Bericht angezeigt werden sollen.
Sie können nach folgenden Kriterien filtern:

- **Zone** —Wählen Sie eine oder mehrere Zonen aus, die eingeschlossen werden sollen.
- **Ressource** —Wählen Sie einen oder mehrere Hostnamen aus, die aufgenommen werden sollen.
- **DNS-Anforderungstyp** —Wählen Sie einen oder mehrere DNS-Anforderungstypen aus, die eingeschlossen werden sollen.
- **Standort** —Wählen Sie einen oder mehrere geografische Standorte (Markt, Region, Bundesland oder Netzwerk) aus, die Sie einbeziehen möchten.



Primäre Dimension

Primäre Dimensionen werden anhand von Listen über dem Diagramm ausgewählt. Sie können dies als wichtigen Dreh- und Angelpunkt für den Bericht verwenden.

Zusammenfassung Die Zusammenfassung gibt Ihnen die Gesamtzahl der Anfragen mit allen angewendeten Filtern.

Nach voreingestellten Zeitbereichen filtern

Relative voreingestellte Zeitbereiche können als zusätzlicher Filter ausgewählt werden, um die Berichterstattung weiter zu verfeinern.

Berichte mit einem Lesezeichen versehen

Sobald Sie einen Bericht auf der Grundlage der Filterkriterien generiert haben, können Sie die angewendeten Filter speichern, indem Sie den Bericht mit einem Lesezeichen versehen. Jedes Mal, wenn Sie dieses Lesezeichen besuchen, wird ein aktualisierter Bericht generiert, der auf allen ausgewählten Filtern basiert.
Gehen Sie wie folgt vor, um einen Bericht mit einem Lesezeichen zu versehen:

- Klicken Sie oben rechts auf der Seite auf das Lesezeichensymbol.
- Geben Sie im Dialogfeld Neues Lesezeichen hinzufügen dem Lesezeichen einen passenden Namen und klicken Sie auf Erstellen.
- Ein neues Lesezeichen wird jetzt erstellt. Sie können auf das Lesezeichen zugreifen, indem Sie auf das Lesezeichensymbol (oben rechts auf jeder Berichtsseite) klicken und das Lesezeichen auswählen.

Sonar

June 4, 2021

Sonar ist ein Liveness Check Service, der verwendet werden kann, um webbasierte Dienste auf Verfügbarkeit zu überwachen. Sonar funktioniert, indem HTTP- oder HTTPS-Anfragen von mehreren Points of Presence auf der ganzen Welt zu einer URL, die Sie angeben.

Sonar Grundlagen

Von Sonar getestete Endpunkte werden anhand der folgenden Kriterien als hoch- oder heruntergefahren betrachtet:

- Anforderungen, die zu HTTP 2xx führen, werden als Erfolge betrachtet, und alle anderen Ergebnisse, einschließlich Netzwerkprobleme und Timeouts, werden als Fehler behandelt.
- Sonar folgt Redirect-Antworten, die 3xx Statuscodes zurückgeben, für bis zu 6 Weiterleitungen, bis es nicht 3xx Antwort erhält oder ein Fehler auftritt.
- Der Endpunktstatus wird basierend auf einem Quorum der Berichtsorte festgelegt. Sonar meldet, welches Ergebnis (Erfolg oder Misserfolg) von den meisten Anwesenspunkten zurückgegeben wird.

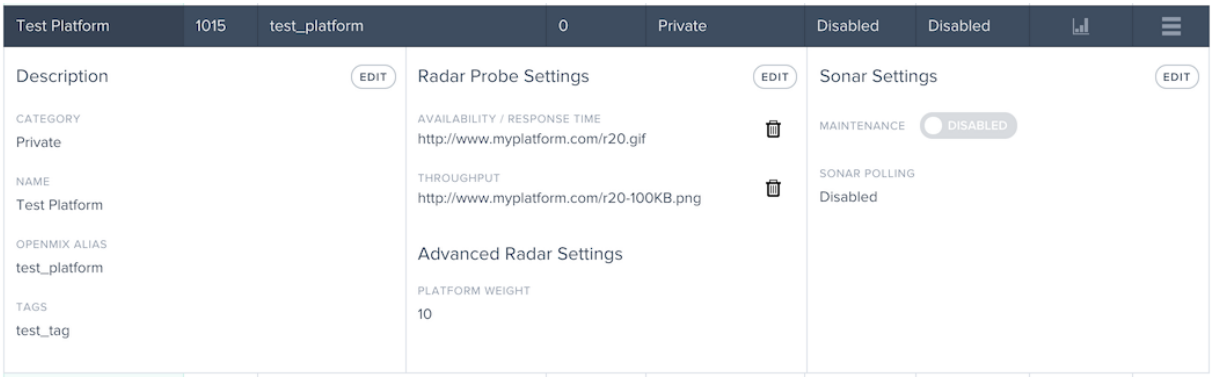
Sonar-Prüfungen werden von mehreren Teststandorten aus der ganzen Welt durchgeführt. Zu den Standorten gehören:

- Singapur
- South Carolina, Vereinigte Staaten
- Tokio, Japan
- St Ghislain, Belgien
- Washington, Vereinigte Staaten
- New York, Vereinigte Staaten von Amerika
- London, England
- Hongkong
- Frankfurt, Deutschland
- Dublin, Irland
- Iowa, Vereinigte Staaten
- Virginia, Vereinigte Staaten
- Amsterdam, Niederlande

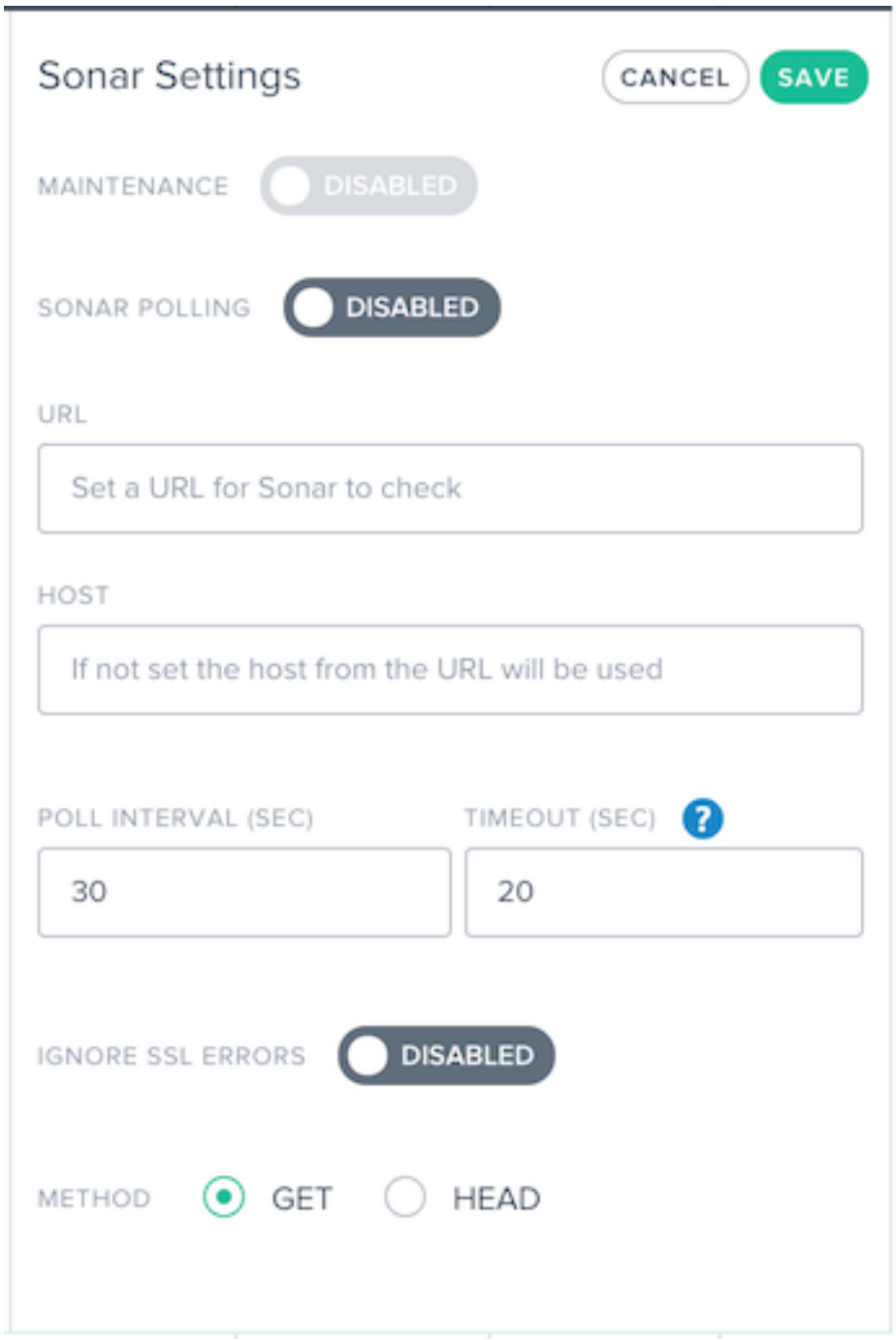
Die Sonar-Plattform ist eng mit den globalen Radar, Fusion & Openmix Plattformdiensten integriert. Sonar-Daten werden in Echtzeit an alle Openmix-Knoten auf der ganzen Welt übertragen, um als zusätzliche Eingabe für die Entscheidungsfindung verwendet werden.

Plattform-Sonar-Konfiguration

Sonar ist für jede Plattform auf derPlattformenSeite konfiguriert. Klicken Sie auf eine Plattform in der Liste, um den Abschnitt “**Sonar-Einstellungen**”anzuzeigen.



Um die Sonar-Überwachung der Plattform hinzuzufügen, klicken Sie im Abschnitt **Sonar-Einstellungen** auf die Schaltfläche **Bearbeiten** .

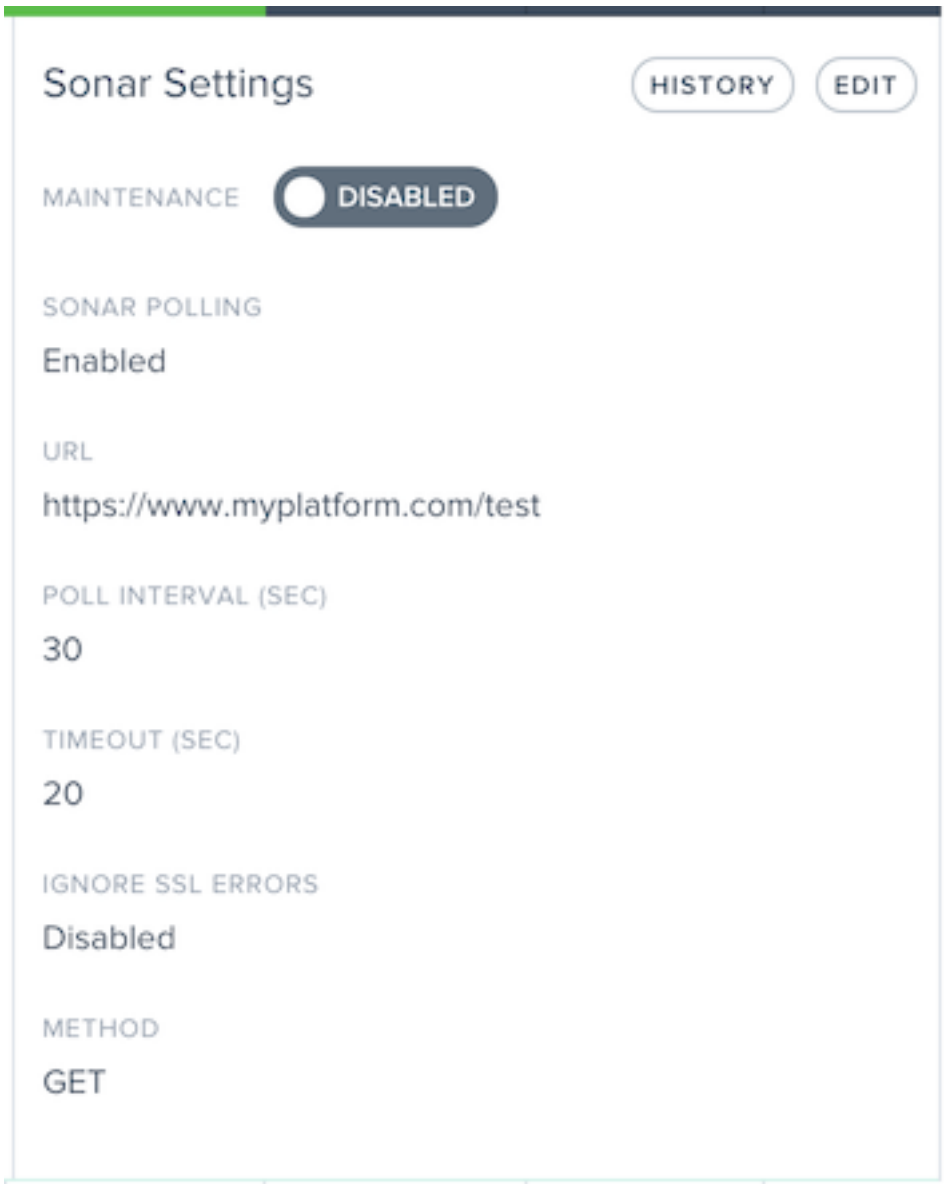


Eine Beschreibung der Felder ist unten:

Eingabeelement	Beschreibung	Standard
Wartung	Wenn diese Option aktiviert ist, meldet Sonar den Dienst als heruntergefahren, unabhängig vom aktuellen Status. Dies ist nützlich, wenn Sie eine Plattform aus dem Openmix Routing entfernen möchten, um Ausfallzeiten zu erwarten.	Deaktiviert
Sonar Polling	Wenn diese Option aktiviert ist, überprüft Sonar die konfigurierte URL.	Deaktiviert
URL	Die URL Sonar ruft auf, um die Verfügbarkeit des Dienstes zu überprüfen.	
Host	Der Wert, der für den Host-Header-Wert in der Anforderung verwendet werden muss.	v
Abfrageintervall	Die Häufigkeit, die in Sekunden angegeben wird, um auf Verfügbarkeit des Dienstes zu testen. Prüfungen können ein Mindestintervall von 1 Sekunde bis zu 300 Sekunden (5 Minuten) haben.	60 v

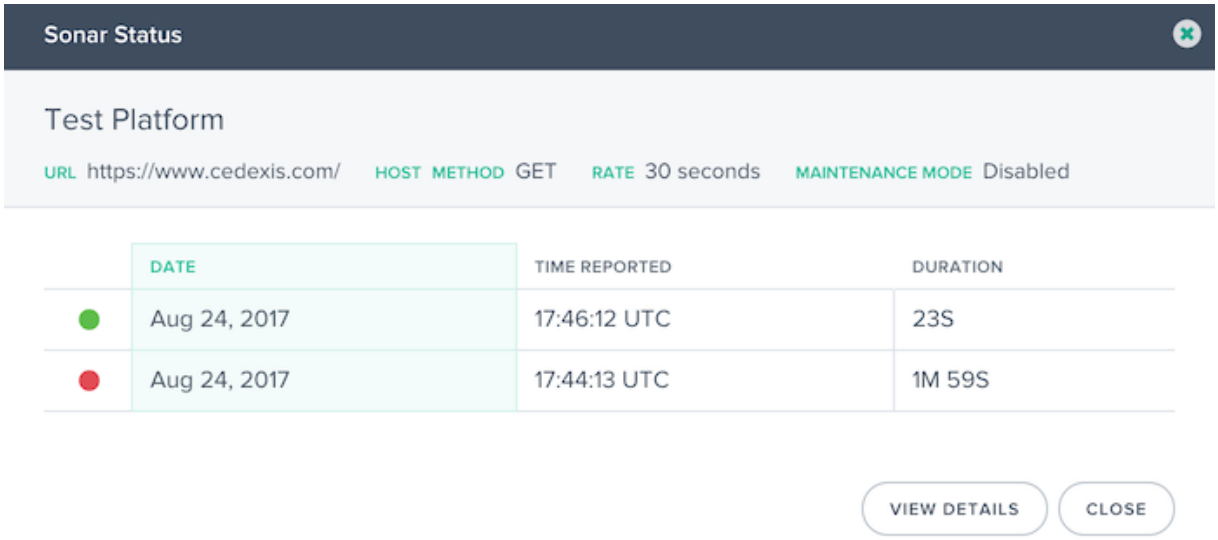
Eingabeelement	Beschreibung	Standard
Timeout	Die Zeit, die in Sekunden angegeben wird, um auf eine Antwort zu warten, bevor eine fehlgeschlagene Überprüfung an den Dienst angenommen wird. Prüfungen können eine minimale Zeitüberschreitung von 1 Sekunde bis zu 30 Sekunden haben. Bei niedrigeren Abfrageintervallen, z. B. unter 5 Sekunden, ist die Zeitüberschreitung auf 4 Sekunden begrenzt.	20
SSL-Fehler ignorieren	Wenn diese Option aktiviert ist, ignoriert Sonar SSL-Fehler, die während der Anforderung auftreten, z. B. ein falsch konfiguriertes SSL-Zertifikat.	Deaktiviert
Methode	Die HTTP-Methode, die für die Prüfung verwendet wird: GET oder HEAD.	

Um Sonar zu aktivieren, schalten Sie **Sonar Polling** auf **Aktiviert** ein, und geben Sie die Service-URL ein. Klicken Sie auf **Speichern**, und die Prüfungen werden gestartet.



Wenn Sonar aktiviert ist, werden in den Einstellungen die aktuellen Sonar-Einstellungen angezeigt.

Nachdem Sonar aktiviert wurde, können Sie im Abschnitt "**Sonar-Einstellungen**"auf die Schaltfläche "**Verlauf**"klicken, um die letzten Statusänderungen und die Dauer anzuzeigen. Klicken Sie auf die Schaltfläche "**Details anzeigen**", um zur Seite "Status der Sonar-Plattform"zu gelangen, um weitere Details und langfristige Statusberichte zu erhalten.



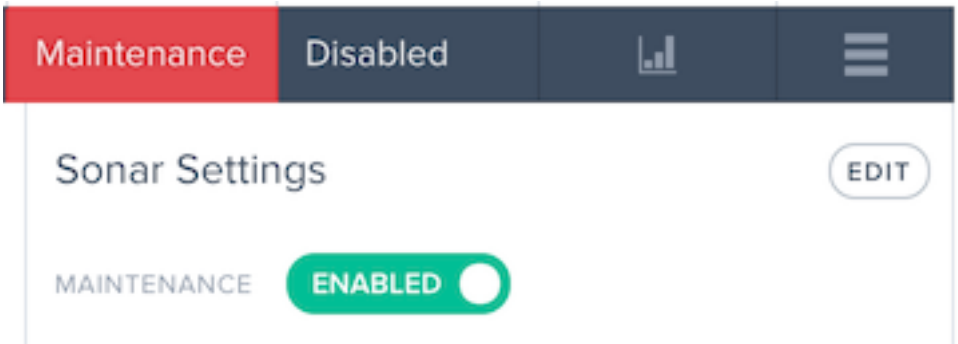
Plattform-Sonar-Status

Wenn Sonar für eine Plattform aktiviert ist, wird der Status “Sonar”in der Plattformliste in der Spalte “**Sonar**”angezeigt. Wenn die Sonar-Überwachung mit der Plattform überprüft wird, ist die Spaltenzelle grün und zeigt an, wie lange die Plattform erreichbar war.

Wenn die Plattformüberwachungsprüfungen fehlgeschlagen sind, ist die **Sonar-Zelle** rot und zeigt an, wie lange die Plattform nicht erreichbar war.

Wartungsmodus

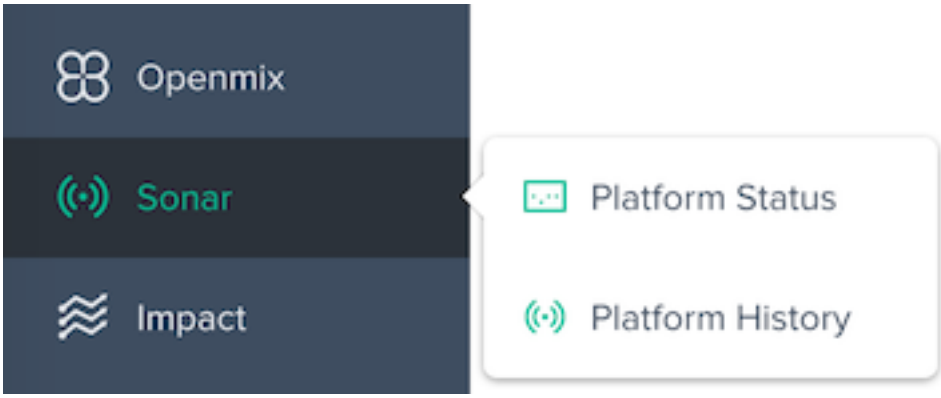
Der Status “Sonar”zeigt die Verfügbarkeit des Dienstes basierend auf dem Erfolg oder Ausfall der synthetischen Prüfungen an. Wenn Sie die Plattform auch dann als **heruntergefahren** markieren möchten, wenn sie erreichbar ist, können Sie beispielsweise im Vorgriff auf die Wartung auf der Plattform den Wartungsmodus aktivieren. Dieser Modus meldet die Plattform in den Openmix-Anwendungen als nicht verfügbar und stoppt automatisch den Datenverkehr an die Plattform in jeder Openmix-Anwendung, für die Sonar aktiviert ist.



Aktivieren Sie den Wartungsmodus, schalten Sie die Option **Wartung** auf **Aktiviert** .

Nach der Aktivierung zeigt das Plattformlistenelement den Sonar-Status als **Wartung**an.

Sonar-Menü



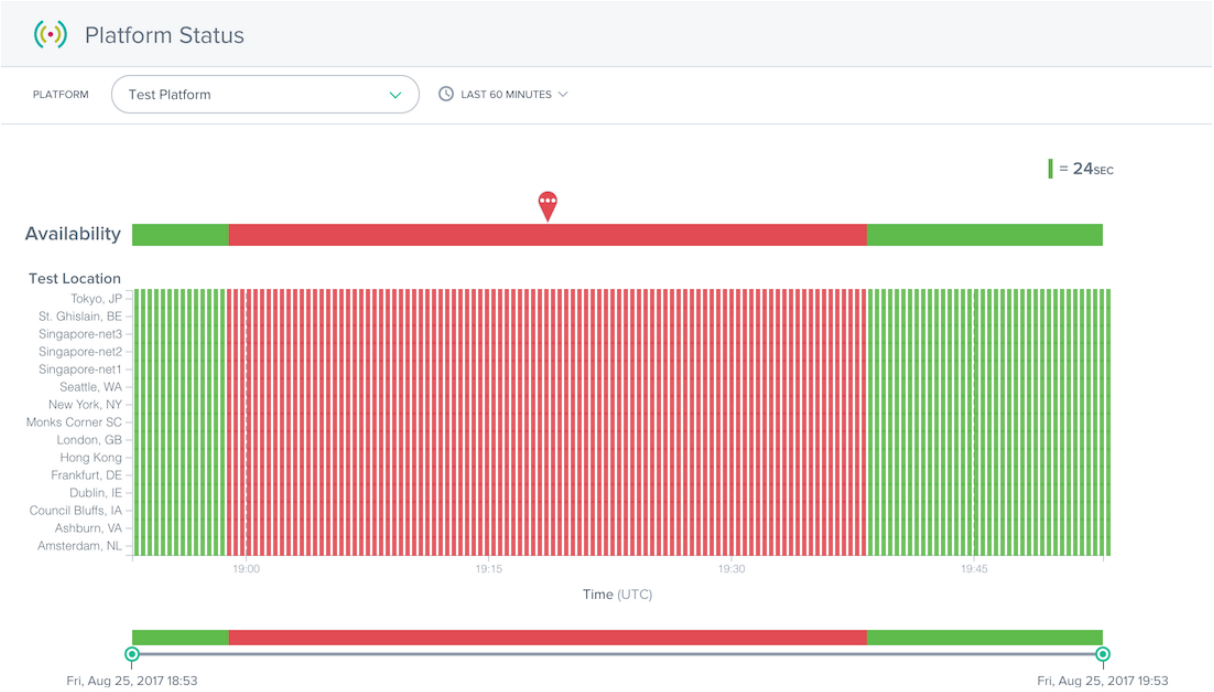
Das **Sonar-Menü** besteht aus folgenden Optionen:

1. **Plattformstatus** —Detaillierte Ergebnisse pro Teststandort und Gesamtverfügbarkeitsstatus.
2. **Plattformverlauf** —Überblick über den Verfügbarkeitsstatus der letzten drei Monate.

Plattformstatus

Der Bericht “Sonar Platform Status”zeigt Details zu den Prüfungen, die von den einzelnen Teststandorten durchgeführt werden, und den Gesamtstatus, der aus den aggregierten Daten berechnet wird.

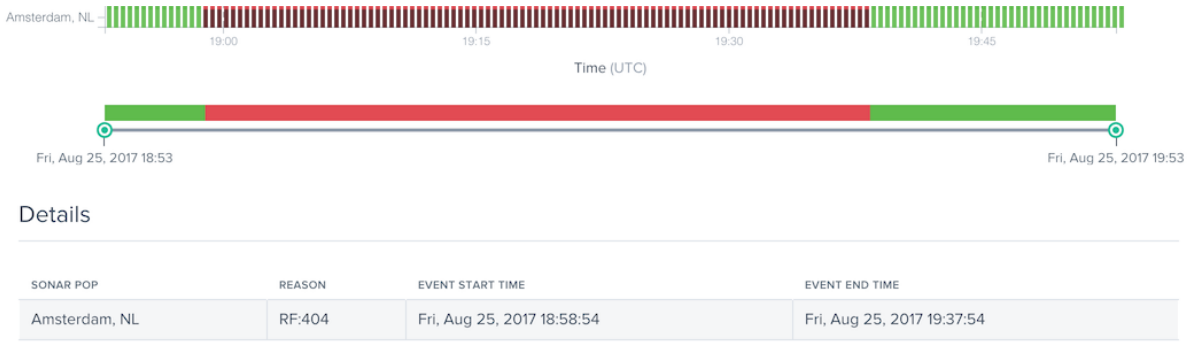
Um Informationen zu einer bestimmten Plattform zu erhalten, wählen Sie im Menü “**Plattformen**” eine Plattform aus.



Der Statusbericht enthält die folgenden Abschnitte:

- Verfügbarkeit: Am Anfang des Berichts steht die Verfügbarkeit, die Openmix basierend auf den aggregierten Ergebnissen der einzelnen Teststandorte gemeldet wird. Dies ist der Sonar-Status, der in den Openmix-Anwendungen während der angegebenen Zeiten verwendet wurde.
- Teststandorte: Die Ergebnisse der einzelnen Teststandorte werden angezeigt.
- Zeitschieberegler: Mit dem Zeitschieberegler können Sie ganz einfach detaillierte Zeiträume eingliedern. Ziehen Sie die Zeitschieberegler, um den Zeitraum des Berichts anzupassen und detailliertere Zeitintervalle anzuzeigen.

Die Details der fehlgeschlagenen Prüfungen können durch Klicken auf eine rote Markierung in einer Zeile der Testposition angezeigt werden. Die Details zu den Testfehlern werden im Abschnitt **Details** unterhalb des Berichts angezeigt.

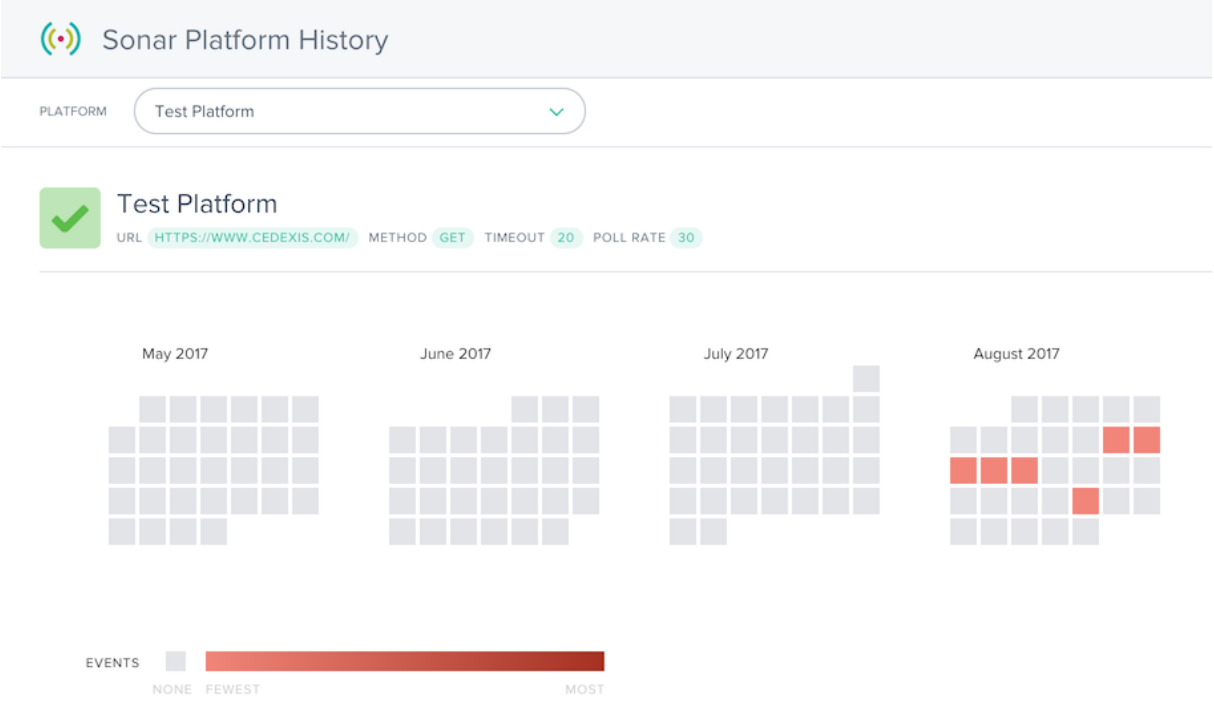


Die Spalte **Grund** enthält Details wie den Fehlercode, der von den Sonar-Prüfungen zurückgegeben wurde, die an diesem Testort aufgetreten sind.

Plattform-Historie

Der Bericht “Sonar Platform History”zeigt den Verfügbarkeitsstatus der aggregierten Prüfungen, die von jedem Teststandort in den letzten Monaten durchgeführt wurden.

Um Informationen zu einer bestimmten Plattform zu erhalten, wählen Sie im Menü “**Plattformen**” eine Plattform aus.



Der Bericht Historie zeigt einen Kalender der letzten Monate an. Die Tage mit Dienstausfällen werden in roten Farbverläufen angezeigt. Je mehr Verfügbarkeitsereignisse am Tag aufgetreten sind, desto rötlicher wird es angezeigt.

Unterhalb des Kalenders befindet sich eine Liste der aufgetretenen Dienstausfälle und einige grundlegende Details zu den Ereignissen.

Details

DATE	OUTAGES	START TIME - FIRST OUTAGE	END TIME - LAST OUTAGE	DURATION
2017-08-11	1	21:29:35	23:59:59	2 hours, 30 minutes, 25 seconds
2017-08-12	1	00:00:00	23:59:59	24 hours, 0 minutes, 0 seconds
2017-08-13	1	00:00:00	23:59:59	24 hours, 0 minutes, 0 seconds
2017-08-14	1	00:00:00	21:21:18	2 days, 23 hours, 51 minutes, 43 seconds
2017-08-15	3	14:50:00	15:50:05	0 hours, 4 minutes, 3 seconds
2017-08-24	3	17:44:12	18:03:21	0 hours, 15 minutes, 25 seconds

Sie können in den Spalten **Details** auf den Kalendertag oder das Datum klicken, um den Statusbericht

zu laden, um weitere Details zum Dienstausfall zu erhalten.

Auswirkung

April 21, 2020

Impact bietet einen leistungsstarken Einblick in die Performance- und Geschäftskennzahlen, die gesammelt werden, während Besucher auf Ihrer Website sind. Klicken Sie auf den Link für die Berichtsdaten, die Sie interessieren, um weitere Details anzuzeigen.

Cloud-Plattform-Visualisierungsberichte

Das Menü "**Auswirkungen**"besteht aus folgenden Optionen:

1. Navigationszeitdaten —Performance-Details auf Seitenebene, auch bekannt als unsere Seitenladezeitberichte.
2. Videowiedergabedaten —Qualität der Erfahrung und Videobereitstellungsdaten.
3. Ressourcen-Timing-Daten —Leistungsdetails einzelner Ressourcen auf Seiten.

Navigations-Timing-Daten

September 14, 2023

Navigationszeitberichte bieten einen aussagekräftigen Einblick in die umfangreichen Daten zum Laden von Seiten und zur Leistung von Ereignissen, die während des Besuchs Ihrer Website gesammelt wurden. Nach einer kurzen Beschreibung der Berichte finden Sie Einzelheiten zum Pivotieren, Filtern und Anpassen der Navigationszeitberichte.

Zeitberichte für die Navigation

Das Menü **Navigation Timing** enthält die folgenden Berichte:

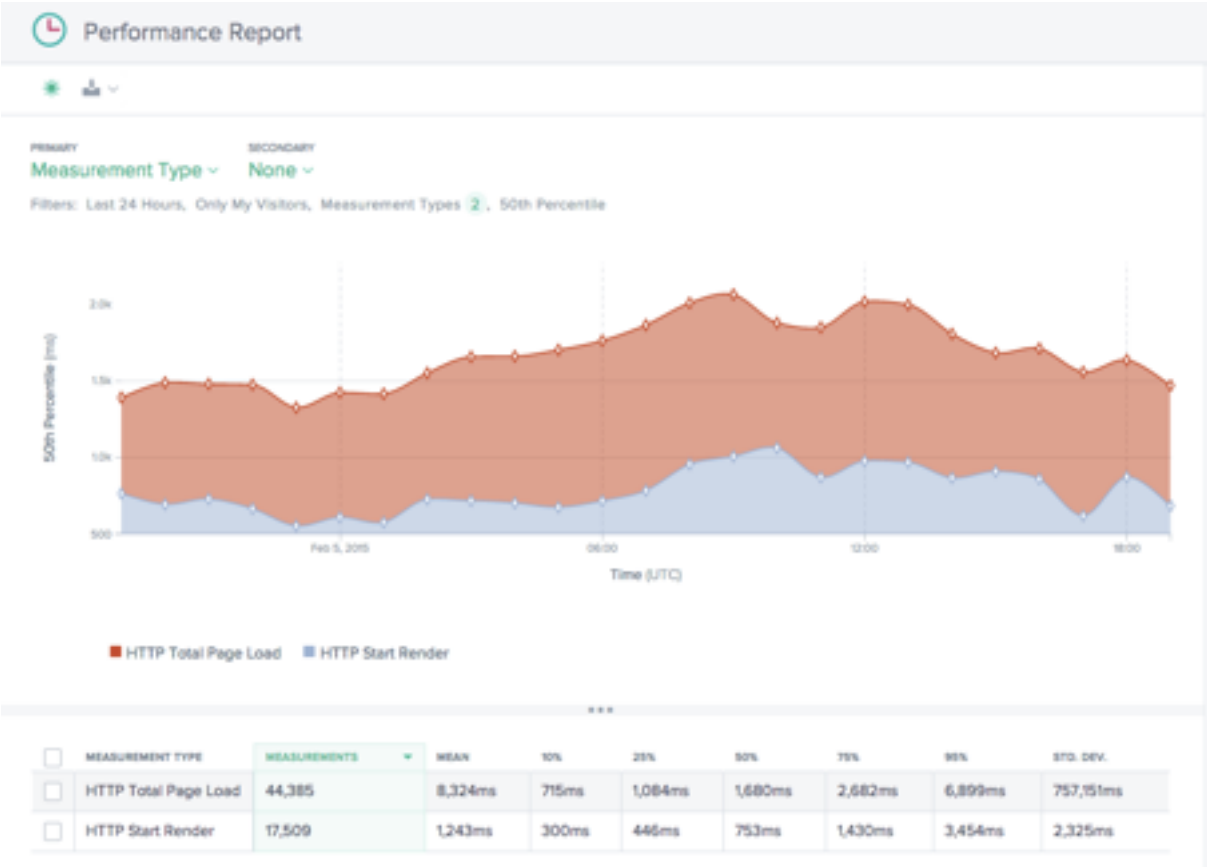
1. **Geolokalisierungsbericht** —Bericht über den Navigationszeitpunkt nach geografischer Dimension.
2. **Leistungsbericht** —Messdaten zum Navigations-Timing im Zeitverlauf.
3. **Statistischer Verteilungsbericht** —Eine Ansicht der Navigations-Timing-Daten in einer statistischen Verteilungsberichtsansicht.

Geolokalisierungsbericht

Dieser Bericht zeigt die Leistung der Seitenladezeit für jedes Land. Zoomen Sie in die Karte hinein, um bei Bedarf eine größere Granularität zu erhalten.

In der Tabelle sind die einzelnen Länder mit der zugehörigen Leistung bei der Seitenladezeit sowie der Anzahl der Messungen (Seitenaufrufe) aufgeführt.

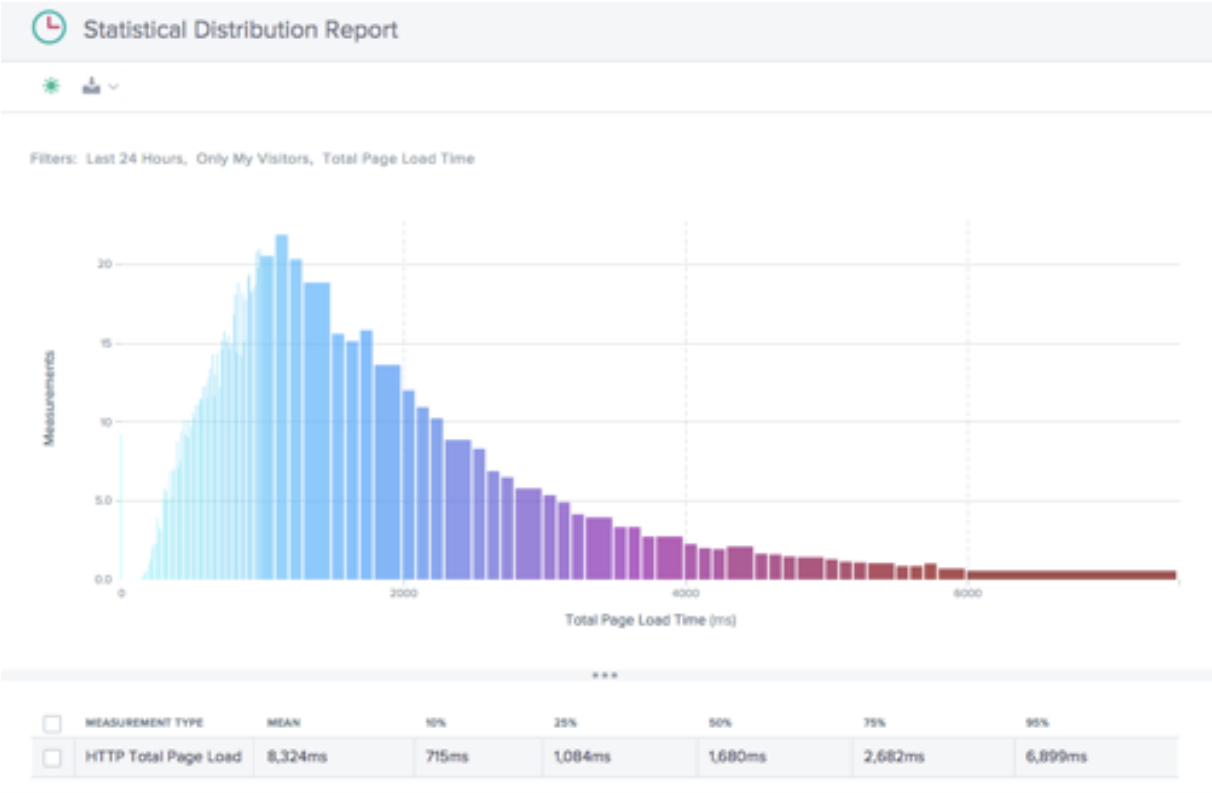
Leistungsbericht



Dieser Bericht zeigt die Leistung des Navigations-Timing-KPIs im Zeitverlauf, aufgeschlüsselt nach Messtyp.

Standardmäßig sind Rendern starten und Gesamtladezeit der Seite ausgewählt. Andere Messtypen können nach Bedarf hinzugefügt werden.

Statistischer Verteilungsbericht



Dieser Bericht zeigt die statistische Verteilung der Werte für Navigationszeit und Seitenladezeit.

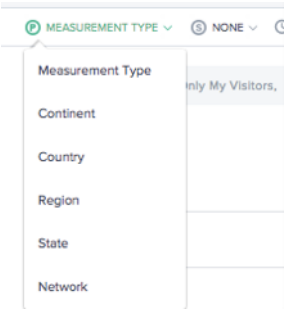
Der Bericht gibt Aufschluss darüber, wie viele Messungen (Seitenaufrufe) pro Seitenladezeitwert erfasst wurden.

Verwenden von Navigations-Timing-Berichten

Verwenden Sie die folgenden Funktionen in den Navigationszeitberichten, um die Berichtsansichten für spezifische Berichtsanforderungen zu verfeinern und anzupassen.

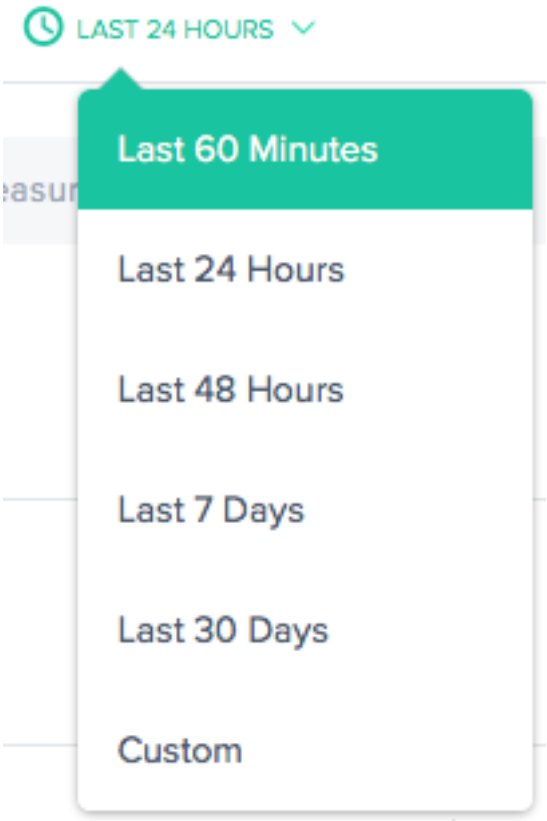
Zusätzlich zu den Standardfunktionen der Berichte wie Teilen von Berichten, Umschalten im Hintergrund, Datenexport und mehr sind die folgenden Funktionen verfügbar:

Primäre und sekundäre Dimensionen



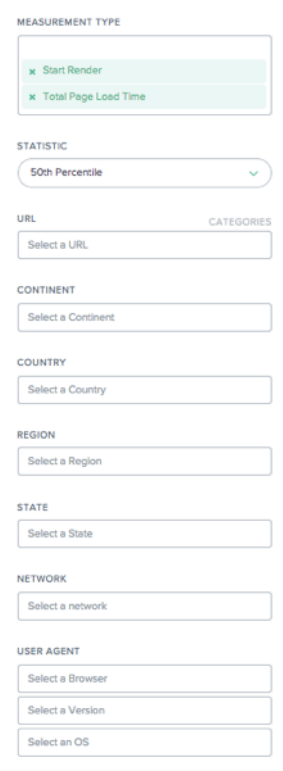
Die primäre Dimension des Diagramms wird über eine Auswahlliste über dem Diagramm ausgewählt. Verwenden Sie dies als wichtige Grundlage für den Bericht, um die Daten als Messtyp (Standard), Kontinent, Land, Region, Bundesstaat oder Netzwerk (ASN) auszudrücken. Eine sekundäre Dimension kann ebenfalls ausgewählt werden, um die Berichterstattung weiter zu verfeinern.

Filter: Berichts-Zeitbereich



Die Berichte können mit einem Zeitraum von „Letzte 60 Minuten“, „Letzte 24 Stunden“, „Letzte 48 Stunden“, „Letzte 7 Tage“, „Letzte 30 Tage“oder mit einem benutzerdefinierten Bereich generiert werden. Die Standardansicht ist die Letzte 24 Stunden.

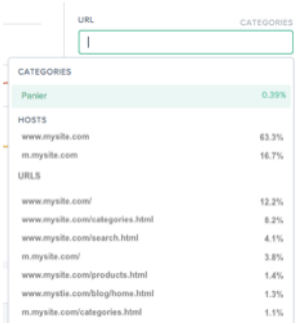
Filter: Leistungsstarke Drilldown-Funktionen



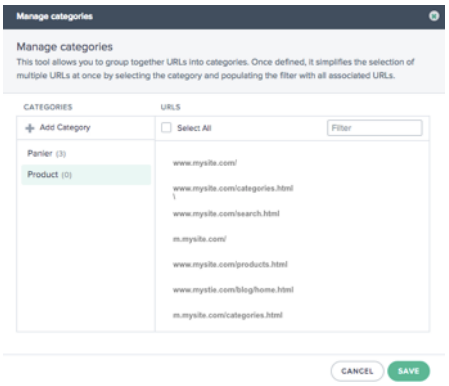
Die Berichte unterscheiden sich geringfügig in Bezug darauf, welche Filter basierend auf den Daten geeignet sind. Folgendes ist in den Navigations-Timing-Berichten verfügbar:

- **Messtyp** —Wählen Sie einen oder mehrere Messtypen für die Anzeige aus. Rendern starten und Gesamtladezeit der Seite sind standardmäßig ausgewählt.
- **Statistik** —Wählen Sie eine statistische Kennzahl aus, um die Daten anzuzeigen.
- **URL** —Wählen Sie eine oder mehrere URLs zum Anzeigen aus. Sie können auch einen Hostnamen oder eine Kategorie von URLs auswählen (siehe unten).
- **Kontinent** —Wählen Sie einen oder mehrere Kontinente aus, die Sie einbeziehen möchten
- **Land** —Wählen Sie ein oder mehrere Länder aus, die Sie einbeziehen möchten
- **Region** —Wählen Sie eine oder mehrere geografische Regionen (falls zutreffend) aus, die aufgenommen werden sollen
- **Bundesstaat** —Wählen Sie einen oder mehrere geografische Staaten (falls zutreffend) aus, die aufgenommen werden sollen
- **Netzwerk** —Wählen Sie ein oder mehrere Netzwerke (ASN) aus, die Sie einbeziehen möchten
- **Benutzeragent** —Wählen Sie einen oder mehrere Browser, Browserversion und/oder Betriebssystem aus, um die Berichtsdaten weiter zu verfeinern.

URL-Kategorien



Navigationszeitberichte können nach URLs, Hosts oder Kategorien gefiltert werden. Finden Sie schnell einen oder mehrere interessante Artikel, indem Sie ihn in das **URL-Suchfeld** eingeben.



Um eine Kategorie zu erstellen, klicken Sie rechts neben dem **URL-Feld** auf **KATEGORIEN** . Das Dialogfeld **„Kategorien verwalten** “wird angezeigt.

Wählen Sie **Kategorie hinzufügen**, um eine Kategorie zu erstellen und sie wie gewünscht zu benennen. Wählen Sie dann die URLs aus, die für die neue Kategorie von Interesse sind. Um URLs zu finden, beginnen Sie einfach mit der Eingabe in das Suchfeld und die URL-Liste wird nach dem Suchtext gefiltert.

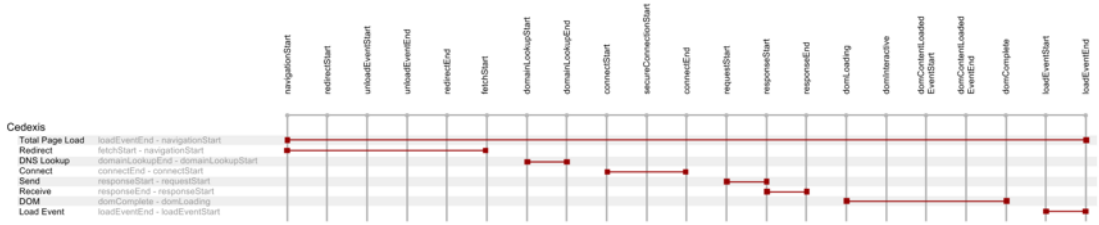
Wenn alle URLs für die Kategorie ausgewählt wurden, klicken Sie auf die Schaltfläche **Speichern**, um die Definition der **Kategorie** abzuschließen.

Daten zum Navigations-Timing und zur Ladezeit der Seite

Das Radar-Tag kann detaillierte Informationen zur Download-Leistung für Seiten sammeln, die das Tag implementieren. Die Leistungsinformationen der NavTiming-API werden von den Browsern gesammelt, die die API unterstützen (Chrome 6.5+, Firefox 8+, IE9+).

NetScaler zeigt diese Informationen im Kundenportal an, wo dieser sehen kann, welche Leistung Endbenutzer tatsächlich bei der Interaktion mit Ihren Webseiten erleben.

Im Folgenden finden Sie ein Diagramm und eine Beschreibung der einzelnen Seitenlademetriken, die Radar über Navigation Timing bereitstellt:



Messung	Beschreibung	Berechnung des Nav-Timings
Gesamte Seitenladezeit	Der vollständige Download der Webseite und der entsprechenden Komponenten.	`loadEventEnd` – `navigationStart`
Umleiten	Die erste Zeit, die für die Weiterleitung auf die Seite verwendet wurde.	`fetchStart` – `navigationStart`
DNS-Suche	Die Zeit, die benötigt wird, bis die DNS-Auflösung des Basisseiten-URI abgeschlossen ist.	`domainLookupEnd` – `domainLookupStart`
Verbinden	Die Zeit, um eine TCP-Verbindung herzustellen, einschließlich SSL, falls es verwendet wird.	`connectEnd` – `connectStart`
Senden	Die HTTP-Anforderungs- und Antwortzeit der ersten Basisseite, ohne jeglichen Nachrichtentext. Ein guter Indikator für die Latenz des Backend-Servers.	`responseStart` – `requestStart`
Empfangen	Die Zeit, die benötigt wurde, um den Hauptteil des HTML-Codes des Basisdokuments zu erhalten.	`responseEnd` – `responseStart`

Messung	Beschreibung	Berechnung des Nav-Timings
DOM	Die Zeit, um alle Medien, Objekte, die aus dem Basis-HTML aufgerufen werden, herunterzuladen und in den Browser zu laden.	`domComplete - domLoading`
Load-Ereignis	Die Zeit für die Ausführung von JavaScript und das Rendern der Seite im Browser.	`loadEventEnd - loadEventStart`
Rendern starten	Die Start-Render-Zeit ist der erste Zeitpunkt, zu dem etwas auf dem Bildschirm verfügbar gemacht wurde.	Mehr Timing von Chrome/IE als Erweiterung der NavTiming-API hinzugefügt.

Videowiedergabedaten

June 4, 2021

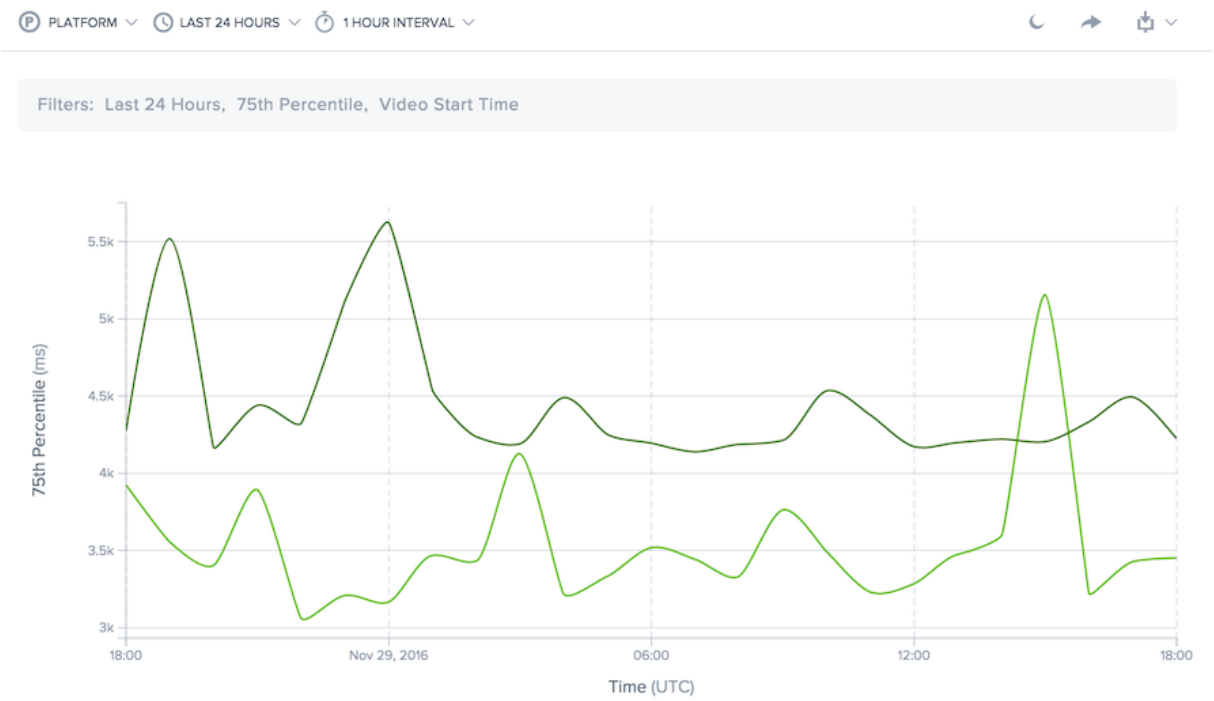
Cloud Platform Visualization sammelt die relevanteste Leistung der Videonetzwerkbereitstellung und Qualität der Erfahrungsdaten für die Berichterstellung. Die Videoqualität der Erfahrung wird direkt von der Qualität der Video-Chunk-Bereitstellung gesteuert. Openmix optimiert auf Basis von Radarnetzwerk-Zustellungsmetriken, um Benutzern ein bestmögliches Anzeigeerlebnis zu bieten. Nach einer kurzen Beschreibung der Berichte finden Sie Details zum Pivotieren, Filtern und Anpassen der Berichte.

Berichte zur Videowiedergabe

Das Menü **Videowiedergabedaten** enthält die folgenden Berichte:

1. **Leistungsbericht** —Video-Erlebnis- und Lieferdaten im Zeitverlauf.
2. **Statistischer Verteilungsbericht** —Variation der Videowiedergabe im Laufe der Zeit.
3. **Histogramm-Vergleichsbericht** - Vergleichen Sie Video-Chunk-Übermittlungsdaten mit KPIs der Qualität der Erfahrung.

Leistungsbericht



Dieser Bericht zeigt die Videowiedergabe im Laufe der Zeit an. Es ermöglicht Ihnen, Liefertrends im Laufe der Zeit zu visualisieren, zu sehen, wie viel Video angesehen wird, und die Gesamtqualität des Seherlebnisses.

Die Daten können mit Dimensionen angezeigt werden, die einen Vergleich mehrerer Werte ermöglichen. Beispielsweise können die Daten nach Domäne angezeigt werden, um die Leistung der Lieferung über mehrere Videodomänen hinweg zu vergleichen.

Der Zeitraum für den Bericht kann von den letzten 60 Minuten bis zu 30 Tagen innerhalb der letzten 13 Monate angepasst werden.
Die Daten können nach der Plattform gefiltert werden, die zum Bereitstellen des Inhalts, des Hostnamens und des Pfades des Inhalts oder der Videoblöcke, des geografischen Standorts, des Netzwerks oder des Viewer-Benutzer-Agents verwendet wird.

Statistischer Verteilungsbericht

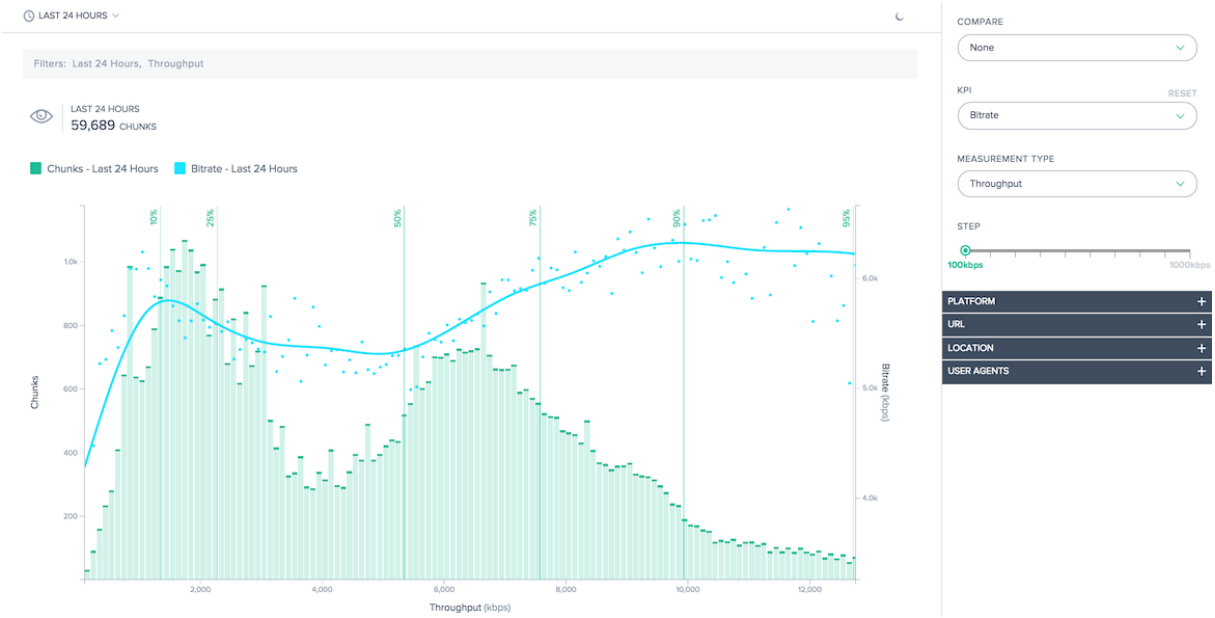
Dieser Bericht zeigt die Variation der Videowiedergabe im Laufe der Zeit. Es ermöglicht Ihnen, die einheitliche Videobereitstellung zu visualisieren und die Anzeigeerlebnisse für die gesamte Nutzerpopulation besser zu verstehen. Der Bericht berechnet die Benutzerleistung am 10., 25., 50., 75. und 95. Perzentil sowie den Mittelwert.

Wie der Performance-Bericht können die Daten mit Dimensionen angezeigt werden, die einen Vergleich mehrerer Werte ermöglichen. Beispielsweise können die Daten nach Plattform (Dienstanbieter oder Server) angezeigt werden, um die Konsistenz der Bereitstellung für mehrere Plattformen zu vergleichen.

Der Zeitraum für den Bericht kann von den letzten 60 Minuten bis zu 30 Tagen innerhalb der letzten 13 Monate angepasst werden.

Die Daten können nach der Plattform gefiltert werden, die zum Bereitstellen des Inhalts, des Hostnamens und des Pfades des Inhalts oder der Videoblöcke, des geografischen Standorts, des Netzwerks oder des Viewer-Benutzer-Agents verwendet wird.

Histogramm-Vergleichsbericht



Dieser Bericht behandelt die Beziehungen zwischen Video-Chunk-Übermittlungsdaten und den KPIs für die Qualität der Erfahrung.

Es gibt zwei Hauptmerkmale in diesem Bericht:

- Das Histogramm zeigt, wie oft Videoblöcke mit einem bestimmten Qualitätsniveau geliefert wurden, entweder Reaktionszeit oder Durchsatz.
- Einzelne KPIs können im Histogramm überlagert werden. Die Liniendiagramme, die der KPI erzeugt wurde, wenn ein Stück mit der angegebenen Qualität geliefert wurde.

Das Histogramm zeigt beispielsweise den von Radar gemessenen Durchsatz an. Die KPIs zeigen wahrscheinlich, dass die Bitrate höher ist und die Rebuffering niedriger ist, wenn der gemessene Durchsatz höher ist. Gemeinsam helfen diese Funktionen, die Beziehung zwischen Lieferqualität und der Qualität der Erfahrung, die für den Betrachter produziert wird, zu quantifizieren.

Wenn die Standard-Berichtsgenerierung nicht ausreicht, kann die Histogramm-Bucket-Größe angepasst werden, und bestimmte Abschnitte der Verteilung können zur Anzeige ausgewählt werden.

Zusätzlich zu den Histogrammen auf KPIs können Daten direkt verglichen werden. Es können mehrere KPIs für die Anzeige ausgewählt werden, und frühere Zeiträume können verglichen werden, um Leistungsänderungen im Laufe der Zeit anzuzeigen.

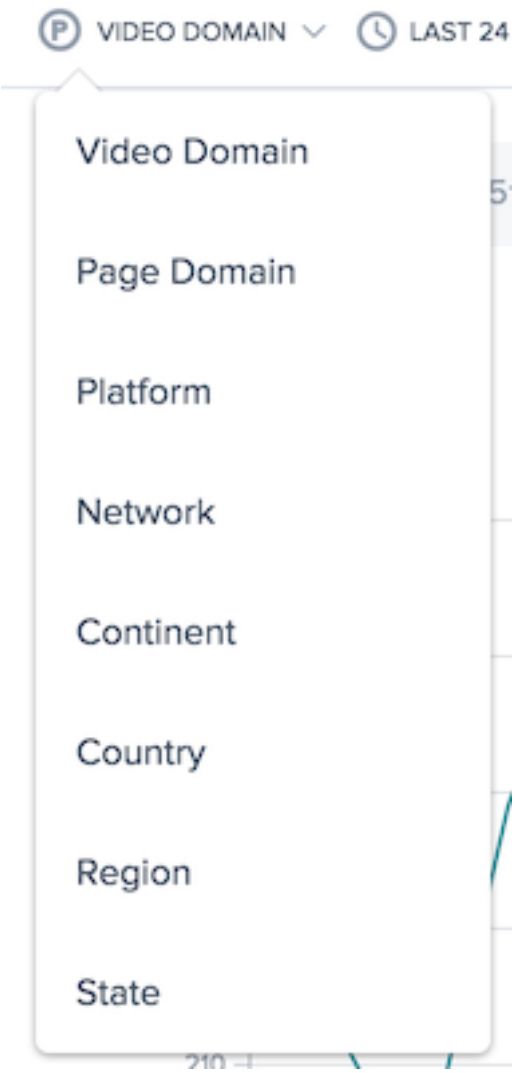
Die Daten können nach der Plattform gefiltert werden, die zum Bereitstellen des Inhalts, des Hostnamens und des Pfades des Inhalts oder der Videoblöcke, des geografischen Standorts, des Netzwerks oder des Viewer-Benutzer-Agents verwendet wird.

Verwenden von Videowiedergabeberichten

Zum Verfeinern und Anpassen der Berichtsansichten an bestimmte Berichtsanforderungen verwenden Sie die folgende Funktionalität in den Berichten zur Videowiedergabe für Leistung und statistische Verteilung.

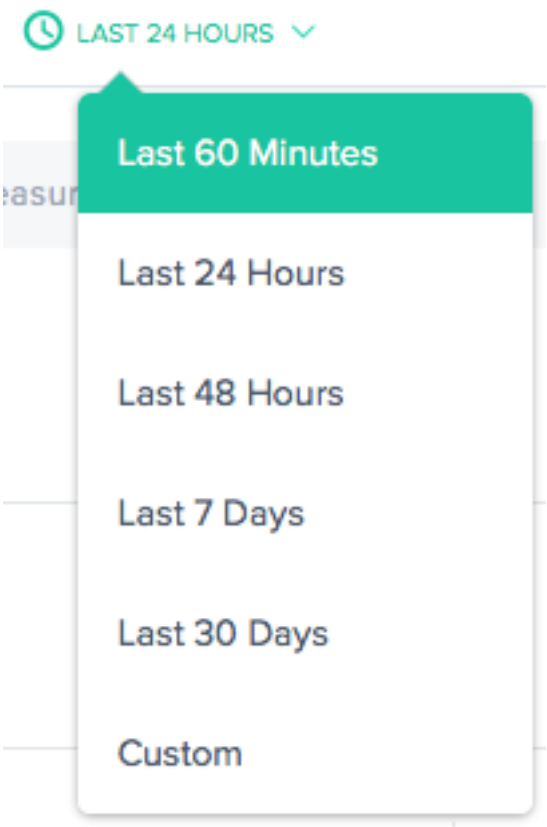
Zusätzlich zu den Standardfunktionen der Berichte wie Berichtsfreigabe, Hintergrundumschaltung, Datenexport und mehr stehen folgende Funktionen zur Verfügung:

Primäre Dimension



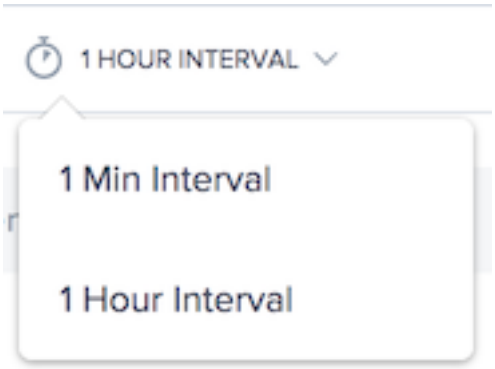
Die primäre Dimension des Diagramms wird über eine Auswahlliste oberhalb des Diagramms ausgewählt. Verwenden Sie diese Funktion als leistungsstarke Pivot für den Bericht, um die Daten in Bezug auf Video Domain, Page Domain, Plattform, Netzwerk (ASN), Kontinent, Land, Region oder Staat auszudrücken.

Filter: Berichtszeitbereich



Die Berichte können mit einem Zeitbereich von den letzten 60 Minuten, den letzten 24 Stunden, den letzten 48 Stunden, den letzten 7 Tagen, den letzten 30 Tagen oder einem benutzerdefinierten Bereich erstellt werden. Die Standardansicht ist die Letzte 24 Stunden.

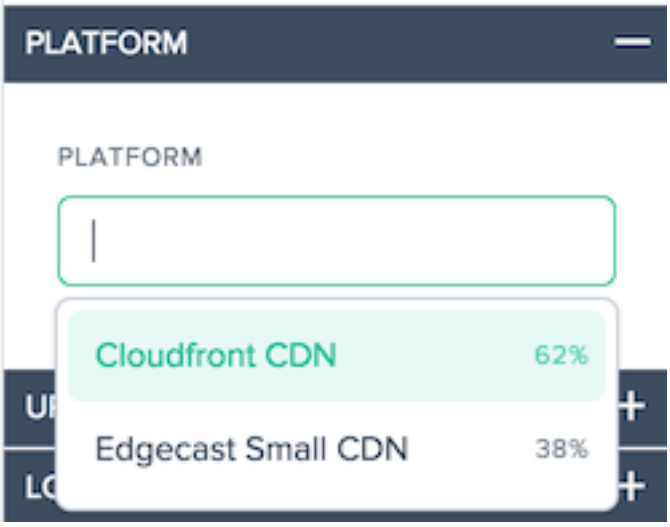
Berichtsintervall



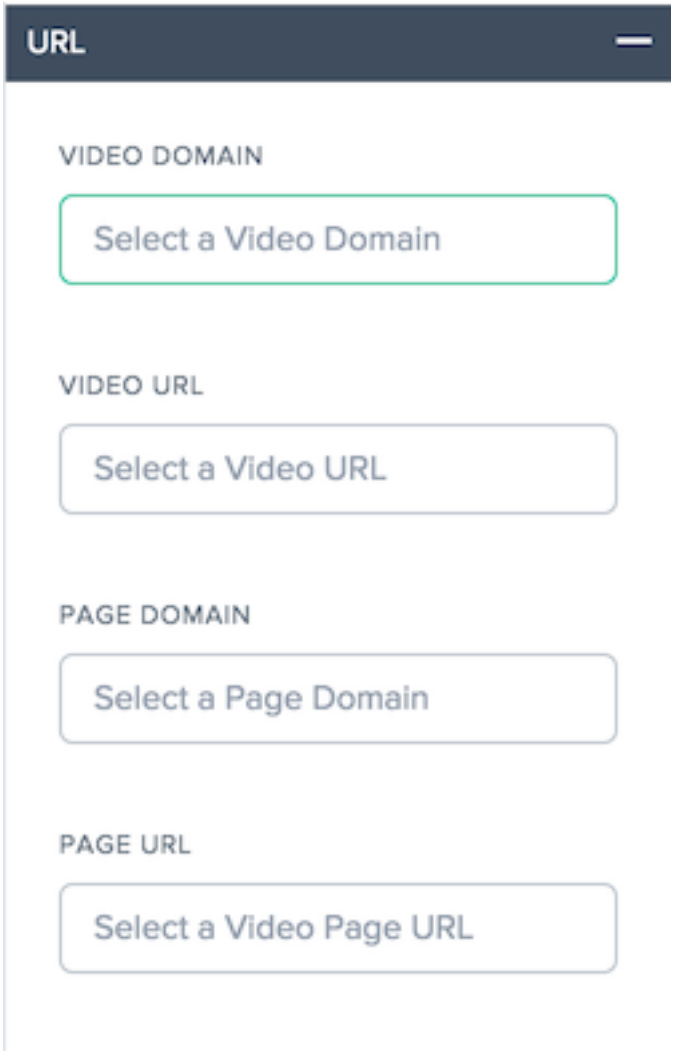
Die primäre Dimension des Diagramms wird über eine Auswahlliste oberhalb des Diagramms ausgewählt. Dies ermöglicht eine detaillierte Berichterstellung von Performance-Daten.

Filter: Leistungsstarke Drilldown-Funktionen

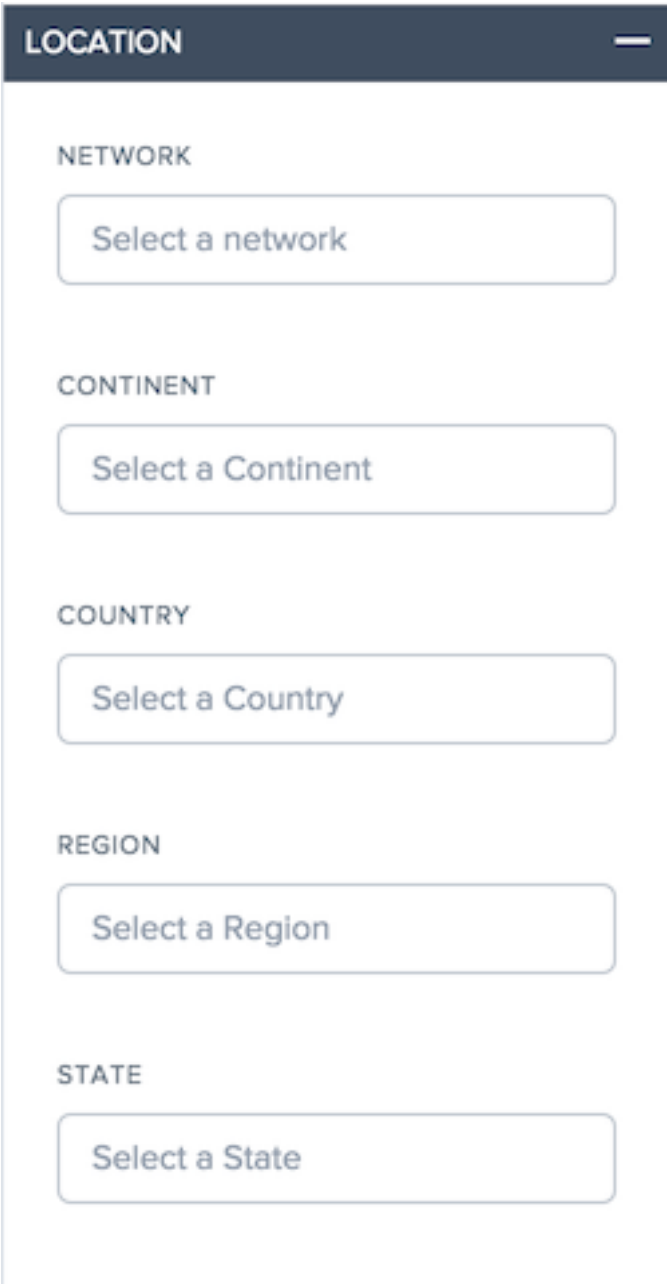
Die Berichte unterscheiden sich geringfügig in Bezug darauf, welche Filter basierend auf den Daten geeignet sind. Die folgenden Berichte sind in den Videowiedergabeberichten verfügbar:



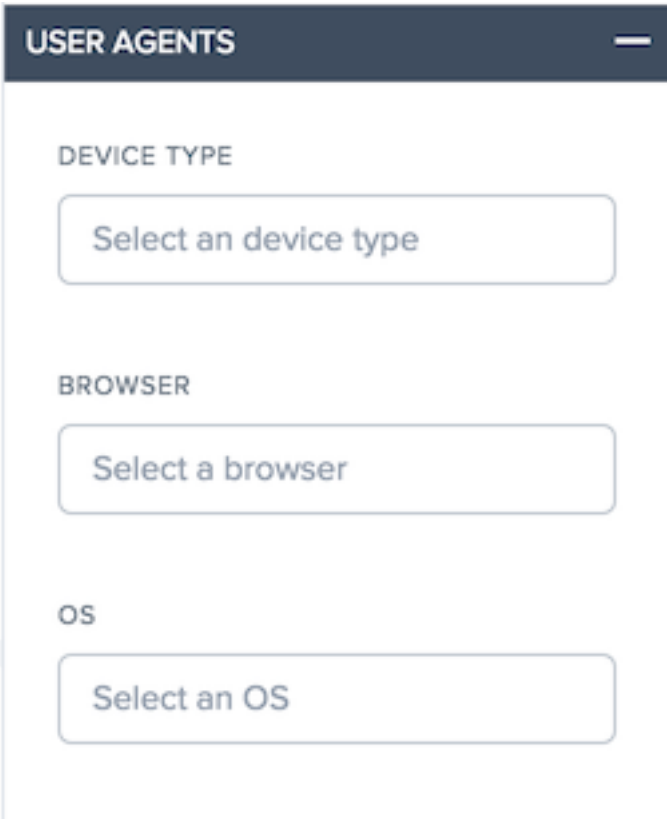
- **Plattform** - Wählen Sie eine oder Plattformen aus, die gefiltert werden sollen. Standardmäßig sind alle Plattformen im Bericht enthalten.



- **Videodomäne** - Wählen Sie einen oder mehrere Hostnamen aus, auf denen Videos gehostet werden. Standardmäßig sind alle Hostnamen im Bericht enthalten.
- **Video-URL** - Wählen Sie einen oder mehrere Pfade für die Videos aus, standardmäßig sind alle Pfade im Bericht enthalten.
- **Seitendomäne** - Wählen Sie einen oder mehrere Hostnamen aus, auf denen Seiten gehostet werden. Standardmäßig sind alle Hostnamen im Bericht enthalten.
- **Seiten-URL** - Wählen Sie einen oder mehrere Pfade für die Seiten aus, standardmäßig sind alle Pfade im Bericht enthalten.



- **Netzwerk** —Wählen Sie ein oder mehrere Netzwerke (ASN) aus, die eingeschlossen werden sollen
- **Kontinent** —Wählen Sie einen oder mehrere Kontinente aus, die eingeschlossen werden sollen
- **Land** —Wählen Sie ein oder mehrere Länder aus, die einbezogen werden sollen
- **Region** —Wählen Sie (falls zutreffend) eine oder mehrere geografische Regionen aus, die berücksichtigt werden sollen.
- **Bundesstaat** —Wählen Sie einen oder mehrere geografische Staaten (falls zutreffend) aus, die eingeschlossen werden sollen.

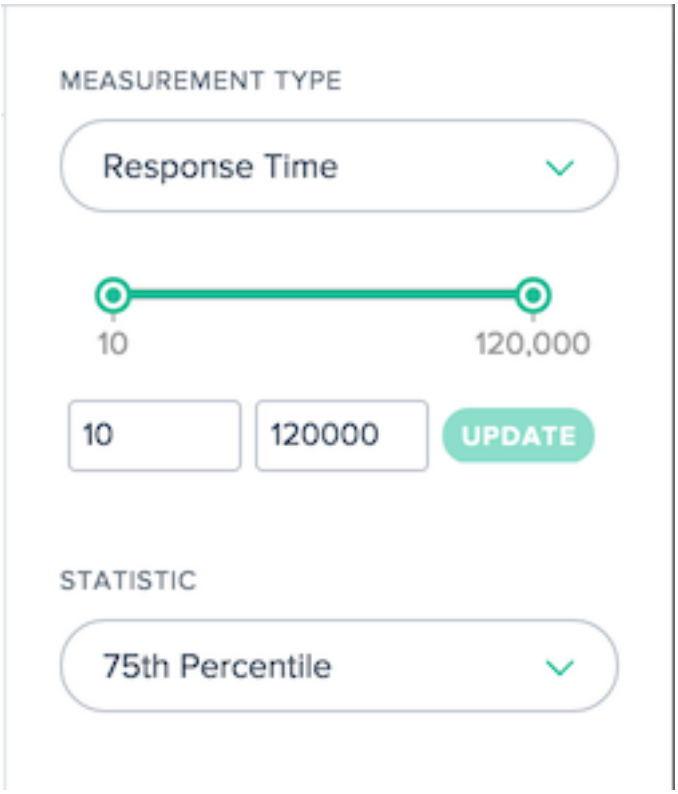


- **User Agent** —Wählen Sie einen oder mehrere Gerätetypen, Browser und/oder Betriebssystemtypen aus, um die Berichtsdaten weiter zu verfeinern.

Leistungsbericht für die Videowiedergabe verwenden

Verwenden Sie die folgende Funktionalität im Leistungsbericht, um den Leistungsbericht für bestimmte Berichtsanforderungen zu verfeinern und anzupassen.

Filter: Leistungsstarke Drilldown-Funktionen



Die Berichte unterscheiden sich geringfügig in Bezug darauf, welche Filter basierend auf den Daten geeignet sind. Die folgenden Berichte sind in den Videowiedergabeberichten verfügbar:

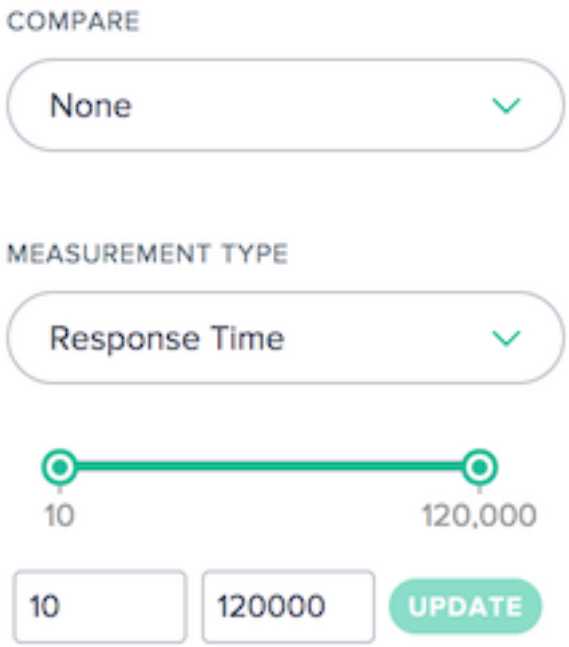
- **Messart** —Wählen Sie den anzuzeigenden Messtyp aus, die Reaktionszeit wird zunächst ausgewählt.
- **Count Slider** - Filtern Sie die Daten nach der minimalen und maximalen Messanzahl, die in den Bericht aufgenommen werden müssen.
- **Statistik** —Wählen Sie die anzuzeigende statistische Kennzahl aus.

Zusätzlich zu diesen berichtspezifischen Filtern stehen die standardmäßigen Videowiedergabefilter zur Verfügung, um die Ergebnisse anzupassen.

Statistischer Verteilungsbericht für die Videowiedergabe verwenden

Um den Bericht für bestimmte Berichtsanforderungen zu verfeinern und anzupassen, wenden Sie die folgende Funktionalität im Bericht “Statistische Verteilung”an.

Filter: Leistungsstarke Drilldown-Funktionen



Die Berichte unterscheiden sich geringfügig in Bezug darauf, welche Filter basierend auf den Daten geeignet sind. Die folgenden Berichte sind in den Videowiedergabeberichten verfügbar:

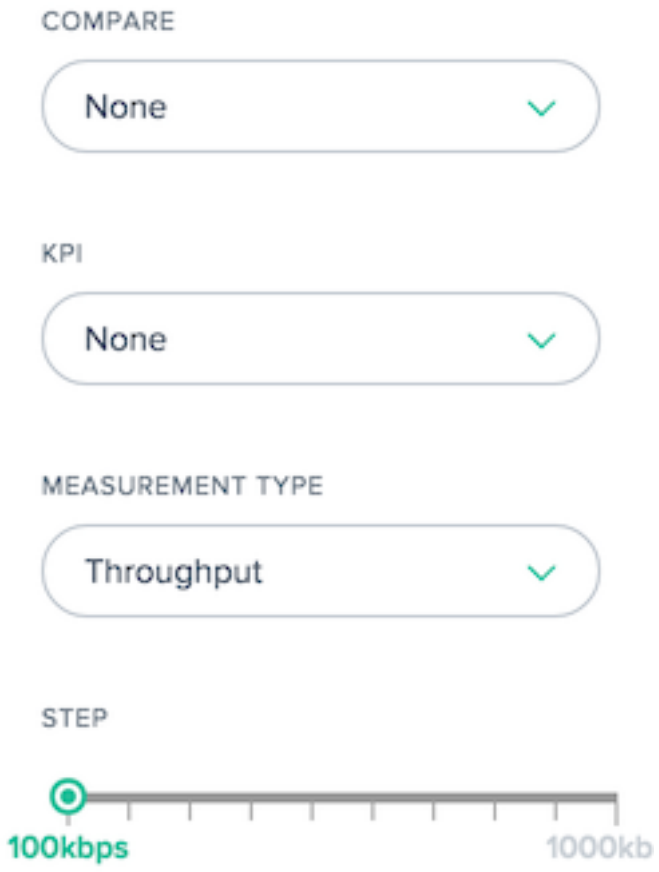
- **Vergleichen** —Wählen Sie den Wert aus, der zum Erstellen eines Vergleichs im Bericht verwendet wird. Basierend auf der getroffenen Auswahl müssen die für den Vergleich verwendeten Werte ausgewählt werden. Die resultierenden Verteilungen werden nebeneinander angezeigt, so dass sie leicht verglichen werden können.
- **Messart** —Wählen Sie den anzuzeigenden Messtyp aus, die Reaktionszeit wird zunächst ausgewählt.
- **Count Slider** - Filtern Sie die Daten nach der minimalen und maximalen Messanzahl, die in den Bericht aufgenommen werden müssen.

Zusätzlich zu diesen berichtspezifischen Filtern stehen die standardmäßigen Videowiedergabefilter zur Verfügung, um die Ergebnisse anzupassen.

Histogramm-Vergleichsbericht für die Videowiedergabe verwenden

Um den Bericht für bestimmte Berichtsanforderungen zu verfeinern und anzupassen, wenden Sie die folgende Funktionalität im Histogramm-Vergleichsbericht an.

Filter: Leistungsstarke Drilldown-Funktionen



Die Berichte unterscheiden sich geringfügig in Bezug darauf, welche Filter basierend auf den Daten geeignet sind. Die folgenden Berichte sind in den Histogramm-Vergleichsberichten verfügbar:

- **Vergleichen** —Wählen Sie den Wert aus, der zum Erstellen eines Vergleichs im Bericht verwendet wird. Basierend auf der getroffenen Auswahl müssen die für den Vergleich verwendeten Werte ausgewählt werden. Die resultierenden Histogramme und KPIs werden übereinander überlagert, so dass sie leicht verglichen werden können.
- **KPI** —Wählen Sie den Kennzahlenwert aus, der mit dem Histogrammmesstyp dargestellt wird.
- **Messart** —Wählen Sie den Messtyp aus, der zum Auffüllen des Histogramms verwendet wird.
- **Step Slider** - Legen Sie die Größe der Buckets verwendet, um das Histogramm zu generieren.

Zusätzlich zu diesen berichtspezifischen Filtern stehen die standardmäßigen Videowiedergabefilter zur Verfügung, um die Ergebnisse anzupassen.

Videowiedergabedaten

Die Datenerhebung erfolgt unter Verwendung der Eigenschaften und Ereignisse der DatenHTML5-Videoelementfür die Qualität der Erfahrung und derRessourcen-Timing-API für die Video-Chunk-Daten aus den Browsern, die die APIs unterstützen.

Videodaten werden im Portal angezeigt, wo Berichte mit Informationen über die Qualität der Endbenutzer und die Leistung der Netzwerkbereitstellung erstellt werden können.

Im Folgenden finden Sie ein Diagramm und eine Beschreibung der einzelnen Videometriken, die gesammelt werden:

Messung	Beschreibung
Reaktionszeit pro Chunk	Die Zeit, die benötigt wird, bis die Chunks die Lieferung basierend auf den Ressourcen-Timing-Messungen starten (`responseStart – requestStart`)
Durchsatz pro Chunk	Die Geschwindigkeit, mit der Video-Blöcke basierend auf den Ressourcen-Timing-Messungen heruntergeladen wurden. (kBit/s)
Ausgelieferte Bitrate	Die Sekunden-Bitrate des Videos basierend auf der Größe der gelieferten Blöcke. (KB)
Rebuffering-Verhältnis	Der Prozentsatz der Zeit, die während der Wiedergabe verbracht wurde. (%)
Fehler beim Videostart	Die HTTP-Request- und Antwortzeit der anfänglichen Basisseite, ohne jeden Nachrichtentext. Ein guter Indikator für die Back-End-Server-Latenz.
Videostartzeit	Die Zeit, die zum Starten der Videowiedergabe nach dem Wiedergabeversuch gedauert hat. (ms)

Ressourcen-Timing-Daten

June 4, 2021

Übersicht

Resource Timing Daten bieten einen leistungsstarken Einblick in die Leistung einzelner Ressourcen auf Objektebene Ihrer Website.

Resource Timing hilft Kunden, die Netzwerkleistung von Objekten auf Seitenebene zu betrachten, basierend auf den Daten, die wir zur Verbindungszeit, Downloadzeit und unterschiedlichen Reaktionszeiten bereitstellen. Beispiele für Objekte auf Seitenebene sind Bilder, JavaScript-Dateien, API-Aufrufe usw. Es gibt Kunden eine bessere Einsicht in die Leistung der Seitenebene. Das Endergebnis ist, dass Kunden ihre Lieferung besser verwalten und eine insgesamt bessere Benutzererfahrung gewährleisten können.

In den folgenden Abschnitten werden Sie anhand der Konfiguration, der Datenbeschreibung und der Berichterstellung von Ressourcenzeitdaten beschrieben.

Ressourcenzeitkonfiguration

Über die Benutzeroberfläche im Portal können Sie Einstellungen für die Resource Timing-Konfiguration als Alternative zur JSON-Codierung direkt eingeben.

Hinweis: Auch wenn die Konfiguration über JSON-Codierung noch verfügbar ist, wird dringend empfohlen, die Benutzeroberfläche für die Konfiguration zu verwenden.

Navigation

Wählen Sie im linken Navigationsbereich Auswirkung -> Resource Timing Data -> Resource Timing Configuration.

Erstkonfiguration

- Wählen Sie “**Jetzt starten**”auf der ersten Seite aus, um loszulegen.
- Ein Dialogfeld “**Standardkonfigurationseinstellungen**”wird geöffnet, in dem Sie Ressourcen ein- oder ausschließen und eine Abtastrate eingeben können.

Standardkonfigurationseinstellungen Die Standardkonfigurationseinstellungen sind die Mindesteinstellungen, die für den Einstieg erforderlich sind. Es gibt drei Hauptkonfigurationseinstellungen:

- Ein- und Auszuschließende Ressourcen
- Abtastrate
- Standardanbietererkennung

Ein- oder Auszuschließende Ressourcen Mit dieser Funktion können Sie bestimmte Ressourcen ein- oder ausschließen, aus denen Zeitdaten gesammelt werden. Wenn leer gelassen wird, werden standardmäßig alle Ressourcen eingeschlossen (d. h. nichts ist ausgeschlossen).

Sie können Ressourcen wie Dateiname, Dateinamenerweiterung, Ordnername, Dateipfad oder sogar eine Zeichenfolge eingeben. Alles, was in der Zeichenfolge enthalten ist, wird als Ressource abgeholt.

Drücken Sie bei jeder Eingabe eines **Ressourcennamens** die **Eingabetaste**. Wenn Sie bestimmte Ressourcen im Feld **Einschließen** eingeben, werden nur diese Ressourcen berücksichtigt, und alle anderen Ressourcen werden ausgeschlossen. Um bestimmte Ressourcen auszuschließen, geben Sie sie in das Feld **Ausschließen** ein, und alles andere wird eingeschlossen. Sie können sogar eine benutzerdefinierte Regex-Logik schreiben, um den Ein- oder Ausschlussprozess anzupassen.

Abtastrate Mit der **Abtastrate** können Sie eine kleine Stichprobe von Besuchern eingeben, von denen Sie IRT-Daten sammeln möchten. Geben Sie einen Wert zwischen 0 und 100 ein (in Prozent genommen). Idealerweise müssen Sie den niedrigsten Prozentsatz für die Abtastrate eingeben - ein Wert, der ausreicht, um die erforderliche Anzahl von Ressourcen-Timing-Messungen zu erfassen.

Hinweis: Resource Timing Datenerfassung belastet das System stark. Diese Funktion ist für Kunden, Daten zu Beispielen, und soll nicht für jede Radar-Sitzung Daten sammeln.

Achtung: Bei Kunden mit einem hohen Datenvolumen beginnen Sie mit einer Abtastrate von 1%. Erhöhen Sie es langsam, bis eine statistisch nützliche Rate erreicht ist. Eine hohe Abtastrate kann möglicherweise eine Serverüberlastung, eine Verlangsamung oder sogar einen Absturz verursachen.

Schritte für die Einstellung der ersten Abtastrate

1. Beginnen Sie mit einer Abtastrate von 1%. Warten Sie 24-48 Stunden, bis Sie einige Messungen erhalten.
2. Überprüfen Sie das **IRT-Diagramm**, um zu sehen, ob es über mehrere Assets hinweg glatt aussieht.
3. Wenn ja, dann belassen Sie die Samplerate auf diesem Wert, es sei denn, der Kunde verfügt über einen hohen Web-Traffic.
4. Alternativ, wenn der Graph aufgrund der geringen Datenmenge abgehackt aussieht, drehen Sie ihn langsam hoch.
5. Wiederholen Sie alle Prüfungen und drehen Sie die Rate langsam (idealerweise alle 24-48 Stunden), bis Sie genügend Daten erhalten (bei etwa 10%).
6. Für Kunden mit geringem Web-Traffic können Sie mehr als 10% steigen. Aber für jede kleine Erhöhung, stellen Sie sicher, dass Sie alle genannten Prüfungen durchführen.

Wählen Sie **Weiter**, um zum Dialogfeld **Standardeinstellung für die Anbietererkennung** zu wechseln.

Standardanbietererkennung Mit der Anbietererkennung können Sie den Provider oder die Plattform identifizieren, von der aus die Ressource bereitgestellt wird. Geben Sie einen Hostnamen ein, der für die Erkennung des Providers konfiguriert ist, der die Ressource dient. Sie können mehrere Hostnamen eingeben und die Providererkennung für jeden von ihnen individuell konfigurieren. Weitere Informationen zum Konfigurieren der Anbietererkennung finden Sie imAnbietererkennungAbschnitt.

Wählen Sie **Abgeschlossen**, um die Erstkonfiguration abzuschließen.

Sites

Die **Resource Timing Daten** sind in drei Hauptbereichen eingerichtet:

1. **Sites**
2. **Konfiguration**
3. **Anbietererkennung**

- Gehen Sie im linken Navigationsbereich zu **Auswirkung -> Resource Timing Data -> Resource Timing**.
- Die Seite **Sites** unter **Resource Timing Data** wird geöffnet.

Geben Sie den Hostnamen der Site ein, von der Sie Ressourcenstiming-Daten erfassen möchten. Unter **Sites**finden Sie die Liste der Hostnamen, die sich bereits im System befinden. Wenn Sie die gewünschte Site (Hostname) nicht finden, können Sie sie eingeben, indem Sie auf die Schaltfläche **Hinzufügen** klicken. Im Dialogfeld **"Site hinzufügen** "können Sie eine neue Site hinzufügen, auf der die Ressourcenzeitdaten konfiguriert werden können.

Konfiguration

Navigieren Sie im Navigationsmenü des Portals zu **Auswirkung > Ressourcenzeitdaten > Ressourcenzeitkonfiguration** . Die Seite **Sites** wird unter **Resource Timing Data** geöffnet.

Wählen Sie in der oberen Navigationsleiste **Konfiguration**aus.

Sie können eine neue Konfiguration hinzufügen, indem Sie auf die Schaltfläche Hinzufügen in der oberen rechten Ecke der Seite klicken.

Hinweis: Möglicherweise wird auf der Seite auch eine Liste der Konfigurationen angezeigt, einschließlich der Standardkonfiguration. Anstatt eine neue Konfiguration hinzuzufügen, können Sie

entweder eine Standardkonfiguration auswählen oder eine vorhandene Konfiguration aus der Liste bearbeiten.

Konfiguration hinzufügen

Um eine neue Konfiguration hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** in der oberen rechten Ecke der Seite.

Das Dialogfeld **Ressourcenzeitkonfiguration hinzufügen** wird geöffnet. Auf diese Weise können Sie einen neuen **Konfigurationsnamen**eingeben, **Ressourcen zum Einschließen oder Ausschließen**hinzufügen und die **Abtastrate**hinzufügen.

Konfiguration bearbeiten

Um eine vorhandene Konfiguration zu bearbeiten, wählen Sie die Schaltfläche **Konfiguration bearbeiten** neben dem Konfigurationsnamen.

Anbietererkennung

Die Anbietererkennung bestimmt, welche Plattform eine Anforderung für eine Domäne verarbeitet, wenn diese Domäne hinter Openmix Lastenausgleich ist. Es wird empfohlen, dass alle Kunden, die Ressourcen Timing-Daten aktiviert haben, Provider-Erkennungsdienste konfigurieren.

- Um die Anbietererkennung zu konfigurieren, navigieren Sie im linken Navigationsbereich zu **Auswirkung > Resource Timing Data > Resource Timing Configuration** .
- Die Seite **Sites** unter **Resource Timing Data** wird geöffnet. Wählen Sie in der oberen Navigationsleiste die Option **Provider Detection**.

Klicken Sie auf die Schaltfläche Hinzufügen in der oberen rechten Ecke der Seite.

Geben **Sie im Dialogfeld "Konfiguration der Anbietererkennung hinzufügen**"Folgendes ein.

Konfigurationsname

Geben Sie einen Namen für die Konfiguration ein. Der Name darf keine Leerzeichen oder Sonderzeichen enthalten und muss eindeutig sein.

Hostname

Geben Sie den Hostnamen ein, für den Sie die Anbietererkennung konfigurieren möchten. Sie können mehrere Hostnamen eingeben und Erkennungsmethoden für jeden einzelnen von ihnen einzeln angeben.

Erkennungsmethode

Bei der Erkennungsmethode wird der Typ des Testobjekts (ob Standard oder Benutzerdefiniert) und der Pfad (zum Testobjekt) für jeden eingegebenen Hostnamen angegeben.

Standard-Testobjekte Bei Standardtestobjekten kann der Pfad als **/provider-detection/platform.html** und **/provider-detection/platform.png** angegeben werden. Für dieses Setup wäre **/provider-detection/** Ihr Verzeichnispfad.

Hinweis: Es ist nicht zwingend erforderlich, den oben beschriebenen Pfad einzugeben. Stellen Sie jedoch sicher, dass sich die Dateien **platform.html** und **platform.png** im Verzeichnispfad befinden.

Benutzerdefinierte Testobjekte Bei benutzerdefinierten Testobjekten müssen Sie sicherstellen, dass die Testobjekte im genauen Pfad gefunden werden, den Sie eingeben. Beispielsweise`foo.com` muss die URL für Hostname`static/bar.css` und Pfad`http://foo.com/static/bar.css` gültig sein.

Kopfzeilen

Plattform-Header Wenn Sie **Platform Header**auswählen, stellen Sie sicher,`X-CDN-Forward: <CDN name>`dass die auf die Testobjekte gesendet wird. Wenn der`X-CDN-Forward: <CDN name>` nicht in den Antwort-Headern gefunden wird, wechselt der Client zum nächsten Test, der mit **Custom** angegeben werden kann.

Benutzerdefiniert Wenn Sie **Benutzerdefiniert**auswählen, stellen Sie sicher, dass der von Ihnen eingegebene reguläre Ausdruck exakt mit einem der Antwort-Header des CDN übereinstimmt.

Wenn Sie mehrere Antwort-Header hinzufügen, werden diese jeweils mit den regulären Ausdrücken in der gleichen Reihenfolge wie im Portal eingegeben getestet.

Klicken Sie auf **Erstellen**, um den Vorgang abzuschließen. Die neu erstellte Konfiguration wird nun in der Liste unter **Provider Detection**angezeigt. Klicken Sie auf die Symbole zum Bearbeiten oder Löschen, wenn Sie die Konfiguration ändern oder löschen möchten.

Ihre Konfiguration ist nun abgeschlossen. Wenden Sie sich an Ihren Kundenbetreuer, um die Providererkennung alternativ über JSON-Codierung zu konfigurieren.

Beschreibung der Ressourcenzeitmessung

Die folgende Tabelle zeigt die gesammelten Resource Timing-Messungen.

Messung	Beschreibung	Ressourcenzeitberechnung
DNS-Nachschlagezeit	Die Zeit, die für die DNS-Auflösung der Ressource erforderlich ist. Die DNS-Phase wird als DNS-Phase bezeichnet.	`domainLookupEnd – domainLookupStart`
TCP-Verbindungszeit	Die Zeit, die ein Browser benötigt, um eine Verbindung mit einem Server herzustellen. Bekannt als TCP-Phase.	`connectEnd – connectStart`
Wartezeit bis zum ersten Byte (TTFB)	TTFB ist die Zeit, die ein Browser vor dem Empfang der Ressource wartet.	`responseStart – startTime`
Roundtrip-Zeit (RTT)	Die Zeit vom Beginn der Anforderung bis zum Beginn der Antwort. Bekannt als Anforderungsphase.	`responseStart – requestStart`
Wartezeit	Der Unterschied zwischen dem Anfang der Antwort und dem Ende der Antwort. Bekannt als Antwortphase. Die Antwort stammt normalerweise von einem Server, einem Cache oder einer lokalen Ressource.	`responseEnd – responseStart`
Dauer	Die Gesamtzeit vom Beginn des Prozesses bis zum vollständigen Empfang der Ressource.	`responseEnd – startTime`

Erfahren Sie mehr unterhttps://www.w3.org/TR/resource-timing-1/#process

Ressourcenzeitberichte

Das Menü **Resource Timing** enthält die folgenden Auswertungen:

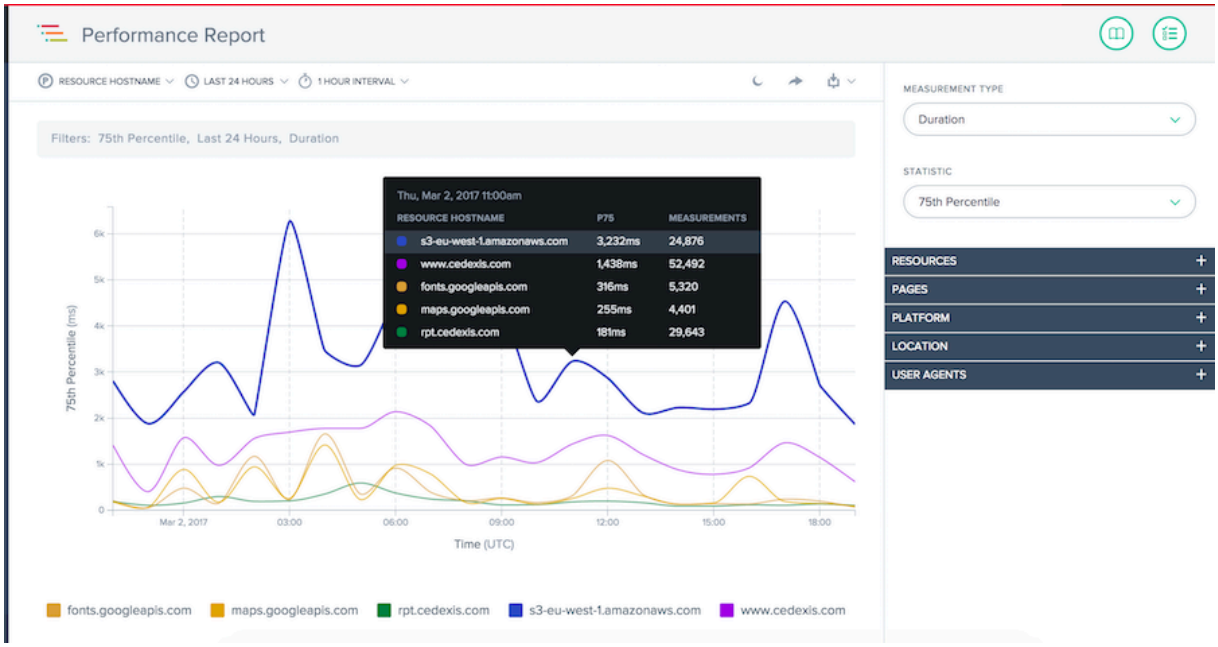
1. **Leistungsbericht** —Messdaten für die Ressourcenzeitmessung im Zeitverlauf.
2. **Statistischer Verteilungsbericht** —Eine Ansicht der Ressourcenzeitdaten über eine Berichtsansicht für statistische Verteilung.

Leistungsbericht

Der Bericht gibt einen Einblick in die Performance-Daten des Ressourcentimings im Laufe der Zeit pro ausgewähltem Wert.

Standardberichterstattungsansicht:

1. Dimension: Ressourcen-Hostname
2. Messung: Dauer
3. Zeitbereich: Letzte 24 Stunden



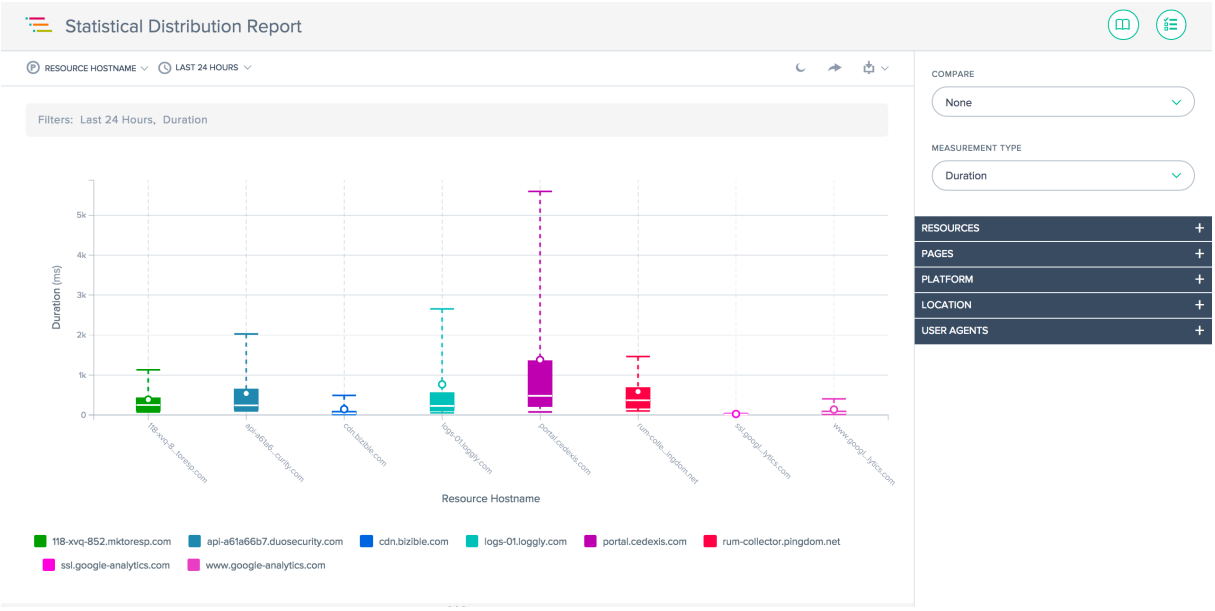
Statistischer Verteilungsbericht

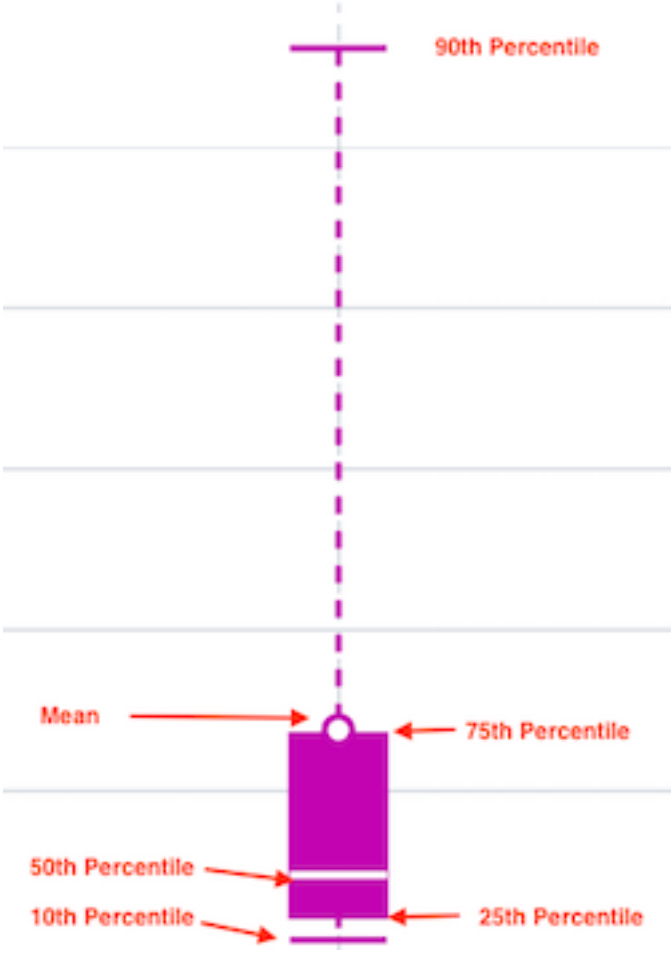
Dieser Bericht zeigt die statistische Verteilung des Ressourcenzeitpunkts. Der Bericht gibt Einblick in die Anzahl der Messungen pro Ressourcenwert. Sie können basierend auf Ressource, Seite, Plattform,

Standort und User Agent filtern, zwischen Messtypen wechseln und Vergleiche zwischen bestimmten Seite, Standort und Benutzer-Agent-Details durchführen.

Standardberichterstattungsansicht:

1. Dimension: Ressourcen-Hostname
2. Messung: Dauer
3. Zeitbereich: Letzte 24 Stunden



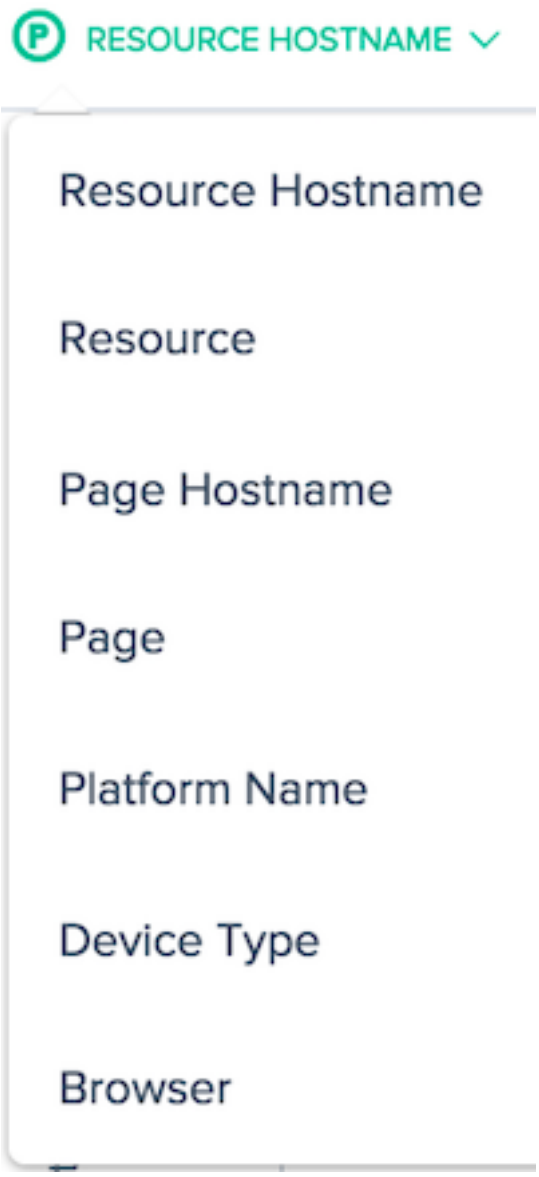


Das Whisker-Diagramm

Verwenden der Berichte

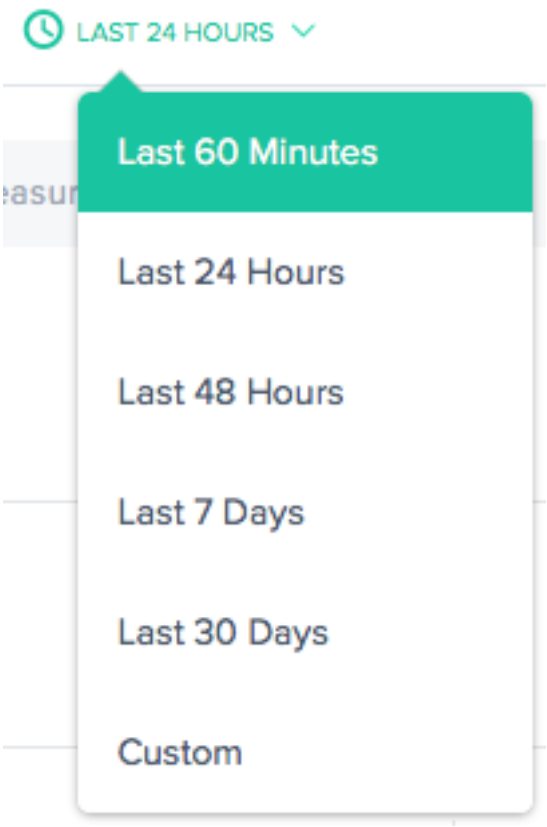
Zum Verfeinern und Anpassen der Berichtsansichten an bestimmte Berichtsanforderungen verwenden Sie die folgende Funktionalität in den Berichten Performance und Statistische Verteilung. Zusätzlich zu den Standardfunktionen der Berichte wie Berichtsfreigabe, Hintergrundumschaltung, Datenexport und mehr stehen folgende Funktionen zur Verfügung:

Primäre Dimension



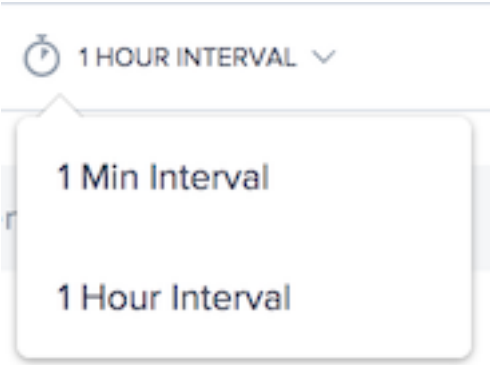
Die primäre Dimension des Diagramms wird über ein Menü oberhalb des Diagramms ausgewählt. Sie können es als leistungsfähiges Pivot für den Bericht verwenden, um Daten in Bezug auf Ressourcen-Hostname, Seiten-Host-Name, Seite und Plattformname auszudrücken.

Filter: Berichtszeitbereich



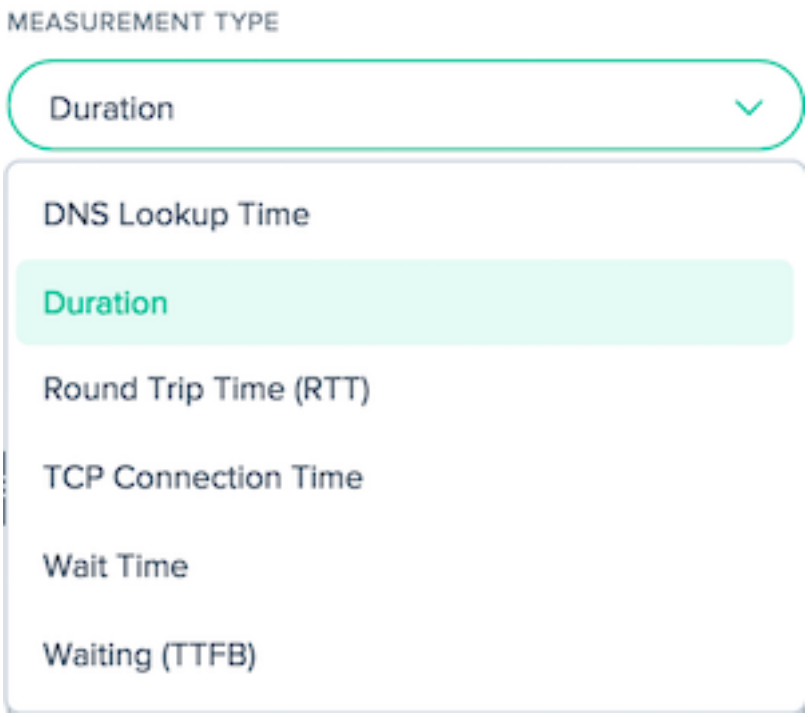
Die Berichte können mit einem Zeitbereich von den letzten 60 Minuten, den letzten 24 Stunden, den letzten 48 Stunden, den letzten 7 Tagen, den letzten 30 Tagen oder einem benutzerdefinierten Bereich erstellt werden. Die Standardansicht ist die Letzte 24 Stunden.

Berichtsintervall



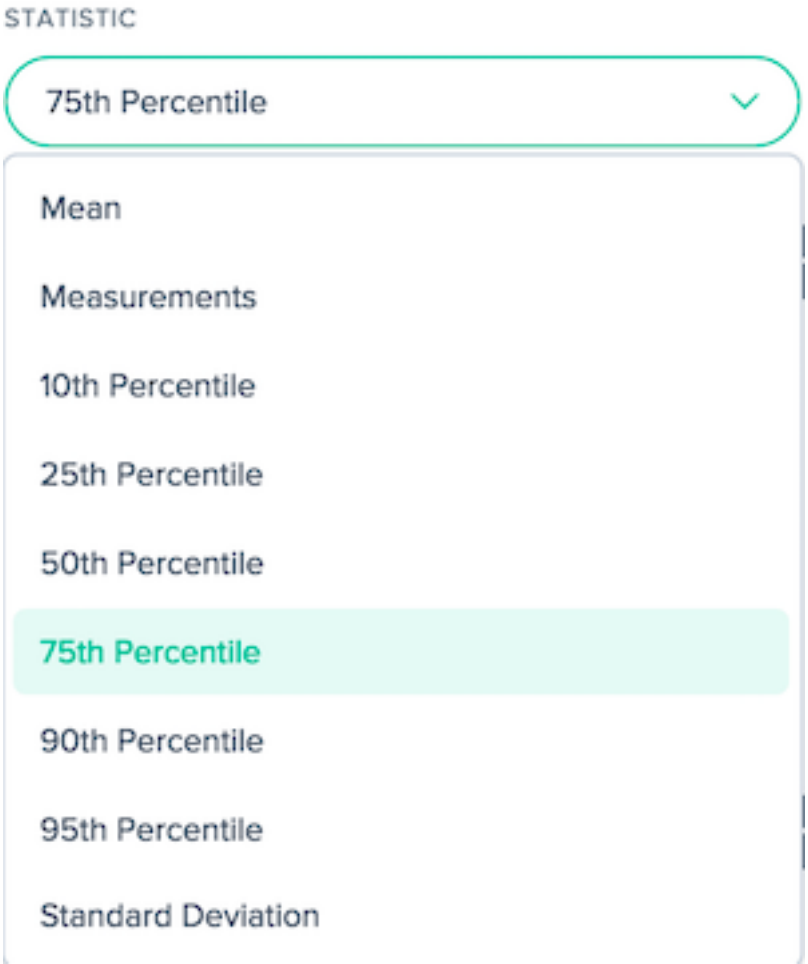
Wählen Sie das Zeitintervall aus, in dem Sie das Trenddiagramm anzeigen möchten. Je nach Datumsbereich, den Sie anzeigen, können Sie das Diagramm in Intervallen von einer Minute, einer Stunde oder einem Tag anzeigen.

Messarten



Wählen Sie den Messtyp aus, für den Sie das Ressourcen-Timing anzeigen möchten. Wählen Sie aus Dauer, DNS-Suchzeit, Round Trip Time (RTT), TCP-Verbindungszeit, Wartezeit und Warten (TTFB).

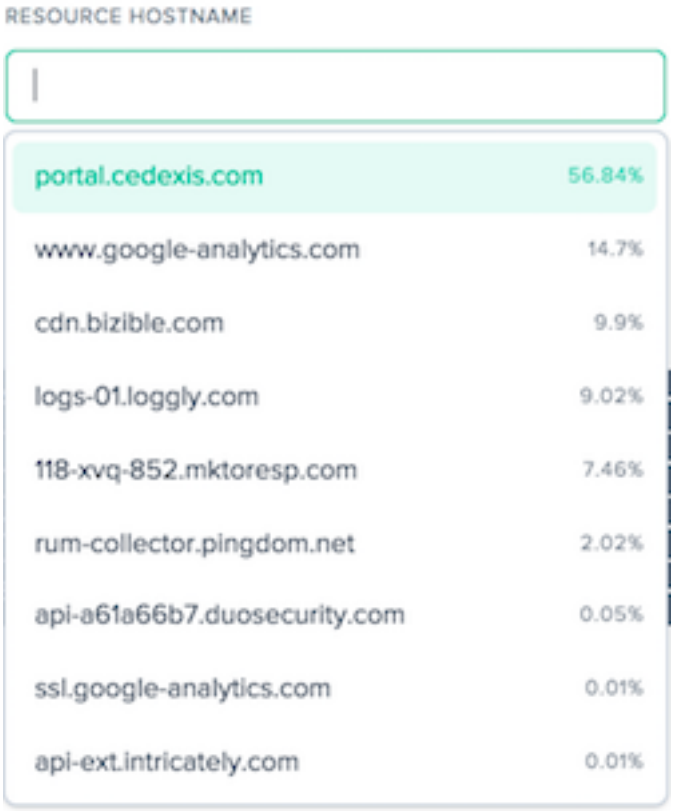
Wählen Sie eine statistische Kennzahl aus, um die Daten anzuzeigen.



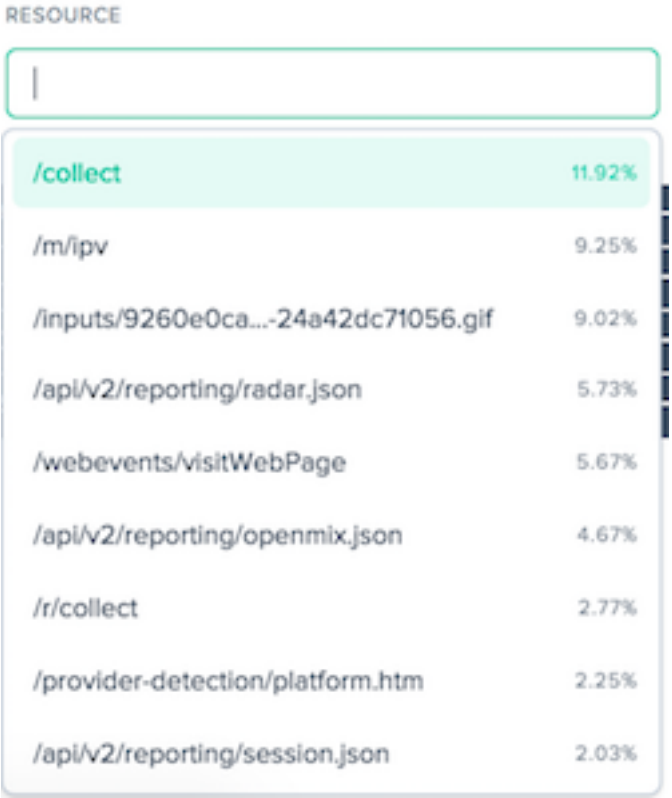
Filter: Leistungsstarke Drilldown-Funktionen

Die Berichte unterscheiden sich geringfügig in Bezug darauf, welche Filter basierend auf den Daten geeignet sind. Die folgenden Filteroptionen sind in den Berichten verfügbar:

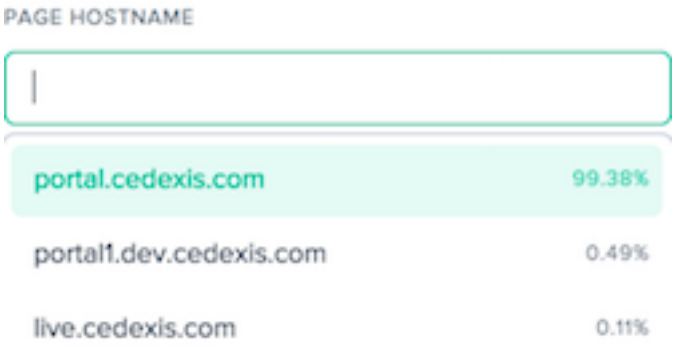
Ressourcen-Hostname:



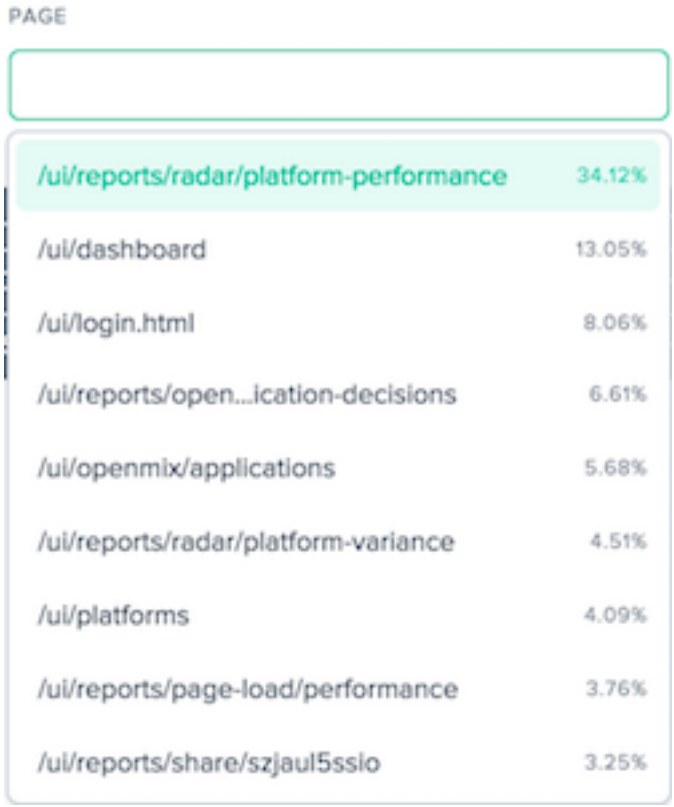
Ressourcen:



Seite Hostname:

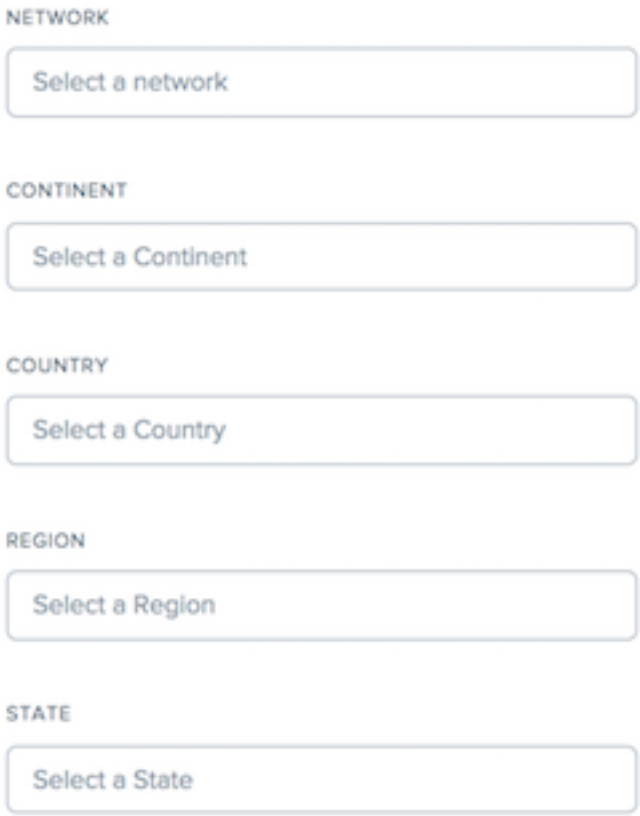


Seite:

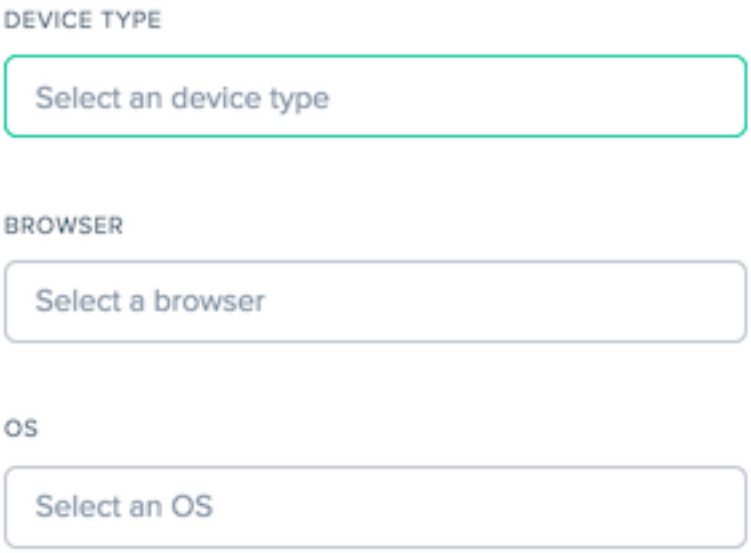


Plattformname:

Standort: Netzwerk, Kontinent, Land, Region und Bundesland:



User Agents: Gerätetyp, Browser und IOS:

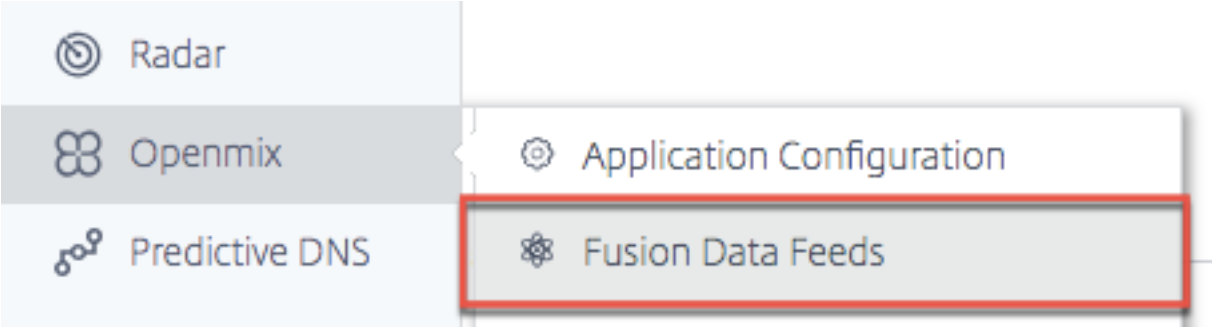


Fusion-Integrationen

September 14, 2023

Zusätzlich zu Radar- und Sonardaten kann Openmix Daten von Drittanbietern in seinen Entscheidungskriterien verwenden. Sie können beispielsweise einen vorhandenen synthetischen Überwachungsdienst integrieren, den Sie bereits verwenden. Oder Sie können kostenbasierte Entscheidungen anhand aktueller Nutzungsdaten Ihres CDN-Anbieters treffen.

Fusion-Menü



Fusion Data Feeds können über das Navigationsmenü unter **Openmix**aufgerufen werden.

Zum Beispiel einige gängige Fusion-Datenfeeds, die mit Openmix-Anwendungen funktionieren:

1. **Serververfügbarkeit** —Nimmt Daten von Drittanbietern wie CatchPoint, Rigor und Pingdom auf, um die Erreichbarkeit eines bestimmten Hosts oder einer bestimmten Anwendung zu ermitteln.
2. **Serverüberwachung** —Metriken von Anbietern wie Rackspace und New Relic ermöglichen Openmix bei der Routing-Entscheidung die Berücksichtigung von Serverlaufzeitmetriken wie Speicherauslastung, CPU-Verbrauch, freier Speicherplatz und Netzwerklatenz. Openmix kann die Metriken verwenden, um Routing-Entscheidungen ein- und auszuschalten oder um abgestufte Routing-Änderungen vorzunehmen, indem der Datenverkehr von einem ausgelasteten Server abgewiesen wird.
3. **CDN-Kostenkontrolle** —**Nimmt** Bandbreiten- und Nutzungsstatistiken von allen wichtigen CDNs auf und stellt diese Daten in Echtzeit in Openmix-Anwendungen zur Verfügung, um Routing-Entscheidungen zu treffen.
4. **Kundendefinierte benutzerdefinierte Datenfeeds** —Alle Daten an einem von Ihnen bereitgestellten Endpunkt können in einer benutzerdefinierten Openmix-Anwendung aufgenommen und zur Verwendung bei der Routing-Entscheidung zur Verfügung gestellt werden.

Fusion-Integrationen

Service	Typ
Akamai	CDN-Bandbreite, CDN-Nutzung
AWS CloudFront	CDN-Nutzung
AWS CloudWatch	Instanzmetriken
ALS ELB	Load Balancer-Metriken
AWS S3	Benutzerdefinierter Datenfeed
Azure	Instanzmetriken
Catchpoint	Warnungen
CDNetworks	CDN-Bandbreite, CDN-Nutzung
ChinaCache	CDN-Bandbreite
ChinaNetCenter	CDN-Bandbreite
NetScaler	Benutzerdefinierter Datenfeed
Datadog	Warnungen
Edgecast	CDN-Bandbreite, CDN-Nutzung
Fastly	CDN-Nutzung
Fusion Direkt	Benutzerdefinierter Datenfeed
Highwinds	CDN-Nutzung
HTTP ABRUFEN	Benutzerdefinierter Datenfeed
HTTP GET mit Verfügbarkeit	Benutzerdefinierter Datenfeed
JSON	Benutzerdefinierter Datenfeed
Keynote	Webmonitor
Level3	CDN-Bandbreite, CDN-Nutzung
Limelight	CDN-Nutzung
Max CDN	CDN-Bandbreite, CDN-Nutzung
Neues Relikt Apdex	Bewerbungspunktzahl
New Relic Serverüberwachung	Instanzmetriken
NGINX	Load Balancer-Metriken
NGINX+	Load Balancer-Metriken

Service	Typ
Pingdom	Webmonitor
Qbrick	CDN-Nutzung
Rackspace	Instanzmetriken
Strenge	Webmonitor
SFR	CDN-Bandbreite, CDN-Nutzung
TCP-Ping	Webmonitor
Touchstream	Videoüberwachung

Fusions-Feeds

Der folgende Bildschirm zeigt alle konfigurierten Fusion-Datenfeeds. Die Liste bietet einen Überblick über die Datenfeeds und den aktuellen Status.

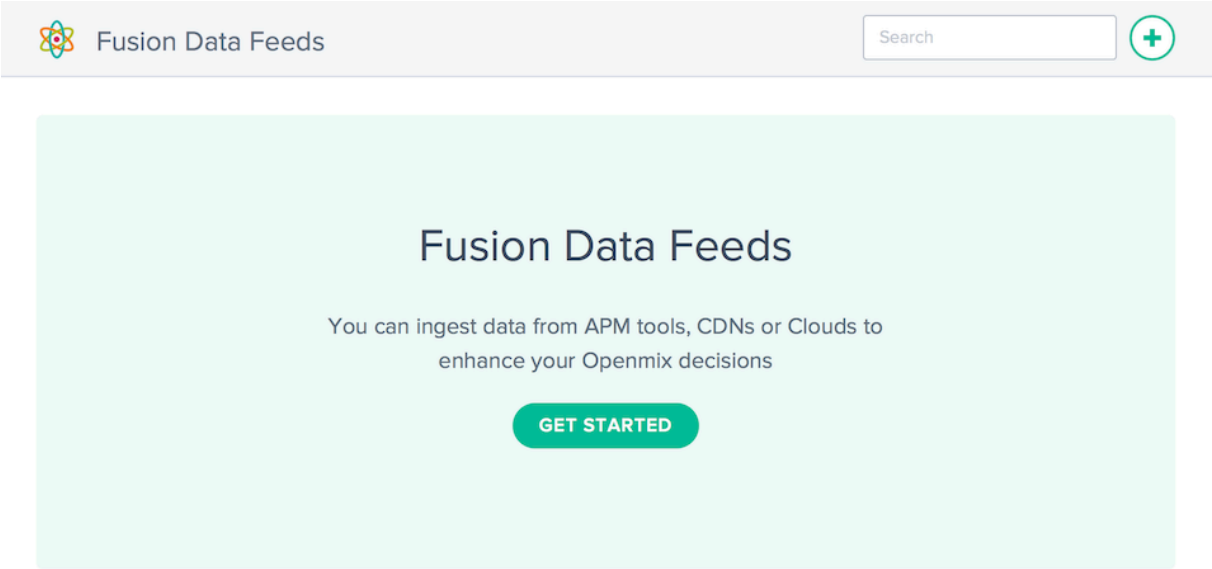
Die Spalten enthalten die folgenden Informationen:

Überschrift	Beschreibung
Status	Der aktuelle Status des Datenfeeds. Der Status zeigt entweder: + grün bedeutet, dass der Feed erfolgreich Daten vom Service abruft; + gelb bedeutet, dass der Feed darauf wartet, dass Daten vom Service abgerufen werden; oder + rot bedeutet, dass der Feed nicht vom Service abgerufen werden kann
Name des Datenfeeds	Der im Datenfeed angegebene Name. Optional, wird standardmäßig „Service —Plattformname “verwendet, falls nicht angegeben.

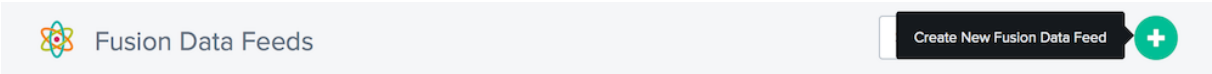
Überschrift	Beschreibung
Service	Der Name des Dienstes, der vom Datenfeed verwendet wird.
ID	Die ID des Datenfeeds. Dies ist für den Zugriff auf Fusion über die API erforderlich.
Plattformname	Der Name der Plattform, die mit dem Datenfeed verknüpft ist.
Führen Sie jeden aus	Wie oft der Datenfeed vom Dienst aktualisiert wird.

Datenfeeds erstellen

Wenn keine Fusion-Datenfeeds konfiguriert sind, werden Sie auf einem Willkommensbildschirm aufgefordert, einen Datenfeed zu erstellen.

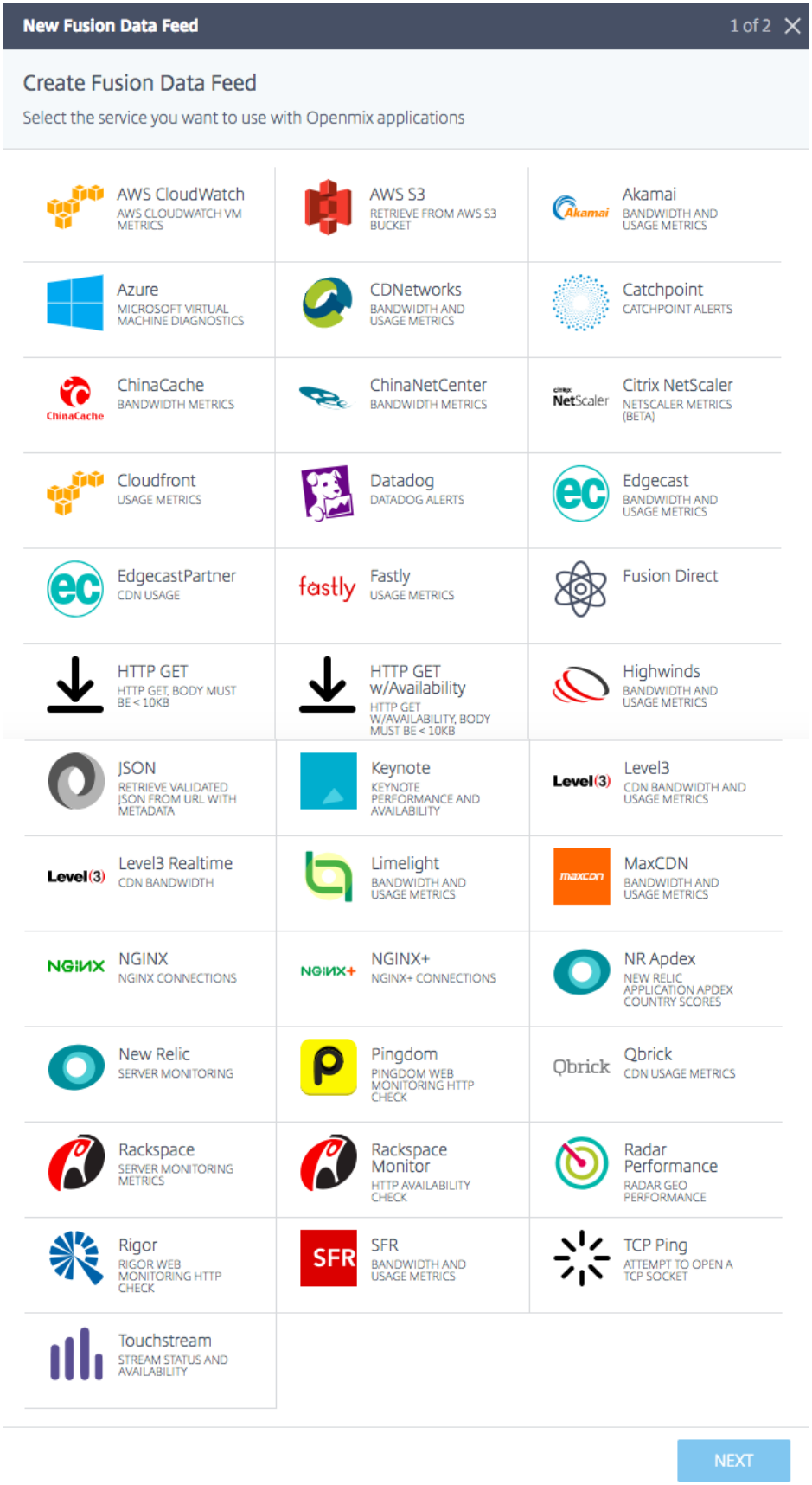


Klicken Sie auf die Schaltfläche **Erste Schritte** oder **+**, um einen neuen Datenfeed einzurichten.

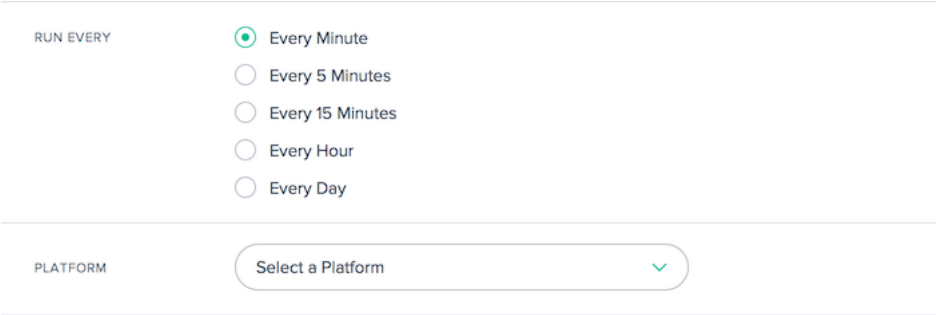


Neue Datenfeeds

Klicken Sie auf das Symbol des Dienstes, den Sie integrieren möchten, und füllen Sie die erforderlichen Konfigurationsfelder aus.



Jeder Dienst benötigt unterschiedliche Konfigurationsparameter. Sie benötigen einen Benutzernamen und ein Passwort oder ein generiertes Token für die Authentifizierung und jede zusätzliche dienstspezifische Konfiguration.



Alle Fusion-Datenfeeds sind mit einer Plattform verknüpft, die zuvor im NetScaler Intelligent Traffic Management-Portal erstellt wurde. Auf diese Weise kann die Openmix-Anwendung die externen Fusion-Daten für jede Plattform abfragen und anhand der Routing-Logik feststellen, ob die Plattform für eine Routing-Entscheidung als verfügbar angesehen werden muss.

Die meisten Feeds benötigen bei der Konfiguration die folgenden Werte:

Artikel eingeben	Beschreibung
Führen Sie jeden aus	Wie oft der Datenfeed vom externen Dienst aktualisiert wird. Fusion ruft den Dienst im angegebenen Intervall auf und aktualisiert die Openmix-Anwendungen auf der Grundlage der neuen Daten.
Plattform	Die Plattform, die den Fusion-Daten in der Openmix-Anwendung zugeordnet ist.

Datenfeeds bearbeiten

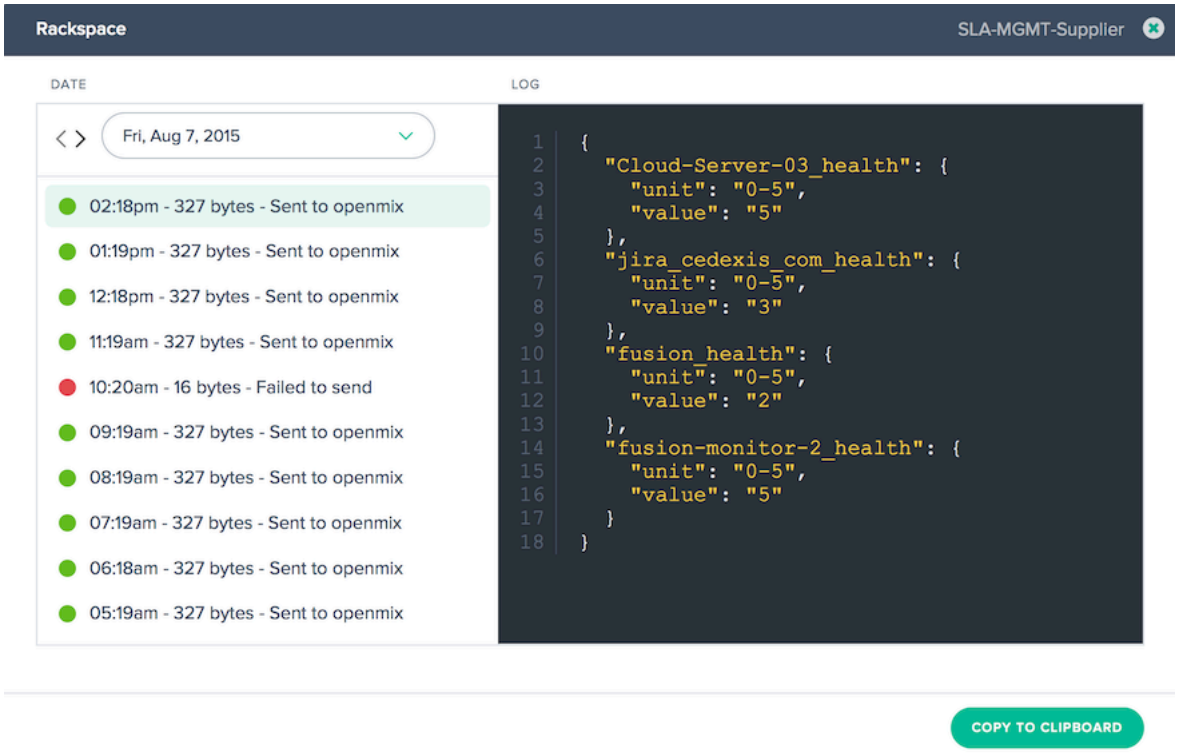
Das Bearbeiten eines Fusion-Datenfeeds ist so einfach wie das Klicken auf den Datenfeed in der Tabelle und das Klicken auf die Schaltfläche **Bearbeiten** .

Nachdem Sie die Konfiguration geändert haben, klicken Sie auf **Speichern**. Dadurch werden Sie wieder in der Datenfeed-Liste angezeigt, in der Ihre Änderungen gespeichert und im Datenfeed übernommen wurden.

Datenfeed-Verlauf

Fusion erfasst die letzten 100 Antworten von jeder Ausführung im Datenfeed-Verlauf. Sie können den Status des Datenfeeds, Informationen zu den Daten und die vom Dienst zurückgegebene Nutzlast

anzeigen. Nachdem Sie den spezifischen Datenfeed in der Liste ausgewählt haben, klicken Sie **unter Verlauf für den Datenfeed anzeigen auf die Schaltfläche Protokollverlauf** .



Um das gewählte Datum zu ändern, können Sie auf die Schaltflächen **<** oder ** klicken, um vom aktuell ausgewählten Datum aus vor- oder zurückzugehen, oder Sie können ein bestimmtes Datum aus der Liste auswählen. Wählen Sie den Zeitstempel der jeweiligen Instanz aus und die vom Service zurückgegebenen Daten werden angezeigt.

Fehlgeschlagene Datenfeeds

Fusion Quarantine for Failing Fusion Feeds
Fusion Quarantine gilt für den fehlerhaften Fusion-Datenfeed eines Kunden, wenn der Feed so konfiguriert ist, dass er in einem Abfrageintervall von weniger als 24 Stunden ausgeführt wird. Fusion wendet Quarantänelogik an, um zu verhindern, dass diese fehlgeschlagenen Feeds ausgeführt werden. Dies geschieht, um Ressourcen (CPU/Speicher) zu schonen und negative Auswirkungen auf andere gültige Fusion-Datenfeeds zu vermeiden.

Die Quarantänelogik wird angewendet, indem der fehlerhafte Fusion-Feed in schrittweisen Intervallen „zurückgesetzt“wird. Dies geschieht so lange, bis der Fusion-Feed für 24 Stunden unter Quarantäne gestellt wird. Zu diesem Zeitpunkt versucht der Fusion-Feed alle 24 Stunden zu starten. Der fehlerhafte Fusionsdatenfeed wird niemals vollständig heruntergefahren. Es wird weiterlaufen, mindestens zweimal alle 24 Stunden.

Wichtig:

- Der Fusion-Datenfeed wird immer mindestens zweimal hintereinander ausgeführt und schlägt zweimal fehl, bevor er in die Quarantänelogik aufgenommen wird. Wenn beispielsweise ein einminütiger Feed ausgeführt wird und zweimal hintereinander ausfällt, wird er in die Quarantänelogik aufgenommen.
- Wenn der Fusion-Datenfeed zu irgendeinem Zeitpunkt erfolgreich ausgeführt wird, wird er aus der Quarantänelogik entfernt und in seinem regulären geplanten Intervall erneut ausgeführt.
- Wenn der Fusion-Feed zu irgendeinem Zeitpunkt aktualisiert wird (d. h. wenn der Benutzer eine fehlerhafte URL eingegeben und diese korrigiert hat), versucht der Fusion-Feed unabhängig vom Abfrageintervall innerhalb einer Minute erneut zu starten. Wenn es erfolgreich ist, wird es aus der Quarantänelogik entfernt. Wenn es weiterhin fehlschlägt, wird die Quarantänelogik angewendet.

Globale CDN-Bereinigung

June 4, 2021

Global CDN Purge ist eine Möglichkeit, Daten von mehreren CDNs gleichzeitig zu löschen, was die Verwaltung mehrerer CDNs vereinfacht. Sie können die zu löschenden CDNs verbinden, die URIs angeben, die für alle angehängten Dienste gelöscht werden sollen, und klicken Sie auf die Schaltfläche **Löschen** . Die Bereinigung wird über alle verbundenen CDNs initiiert.

Die globale CDN-Bereinigungsfunktion basiert auf drei Hauptkomponenten:

1. **CDN-Bereinigungsadapter** —Für jede Kombination von CDN/Hostnamen, die Sie löschen möchten, muss ein CDN-Bereinigungsadapter erstellt werden. Der CDN-Bereinigungsadapter sammelt Informationen, die zum Ausführen von Bereinigungen erforderlich sind, z. B. Dienstauswahl, Authentifizierungsinformationen, Hostname und andere dienstspezifische Informationen. Sie benötigen einen CDN-Bereinigungsadapter für jeden Hostnamen, der auf einem CDN gelöscht werden soll.
2. **URI** —Bereinigungen werden an einem bestimmten Speicherort auf den CDNs ausgeführt.
3. **Löschgruppe** —Bereinigungsgruppen ermöglichen es Ihnen, eine logische Sammlung von CDN-Bereinigungsadaptern und URIs zu erstellen, die mit einem Befehl gelöscht werden. Beispielsweise können Sie das Verzeichnis ‘/media’auf 2 verschiedenen CDNs oder einem Verzeichnis löschen, das in Entwicklungs-, Test- und Produktionsumgebung vorhanden ist.

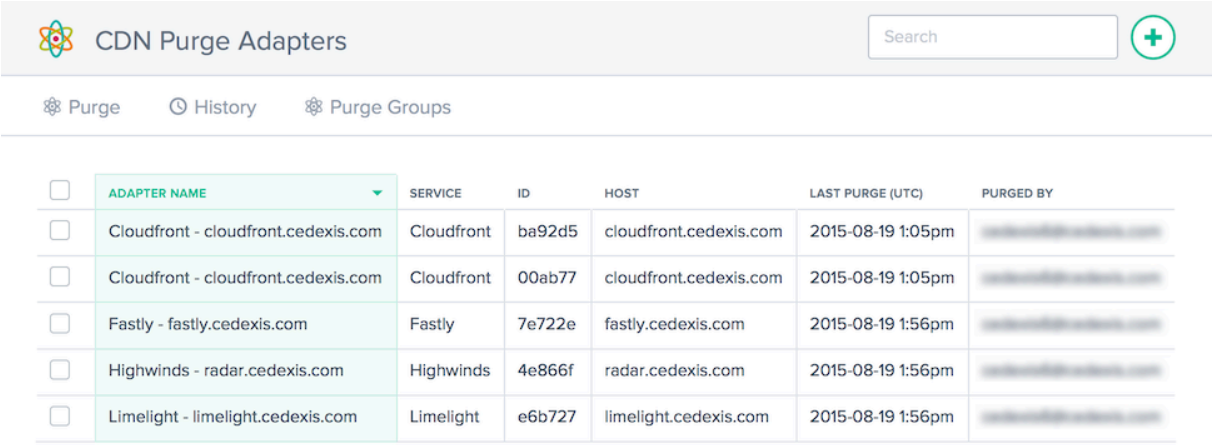
CDN-Bereinigungsadapter müssen so eingerichtet sein, dass Bereinigungen ausgeführt werden. URIs und mehrere CDN-Bereinigungen können einzeln angegeben werden. Es wird jedoch empfohlen, dass

Ihre Setup-Bereinigungsgruppen zum Verwalten häufig ausgeführter Bereinigungen verwendet werden.

Global CDN Purge kann über die oberste Ebene des Navigationsmenüs als CDN Purge aufgerufen werden.

CDN Bereinigungsadapter

Im folgenden Bildschirm werden alle konfigurierten CDN-Bereinigungsadapter angezeigt. Die Liste bietet einen Überblick über die konfigurierten CDN-Adapter und ermöglicht die Bereinigung.

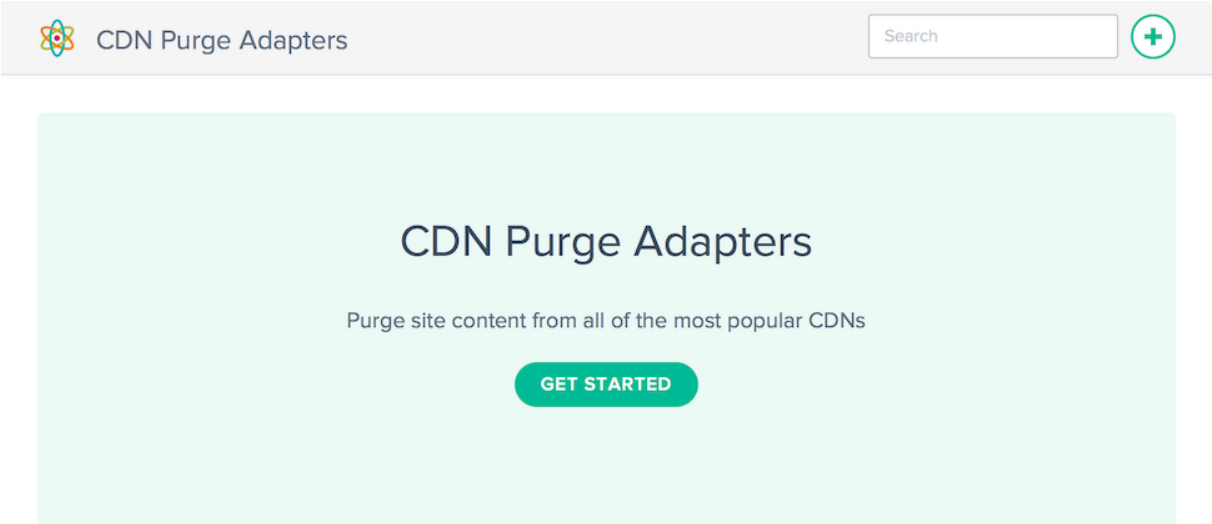


Die Spalten enthalten folgende Informationen:

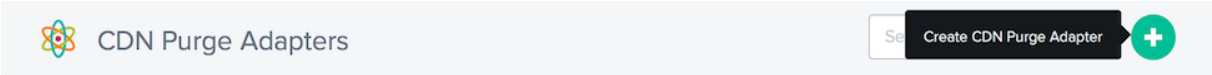
Überschrift	Beschreibung
Adaptername	Der Name des Adapters. Optional, wird standardmäßig auf “Service - Host”gesetzt, wenn nicht angegeben.
Service	Der Name des CDN-Dienstes, für den der Bereinigungsvorgang konfiguriert ist.
ID	Die ID des CDN-Adapters. Dies wird für den Zugriff auf Fusion über die API benötigt.
Host	Der Host, für den die Bereinigung konfiguriert ist. Dienste rufen manchmal diese Einstellung auf: Host, Hostname, Plattform usw.
Letzte Bereinigung (UTC)	Uhrzeit und Datum in UTC, zu dem die Bereinigung zuletzt ausgeführt wurde.
Bereinigt von	Der Benutzer, der zuletzt eine Bereinigung ausgeführt hat.

Erstellen von CDN-Bereinigungsadaptern

Um Global CDN Purge zu verwenden, müssen Sie Ihre CDN- und Hostnamen-Konfigurationen hinzufügen. Wenn Sie **CDN Purge**zum ersten Mal öffnen, werden Sie aufgefordert, einen CDN-Bereinigungsadapter zu erstellen.

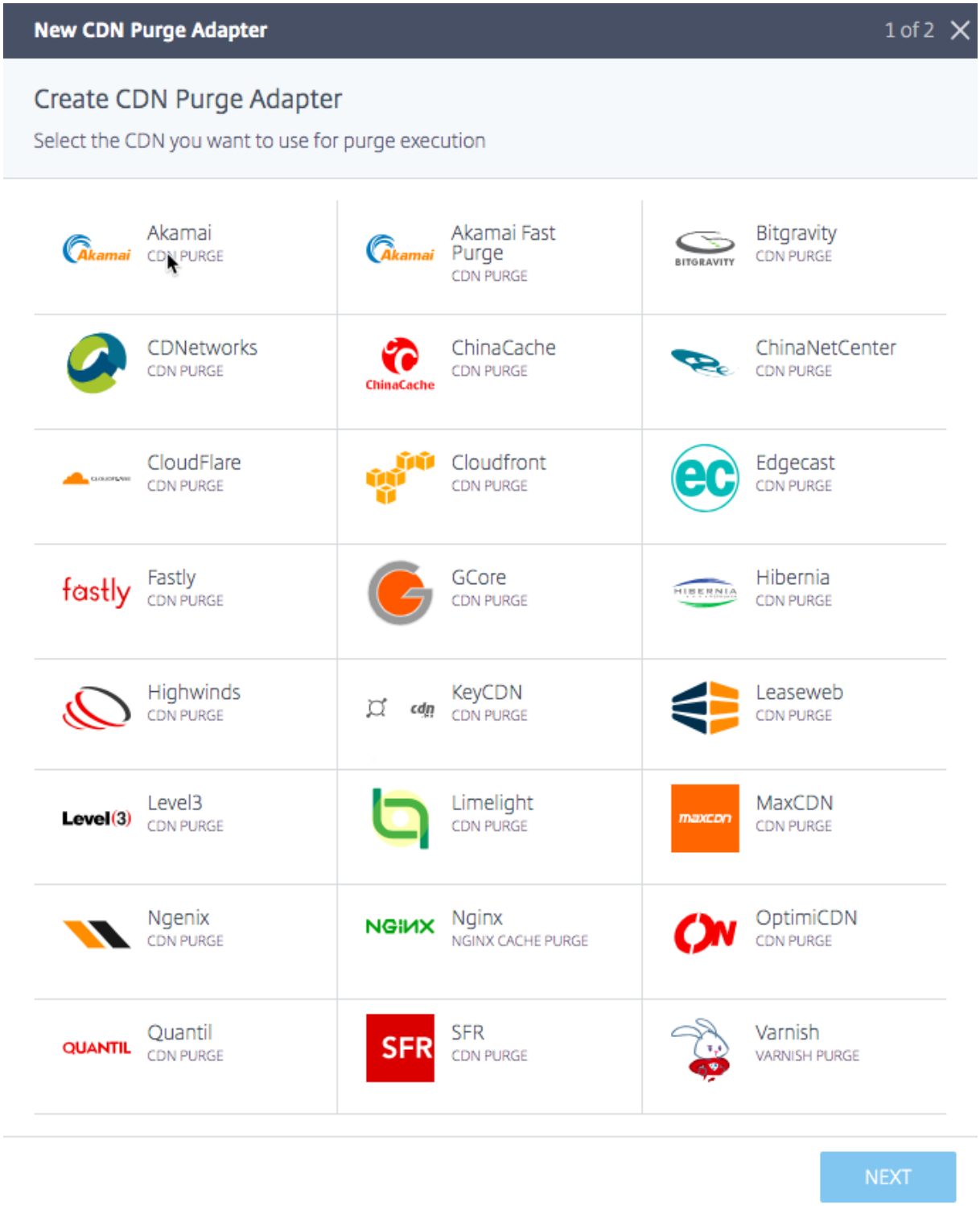


Klicken Sie auf die Schaltfläche **Erste Schritte** oder **+**, um ein CDN einzurichten, das zum Löschen verfügbar ist.

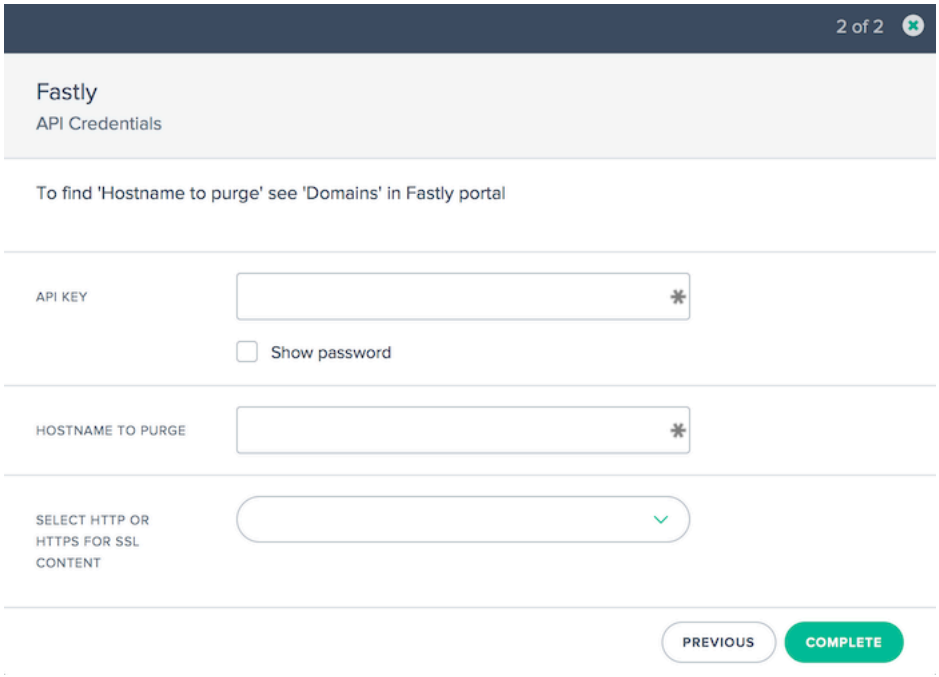


Neue CDN-Bereinigungsadapter

Klicken Sie auf das Symbol des Dienstes, für den Sie einen CDN-Bereinigungsadapter erstellen möchten, und füllen Sie die erforderlichen Konfigurationsfelder aus.



Jeder Bereinigungsadapter benötigt unterschiedliche Konfigurationsparameter. Sie benötigen einen Benutzernamen und ein Kennwort oder ein generiertes Token für die Authentifizierung und jede zusätzliche dienstspezifische Konfiguration.



CDN-Bereinigungsadapter bearbeiten

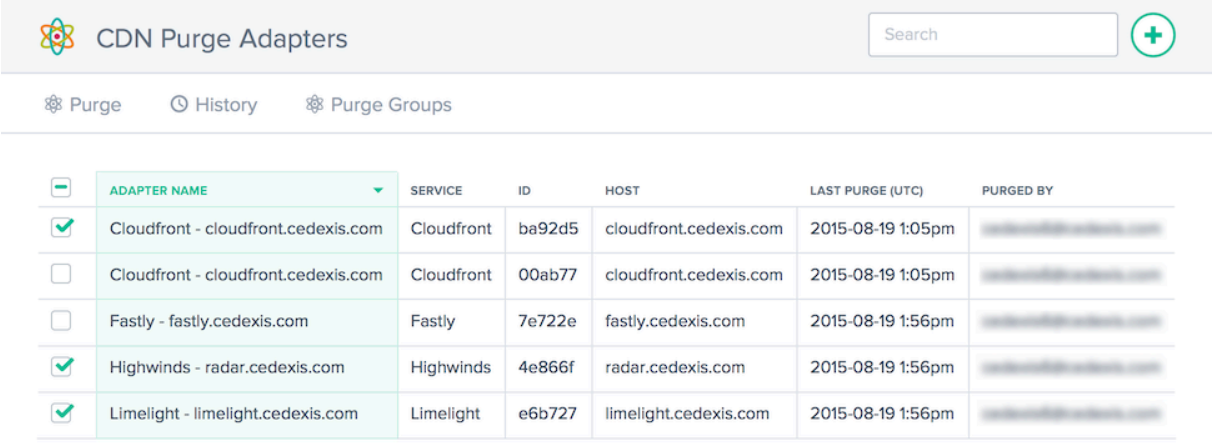
Das Bearbeiten eines CDN-Bereinigungsadapters ist ganz einfach, indem Sie auf den CDN-Bereinigungsadapter in der Tabelle klicken und auf die Schaltfläche **Bearbeiten** klicken.

Nachdem Sie die Konfiguration geändert haben, klicken Sie auf **Speichern**. Dadurch gelangen Sie zurück zur Liste des Bereinigungsadapters, in der Ihre Änderungen gespeichert und auf den spezifischen CDN-Bereinigungsadapter angewendet werden.

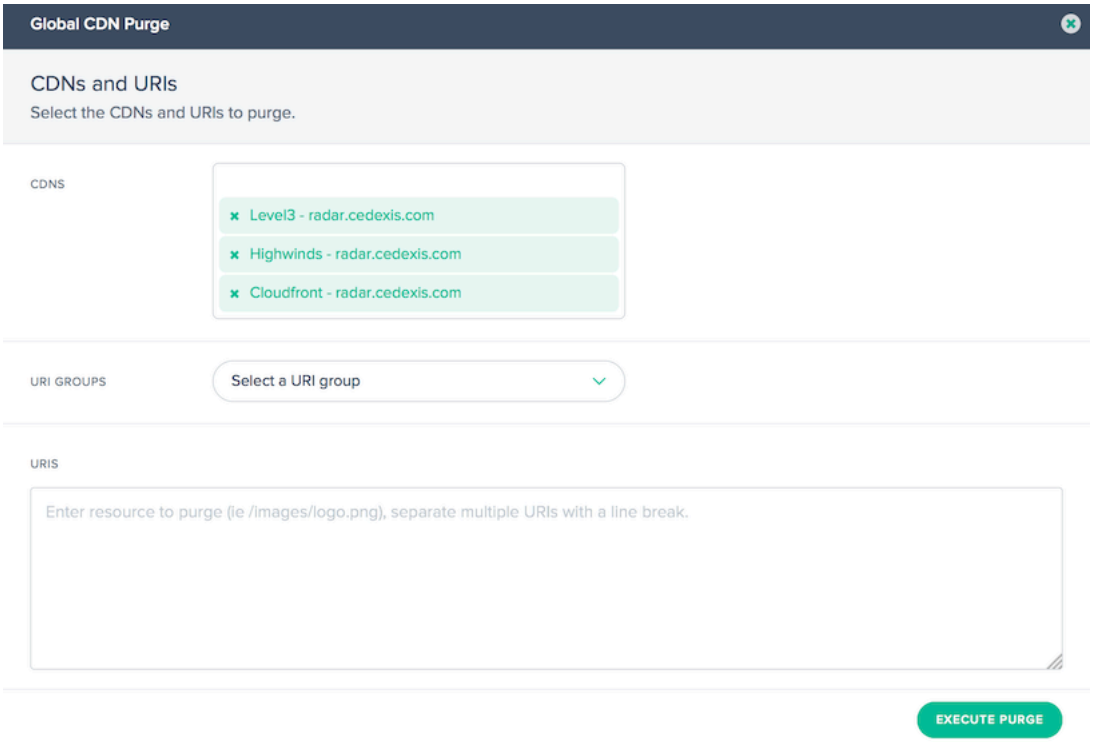
Bereinigungsvorgang ausführen

Um eine Bereinigung auszuführen, wählen Sie die CDN-Bereinigungsadapter aus, die in die Bereinigung einbezogen werden müssen.

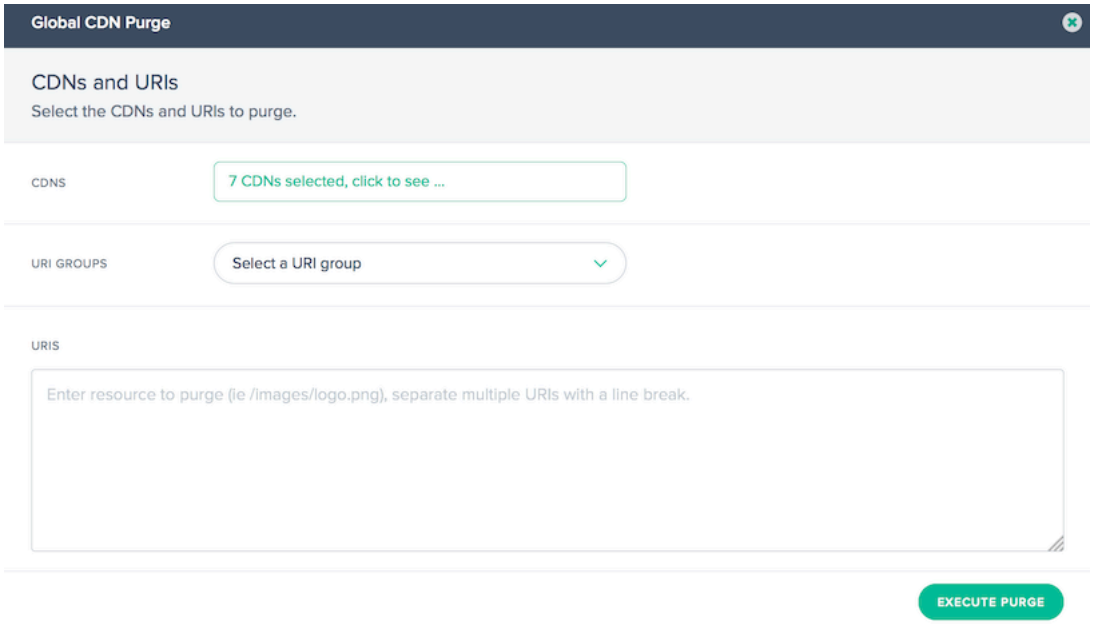
Klicken Sie auf die Schaltfläche **Bereinigen**, um den Bereinigungsvorgang zu starten.



Das Dialogfeld **Globale CDN-Bereinigung** wird geöffnet. Das Dialogfeld zeigt die ausgewählten CDN-Bereinigungsadapter und die URIs, die bei der Bereinigung verwendet werden.

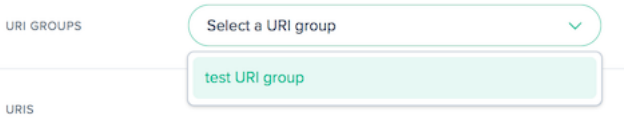


Wenn 5 oder weniger CDN-Bereinigungsadapter ausgewählt sind, wird im Bereinigungdialog die gesamte Liste der ausgewählten CDN-Bereinigungsadapter angezeigt. Wenn nicht alle CDN-Bereinigungsadapter angezeigt werden, klicken Sie auf das Textfeld **CDNs**, in dem **X CDNs ausgewählt ist, klicken Sie hier, um zu sehen…**, um alle ausgewählten Bereinigungsadapter anzuzeigen.

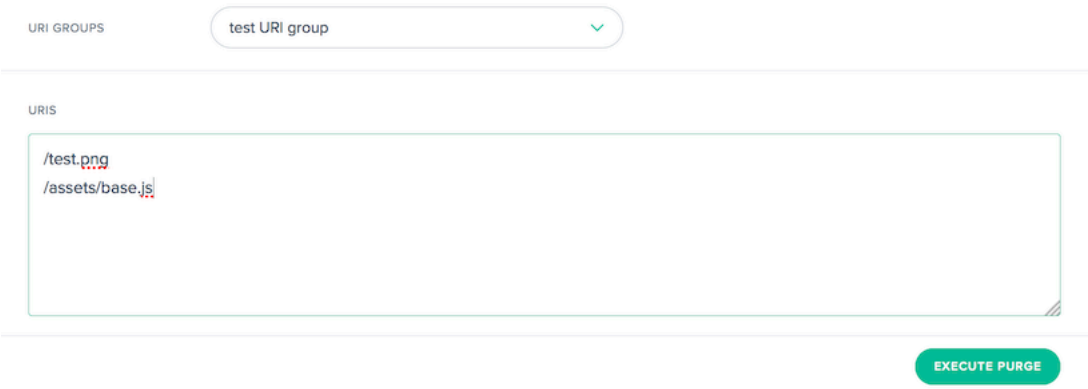


Die Liste kann ausgeblendet werden, indem Sie rechts neben der Liste der Bereinigungsadapter auf die Schaltfläche **Ausblenden** klicken.

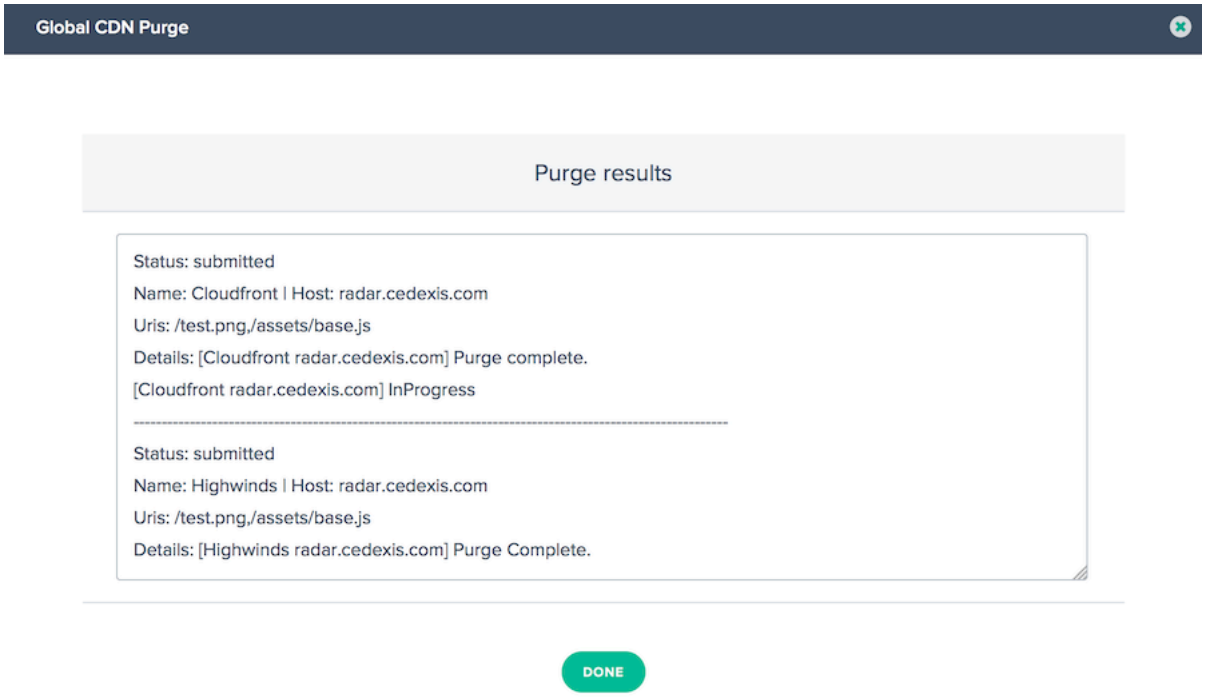
Sie können die in der Bereinigung verwendeten URIs auffüllen, indem Sie die URIs manuell eingeben oder aus den verfügbaren URI-Gruppen auswählen. Wenn Sie eine URI-Gruppe auswählen, werden die URI-Eingaben mit den URIs aus der ausgewählten Bereinigungsgruppe gefüllt.



Geben Sie die URIs für die Ressourcen ein, die gelöscht werden müssen, oder ändern Sie sie.

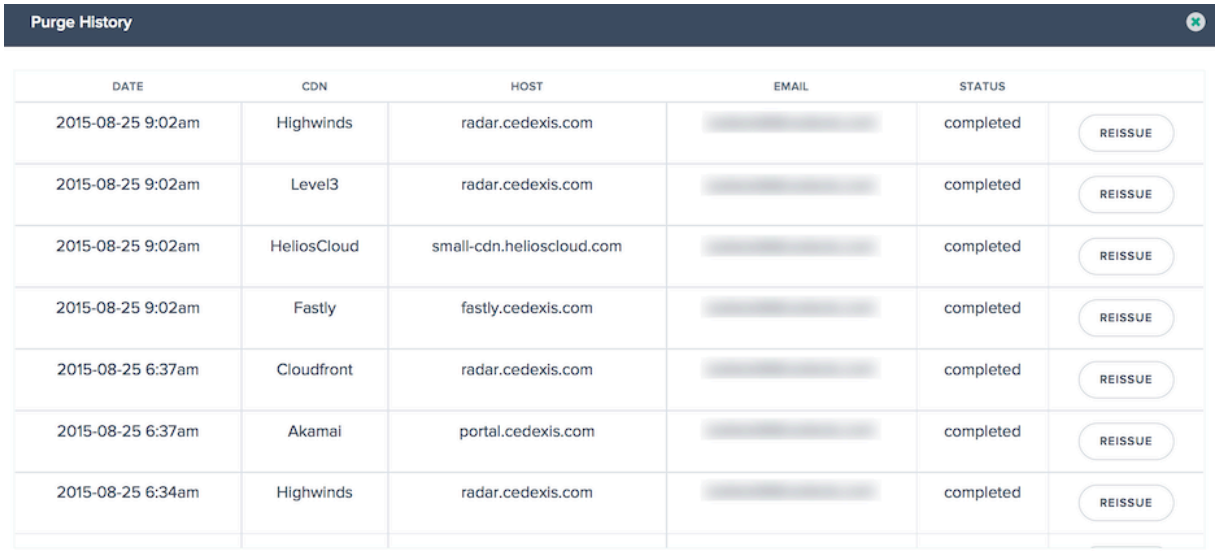


Wenn Sie bereit sind, den Bereinigungsvorgang zu starten, klicken Sie auf die Schaltfläche **Löschen ausführen** . Die Bereinigung wird an alle ausgewählten CDNs gesendet. Die Übermittlungen und API-Antworten werden im Dialogfeld **Ergebnisse löschen** angezeigt.

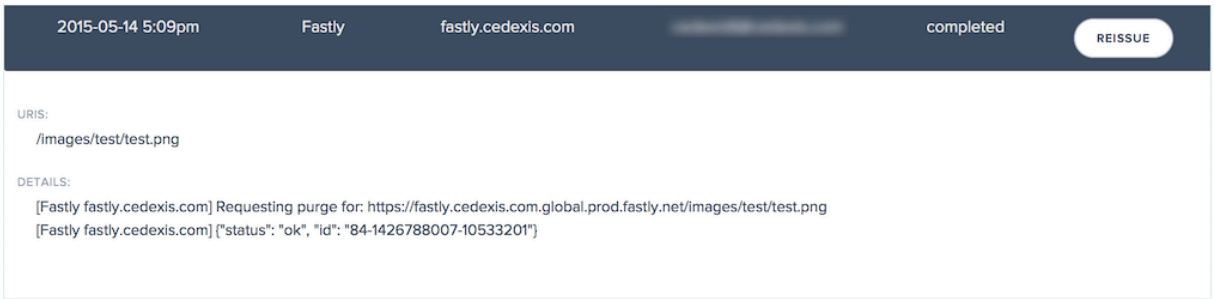


CDN-Bereinigungsadapter - Verlauf

Die Fusion sammelt den Bereinigungsverlauf jedes Mal, wenn sie ausgeführt wird. Sie können den Bereinigungsstatus, Informationen zur Bereinigung und die vom Dienst zurückgegebenen Nachrichten anzeigen. Um den Bereinigungsverlauf anzuzeigen, klicken Sie auf die Schaltfläche **Verlauf** auf der Bildschirme **CDN Purge Adapters oder Purge Groups**.



Die Liste enthält die Zeit und den Status der letzten 100 Löschausführungen. Sie können die Details einer Löschanforderung anzeigen, die an den CDN-Dienst gesendet wird, indem Sie auf die gewünschte Zeile in der Tabelle klicken. Die Detailinformationen umfassen die für die Bereinigung angegebenen URIs und die API-Antworten, die vom Dienst während des Bereinigungsvorgangs zurückgegeben wurden.



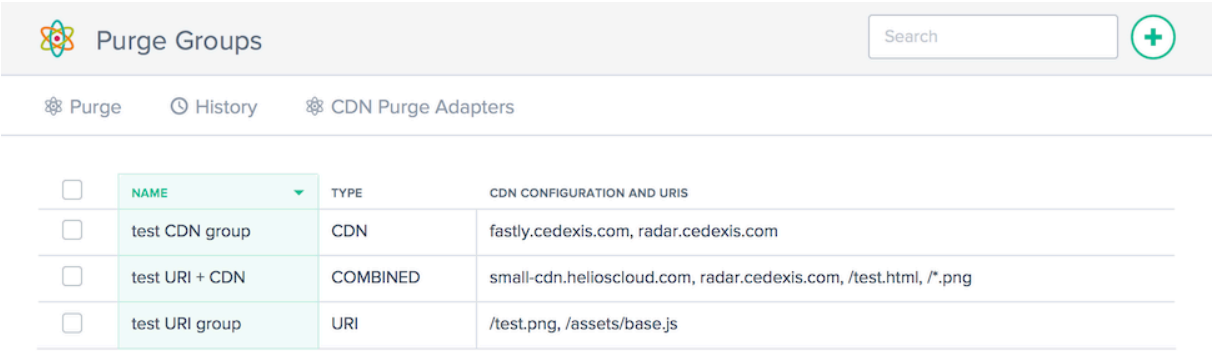
Wenn Sie eine bestimmte Bereinigung erneut ausführen möchten, die den Verlauf enthält, klicken Sie rechts neben den Statusinformationen zum Löschen auf die Schaltfläche **Neuausgabe**. Der Löschdialog wird mit den Daten aus der vorherigen Bereinigung angezeigt, die für die Ausführung vorgeladen wurden.

Gruppen löschen

Mit Bereinigungsgruppen können Sie CDN-Bereinigungsadapter und URIs organisieren, um das Löschen logischer Ressourcen zu erleichtern. Beispielsweise können Sie Entwicklungs-, Test- und Produktionsumgebungen gruppieren und alle gleichzeitig löschen. Oder löschen Sie alle Imageressourcen über mehrere CDNs gleichzeitig.

Bereinigungsgruppen können aus einer Sammlung von CDN-Bereinigungsadaptern, Bereinigungs-URIs oder beides bestehen. In der Regel wird eine Gruppe, die nur CDN-Bereinigungsadapter enthält, zum Löschen verschiedener Ressourcen über mehrere Dienste hinweg verwendet. Eine kombinierte Gruppe wird häufig verwendet, um eine standardmäßige, wiederverwendbare Säuberung vorab festzulegen, z. B. “alle Medien auf allen meinen regionalen Websites und CDNs”.

Wenn Sie mindestens eine Löschgruppe einrichten, wird dieser Bildschirm beim Öffnen von CDN Purge angezeigt.



Die Spalten enthalten folgende Informationen:

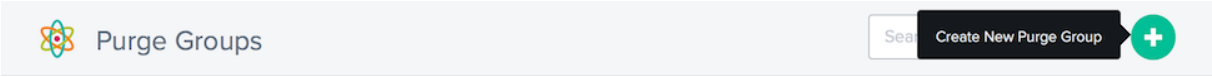
Überschrift	Beschreibung
Name	Der Name der Bereinigungsgruppe.
Typ	Der Inhaltstyp der Gruppe. + CDN —Die Bereinigungsgruppe enthält nur CDN-Bereinigungsadapter und der Benutzer muss URIs angeben, wenn der Bereinigungs-URI ausgeführt wird —die Bereinigungsgruppe enthält nur URIs und der Benutzer muss beim Ausführen der Bereinigung Dienste angeben + Kombiniert —die Bereinigungsgruppe enthält beides CDN bereinigen von Adaptern und URIs; der Benutzer kann die Bereinigung ausführen, ohne weitere Informationen angeben zu müssen
CDN-Konfiguration und URIs	Die CDN-Bereinigungsadapter und/oder URIs, die in der Gruppendefinition enthalten sind.

Bereinigungsgruppen erstellen

Um Bereinigungsgruppen verwenden zu können, müssen Sie die CDN-Bereinigungsadapter oder URIs angeben, die enthalten sein müssen. Es gibt zwei Möglichkeiten, Gruppen zu erstellen:

Auf der Seite CDN-Bereinigungsadapter können Sie die gewünschten Bereinigungsadapter überprüfen und dann auf **Löschgruppe erstellen** klicken.

Klicken Sie auf der Seite "Gruppen bereinigen"auf **+**, um eine Gruppe zu erstellen.

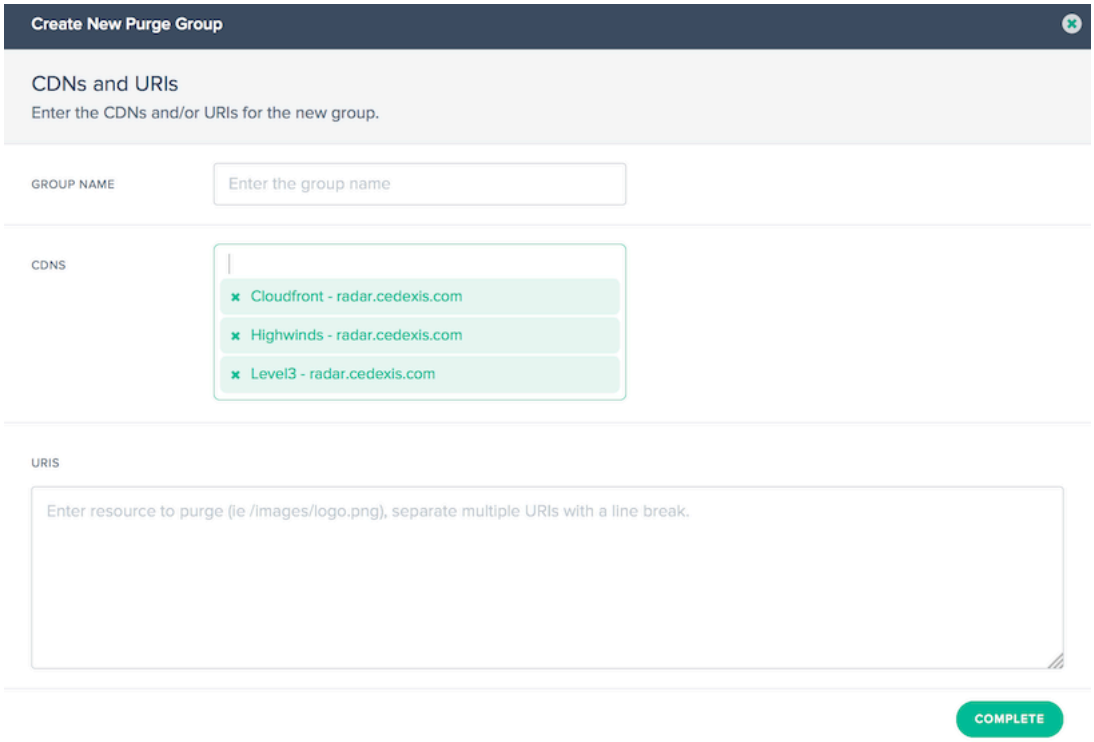


In beiden Fällen wird das Dialogfeld **Neue Gruppe erstellen** angezeigt.

Geben Sie den Namen für die Löschgruppe ein.

> **HINWEIS:** Sie können CDN-Bereinigungsadapter hinzufügen oder aus der Liste entfernen.

Klicken Sie auf **Abgeschlossen**, um die Gruppe zu erstellen.



GruppenBereinigungen ausführen

Wählen Sie auf der Seite "Gruppe löschen"eine oder mehrere Gruppen aus und klicken Sie dann auf die Schaltfläche **Löschen**. Das Dialogfeld **CDN Löschen** wird mit den Parametern geöffnet, die in der Definition der Löschgruppe angegeben werden.

Klicken Sie auf die Schaltfläche **Löschen ausführen**, um die konfigurierte Bereinigung zu starten.

Warnungen

September 14, 2023

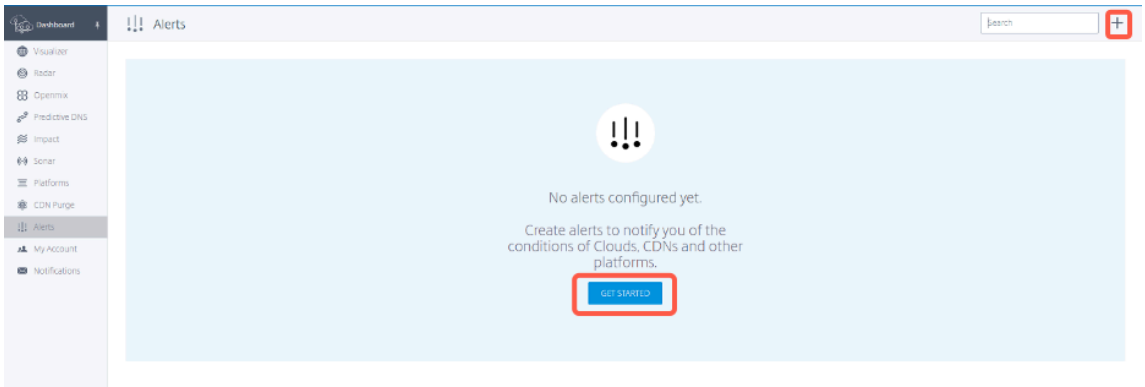
Die Funktion **Alerts** überwacht Leistungsprobleme oder Anomalien Ihrer konfigurierten Plattformen von einem Endbenutzer-Netzwerk auf der ganzen Welt aus.

Erstellen Sie Benachrichtigungen

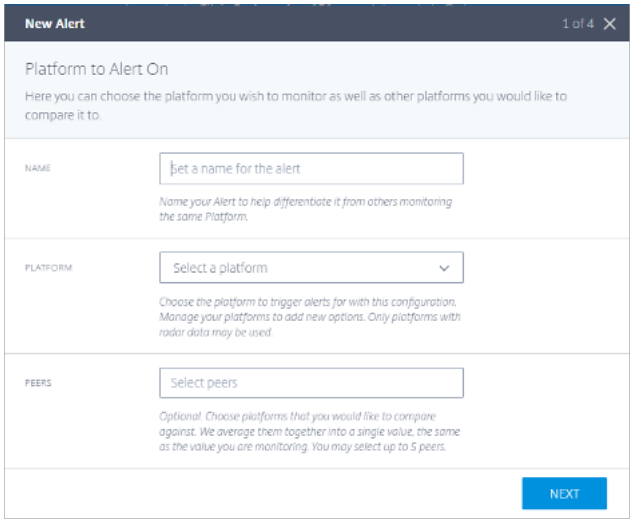
Um Warnmeldungen zu erstellen, die die Leistung Ihrer Plattformen überwachen, müssen Sie zunächst Ihre Plattformen einrichten. Klicken Sie in der linken Seitenleiste auf **Plattformen**, um zum Plattformbildschirm zu gelangen und Ihre Plattformen einzurichten.

So fügen Sie eine neue Warnung hinzu:

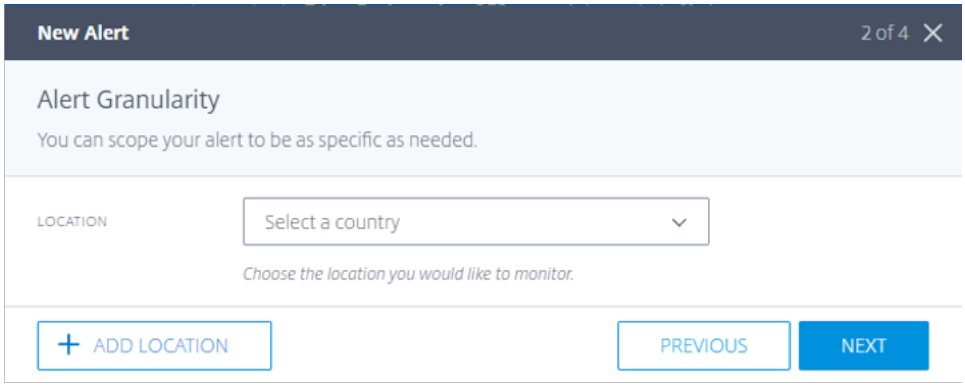
1. Klicken Sie in der linken Seitenleiste auf **Benachrichtigungen**, um zur Seite Alerts zu gelangen und Alerts zu erstellen.
2. Klicken Sie auf der Seite Alerts auf **ERSTE SCHRITTE** oder auf das **+-Symbol** in der oberen rechten Ecke.



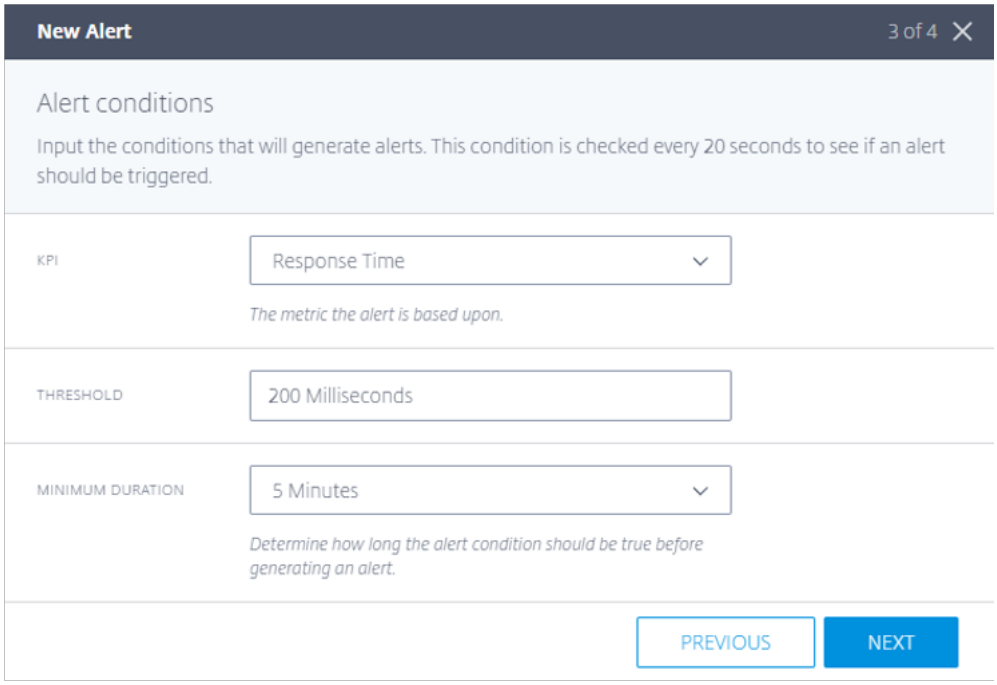
3. Gehen Sie im Fenster **Neue Warnung** wie folgt vor
   - den Namen der Warnung eingeben
   - Wählen Sie die relative Plattform aus, die überwacht werden soll
   - Wählen Sie Peer-Plattformen aus, mit denen Sie vergleichen möchten (Sie können bis zu 5 Peers auswählen). Dieser Parameter ist optional.
   - klicken Sie auf **Weiter**.



4. Wählen Sie den **Standort** und das **Netzwerk** aus, für die Sie die Warnungen überwachen möchten, und klicken Sie auf **Weiter**.



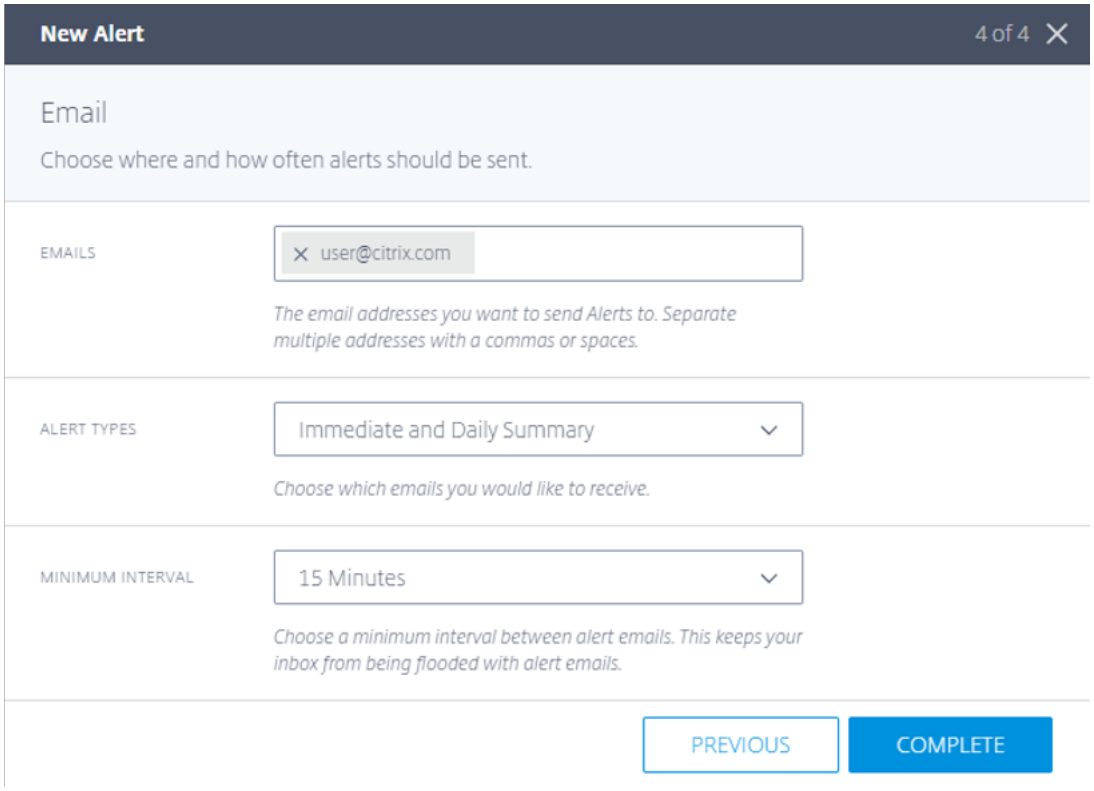
5. Wählen Sie den entsprechenden **KPI**, den **Schwellenwert**und die **Mindestdauer** des Ereignisses, das die Warnung auslöst.



NetScaler Intelligent Traffic Management bietet die folgenden KPIs:

- **Reaktionszeit:** Der Wert des Schwellenwerts gibt den Maximalwert (in Millisekunden) an, der akzeptiert wird, bevor die Warnung ausgelöst wird. Damit eine Warnung ausgelöst wird, sollte die Messung mindestens für die vom Benutzer gewählte **Zeit ≥ minimum_duration** über dem Schwellenwert liegen. Derselbe Alarm wird ausgelöst, nachdem die Messung erneut für mindestens eine Zeit ≥ Mindestdauer unterhalb des Schwellenwerts empfangen wurde.
- **Verfügbarkeit:** Der Wert des Schwellenwerts gibt den minimal akzeptierten Wert an, bevor die Warnung ausgelöst wird. Damit eine Warnung ausgelöst wird, sollte die Messung mindestens für die vom Benutzer gewählte **Zeit ≥ minimum_duration** niedriger sein als der Schwellenwert. Derselbe Alarm wird ausgelöst, nachdem eine Messung über dem Schwellenwert für mindestens eine Zeit größer oder gleich ≥ Mindestdauer erneut empfangen wurde.
- **Durchsatz:** Der Wert des Schwellenwerts gibt den Mindestwert (in kbps) an, der akzeptiert wird, bevor die Warnung ausgelöst wird. Damit eine Warnung ausgelöst wird, sollte die Messung mindestens für die vom Benutzer gewählte **Zeit ≥ minimum_duration** niedriger sein als der Schwellenwert. Derselbe Alarm wird ausgelöst, nachdem eine Messung über dem Schwellenwert für mindestens eine Zeit größer oder gleich ≥ Mindestdauer erneut empfangen wurde.

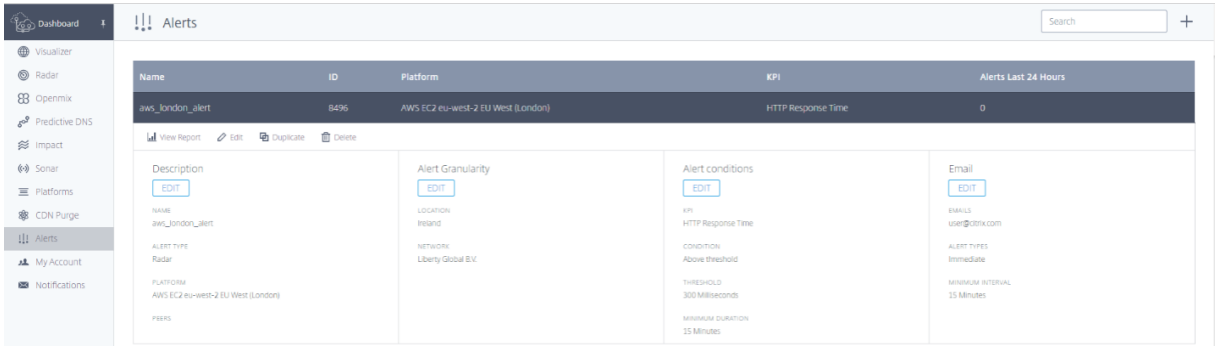
6. Geben Sie die E-Mail-Adressen ein, an die Sie Benachrichtigungen senden möchten, wählen Sie den Warnungstyp und das Mindestintervall zwischen Warnungs-E-Mails aus.



Die Warnungstypen sind wie folgt:

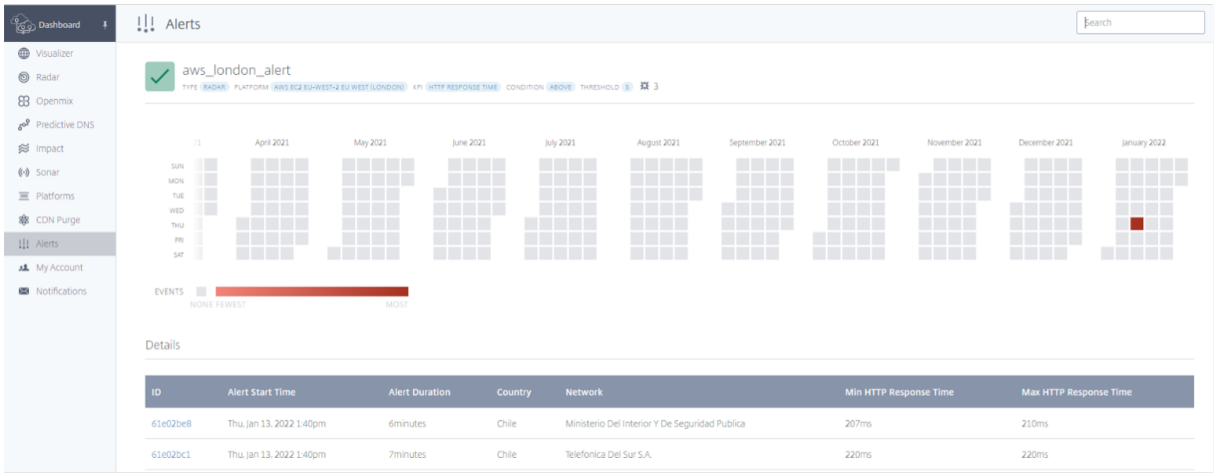
- **Sofort:** Diese Option sendet sofort eine E-Mail, wenn eine Warnung ausgelöst wird.
- **Tägliche Zusammenfassung:** Diese Option sendet nur eine E-Mail pro Mitternacht in Universal Time Coordinated (UTC), einschließlich aller Ereignisse, die ausgelöst werden.
- **Sofortige und tägliche Zusammenfassung:** Diese Option ist eine Kombination aus sofortigem und täglichem E-Mail-Versand.

7. Nachdem Sie eine Warnung konfiguriert haben, können Sie die Alerts auf der Registerkarte **Alerts** und die globale Map auf der Registerkarte **Visualizer** sehen. Um den Bericht für eine bestimmte Warnung anzuzeigen, klicken Sie auf der Registerkarte **Alerts** auf **Bericht anzeigen** .



Auf der folgenden Berichtsseite werden Ereignisse angezeigt, die pro Tag für jeden Monat überwacht

werden. Im folgenden Screenshot werden beispielsweise 3 Vorfälle am selben Tag im Januar 2022 überwacht.



Sie können auf einen bestimmten Vorfall oder ein Ereignis klicken, um die Details anzuzeigen, wie in der folgenden Abbildung gezeigt:

Überwachung der Netzwerkerfahrung

September 14, 2023

Übersicht

Der **Citrix Network Experience Monitoring Service (NEM)** (früher **Netscope**) ermöglicht Dienstanbietern, Unternehmen, ISPs und Drittanbietern den Zugriff auf detaillierte Radarmessprotokolle und

Standardberichte in Form von zusammengefassten verwertbaren Daten. NEM bietet mehrere Standardprotokolle und Berichte an, mit denen Kunden die Qualität ihrer Dienste messen können.

Diese Lösung umfasst die Bereitstellung von "rohen"Radarmessungen und den Zugriff auf die Citrix ITM Data API. NEM stellt sowohl die granularen Daten (als Rohmessungen oder Datenaggregate) als auch Datenschwellenwarnungen bereit. Diese Services helfen bei der Erkennung, Isolierung der Plattformverfügbarkeit und Performanceprobleme bei Plattformkollegen und den zugrunde liegenden ISPs.

"Raw"-Radarmessungen: Radarmessungen liefern pro Ereignis granulare Informationen, die täglich gechargt werden. Radarmessungen umfassen öffentliche, gemeinschaftliche und private Messdaten, die vom Tag erfasst werden. Daten wie Verfügbarkeit, Reaktionszeit, Durchsatz für HTTP- und HTTPS-Messungen sind enthalten. Die folgenden Datenfelder werden bereitgestellt:

- Anbieter-ID, Resolver-IP, verschleierte (/28) Client-IPs
- Verschleierter Referrer-Header, Benutzeragent, Endbenutzer-ASN
- Geodaten für Resolver- und Kundenfelder

Radar-Metriken, die in den "Raw"-Messungen verfügbar sind, sind:

- Verfügbarkeit, Reaktionszeit und Durchsatz (wenn gemessen)
- DNS-Suchzeit (optional), TCP-Verbindungszeit (optional) und sichere Verbindungszeit (optional)
- Latenz (optional)
- Downloadzeit (optional)

Radarmessungen sind verfügbar, damit Kunden die gesammelten Daten selbst analysieren können. Der Datensatz enthält Informationen zur Providerleistung und -verfügbarkeit (Fehler) für eine Reihe von Kommunikationsprotokollen.

Protokolldateidaten sind 7 Tage lang über einen AWS S3 oder Google Cloud Storage-Bucket verfügbar. Kunden können Protokolldateien von Community- und privaten Daten mithilfe von Standard-Bucket-Zugriffsmethoden abrufen.

"Raw"-Messungen in Echtzeit (optional): Raw-Radar-Messungen werden in Echtzeit an einen AWS S3-Bucket geliefert. Diese Protokolle sind in der Regel innerhalb von 5 Minuten nach der Erfassung verfügbar. Sie bieten so viel Granularität wie die zuvor erwähnten Radar-Rohmessungen.

Daten-API: Die Citrix ITM Radar-Daten-API stellt Aggregate der öffentlichen Gemeinschaft und private Messdaten zur Verfügung. Die Daten werden kontinuierlich aktualisiert und etwa alle 60 Sekunden gestapelt, um sie von der API abzurufen. Die Daten-API wird bereitgestellt, damit Kunden Radar-Daten in ihre eigenen Berichte und Dashboards integrieren können.

Teilen von Protokollen und

- Radarprotokolle können in Echtzeit und täglich geliefert werden.
- Berichte werden täglich ausgeführt.
- Die Ergebnisse werden in AWS S3 (S3) oder Google Cloud Storage (GCS) gespeichert.
- Protokolle und Berichte haben beide eine Aufbewahrungsfrist von 7 Tagen und werden automatisch eine Woche nach der Erstellung gelöscht.
- Berichte liegen normalerweise je nach Berichtstyp im TSV- (tabulatorseparierter Wert) oder JSON-Format vor.

Kunden erhalten Anmeldeinformationen für den Zugriff auf die S3- und GCS-Buckets. Für die Anmeldung kann ein Befehlszeilentool wie s3cmd oder die AWS-CLI für S3 oder gsutil für GCS verwendet werden. Die S3cmd-Konfigurationsdatei erkennt die über die Portal-Benutzeroberfläche erhaltenen Zugriffsschlüssel und hilft dem Benutzer, sich mit dem S3-Bucket zu verbinden.

Die AWS CLI muss auf dem Computer des Kunden installiert werden, um eine Verbindung mit S3 herzustellen und auf die Protokolle zuzugreifen. Für GCS erhält der Kunde die Zugriffsschlüsseldatei als Download über die Portal-Benutzeroberfläche, die mit dem gsutil-Tool verwendet werden kann. Weitere Informationen finden Sie in den häufig gestellten Fragen.

Kunden erhalten E-Mail-Benachrichtigungen, sobald Berichte verfügbar sind.

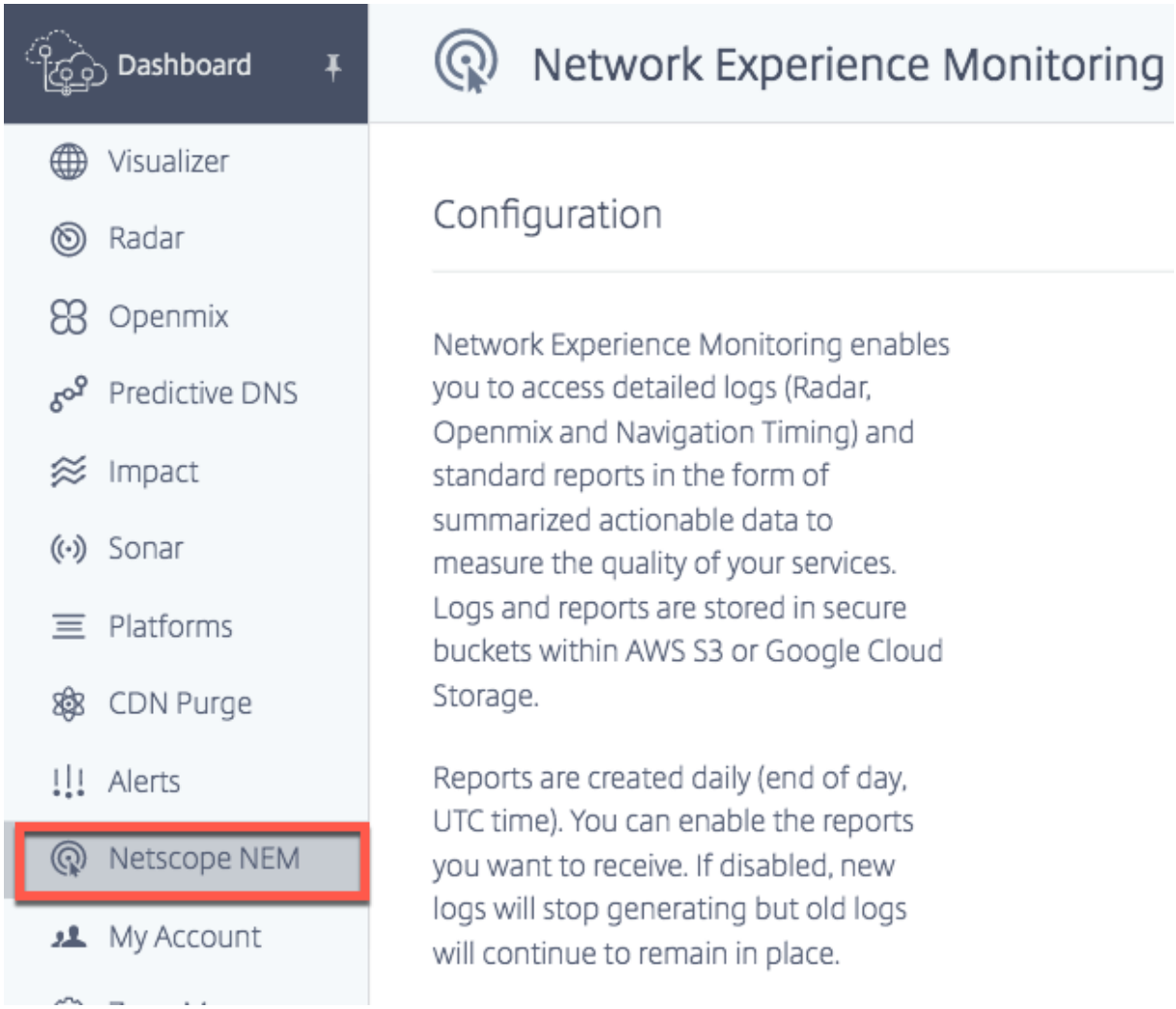
Plattformeinstellungen

Sie müssen Ihre Plattform so konfigurieren, dass die für Netscope NEM erforderlichen Daten unterstützt und erstellt werden. Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Einstellungen für Ihre Plattform aktiviert sind:

- Aktivieren Sie für Anonyme beste Berichte die **Einstellungen für die Radarsonde**.
  - Aktivieren Sie für Anonymous Best RTT **Reaktionszeit und Verfügbarkeit**.
  - Aktivieren Sie für den besten anonymen **Durchsatz die Option Durchsatz und Verfügbarkeit**.
- Aktivieren Sie für Cache-Knoten-ID-Berichte die **Radarsondeneinstellungen**und aktivieren Sie unter **Erweiterte Radareinstellungen**die **Knoten-ID**.
- Aktivieren Sie für Details zum Ressourcen-Timing die **Option Zeitstempel** in den **erweiterten Radar**

Navigation

Wählen Sie im Hauptmenü **Netscope NEM**aus. Die Seite Konfiguration der **Network Experience Monitoring** wird geöffnet.



Plattformen und Netzwerke

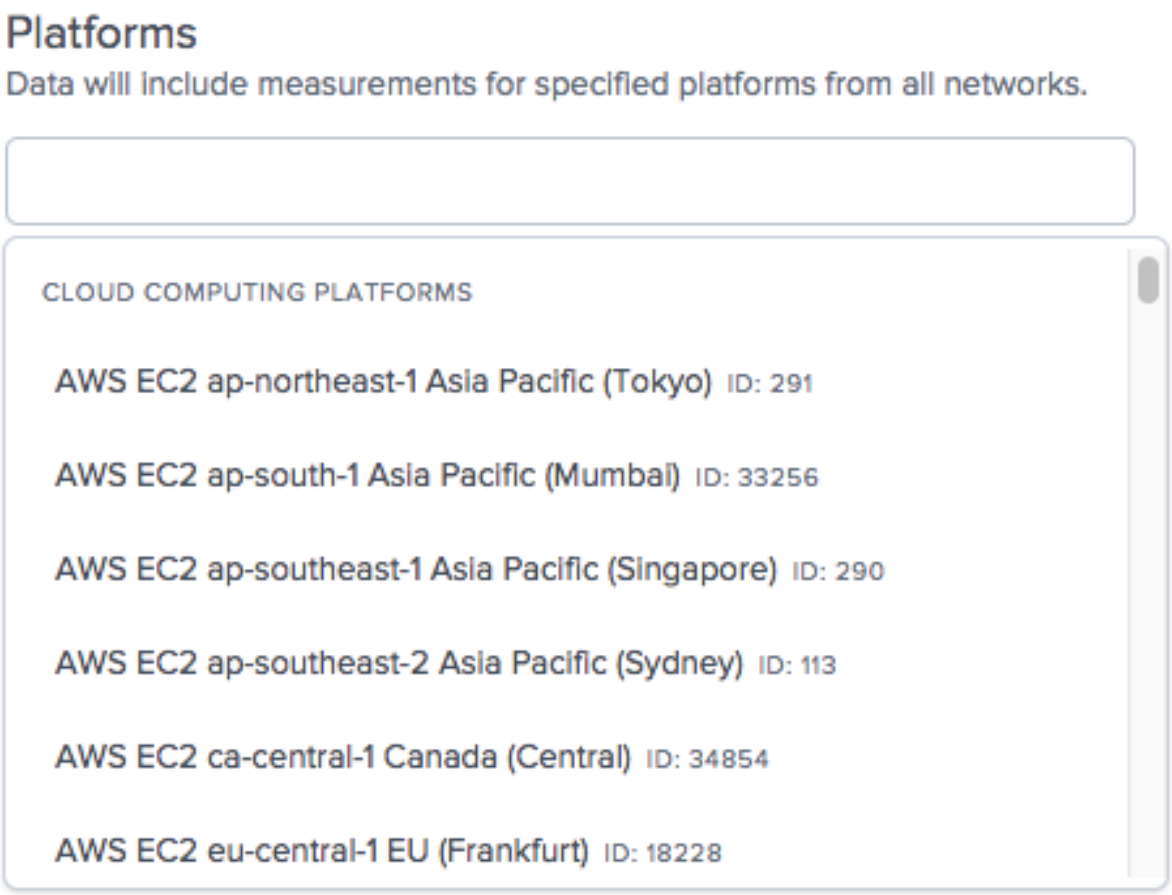
Wählen Sie die erforderlichen **Plattformen** oder **Netzwerke** (oder beide) aus, um den Konfigurationsprozess zu starten.

> **HINWEIS:**
>
> Protokolle und Berichte können nur konfiguriert und generiert werden, wenn mindestens eine **Plattform** oder ein **Netzwerk** ausgewählt ist.

Die zusammengefassten Daten, die der Kunde erhält, umfassen Radarmessungen von ausgewählten Plattformen (für alle zugehörigen Netzwerke) oder ausgewählte Netzwerke (für alle zugehörigen Plattformmessungen).

Auswählen von Plattformen

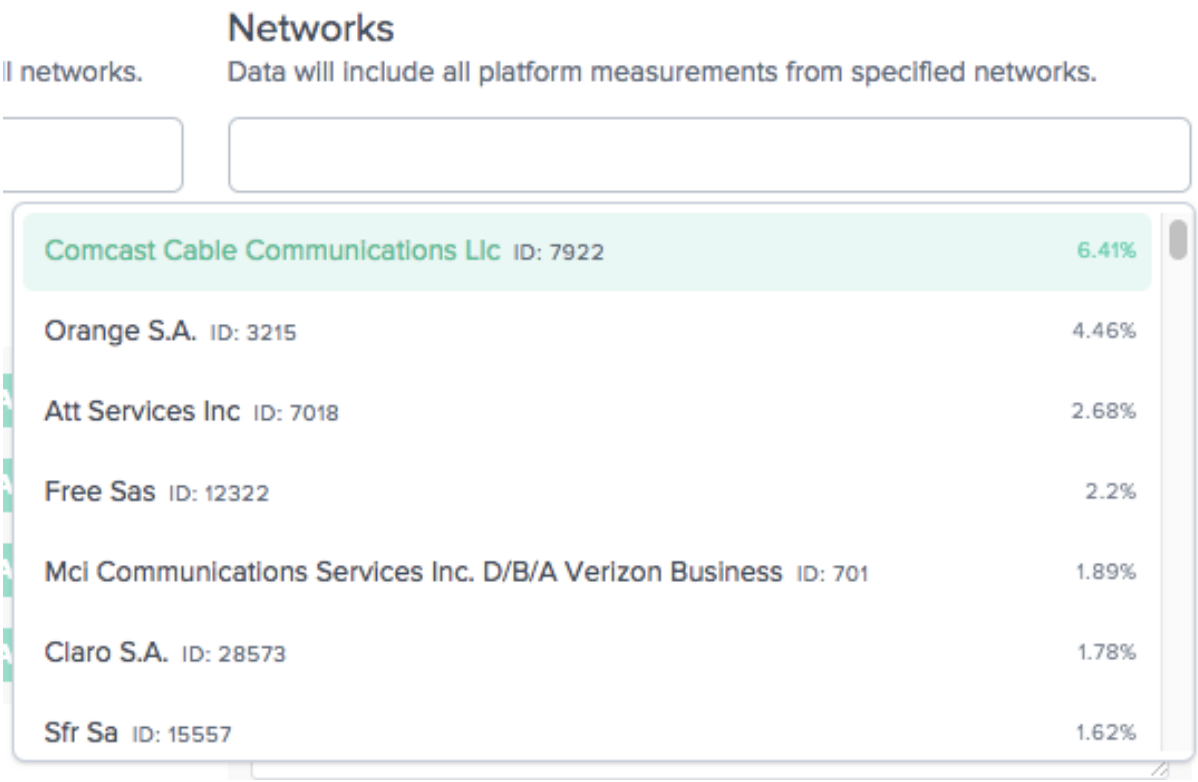
Wählen Sie für Content Service Provider oder Unternehmen Plattformen wie CDNs, Clouds, Rechenzentren oder andere Endpunkte aus. Wählen Sie Plattformen aus, für die Messungen erforderlich sind.



Netzwerke auswählen

Wählen Sie für ISPs die **Netzwerke** aus der Liste aus, die verschiedenen Plattformen oder Endpunkten zugeordnet ist, für die Messungen erforderlich sind.

> **HINWEIS:**
>
> Wenn Sie die erforderliche Plattform nicht in der Liste finden, können Sie sie im Abschnitt **Plattform** des Portals konfigurieren. Wenden Sie sich für nicht verfügbare Netzwerke an das Support-Team .



Plattformberichte

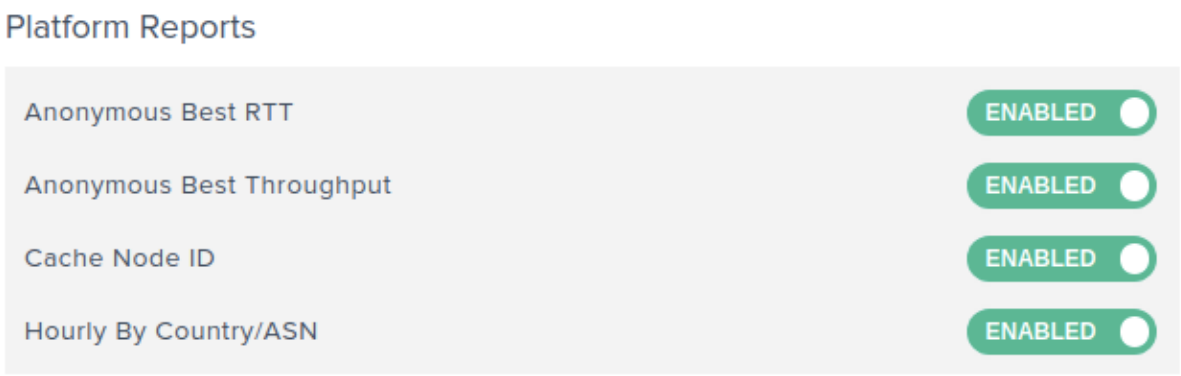
Es gibt vier Arten von **Plattformberichten**:

1. **Anonym Best for Round Trip Time (RTT)**
2. **Anonym Best for Through**
3. **Cache-Knoten-ID**
4. **Stündlich nach Land/ASN**

Eine Beschreibung der Protokolle finden Sie unter Radarprotokollbeschreibungen und Berichte für Dienstanbieter und Unternehmen.

Plattformberichte aktivieren

Klicken Sie auf den Umschalter, um die Berichte, die Sie erhalten möchten, zu aktivieren oder zu deaktivieren. Wenn Sie einen vorhandenen Bericht deaktivieren, werden keine neuen Protokolle generiert, aber alte Berichte bleiben am aktuellen Speicherort.



Anonymer Bester Bericht für Plattformen

- Diese Berichte helfen Anbietern dabei, ihre Leistung mit der von anderen Plattformen innerhalb ihrer Peer-Gruppe, d. h. innerhalb desselben Landes, derselben Region oder ASN zu vergleichen.
- Die Leistungsdaten der 15 wichtigsten Anbieter in der Peer-Group werden auf der Grundlage derselben Kategorien aggregiert. Der beste Wert wird neben dem besten Wert des jeweiligen Anbieters aufgeführt.
- Anonymer Best Report für SSL-Plattformen ist verfügbar, damit ihre Leistung mit anderen SSL-Plattformen verglichen werden kann.
- Die Client-IPs werden auf /28 gekürzt.
- Die Ergebnisse des "besten"Anbieters helfen Clouds/CDNs dabei, ihre Leistung auf hochvolumige oder geschäftskritische ASNs zu konzentrieren, die für ihre Mitbewerber wettbewerbsschwach sind.
- Der Bericht enthält Details zur Leistung, aufgeschlüsselt nach DNS-Resolver-IP, Client-IP /28 und dem Caching-Knoten, der die Objekte bedient hat. Dasselbe wird mit der "besten"Plattform für dieselben Kriterien verglichen.

Verfügbar für RTT und Durchsatz.

- Beschreibungen der Protokolle finden Sie unter Radarprotokollbeschreibungen und Berichte für Service Provider and Enterprises.

Cache-Knoten-ID-Bericht für Plattformen

- Dieser Bericht wird verwendet, um den spezifischen Server oder das Datencenter zu identifizieren, das auf eine Anfrage reagiert hat, und hilft bei der Diagnose von Serverproblemen.
- Es liefert die ID des Rechenzentrums oder der Maschine, die auf eine bestimmte Anfrage geantwortet hat.

- Es hilft zu verstehen, warum die Leistung über einen bestimmten Knoten (POP oder Maschine oder Knoten-ID) gut oder schlecht war.
- Die Leistung besteht aus Reaktionszeit, Durchsatz, Verfügbarkeit (Probentyp), der DNS-Resolver-IP, Client IP /28 und dem Caching-Knoten, der die Objekte bedient hat.
- Protokollbeschreibungen finden Sie unter [Radarprotokollbeschreibungen und -berichte für Service Provider and Enterprises] (#radar -log-descriptions-and-reports-for-service-providers-and-enterprises)

Stündlich nach Land/ASN

- Mit diesem Bericht können Sie überprüfen, ob die Leistung Ihrer Anbieter im Laufe eines Tages erheblich variiert.
- Es zeigt die Zeit, zu der die Messungen auf die Stunde abgeschnitten wurden, zum Beispiel `2018-03-11T23:00:00`.
- Beschreibungen der Protokolle finden Sie unter Radarprotokollbeschreibungen und Berichte für Service Provider and Enterprises.

Netzwerkberichte

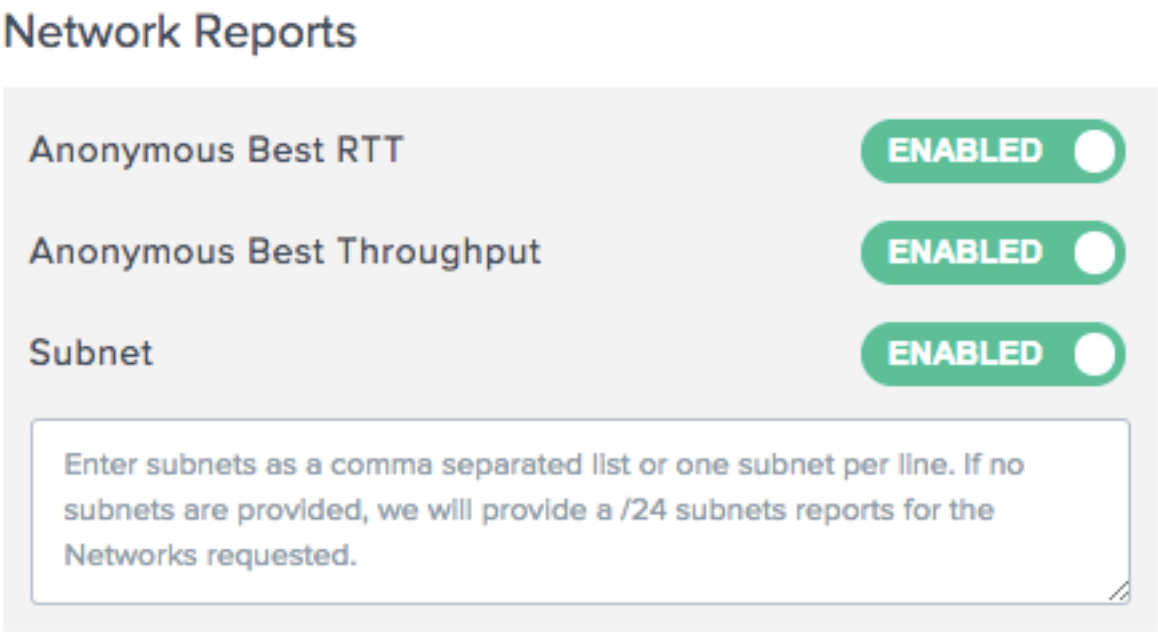
Es gibt drei Arten von **Netzwerkberichten**:

1. **Anonym Best for Round Trip Time (RTT)**
2. **Anonym Best for Through**
3. **Subnetz**

Eine Beschreibung der Protokolle finden Sie unter Radarprotokollbeschreibungen und Berichte für ISPs.

Netzwerkberichte aktivieren

Klicken Sie auf den Umschalter, um die Berichte, die Sie erhalten möchten, zu aktivieren oder zu deaktivieren. Wenn diese Option deaktiviert ist, werden keine neuen Protokolle mehr generiert, aber alte Berichte sind vorhanden.
Um einen Subnetzbericht zu generieren, geben Sie die spezifischen Subnetze Ihrer Netzwerke ein. Wenn keine Subnetze eingegeben wurden, werden Berichte mit dem ASN-CIDR-Block als Standardsubnetz generiert.



Anonymer Bester Bericht für ISPs

- Im Bericht Anonymous Best für ISPs wird eine Peer-Group für den "besten"Vergleich verwendet. Die Peer-Gruppe basiert auf dem Standort des ISP. Normalerweise sind es die 10 am häufigsten gemessenen ISPs in einem bestimmten Land mit einem Minimum von über 1.000 Sitzungen.
- Die Ergebnisse des "besten"ISP helfen ISPs dabei, ihre Leistungsbemühungen auf hochvolumige oder geschäftskritische Plattformen und Bereiche zu konzentrieren, die gegenüber ihren Mitbewerbern wettbewerbsschwach sind.
- Der Bericht enthält Details zur Leistung, aufgeschlüsselt nach Geographie und Plattform, und vergleicht sie mit dem "besten"ISP für dieselben Kriterien.
- Verfügbar für RTT und Durchsatz.
- Eine Beschreibung der Protokolle finden Sie unter Radarprotokollbeschreibungen und Berichte für ISPs.

Subnetzbericht für ISPs

- Dieser Bericht liefert ISPs Informationen darüber, wie sich die spezifischen Subnetze ihrer Netzwerke für Benutzer über die von uns gemessenen Plattformen verhalten.
- Es enthält Informationen über den Dienstanbieter, der auf eine bestimmte Anforderung geantwortet hat.
- Es hilft, die Leistung eines Netzwerksubnetzes zu verstehen.

- Die Leistung besteht aus Reaktionszeit, Durchsatz, Verfügbarkeit (Probentypen), der DNS-Resolver-IP, Client IP /28 und dem Subnetz des Benutzers.
- Eine Beschreibung der Protokolle finden Sie unter Radarprotokollbeschreibungen und Berichte für ISPs.

Radarprotokolle

- Radarprotokolle sind für Plattformen und Netzwerke verfügbar.
- Sie enthalten eine Teilmenge der Felder, die in den Rohprotokollen verfügbar sind, mit einigen Daten anonymisiert: Client IP /28, Referer MD5-Hash.
- Jede Messung für öffentliche Plattformen wird bereitgestellt, unabhängig von der Seite, auf der die Messung generiert wurde.

> **HINWEIS:**
>
> NEM stellt niemals vollständige Client-IPs bereit. Stattdessen wird /28 offen gelegt. Beispielsweise wird eine IP von 255.255.255.255 in einem Bericht als 255.255.255.240/28 angezeigt.

Protokollfrequenz

Radarprotokolle können täglich (alle 24 Stunden) erstellt werden, d.h. am Ende des Tages, UTC-Zeit. Protokolle können auch in Echtzeit (Minute für Minute) generiert werden.

Datei-Format

Wählen Sie **TSV oder JSON**, um Protokolle und Berichte in einem dieser Formate zu empfangen.

Messungstyp

Sie können Protokolle für die folgenden Messarten konfigurieren: Verfügbarkeit, Reaktionszeit und Durchsatz. Im Bericht: 1: Verfügbarkeit, 0: HTTP-Antwortzeit und 14: HTTP-Durchsatz.

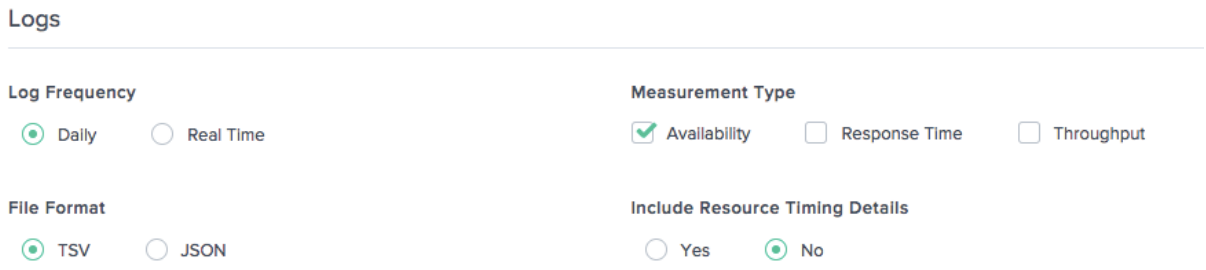
Details zur Ressourcenzeitplanung

Sie können festlegen, dass auch Details zum Ressourcen-Timing einbezogen werden sollen, indem Sie auf die Schaltflächen **Ja** oder Nein klicken. Zu den Details des Ressourcen

- DNS-Nachschlagezeit
- TCP-Verbindungszeit
- Sichere Verbindungszeit

- Download-Zeit

Beschreibungen der Protokolle finden Sie unter Radarprotokollbeschreibungen und Berichte für Service Provider and Enterprises.



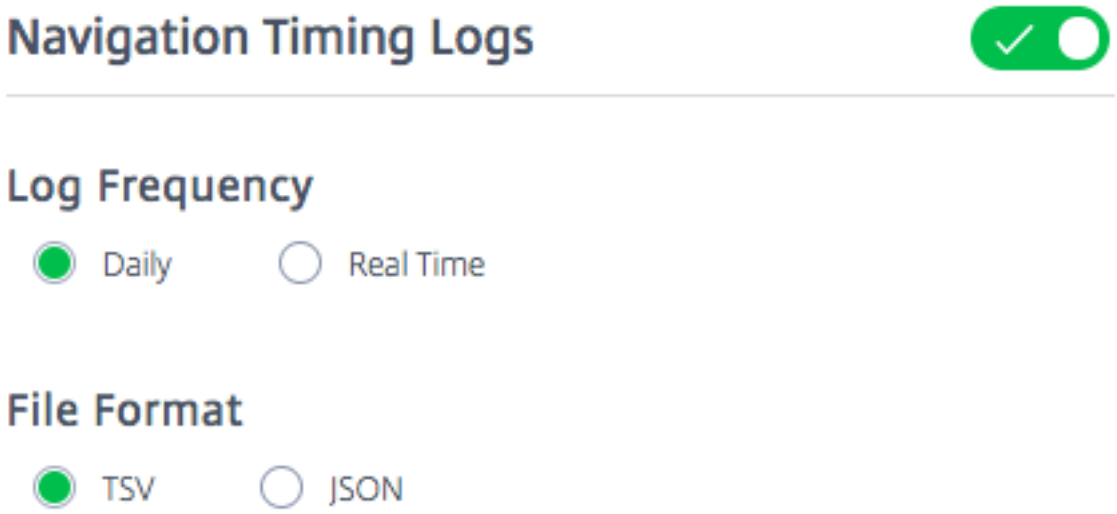
Navigationszeitprotokolle

Protokollfrequenz

Navigations-Timing-Protokolle können täglich (alle 24 Stunden) generiert werden, dh am Ende des Tages, UTC-Zeit. Protokolle können auch in Echtzeit (Minute für Minute) generiert werden.

Datei-Format

Wählen Sie **TSV** oder **JSON**, um Navigationszeitprotokolle in einem dieser Formate zu empfangen. Beschreibungen der Protokolle finden Sie unter Beschreibungen des Navigationszeitprotokolls.



Openmix Protokolle

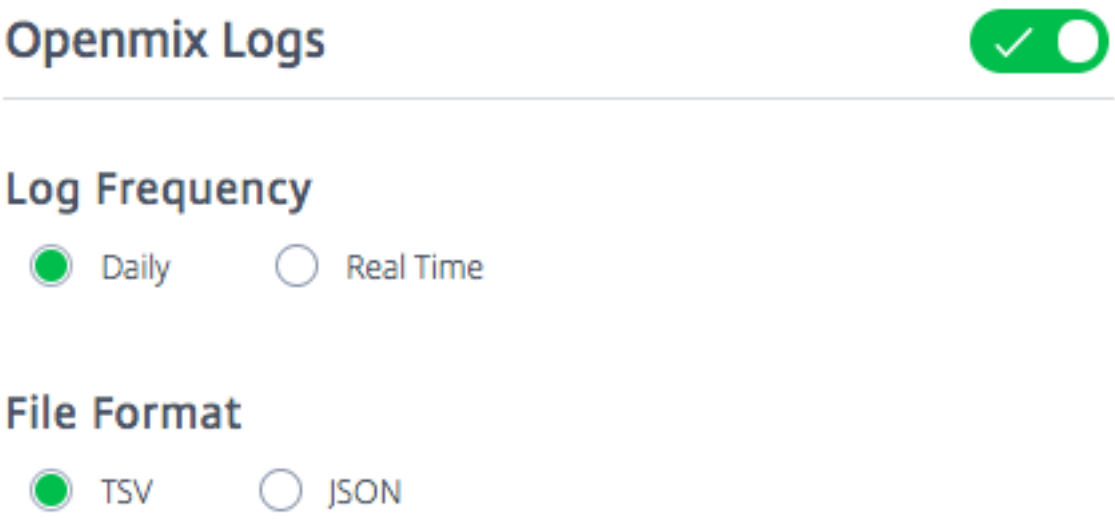
Protokollfrequenz

Openmix-Protokolle werden in Echtzeit (d. h. Minute für Minute) generiert. Diese Protokolle bieten Echtzeitmessungen für Openmix-Kunden.

Datei-Format

Wählen Sie **TSV** oder **JSON**, um Openmix- und HTTP Openmix-Protokolle in einem dieser Formate zu empfangen. JSON ist jedoch das empfohlene Format.

Logbeschreibungen finden Sie unter Openmix Log Descriptions.



Bereitstellung von Cloud-Diensten

Mit dieser Option können Sie die Art der Lieferung auswählen. Sie können Protokolle und Berichte entweder im AWS S3-Bucket oder im Google Cloud Storage (GCS) -Bucket empfangen.
Sie können mit den bereitgestellten Anmeldeinformationen auf die S3- und GCS-Buckets zugreifen und s3cmd oder die AWS-CLI für S3. und die gsutil-Befehlszeile für GCS verwenden.

AWS S3

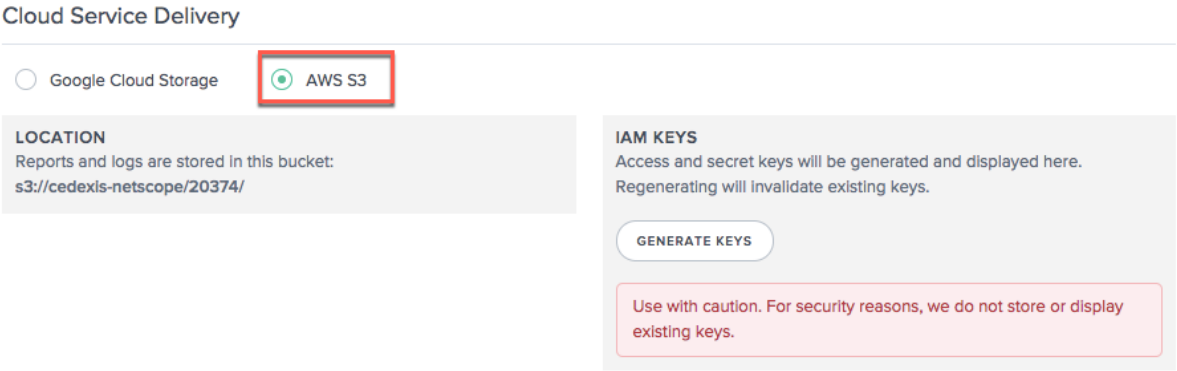
Wählen Sie AWS S3 aus, um Protokolle und Berichte an den AWS S3-Bucket zu **übermitteln**.

Standort Der Standort stellt den Bucket in AWS S3 dar, in dem die Protokolle und Berichte gespeichert werden.

IAM-Schlüssel Wenn Sie unter AWS S3 auf die Schaltfläche **Schlüssel generieren** klicken, werden die AWS IAM-Schlüssel (Access und Secret Keys) generiert und unter IAM-Schlüssel angezeigt. Achten Sie darauf, die Schlüssel aufzuzeichnen, da sie nirgends gespeichert sind, um sie später anzusehen.

> **HINWEIS:**
>
> Das Paar von Access- und Secret-Schlüsseln ist die einzige Kopie der privaten Schlüssel. Der Kunde muss sie sicher aufbewahren. Durch das Regenerieren der neuen Schlüssel werden die vorhandenen ungültig.
> Die Konfigurationsdatei S3cmd erkennt die Zugriffsschlüssel (die über die Portal-Benutzeroberfläche empfangen werden) und hilft dem Kunden, sich mit dem S3-Bucket zu verbinden. Die AWS-CLI muss auf dem Computer des Kunden installiert sein, um eine Verbindung zum S3 herzustellen.

Informationen zur Verwendung der Access- und Secret-Keys mit s3cmd zum Herunterladen von Berichten aus dem S3-Bucket finden Sie in den FAQ.



Google Cloud-Speicher

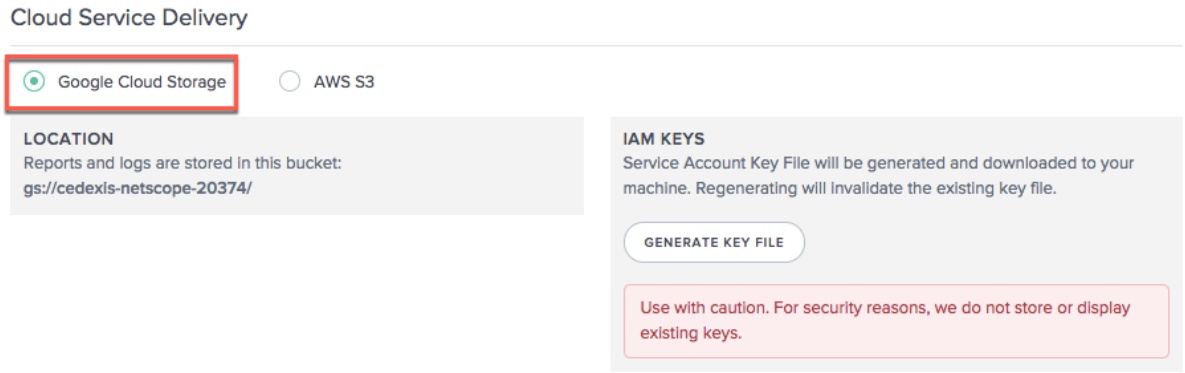
Wählen Sie **Google Cloud Storage aus, um Protokolle und Berichte an GCS zu übermitteln**.

Standort Der Standort stellt den Bucket in Google Cloud Storage dar, in dem Protokolle und Berichte gespeichert werden.

IAM-Schlüssel Wenn Sie die Schaltfläche **Schlüsseldatei generieren** auswählen, wird die Google Service-Kontoschlüsseldatei auf Ihren Computer heruntergeladen.

> **HINWEIS:**
>
> Diese Schlüsseldatei dient als einzige Kopie des privaten Schlüssels. Notieren Sie sich die E-Mail-Adresse Ihres Dienstkontos und speichern Sie die private Schlüsseldatei des Dienstkontos sicher. Durch das erneute Generieren einer neuen Schlüsseldatei wird die vorhandene Datei ungültig.

Diese Schlüsseldatei kann mit dem gsutil-Tool verwendet werden, um Protokolle und Berichte aus dem GCS-Bucket herunterzuladen. Einzelheiten zur Verwendung der Schlüsseldatei zum Herunterladen von Protokolldateien finden Sie in den häufig gestellten Fragen.



Radarprotokollbeschreibungen und Berichte für Service Provider und Unternehmen

Radarprotokolle für Anbieter

- Diese Protokolle bieten Radarmessungen für Benchmark-Partner.
- Sie liefern alle Messungen, die für öffentliche Plattformen durchgeführt wurden, unabhängig von der Seite, auf der die Messung generiert wurde.
- Radarprotokolle enthalten eine Teilmenge der Felder, die in den Rohprotokollen verfügbar sind, mit einigen Daten anonymisiert: Client IP /28, Referer MD5-Hash.
- Hier ist ein Beispiel für eine Platform Radar Log Share im TSV-Dateiformat.

> **HINWEIS:**
>
> - NEM stellt niemals vollständige Client-IPs bereit. Stattdessen wird /28 offen gelegt. Beispielsweise wird eine IP von 255.255.255.255 in einem Bericht als 255.255.255.240/28 angezeigt.
> - Die GEO-Informationen des Kunden werden basierend auf dem IPv4 des Kunden extrahiert, das detaillierter ist.

Protokollbeschreibungen Im Folgenden finden Sie die Spaltenüberschriften und Beschreibungen für die Radarprotokolle. Die Felder werden in der folgenden Reihenfolge in den Ausgabedateien angezeigt:

Protokoll	Beschreibung
Zeitstempel	Es ist die UTC-Zeit der Anforderung im Format YYYY-MM-DDTHH:MI:SSZ. Der tatsächliche Wert (auf die Sekunde herunter) in den Protokolltabellen wird auf die nächste Stunde (2018-03-30T23:00:00Z) bzw. den nächsten Tag (2018-03-30T00:00:00Z) in den Stunden-/Tag-Tabellen gerundet. Der Zeitstempel ist in allen Datensätzen immer in UTC angegeben.
Eindeutige Knoten-ID	Wird auch als Cache-Knoten-ID bezeichnet. Es ist ein willkürlicher Wert. In der Regel eine IP, die die CDN Edge-Server zurückgeben, um CDNs dabei zu helfen, intern zu identifizieren, welcher Server eine bestimmte Anfrage bearbeitet hat. (leere Zeichenfolge): Stammt von Radar-Clients, die die UNI-Erkennung nicht unterstützen.0: Der Benutzeragent unterstützt die für die UNI-Erkennung erforderlichen Funktionen nicht.1: Der Client ist während der UNI-Erkennung auf einen Fehler gestoßen, z. B. eine HTTP 404 oder eine andere erfolglose Antwort.2: Es wurde versucht, eine UNI-Erkennung durchzuführen, führte jedoch zu einem Fehler.
Anbieter-ID	Interne ID der Plattform, die gemessen wird.
Sonden-Typ	Der Prüfpunkttyp, der gemessen wird (z. B. 1: HTTP-Verbindungszeit, 0: HTTP-Antwortzeit, 14: HTTP-Durchsatz usw.). Verwenden Sie die Informationen, die innerhalb der zulässigen Zeit erfolgreich zurückgegeben wurden, um anzuzeigen, dass der Dienst verfügbar ist.

Protokoll	Beschreibung
Antwortcode	Ergebnis der Messung, z. B. 0: Erfolg, 1: Timeout, 4: Fehler. Für Verfügbarkeitsberechnungen wird der Prozentsatz der Messungen mit einer Antwort von 0 (Erfolg) im Vergleich zur Gesamtzahl der Messungen (insgesamt, unabhängig von der Reaktion) ermittelt. Bei anderen Sondentypen (RTT und Durchsatz) darf der Filter bei der Berechnung von Statistiken im RTT nur RTT-Datenpunkte mit einem Erfolgscode von 0 berücksichtigen. Gleiches für den Durchsatz.
Messwert	Der aufgezeichnete Messwert, dessen Bedeutung je nach Sondentyp variiert. Sie stellt Verfügbarkeits- (1) /Reaktionszeit (0) -Messungen in Millisekunden und Durchsatz (14) in kBit/s dar.
Resolver-Markt	Der Markt des DNS-Resolvers, der die Anfrage bearbeitet hat. Im Allgemeinen der Kontinent, auf dem sich der DNS-Resolver befindet, wo, 0: Unbekannt (XX), 1: Nordamerika (NA) 5: Afrika (AF), 3: Europa (EU), 4: Asien (AS), 2: Ozeanien (OC), 6: Südamerika (SA).
Resolver Land	Das Land des DNS-Resolvers, der die Anforderung bearbeitet hat. IDs können unter https://community-radar.citrix.com/ref/countries.json.gz Namen zugeordnet werden.
Region “Resolver”	Die Region der DNS-Auflösungsinstanz, die die Anfrage bearbeitet hat. IDs können Namen zugeordnet werden. https://community-radar.citrix.com/ref/regions.json.gz **Hinweis:** Nicht alle Länder der Welt haben definierte Regionen.

Protokoll	Beschreibung
Auflösungsstatus	Der Status des DNS-Resolvers, der die Anfrage bearbeitet hat. IDs können unter https://community-radar.citrix.com/ref/states.json.gz Namen zugeordnet werden. Hinweis: Nicht alle Länder der Welt haben definierte Staaten zugeordnet.
Resolver Stadt	Die Stadt des DNS-Resolvers, der die Anfrage bearbeitet hat. Die Stadt des Resolvers wird hinzugefügt, indem eine Resolver-IP-Adresse gesucht wird.IDs können Namen unter https://community-radar.citrix.com/ref/cities.json.gz
Auflösungsvorabschuss-ASN	Die Autonomous System Number (ASN) des DNS-Resolvers, der die Anforderung bearbeitet hat. Im Allgemeinen kann die ASN mit den DNS-Resolver-IDs Namen zugeordnet werden https://community-radar.citrix.com/ref/asns.json.gz
Resolver-IP	Die IP-Adresse des DNS-Resolvers, von dem unsere Infrastruktur die DNS-Anfrage erhalten hat.
Kunden-Markt	Der Markt des Endverbrauchers, der diese Messung generiert hat. Im Allgemeinen der Kontinent, auf dem sich die Client-IP befindet; wobei 0: Unbekannt (XX), 1: Nordamerika (NA) 5: Afrika (AF), 3: Europa (EU), 4: Asien (AS), 2: Ozeanien (OC), 6: Südamerika (SA).
Land des Kunden	Das Land des Endbenutzers, der diese Messung generiert hat.IDs können Namen unter https://community-radar.citrix.com/ref/countries.json.gz
Region des Kunden	Die Region des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die geografische Region, in der die Client-IP ist. IDs können unter https://community-radar.citrix.com/ref/regions.json.gz Namen zugeordnet werden. Hinweis: Nicht alle Länder der Welt haben definierte Regionen zugeordnet.

Protokoll	Beschreibung
Client-Status	Der Status des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen der Bundesstaat, in dem die Client-IP ist. IDs können unter https://community-radar.citrix.com/ref/states.json.gz Namen zugeordnet werden. Hinweis, nicht alle Länder der Welt definierte Staaten haben.
Kunden-Stadt	Die Stadt des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die Stadt, in der sich die Client-IP befindet.IDs können Namen unter https://community-radar.citrix.com/ref/cities.json.gz
Kunden-ASN	Die Autonomous System Number (ASN) des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen kann die ASN, die die Client-IP.IDs enthält, Namen unter https://community-radar.citrix.com/ref/asns.json.gz
Client-IP	Die IP des Endbenutzers, der diese Messung generiert hat.
Referrer-Host MD5	Die Referer-Informationen (Protokoll, Host und Pfad) stammen aus dem Referer-Header der HTTP-Anforderung an Radar. Der Referer-Host ist MD5-Hash.
Benutzeragent	Es ist die Benutzer-Agent-Zeichenfolge von der Browserseite, die das Tag hostet. Wenn Sie beispielsweise Chrome verwenden und eine Seite mit dem Radar-Tag durchsuchen, zeichnet die Radarmessung im Hintergrund den Benutzeragenten in Ihrem Chrome-Browser auf. Die Messungen umfassen den Chrome-Browser, die Version von Chrome, Informationen über das Betriebssystem, auf dem Chrome ausgeführt wird, und so weiter.

Protokoll	Beschreibung
DNS-Nachschlagefunkt (optional)	Mit der Resource Timing API wird die Differenz zwischen dem Ende der Domänensuche und dem Start der Domänensuche berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Sie wird als domainLookupEnd - domainLookupStart berechnet.
TCP-Verbindungszeit (optional)	Mit der Resource Timing API wird der Unterschied zwischen dem Connect End und Connect Start berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Es wird als connectEnd - connectStart berechnet.
Sichere Verbindungszeit (optional)	Mit der Resource Timing API wird der Unterschied zwischen dem Connect End und Secure Connection Start berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Sie wird als connectEnd - secureConnectionStart berechnet.
Latenz (optional)	Mit der Resource Timing API wird die Differenz zwischen dem Start der Antwort und dem Start der Anfrage berechnet. Es wird berechnet, wenn beide Werte nicht Null sind und die Startzeit der Antwort größer als die Startzeit der Anforderung ist. Es wird als responseStart - requestStart berechnet
Downloadzeit (optional)	Mit der Resource Timing API wird die Differenz zwischen dem Ende der Antwort und dem Start der Antwort berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Sie wird als responseEnd - responseStart berechnet.

Protokoll	Beschreibung
Kundenprofil	Dieses Feld hilft bei der Identifizierung, ob die Daten von mobilen Apps oder Browsern stammen. Es ermöglicht uns auch, zwischen iOS, Android Apps und Browsern zu unterscheiden. Eine Zahl wird verwendet, um jedes Kundenprofil zu identifizieren. Die Werte für dieses Feld sind: null, 0, 1, 2, 3, 4. Wo, null: Impliziert im Allgemeinen einen älteren Radar-Client, der das Senden des client_profile-Werts nicht unterstützt. 0: Browser; 1: iOS - Radarläufer für iOS-App in Swift geschrieben; 2: Android; 3: Browser auf mobiler Version der Website; 4: iOS - Radar Runner für iOS-App in Objective-C geschrieben.
Version des Kundenprofils	Die Version des Client-Profils gibt an, welche Version des Radar Runner-Codes (für iOS) oder AndroidRadar SDK (für Android) in der mobilen App verwendet wurde. Dieses Feld ist nur für den internen Gebrauch bestimmt.
Geräte-Kategorie	Alle Geräte sind in eines der folgenden Kategorien unterteilt: Smartphone, Tablet, PC, Smart TV und Andere. ‘Andere’wird als Standardwert verwendet, wenn der Parser den Wert für keines der Felder ermitteln kann.
Gerät	Der Typ des Geräts, auf dem sich der Benutzer befindet, z. B. ein Apple iPhone. Die Benutzer-Agent-Zeichenfolge erkennt sie im Browser, der auf der Seite ausgeführt wird, auf der das Radar-Tag gehostet wird.
Browser	Der Typ des Browsers, den der Benutzer verwendet, z. B. Mobile Safari UI/WKWebView 0.0.0. Die Benutzer-Agent-Zeichenfolge erkennt sie im Browser, der auf der Seite ausgeführt wird, auf der das Radar-Tag gehostet wird.

Protokoll	Beschreibung
Betriebssystem	Das verwendete Betriebssystem. Zum Beispiel iOS 11.0.3. Die Zeichenfolge des Benutzeragenten erkennt sie vom Browser, der auf der Seite ausgeführt wird, auf der das Radar-Tag gehostet wird.
Berichts-Kunden-IP	Diese IP ist die maskierte /48 öffentliche IP des Benutzers, der die Messung durchführt. Es kann entweder IPv4 oder IPv6 sein (sofern unterstützt).

Anonymer Bester Bericht

- Anonyme Best Reports helfen Anbietern dabei, ihre Leistung mit der Peer-Group der anderen Plattform zu vergleichen, die sich innerhalb desselben Landes, derselben Region oder ASN befindet.
- Die Leistungsdaten der 15 wichtigsten Anbieter in der Peer-Group werden auf der Grundlage derselben Kategorien aggregiert. Der beste Wert wird neben dem besten Wert des jeweiligen Anbieters aufgeführt.
- Anonymer Best Report für SSL-Plattformen ist verfügbar, so dass ihre Leistung mit anderen SSL-Plattformen verglichen werden kann.
- Die Client-IPs werden auf /28 gekürzt.
- Die Ergebnisse des “besten”Anbieters helfen Clouds/CDNs dabei, ihre Leistung auf hochvolumige oder geschäftskritische ASNs zu konzentrieren, die für ihre Mitbewerber wettbewerbsschwach sind.
- Der Bericht enthält Details zur Leistung, die aus DNS-Resolver-IP, Client IP /28 und dem Caching-Knoten besteht, der die Objekte bedient hat. Es wird mit der “besten”Plattform für dieselben Kriterien verglichen.
- Verfügbar für RTT oder Durchsatz.
- Das Folgende ist ein Beispiel für einen Platform Anonymous Best Report für RTT im TSV-Dateiformat.

Protokollbeschreibungen Im Folgenden sind die Spaltenüberschriften und Beschreibungen für den anonymen besten Bericht aufgeführt. Die Felder werden in der folgenden Reihenfolge in den Ausgabedateien angezeigt.

Protokoll	Beschreibung
Resolver Land	Das Land des DNS-Resolvers, der die Anfrage bearbeitet hat.
Region “Resolver”	Die Region des DNS-Resolvers, die die Anforderung bearbeitet hat.
Auflösungsstatus	Der Status des DNS-Resolvers, der die Anforderung bearbeitet hat.
ASN-ID des Resolvers	Die Autonome Systemnummer des DNS-Resolvers, der die Anforderung verarbeitet hat. Im Allgemeinen die ASN, die über den DNS-Resolver verfügt.
Name der Resolver-ASN	Der Name der ASN.
Resolver-IP	Die IP-Adresse des DNS-Resolvers, von dem unsere Infrastruktur die DNS-Anfrage erhalten hat.
Land des Kunden	Das Land des Endbenutzers, der diese Messung generiert hat.
Region des Kunden	Die Region des Endbenutzers, der diese Messung generiert hat.
Client-Status	Der Status des Endbenutzers, der diese Messung generiert hat.
ASN-ID des Kunden	Die ASN-Nummer (Autonomous System Number) des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die ASN, die die Client-IP hat.
Name der Client-ASN	Der Name der ASN des Endbenutzers, der die Messung generiert hat.
Client-IP	Die IP des Endbenutzers, der die Messung generiert hat.
Erfolge	Gesamtzahl der Messungen, die erfolgreich waren.Tipp: Erfolg/Total == Verfügbarkeit.
Timeouts	Die Anzahl der Messungen, bei denen das Zeitlimit überschritten wurde.
Errors	Die Anzahl der Messungen, die Fehler waren.
Gesamt	Die Gesamtzahl der Messungen.
Mean	Der Durchschnitt aller Messwerte für diese Zeile.

Protokoll	Beschreibung
Bester Mittelwert	Der beste Mittelwert unter den 15 besten Anbietern in der Peer-Group.
Beste Mittelwertmessungen	Gesamtzahl der Messungen, die den besten Mittelwert ergaben.
Median	Der 50. Perzentilwert ist der mittlere Wert der Messungen für einen bestimmten Anbieter, wenn die Messungen in der Reihenfolge aufgeführt sind.
Bester Median	Der beste 50. Perzentilwert (unter dem 50 Prozent der Messungen zu finden sind) der 15 besten Anbieter in der Peer-Group.
Beste Medianmessungen	Gesamtzahl der Messungen, die den best_median ergaben
5th	Der 5. Perzentilwert für den Anbieter.
Beste 5.	Der beste Wert des 5. Perzentils unter den 15 besten Anbietern in der Vergleichsgruppe.
Beste 5. Messungen	Gesamtzahl der Messungen für best_5th
10th	Der 10. Perzentilwert für den Anbieter.
Beste 10.	Der beste Wert des 10. Perzentils unter den 15 besten Anbietern in der Vergleichsgruppe.
Beste 10. Messungen	Gesamtzahl der Messungen für best_10th
90th	Der 90. Perzentilwert für den Anbieter.
Beste 90.	Der beste Wert des 90. Perzentils unter den 15 besten Anbietern in der Vergleichsgruppe.
Beste 90. Messungen	Gesamtzahl der Messungen für best_90th
95th	Der 95. Perzentilwert für den Anbieter.
Beste 95.	Der beste Wert des 95. Perzentils unter den 15 besten Anbietern in der Vergleichsgruppe.
Beste 95. Messungen	Gesamtzahl der Messungen für best_95.
Stev	Die Standardabweichung für den Anbieter
Best Stdev	Die beste Standardabweichung unter den 15 besten Anbietern in der Vergleichsgruppe.
Best Stdev Measurements	Gesamtzahl der Messungen für best std.dev.

Protokoll	Beschreibung
Verfügbarkeit	Die prozentuale Verfügbarkeit für den Anbieter. Verfügbarkeit ist die Erfolgsrate der Probe, d.h. Erfolge/(Erfolge + Fehlschläge + Timeouts)
Beste Verfügbarkeit	Der beste Verfügbarkeitswert unter den 15 besten Anbietern in der Peer-Group.
Messungen der besten Verfügbarkeit	Die Anzahl der Messungen, die die beste Verfügbarkeit ergaben
Wichtigkeit	Synthetische Werte werden generiert, um verwertbare Daten zu finden.
Eindeutige Knoten-IDs	Diese IDs sind eine durch Kommas getrennte Liste der eindeutigen Knoten-IDs für die Messungen dieser Zeile.
Messungstyp	Der aufgezeichnete Messwert, dessen Bedeutung je nach Sondentyp variiert. Es ist HTTP_COLD (Verfügbarkeit), HTTP_RTT (Roundtrip-Zeit) oder HTTP_KBPS (Durchsatz).
Anbieter-ID	Die interne NetScaler ITM-ID-Nummer für diesen Anbieter.

Cache-Knoten-ID-Bericht (zuvor Multi-Service Provider-Bericht)

Dieser Bericht wird verwendet, um den spezifischen Server oder das Datencenter zu identifizieren, das auf eine Anfrage reagiert hat, und hilft bei der Diagnose von Serverproblemen.

- Es liefert die ID des Rechenzentrums oder der Maschine, die auf eine bestimmte Anfrage geantwortet hat.
- Es hilft zu verstehen, warum die Leistung über einen bestimmten Knoten (POP oder Maschine oder Knoten-ID) gut oder schlecht war.
- Die Leistung besteht aus Reaktionszeit, Durchsatz, Verfügbarkeit (Probentyp), der DNS-Resolver-IP, Client IP /28 und dem Caching-Knoten, der die Objekte bedient hat.
- Das Folgende ist ein Beispiel für einen Plattform-Cache-Knoten-ID-Bericht im TSV-Dateiformat.

Protokollbeschreibungen Im Folgenden sind die Spaltenüberschriften und Beschreibungen für den Cache-Knoten-ID-Bericht aufgeführt. Die Felder werden in der folgenden Reihenfolge in den Ausgabedateien angezeigt:

Protokoll	Beschreibung
Name des Anbieters	Es ist der Name des Anbieters, der gemessen wird.
Messwert	Der aufgezeichnete Messwert, dessen Bedeutung je nach Sondentyp variiert. Es sind connect (1) /RTT (0) -Messungen in Millisekunden und Durchsatzmessungen (14) in Kbit/s.
Eindeutige Knoten-ID	Es ist als Cache-Knoten-ID bekannt. Ein beliebiger Wert, typischerweise eine IP, die CDN Edge-Server zurückgeben, um CDNs dabei zu helfen, intern zu identifizieren, welcher Server eine bestimmte Anfrage bearbeitet hat. (leere Zeichenfolge): Stammt von Radar-Clients, die die UNI-Erkennung nicht unterstützen.0: Der Benutzeragent unterstützt die für die UNI-Erkennung erforderlichen Funktionen nicht.1: Der Client findet während der UNI-Erkennung einen Fehler, z. B. eine HTTP 404 oder eine andere erfolglose Antwort.2: Es wurde versucht, eine UNI-Erkennung durchzuführen, führte jedoch zu einem Fehler.
Resolver Land	Das Land des DNS-Resolvers, der die Anfrage bearbeitet hat.
Region “Resolver”	Die Region des DNS-Resolvers, die die Anforderung bearbeitet hat.
Auflösungsstatus	Der Status des DNS-Resolvers, der die Anforderung bearbeitet hat.
Auflösungsvorabschuss-ASN	Die Autonome Systemnummer des DNS-Resolvers, der die Anforderung verarbeitet hat. Im Allgemeinen die ASN, die über den DNS-Resolver verfügt.
Name der Resolver-ASN	Der Name der ASN.
Resolver-IP	Die IP-Adresse des DNS-Resolvers, von dem unsere Infrastruktur die DNS-Anfrage erhalten hat.
Land des Kunden	Das Land des Endbenutzers, der diese Messung generiert hat.

Protokoll	Beschreibung
Region des Kunden	Die Region des Endbenutzers, der diese Messung generiert hat.
Client-Status	Der Status des Endbenutzers, der diese Messung generiert hat.
Kunden-ASN	Die ASN-Nummer (Autonomous System Number) des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die ASN, die die Client-IP hat.
Name der Client-ASN	Der Name der ASN des Endbenutzers, der die Messung generiert hat.
Client-IP	Die IP des Endbenutzers, der die Messung generiert hat.
Erfolg	Gesamtzahl der Messungen, die erfolgreich waren.Tipp: Erfolg/Total == Verfügbarkeit.
Timeout	Die Anzahl der Messungen, bei denen das Zeitlimit überschritten wurde.
Fehler	Die Anzahl der Messungen, die Fehler waren.
Gesamt	Die Gesamtzahl der Messungen.
Mean	Der Durchschnitt der Messwerte für jede Zeile.
Median	Der 50. Perzentilwert ist der mittlere Wert der Messungen für einen bestimmten Anbieter, wenn die Messungen in der Reihenfolge aufgeführt sind.
5th	Der 5. Perzentilwert für den Anbieter.
10th	Der 10. Perzentilwert für den Anbieter.
90th	Der 90. Perzentilwert für den Anbieter.
95th	Der 95. Perzentilwert für den Anbieter.
Stev	Die Standardabweichung für den Anbieter.
Verfügbarkeit	Die prozentuale Verfügbarkeit für den Anbieter.
Wichtigkeit	Synthetische Werte werden generiert, um verwertbare Daten zu finden.

Stündlich nach Land/ASN-Bericht

- Mit diesem Bericht können Sie überprüfen, ob die Leistung Ihrer Anbieter im Laufe eines Tages erheblich variiert.
- Es zeigt die Zeit, zu der die Messungen auf die Stunde abgeschnitten wurden, zum Beispiel `2018-03-11T23:00:00`.
- Das Folgende ist ein Beispiel für einen Plattform-Hourly by Country/ASN-Bericht im TSV-Dateiformat.

Protokollbeschreibungen Im Folgenden finden Sie die Spaltenüberschriften und Beschreibungen für den Bericht "Stündlich nach Land/ASN". Die Felder werden in der folgenden Reihenfolge in den Ausgabedateien angezeigt:

Protokoll	Beschreibung
Zeitstempel 60 Minuten	Die UTC-Zeit, zu der die Messungen durchgeführt wurden, wurde auf die Stunde verkürzt, zum Beispiel 2018-03-11T 23:00:00.
Name des Anbieters	Es ist der Name des Anbieters, der gemessen wird.
Messungstyp	Der aufgezeichnete Messwert, dessen Bedeutung je nach Sondentyp variiert. Es ist HTTP_COLD (Verfügbarkeit), HTTP_RTT (Roundtrip-Zeit) oder HTTP_KBPS (Durchsatz).
Land des Kunden	Das Land des Endbenutzers, der diese Messung generiert hat.
Kunden-ASN	Die ASN-Nummer (Autonomous System Number) des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die ASN, die die Client-IP hat.
Name der Client-ASN	Der Name der ASN des Endbenutzers, der die Messung generiert hat.
Erfolg	Gesamtzahl der Messungen, die erfolgreich waren.Tipp: Erfolg/Total == Verfügbarkeit.
Timeout	Die Anzahl der Messungen, bei denen das Zeitlimit überschritten wurde.
Fehler	Die Anzahl der Messungen, die Fehler waren.
Gesamt	Die Gesamtzahl der Messungen.
Mean	Der Durchschnitt der Messwerte für jede Zeile.

Protokoll	Beschreibung
Median	Der 50. Perzentilwert ist der mittlere Wert der Messungen für einen bestimmten Anbieter, wenn die Messungen in der Reihenfolge aufgeführt sind.
5th	Der 5. Perzentilwert für den Anbieter.
10th	Der 10. Perzentilwert für den Anbieter.
90th	Der 90. Perzentilwert für den Anbieter.
95th	Der 95. Perzentilwert für den Anbieter.
Stev	Die Standardabweichung für den Anbieter.
Verfügbarkeit	Die prozentuale Verfügbarkeit für den Anbieter.
Wichtigkeit	Synthetischer Wert wird generiert, um verwertbare Daten zu finden.
Anbieter-ID	Die interne NetScaler ITM-ID-Nummer für diesen Anbieter.

Radarprotokollbeschreibungen und Berichte für ISPs

Radarprotokolle für ISPs

Radarprotokolle ermöglichen es ISPs, ihre Leistung anhand globaler Plattformen im Detail zu messen. ISPs können diese Daten verwenden, um Bereiche zu finden, in denen Verbesserungen vorgenommen werden müssen, oder um die erwartete Leistung zu überprüfen.

- Bietet Zugriff auf Radarmessungen.
- Stellt Messungen von ISPs auf öffentlichen Plattformen bereit, unabhängig von der Seite, auf der die Messung generiert wurde.
- Radarprotokolle enthalten eine Teilmenge der in den Rohprotokollen verfügbaren Felder, wobei einige Daten anonymisiert sind: Client IP /28, Referer MD5 gehasht.
- Die Protokolldateien sind im TSV-Format.
- Das Folgende ist ein Beispiel für eine Network Radar Log Share im TSV-Dateiformat.

Protokollbeschreibungen Im Folgenden finden Sie die Spaltenüberschriften und Beschreibungen für die Radarprotokolle für ISPs. Die Felder werden in der folgenden Reihenfolge in den Ausgabedateien angezeigt.

Protokoll	Beschreibung
Zeitstempel	Es ist die UTC-Zeit der Anfrage im Format YYYY-MM-DDTHH: MI: SSZ. Der tatsächliche Wert (auf die Sekunde herunter) in den Protokolltabellen wird auf die nächste Stunde (2018-03-30T23:00:00Z) bzw. den nächsten Tag (2018-03-30T00:00:00Z) in den Stunden-/Tag-Tabellen gerundet. Der Zeitstempel ist in allen Datensätzen immer in UTC angegeben.
Anbieter-ID	Interne ID der Plattform, die gemessen wird.
Sonden-Typ	Der Prüfpunkttyp, der gemessen wird (z. B. 1: HTTP-Verbindungszeit, 0: HTTP-Antwortzeit, 14: HTTP-Durchsatz usw.). Die Informationen, die innerhalb der zulässigen Zeit erfolgreich zurückgegeben wurden, werden verwendet, um anzuzeigen, dass der Dienst verfügbar ist.
Antwortcode	Ergebnis der Messung, z. B. 0: Erfolg, 1: Timeout, 4: Fehler. Für Verfügbarkeitsberechnungen wird der Prozentsatz der Messungen mit einer Antwort von 0 (Erfolg) im Vergleich zur Gesamtzahl der Messungen (gesamt) ermittelt. Bei anderen Sondentypen (RTT und Durchsatz) darf der Filter bei der Berechnung von Statistiken im RTT nur RTT-Datenpunkte mit einem Erfolgscode von 0 berücksichtigen. Gleiches für den Durchsatz.
Messwert	Der aufgezeichnete Messwert, dessen Bedeutung je nach Sondentyp variiert. Es sind Verfügbarkeits- (1) /Reaktionszeit (0) -Messungen in Millisekunden und Durchsatz (14) in KBit/s.
Resolver-Markt	Der Markt des DNS-Resolvers, der die Anfrage bearbeitet hat. Im Allgemeinen der Kontinent, auf dem sich der DNS-Resolver befindet, wo, 0: Unbekannt (XX), 1: Nordamerika (NA) 5: Afrika (AF), 3: Europa (EU), 4: Asien (AS), 2: Ozeanien (OC), 6: Südamerika (SA).

Protokoll	Beschreibung
Resolver Land	Das Land des DNS-Resolvers, der die Anforderungs-IDs bearbeitet hat, kann Namen zugeordnet werden unter https://community-radar.citrix.com/ref/countries.json.gz
Region "Resolver"	Die Region des DNS-Resolvers, die die Anforderungs-IDs bearbeitet hat, kann Namen unter zugeordnet werden https://community-radar.citrix.com/ref/regions.json.gz. Nicht alle Länder der Welt haben definierte Regionen.
Auflösungsstatus	Der Status des DNS-Resolvers, der die Anforderungs-IDs verarbeitet hat, kann Namen unter zugeordnet werden https://community-radar.citrix.com/ref/states.json.gz. Nicht alle Länder der Welt haben definierte Staaten.
Auflösungsvorabschuss-ASN	Die Autonomous System Number (ASN) des DNS-Resolvers, der die Anforderung bearbeitet hat. Im Allgemeinen kann die ASN mit den DNS-Resolver-IDs Namen unter zugeordnet werden https://community-radar.citrix.com/ref/asns.json.gz.
Resolver-IP	Die IP-Adresse des DNS-Resolvers, von dem unsere Infrastruktur die DNS-Anfrage erhalten hat.
Kunden-Markt	Der Markt des Endverbrauchers, der diese Messung generiert hat. Im Allgemeinen der Kontinent, auf dem sich die Client-IP befindet; wobei 0: Unbekannt (XX), 1: Nordamerika (NA) 5: Afrika (AF), 3: Europa (EU), 4: Asien (AS), 2: Ozeanien (OC), 6: Südamerika (SA).
Land des Kunden	Das Land des Endbenutzers, der diese Messung generiert hat.IDs können Namen unter https://community-radar.citrix.com/ref/countries.json.gz

Protokoll	Beschreibung
Region des Kunden	Die Region des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die geografische Region, in der sich die Client-IP befindet. IDs können unter https://community-radar.citrix.com/ref/regions.json.gz Namen zugeordnet werden. Nicht alle Länder der Welt haben definierte Regionen.
Client-Status	Der Status des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen der Staat, in dem sich die Client-IP befindet. IDs können unter https://community-radar.citrix.com/ref/states.json.gz Namen zugeordnet werden. Nicht alle Länder der Welt haben definierte Staaten.
Kunden-ASN	Die Autonomous System Number (ASN) des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die ASN, die die Client-IP hat. IDs können unter https://community-radar.citrix.com/ref/asns.json.gz Namen zugeordnet werden.
Client-IP	Die IP des Endbenutzers, der diese Messung generiert hat.
Referrer-Host MD5	Die Referer-Informationen (Protokoll, Host und Pfad) stammen aus dem Referer-Header der HTTP-Anforderung an Radar. Der Referer-Host ist MD5-Hash.
Benutzeragent	Es ist die Benutzer-Agent-Zeichenfolge von der Browserseite, die das Tag hostet. Wenn Sie beispielsweise Chrome verwenden und eine Seite mit dem Radar-Tag durchsuchen, zeichnet die Radarmessung im Hintergrund den Benutzeragenten in Ihrem Chrome-Browser auf. Die Messungen umfassen den Chrome-Browser, die Version von Chrome, Informationen über das Betriebssystem, auf dem Chrome ausgeführt wird, und so weiter.

Protokoll	Beschreibung
DNS-Nachschlagefunkt (optional)	Mit der Resource Timing API wird die Differenz zwischen dem Ende der Domänensuche und dem Start der Domänensuche berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Sie wird als domainLookupEnd - domainLookupStart berechnet.
TCP-Verbindungszeit (optional)	Mit der Resource Timing API wird der Unterschied zwischen dem Connect End und Connect Start berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Es wird als connectEnd - connectStart berechnet.
Sichere Verbindungszeit (optional)	Mit der Resource Timing API wird der Unterschied zwischen dem Connect End und dem Secure Connection Start berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Sie wird als connectEnd - secureConnectionStart berechnet.
Latenz (optional)	Mit der Resource Timing API wird die Differenz zwischen dem Start der Antwort und dem Start der Anfrage berechnet. Es wird berechnet, wenn beide Werte nicht Null sind und die Startzeit der Antwort größer als die Startzeit der Anforderung ist. Es wird als responseStart - requestStart berechnet
Downloadzeit (optional)	Mit der Resource Timing API wird die Differenz zwischen dem Ende der Antwort und dem Start der Antwort berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Sie wird als responseEnd - responseStart berechnet.

Protokoll	Beschreibung
Kundenprofil	Dieses Feld hilft bei der Identifizierung, ob die Daten von mobilen Apps oder Browsern stammen. Es ermöglicht uns auch, zwischen iOS, Android Apps und Browsern zu unterscheiden. Eine Zahl wird verwendet, um jedes Kundenprofil zu identifizieren. Die Werte für dieses Feld sind: null, 0, 1, 2, 3, 4. Wo, null: Impliziert im Allgemeinen einen älteren Radar-Client, der das Senden des client_profile-Werts nicht unterstützt. 0: Browser; 1: iOS - Radarläufer für iOS-App in Swift geschrieben; 2: Android; 3: Browser auf mobiler Version der Website; 4: iOS - Radar Runner für iOS-App in Objective-C geschrieben.
Version des Kundenprofils	Die Version des Client-Profils gibt an, welche Version des Radar Runner-Codes (für iOS) oder AndroidRadar SDK (für Android) in der mobilen App verwendet wurde. Dieses Feld ist nur für den internen Gebrauch bestimmt.
Geräte-Kategorie	Alle Geräte sind in eines der folgenden Kategorien unterteilt: Smartphone, Tablet, PC, Smart TV und Andere. ‘Andere’wird als Standardwert verwendet, wenn der Parser den Wert für keines der Felder ermitteln kann.
Gerät	Der Typ des Geräts, auf dem sich der Benutzer befindet, z. B. ein Apple iPhone. Die Benutzer-Agent-Zeichenfolge erkennt sie im Browser, der auf der Seite ausgeführt wird, auf der das Radar-Tag gehostet wird.
Browser	Der Typ des Browsers, den der Benutzer verwendet, z. B. Mobile Safari UI/WKWebView 0.0.0. Die Benutzer-Agent-Zeichenfolge erkennt sie im Browser, der auf der Seite ausgeführt wird, auf der das Radar-Tag gehostet wird.

Protokoll	Beschreibung
Betriebssystem	Das verwendete Betriebssystem, z. B. iOS 11.0.3. Die Benutzer-Agent-Zeichenfolge erkennt sie im Browser, der auf der Seite ausgeführt wird, auf der das Radar-Tag gehostet wird.

Subnetzbericht für ISPs

- Der Bericht liefert ISPs Informationen darüber, wie sich die spezifischen Subnetze ihrer Netzwerke für ihre Benutzer über die gemessenen Plattformen verhalten.
- Es enthält Informationen über den Dienstanbieter, der auf eine bestimmte Anforderung geantwortet hat.
- Es hilft, die Leistung des Netzwerksubnetzes zu verstehen.
- Die Leistung besteht aus Reaktionszeit, Durchsatz, Verfügbarkeit (Probentyp), der DNS-Resolver-IP, Client IP /28 und dem Caching-Knoten, der die Objekte bedient hat.
- Das Folgende ist ein Beispiel für einen Netzwerk-Subnetzbericht im TSV-Dateiformat.

Protokollbeschreibungen Im Folgenden finden Sie die Spaltenüberschriften und Beschreibungen für den Subnetzbericht für ISPs. Die Felder werden in der folgenden Reihenfolge in den Ausgabedateien angezeigt:

Protokoll	Beschreibung
ASN Name	Der Name des autonomen Systems, von dem aus die Messung durchgeführt wurde.
Messwert	Der aufgezeichnete Messwert, dessen Bedeutung je nach Sondentyp variiert. Es sind connect (1) /RTT (0) -Messungen in Millisekunden und Durchsatzmessungen (14) in Kbit/s.
Subnetz	Das Subnetz des Benutzers, von dem die Anfrage stammt.
Auflösungsvorabschuss-ASN	Die Autonome Systemnummer des DNS-Resolvers, der die Anforderung verarbeitet hat. Im Allgemeinen die ASN, die über den DNS-Resolver verfügt.
Resolver-IP	Die IP-Adresse des DNS-Resolvers, von dem unsere Infrastruktur die DNS-Anfrage erhalten hat.

Protokoll	Beschreibung
Kunden-ASN	Die ASN-Nummer (Autonomous System Number) des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die ASN, die die Client-IP hat.
Client-IP	Die IP des Endbenutzers, der die Messung generiert hat.
Plattform-ID	Die ID der Service Provider-Plattform, an der die Abfrage durchgeführt wurde.
Plattformname	Der Name der Service Provider-Plattform, an der die Abfrage durchgeführt wurde
Erfolg	Gesamtzahl der Messungen, die erfolgreich waren.Tipp: Erfolg/Total == Verfügbarkeit.
Timeout	Die Anzahl der Messungen, bei denen das Zeitlimit überschritten wurde.
Fehler	Die Anzahl der Messungen, die Fehler waren.
Gesamt	Die Gesamtzahl der Messungen.
Mean	Der Durchschnitt der Messwerte für jede Zeile.
Median	Der 50. Perzentilwert ist der mittlere Wert der Messungen für einen bestimmten Anbieter, wenn die Messungen in der Reihenfolge aufgeführt sind.
5th	Der 5. Perzentilwert für den Anbieter.
10th	Der 10. Perzentilwert für den Anbieter.
90th	Der 90. Perzentilwert für den Anbieter.
95th	Der 95. Perzentilwert für den Anbieter.
Stev	Die Standardabweichung für den Anbieter.
Verfügbarkeit	Die prozentuale Verfügbarkeit für den Anbieter.
Wichtigkeit	Synthetische Werte werden generiert, um verwertbare Daten zu finden.
Messungstyp	Der aufgezeichnete Messwert, dessen Bedeutung je nach Sondentyp variiert. Es ist HTTP_COLD (Verfügbarkeit), HTTP_RTT (Roundtrip-Zeit) oder HTTP_KBPS (Durchsatz).

Anonymer Bester Bericht für ISPs

- Im Bericht Anonymous Best wird eine Peer-Group für den "besten"Vergleich verwendet. Die Peer-Gruppe basiert auf dem Standort des ISP. Normalerweise sind es die 10 am häufigsten gemessenen ISPs in einem bestimmten Land mit einem Minimum von über 1.000 Sitzungen.
- Die Ergebnisse des "besten"ISP helfen ISPs dabei, ihre Leistungsbemühungen auf großvolumige oder geschäftskritische Plattformen und Bereiche zu konzentrieren, die im Vergleich zu ihren Mitbewerbern wettbewerbsschwach sind.
- Der Bericht enthält Details zur Leistung, aufgeschlüsselt nach Geographie und Plattform, und vergleicht sie mit dem "besten"ISP für dieselben Kriterien.
- Verfügbar für RTT und Durchsatz.
- Das Folgende ist ein Beispiel für Network Anonymous Best Report für RTT im TSV-Dateiformat.

Protokollbeschreibungen Im Folgenden sind die Spaltenüberschriften und Beschreibungen für den anonymen besten Bericht aufgeführt. Die Felder werden in der folgenden Reihenfolge in den Ausgabedateien angezeigt.

Protokoll	Beschreibung
Messungstyp	Der aufgezeichnete Messwert, dessen Bedeutung je nach Sondentyp variiert. Es ist HTTP_COLD (Verfügbarkeit), HTTP_RTT (Roundtrip-Zeit) oder HTTP_KBPS (Durchsatz).
Land des Kunden	Das Land des Endbenutzers, der diese Messung generiert hat.
Region des Kunden	Die Region des Endbenutzers, der diese Messung generiert hat.
Client-Status	Der Status des Endbenutzers, der diese Messung generiert hat.
ASN-ID des Kunden	Die ASN-Nummer (Autonomous System Number) des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die ASN, die die Client-IP hat.
Name der Client-ASN	Der Name der ASN des Endbenutzers, der die Messung generiert hat.
Resolver Land	Das Land des DNS-Resolvers, der die Anfrage bearbeitet hat.
Region "Resolver"	Die Region des DNS-Resolvers, die die Anforderung bearbeitet hat.

Protokoll	Beschreibung
Auflösungsstatus	Der Status des DNS-Resolvers, der die Anforderung bearbeitet hat.
Plattform-ID	Die ID der Service Provider-Plattform, an die die Abfrage versucht wurde.
Plattformname	Der Name der Service Provider-Plattform, an die die Abfrage versucht wurde.
Erfolge	Gesamtzahl der Messungen, die erfolgreich waren.Tipp: Erfolg/Total == Verfügbarkeit.
Timeouts	Die Anzahl der Messungen, bei denen das Zeitlimit überschritten wurde.
Errors	Die Anzahl der Messungen, die Fehler waren.
Gesamt	Die Gesamtzahl der Messungen.
Mean	Der Durchschnitt aller Messwerte für diese Zeile.
Bester Mittelwert	Der beste Mittelwert unter den 15 besten Anbietern in der Peer-Group.
Beste Mittelwertmessungen	Gesamtzahl der Messungen, die den besten Mittelwert ergaben.
Median	Der 50. Perzentilwert ist der mittlere Wert der Messungen für einen bestimmten Anbieter, wenn die Messungen in der Reihenfolge aufgeführt sind.
Bester Median	Der beste 50. Perzentilwert (unter dem 50 Prozent der Messungen zu finden sind) der 15 besten Anbieter in der Peer-Group.
Beste Medianmessungen	Gesamtzahl der Messungen, die den best_median ergaben
5th	Der 5. Perzentilwert für den Anbieter.
Beste 5.	Der beste Wert des 5. Perzentils unter den 15 besten Anbietern in der Vergleichsgruppe.
Beste 5. Messungen	Gesamtzahl der Messungen für best_5th
10th	Der 10. Perzentilwert für den Anbieter.
Beste 10.	Der beste Wert des 10. Perzentils unter den 15 besten Anbietern in der Vergleichsgruppe.
Beste 10. Messungen	Gesamtzahl der Messungen für best_10th
90th	Der 90. Perzentilwert für den Anbieter.

Protokoll	Beschreibung
Beste 90.	Der beste Wert des 90. Perzentils unter den 15 besten Anbietern in der Vergleichsgruppe.
Beste 90. Messungen	Gesamtzahl der Messungen für best_90th
95th	Der 95. Perzentilwert für den Anbieter.
Beste 95.	Der beste Wert des 95. Perzentils unter den 15 besten Anbietern in der Vergleichsgruppe.
Beste 95. Messungen	Gesamtzahl der Messungen für best_95.
Stev	Die Standardabweichung für den Anbieter.
Best Stdev	Die beste Standardabweichung unter den 15 besten Anbietern in der Vergleichsgruppe.
Best Stdev Measurements	Gesamtzahl der Messungen für best std.dev.
Verfügbarkeit	Die prozentuale Verfügbarkeit für den Anbieter. Verfügbarkeit ist die Erfolgsrate des Tests, d. h. Erfolge/(Erfolge + Fehlschläge + Timeouts)
Beste Verfügbarkeit	Der beste Verfügbarkeitswert unter den 15 besten Anbietern in der Peer-Group.
Messungen der besten Verfügbarkeit	Die Anzahl der Messungen, die die beste Verfügbarkeit ergaben.
Wichtigkeit	Synthetische Werte werden generiert, um verwertbare Daten zu finden.

Beschreibung des Navigations-Timing-

Navigations-Timing-Daten

Navigation Timing Daten geben Einblicke in die verschiedenen Teile des Seitenladeprozesses für eine Webseite.

Diese Daten variieren aufgrund des Standorts des Endbenutzers, Netzwerkproblemen, Änderungen des Anbieters usw. Kunden können Navigations-Timing-Daten verwenden, um die Erfahrung des Endbenutzers beim Laden der überwachten Webseite zu optimieren.

Messungen können für jede Radarsitzung durchgeführt werden (falls aktiviert). Jede Sitzung ist an eine ID-Nummer angehängt, mit der alle Messungen aus einer Sitzung verfolgt werden können. Diese Messungen werden mit Kunden als Navigation Timing Logs über NEM geteilt.

Das Folgende ist ein Beispiel für die Navigations-Timing-Daten im TSV-Dateiformat.

Im Folgenden sind die Spaltenüberschriften und Beschreibungen für Navigations-Timing-Protokolle aufgeführt. Die Felder werden in der folgenden Reihenfolge in den Ausgabedateien angezeigt:

Protokoll	Beschreibung
Zeitstempel	Es ist die UTC-Zeit der Anfrage im Format YYYY-MM-DDTHH: MI: SSZ. Der tatsächliche Wert (auf die Sekunde herunter) in den Protokolltabellen wird auf die nächste Stunde (2018-03-30T23:00:00Z) bzw. den nächsten Tag (2018-03-30T00:00:00Z) in den Stunden-/Tag-Tabellen gerundet. Es ist in allen Datensätzen immer in UTC.
Antwortcode	Ergebnis der Messung, z. B. 0: Erfolg, 1: Timeout, 4: Fehler. Für Verfügbarkeitsberechnungen wird der Prozentsatz der Messungen mit einer Antwort von 0 (Erfolg) im Vergleich zur Gesamtzahl der Messungen (insgesamt) ermittelt. Bei anderen Sondentypen (RTT und Durchsatz) berücksichtigt der Filter bei der Berechnung von Statistiken im RTT nur RTT-Datenpunkte mit einem Erfolgscode von 0. Gleiches für den Durchsatz.
Resolver-Markt	Der Markt des DNS-Resolvers, der die Anfrage bearbeitet hat. Im Allgemeinen der Kontinent, auf dem sich der DNS-Resolver befindet, wo, 0: Unbekannt (XX), 1: Nordamerika (NA) 5: Afrika (AF), 3: Europa (EU), 4: Asien (AS), 2: Ozeanien (OC), 6: Südamerika (SA).
Resolver Land	Das Land des DNS-Resolvers, der die Anforderung bearbeitet hat. IDs können unter https://community-radar.citrix.com/ref/countries.json.gz Namen zugeordnet werden.
Region "Resolver"	Die Region des DNS-Resolvers, der die Anforderung verarbeitet hat. IDs können unter https://community-radar.citrix.com/ref/regions.json.gz Namen zugeordnet werden. Nicht alle Länder der Welt haben definierte Regionen.

Protokoll	Beschreibung
Auflösungsstatus	Der Status des DNS-Resolvers, der die Anfrage verarbeitet hat. IDs können unter https://community-radar.citrix.com/ref/states.json.gz Namen zugeordnet werden. Nicht alle Länder der Welt haben definierte Staaten.
Auflösungsvorabschuss-ASN	Die Autonomous System Number (ASN) des DNS-Resolvers, der die Anforderung bearbeitet hat. Im Allgemeinen die ASN, die über den DNS-Resolver verfügt. IDs können unter https://community-radar.citrix.com/ref/asns.json.gz Namen zugeordnet werden.
Resolver-IP	Die IP-Adresse des DNS-Resolvers, von dem unsere Infrastruktur die DNS-Anfrage erhalten hat.
Kunden-Markt	Der Markt des Endverbrauchers, der diese Messung generiert hat. Im Allgemeinen der Kontinent, auf dem sich die Client-IP befindet; wobei 0: Unbekannt (XX), 1: Nordamerika (NA) 5: Afrika (AF), 3: Europa (EU), 4: Asien (AS), 2: Ozeanien (OC), 6: Südamerika (SA).
Land des Kunden	Das Land des Endbenutzers, der diese Messung generiert hat.IDs können Namen unter https://community-radar.citrix.com/ref/countries.json.gz
Region des Kunden	Die Region des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die geografische Region, in der sich die Client-IP befindet. IDs können unter https://community-radar.citrix.com/ref/regions.json.gz Namen zugeordnet werden. Nicht alle Länder der Welt haben definierte Regionen.
Client-Status	Der Status des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen der Staat, in dem sich die Client-IP befindet. IDs können unter https://community-radar.citrix.com/ref/states.json.gz Namen zugeordnet werden. Nicht alle Länder der Welt haben definierte Staaten.

Protokoll	Beschreibung
Kunden-ASN	Die Autonomous System Number (ASN) des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die ASN, die die Client-IP hat. IDs können unter https://community-radar.citrix.com/ref/asns.json.gz Namen zugeordnet werden.
Client-IP	Die IP des Endbenutzers, der die Messung generiert hat.
Referrer-Host	Die Referer-Informationen (Protokoll, Host und Pfad) stammen aus dem Referer-Header der HTTP-Anforderung an Radar.
Referrer-Protokoll	Die Referer-Informationen (Protokoll, Host und Pfad) stammen aus dem Referer-Header der HTTP-Anforderung an Radar.
Referrer-Pfad	Die Referer-Informationen (Protokoll, Host und Pfad) stammen aus dem Referer-Header der HTTP-Anforderung an Radar.
Geräte-Kategorie	Alle Geräte sind in eines der folgenden Kategorien unterteilt: Smartphone, Tablet, PC, Smart TV und Andere. ‘Andere’wird als Standardwert verwendet, wenn der Parser den Wert für keines der Felder ermitteln kann.
Gerät	Der Typ des Geräts, auf dem sich der Benutzer befindet, z. B. ein Apple iPhone. Die Benutzer-Agent-Zeichenfolge erkennt sie im Browser, der auf der Seite ausgeführt wird, auf der das Radar-Tag gehostet wird.
Browser	Der Typ des Browsers, den der Benutzer verwendet, z. B. Mobile Safari UI/WKWebView 0.0.0. Die Benutzer-Agent-Zeichenfolge erkennt sie im Browser, der auf der Seite ausgeführt wird, auf der das Radar-Tag gehostet wird.
Betriebssystem	Das verwendete Betriebssystem, z. B. iOS 11.0.3. Die Benutzer-Agent-Zeichenfolge erkennt sie im Browser, der auf der Seite ausgeführt wird, auf der das Radar-Tag gehostet wird.

Protokoll	Beschreibung
DNS-Nachschlagezeit	Mit der Resource Timing API wird die Differenz zwischen dem Ende der Domänensuche und dem Start der Domänensuche berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Sie wird als domainLookupEnd - domainLookupStart berechnet.
TCP-Verbindungszeit	Mit der Resource Timing API wird der Unterschied zwischen dem Connect End und Connect Start berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Es wird als connectEnd - connectStart berechnet.
Sichere Verbindungszeit	Mit der Resource Timing API wird der Unterschied zwischen dem Connect End und dem Secure Connection Start berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Sie wird als connectEnd - secureConnectionStart berechnet.
Load-Ereignis	Dies ist die Dauer oder Zeit, die benötigt wird, um vom Anfang bis zum Ende des Ladeereignisses zu gelangen. Sie wird als LoadEventEnd - LoadEventStart berechnet, wenn beide Werte nicht null sind und die Endzeit größer als die Startzeit ist.
Umleiten	Dies ist die Dauer oder Zeit, die benötigt wird, um vom Navigationsstart zum Abrufen von Start zu gelangen. Sie wird als FetchStart - NavigationStart berechnet, wenn beide Werte nicht null sind und die Endzeit größer als die Startzeit ist.
Gesamte Seitenladezeit	Dies ist die Dauer oder Zeit, die benötigt wird, um vom Beginn der Navigation bis zum Ende des Seitenladevorgangs zu gelangen. Sie wird berechnet als - Ereignisende laden - Navigationsstart, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist.

Protokoll	Beschreibung
DOM	Die Dauer oder Zeit, die vom DOM-Laden zum DOM-Abschluss genommen wird. Sie wird als DomComplete - DomLoading berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist.
Latenz	Mit der Resource Timing API wird die Differenz zwischen dem Start der Antwort und dem Start der Anfrage berechnet. Es wird berechnet, wenn beide Werte nicht Null sind und die Startzeit der Antwort größer als die Startzeit der Anforderung ist. Es wird als responseStart - requestStart berechnet
Download-Zeit	Mit der Resource Timing API wird die Differenz zwischen dem Ende der Antwort und dem Start der Antwort berechnet. Es berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist. Sie wird als responseEnd - responseStart berechnet.
DOM interaktiv	Die Dauer oder Zeit, die für den Wechseln von Navigation Start zu DOM Interactive gebraucht wird. Sie wird als DomInteractive - NavigationStart berechnet, wenn beide Werte nicht null sind und die Endzeit größer als die Startzeit ist.
Rendern starten	Die Dauer oder Zeit, die für das Wechseln von Navigationsstart zum Rendern starten gebraucht wird. Sie wird als startRender - NavigationStart berechnet, wenn beide Werte nicht Null sind und die Endzeit größer als die Startzeit ist.

Openmix und HTTP Openmix Protokolle

Openmix- und HTTP Openmix-Logs ermöglichen es Kunden, Echtzeitmessungen zu verwenden, um das Verhalten ihrer Openmix-Apps zu überwachen. Sie können diese Daten verwenden, um Verbesserungsmöglichkeiten zu finden oder die erwartete Leistung ihrer Apps zu überprüfen.

- Diese Protokolle bieten Echtzeitmessungen für Openmix-Kunden.

- Das empfohlene Dateiformat für diese Protokolle ist JSON, aber sie sind auch im TSV-Format verfügbar.
- Hier sind Beispiele für Openmix - und HTTP Openmix-Log-Sharing-Daten im TSV-Dateiformat.

Openmix Log-Beschreibungen

Protokoll	Beschreibung
Zeitstempel	Es ist die UTC-Zeit der Anfrage im Format YYYY-MM-DDTHH: MI: SSZ. Der tatsächliche Wert (auf die Sekunde herunter) in den Protokolltabellen wird auf die nächste Stunde (2018-03-30T23:00:00Z) bzw. den nächsten Tag (2018-03-30T00:00:00Z) in den Stunden-/Tag-Tabellen gerundet. Der Zeitstempel ist in allen Datensätzen immer in UTC angegeben.
App-Besitzer-Zonen-ID	Die Zonen-ID des Anwendungseigentümers, der die Anforderung bearbeitet. Dieser Wert ist immer gleich 1.
App-Besitzer-Kundennummer	Die Kunden-ID des Anwendungseigentümers, der die Anfrage bearbeitet. Bei HTTP-Anfragen kodieren Sie diese ID im Anforderungspfad und verwenden Sie sie, um nachzuschlagen, welche Anwendung ausgeführt werden soll.
App-ID	Die Anwendungs-ID innerhalb des Kundenkontos, die die Anfrage bearbeitet. Diese ID ist auch im HTTP-Anforderungspfad codiert. Anwendungs-IDs beginnen bei 1 und sind nur für den Kunden eindeutig. Sie müssen Abfragen für eine bestimmte App-ID vollständig qualifizieren, indem Sie die appOwnerCustomerId abfragen.

Protokoll	Beschreibung
App-Version	Die Version der Anwendung, die das Konto bedient hat. Jedes Mal, wenn eine Anwendung über das Portal oder die API aktualisiert wird, wird die Version inkrementiert. Die Version, die zum Zeitpunkt der Anfrage ausgeführt wurde, wird aufgezeichnet. Diese Informationen können verwendet werden, um versionierte Logik im Laufe der Zeit zu trennen, wenn Anwendungen aktualisiert werden. Hosts im gesamten Netzwerk erhalten Updates in der Regel in einem ähnlichen Zeitraum, jedoch fast nie genau zum gleichen Zeitpunkt. Es ist wahrscheinlich, dass sich überlappende Entscheidungen im Laufe der Zeit während des Aktualisierungsprozesses unterschiedliche Versionen einer App verwenden.
App-Name	Der Name der Anwendung, die das Konto bedient hat.
Market	Der Markt des Endverbrauchers, der diese Messung generiert hat.
Land	Das Land des Endbenutzers, der diese Messung generiert hat.
Region	Die Region des Endbenutzers, der diese Messung generiert hat.
Status	Der Status des Endbenutzers, der diese Messung generiert hat.
ASN-ID	Die Autonomous System Number (ASN) des Endbenutzers, der diese Messung generiert hat. Im Allgemeinen die Autonome Systemnummer, die die Client-IP hat.
ASN Name	Der Name der ASN des Endbenutzers, der die Messung generiert hat.

Protokoll	Beschreibung
Effektive IP	Die effektive IP ist die IP, die zur Verarbeitung der Anfrage verwendet wird. Es ist die von der Abfragezeichenfolge angegebene IP, die die anfordernde IP außer Kraft setzt (im Gegensatz zur Resolver/ECS/EDNS-ID für den DNS-Fluss). Es ist die Adresse, die das System bei der Verarbeitung der Informationen als Ziel berücksichtigt. Diese IP ist entweder die IP des anfordernden Resolvers oder die ECS-IP-Adresse des Clients, falls EDNS ECS unterstützt wird. Alle Probe-Performance-Daten, geographische Informationen usw., die an die Anwendungslogik übergeben werden, basieren auf dieser IP.
Resolver-Markt	Der Markt des DNS-Resolvers, der die Anfrage bearbeitet hat.
Resolver Land	Das Land des DNS-Resolvers, der die Anfrage bearbeitet hat.
Region "Resolver"	Die Region des DNS-Resolvers, die die Anforderung bearbeitet hat.
Auflösungsstatus	Der Status des DNS-Resolvers, der die Anforderung bearbeitet hat.
ASN-ID des Resolvers	Die Autonomous System Number (ASN) des DNS-Resolvers, der die Anforderung bearbeitet hat. Im Allgemeinen die Autonome Systemnummer, die über den DNS-Resolver verfügt.
Name der Resolver-ASN	Der Name der ASN des Resolvers, der die Anforderung bearbeitet hat.
Resolver-IP	Die IP-Adresse des DNS-Resolvers, von dem unsere Infrastruktur die DNS-Anfrage erhalten hat.
Name des Entscheidungsanbieters	Alias der Plattform, die eine Anwendung auswählt.
Ursachencode	In der Anwendung festgelegter Ursachencode, der den Grund für die Entscheidung beschreibt.

Protokoll	Beschreibung
Ursache-Protokoll	Dieses Protokoll ist eine vom Kunden definierte Ausgabe der Openmix-App. Es ist ein optionales Zeichenfolgenfeld, mit dem Kunden Informationen über ihre Openmix-App-Entscheidungen protokollieren können.
Fallback-Modus	Dieser Modus zeigt an, ob sich die App bei der Bearbeitung der Anfrage im Fallback-Modus befand. Fallback tritt auf, wenn während der Vorbereitung der Anforderung zur Ausführung etwas fehlgeschlagen ist.
Gebrauchte EDNS	True, wenn die Anwendung eine EDNS Client Subnet-Erweiterung verwendet.
TTL	Die TTL (Time To Live), die zurückgegeben wurde.
Antwort	Der von der Anfrage zurückgegebene CNAME.
Ergebnis	Der Wert in diesem Feld ist immer 1.
Kontext	Es ist die Zusammenfassung der Radardaten, die Openmix zur Verfügung standen, als die Anfrage bearbeitet wurde. Openmix löst Radardaten relativ zu den effektiven Werten für jede Anfrage auf, sodass zwei Clients, die gleichzeitig Anfragen stellen, unterschiedliche Kontext-Strings haben können.

Openmix HTTP-API-Protokollbeschreibungen

Protokoll	Beschreibung
Zeitstempel	Es ist die UTC-Zeit der Anfrage im Format YYYY-MM-DDTHH: MI: SSZ. Der tatsächliche Wert (auf die Sekunde herunter) in den Protokolltabellen wird auf die nächste Stunde (2018-03-30T23:00:00Z) bzw. den nächsten Tag (2018-03-30T00:00:00Z) in den Stunden-/Tag-Tabellen gerundet. Der Zeitstempel ist in allen Datensätzen immer in UTC angegeben.
App-Besitzer-Zonen-ID	Die Zonen-ID des Anwendungseigentümers, der die Anforderung bearbeitet. Dieser Wert ist immer gleich 1.
App-Besitzer-Kundennummer	Die Kunden-ID des Anwendungseigentümers, der die Anfrage bearbeitet. Bei HTTP-Anfragen kodieren Sie diese ID im Anforderungspfad und werden verwendet, um nachzuschlagen, welche Anwendung ausgeführt werden soll.
App-ID	Die Anwendungs-ID innerhalb des Kundenkontos, die die Anfrage bearbeitet. Diese ID ist auch im HTTP-Anforderungspfad codiert. Anwendungs-IDs beginnen bei 1 und sind nur für den Kunden eindeutig. Sie müssen Abfragen für eine bestimmte App-ID vollständig qualifizieren, indem Sie die appOwnerCustomerId abfragen.

Protokoll	Beschreibung
App-Version	Die Version der Anwendung, die das Konto bedient hat. Jedes Mal, wenn eine Anwendung über das Portal oder die API aktualisiert wird, wird die Version inkrementiert. Die Version, die zum Zeitpunkt der Anfrage ausgeführt wurde, wird aufgezeichnet. Diese Informationen können verwendet werden, um versionierte Logik im Laufe der Zeit zu trennen, wenn Anwendungen aktualisiert werden. Hosts im gesamten Netzwerk erhalten Updates in der Regel in einem ähnlichen Zeitraum, jedoch fast nie genau zum gleichen Zeitpunkt. Es ist wahrscheinlich, dass sich überlappende Entscheidungen im Laufe der Zeit während des Aktualisierungsprozesses unterschiedliche Versionen einer App verwenden.
App-Name	Der Name der Anwendung, die das Konto bedient hat.
Market	Der Markt des Endverbrauchers, der diese Messung generiert hat.
Land	Das Land des Endbenutzers, der diese Messung generiert hat.
Region	Die Region des Endbenutzers, der diese Messung generiert hat.
Status	Der Status des Endbenutzers, der diese Messung generiert hat.
ASN-ID	Die ID der Autonomous System Number (ASN) des Endbenutzers, der diese Messung generiert hat, d. h. die Netzwerk-ID-Nummer, die mit dem ASN-Namen verknüpft ist
ASN Name	Der Name der ASN des Endbenutzers, der die Messung generiert hat.

Protokoll	Beschreibung
Effektive IP	Die effektive IP ist die IP, die zur Verarbeitung der Anfrage verwendet wird. Es ist die von der Abfragezeichenfolge angegebene IP, die die anfordernde IP außer Kraft setzt (im Gegensatz zur Resolver/ECS/EDNS-ID für den DNS-Fluss). Es ist die Adresse, die das System bei der Verarbeitung der Informationen als Ziel berücksichtigt. Diese IP ist entweder die IP des anfordernden Resolvers oder die ECS-IP-Adresse des Clients, falls EDNS ECS unterstützt wird. Alle Daten zur Sondenleistung, geografischen Informationen usw., die an die Anwendungslogik weitergegeben werden, basieren auf dieser IP.
Name des Entscheidungsanbieters	Alias der Plattform, die eine Anwendung auswählt.
Ursachencode	In der Anwendung festgelegter Ursachencode, der den Grund für die Entscheidung beschreibt.
Ursache-Protokoll	Dieses Protokoll ist eine vom Kunden definierte Ausgabe der Openmix-App. Es ist ein optionales Zeichenfolgenfeld, mit dem Kunden Informationen über ihre Openmix-App-Entscheidungen protokollieren können.
Fallback-Modus	Dieser Modus zeigt an, ob sich die App bei der Bearbeitung der Anfrage im Fallback-Modus befand. Fallback tritt auf, wenn während der Vorbereitung der Anforderung zur Ausführung etwas fehlgeschlagen ist.

Protokoll	Beschreibung
Antwortcode	Ergebnis der Messung, z. B. 0: Erfolg, 1: Timeout, 4: Fehler. Für Verfügbarkeitsberechnungen wird der Prozentsatz der Messungen mit einer Antwort von 0 (Erfolg) im Vergleich zur Gesamtzahl der Messungen (gesamt, unabhängig von der Reaktion) ermittelt. Bei anderen Sondentypen (RTT und Durchsatz) darf der Filter bei der Berechnung von Statistiken im RTT nur RTT-Datenpunkte mit einem Erfolgscode von 0 berücksichtigen. Gleiches für den Durchsatz.
HTTP-Methode	Die HTTP-Methode (GET/POST/OPTIONS/etc) bezieht sich auf die Anfrage, die von einem Kundendienst an den HTTP Openmix-Server gestellt wurde. Zusammen bilden diese Methoden Teile der eingehenden URL und der ausgehenden HTTP-Antworten.
URI	Es ist der Anforderungspfad. Wenn Kunden nicht das gewünschte Verhalten erhalten, kann dies an einer falsch strukturierten Anfrage liegen. Die Protokolle zeigen, was unsere Server empfangen (Protokoll, Host und Pfad). Die Referer-Informationen (Protokoll, Host und Pfad) stammen aus dem Referer-Header der HTTP-Anforderung an Radar. Für HTTP OPX ist der gesamte Referer (Protokoll, Host und Pfad) in einer Zeichenfolge mit der Bezeichnung Referer enthalten.
Benutzeragent	Es ist die Benutzer-Agent-Zeichenfolge von der Browserseite, die das Tag hostet. Wenn Sie beispielsweise Chrome verwenden und eine Seite mit dem Radar-Tag durchsuchen, zeichnet die Radarmessung im Hintergrund den Benutzeragenten in Ihrem Chrome-Browser auf. Die Messungen umfassen den Chrome-Browser, die Version von Chrome, Informationen über das Betriebssystem, auf dem Chrome ausgeführt wird, und so weiter.

Protokoll	Beschreibung
Kontext	Es ist die Zusammenfassung der Radardaten, die Openmix zur Verfügung standen, als die Anfrage bearbeitet wurde. Openmix löst Radardaten relativ zu den effektiven Werten für jede Anfrage auf, sodass zwei Clients, die gleichzeitig Anfragen stellen, unterschiedliche Kontext-Strings haben können.

Benutzerdefinierte Berichte für Drittanbieter

Kunden können mit NetScaler zusammenarbeiten, um benutzerdefinierte Berichte zu erhalten, die auf Radardaten basieren, die NetScaler sammelt. NetScaler kann Berichte generieren, die nach einem Zeitplan ausgeführt werden. Die Berichte sind als Datendateien verfügbar, normalerweise im TSV-Format.

Häufig gestellte Fragen

Radar

Wie häufig werden Dateien auf S3 und GCS übertragen? Die Häufigkeit der Dateieinzahlungen beträgt einmal pro Minute für Radar und täglich für Berichte.

Wo werden die Berichte gespeichert? S3 Legacy (Standort 1):

```
s3://public-radar/[customer name]/
```

S3 (Standort 2):

```
s3://cedexis-netscope/[customer id]/
```

GCS (Standort 3):

```
gs://cedexis-netscope-[customer id]/
```

Wie erhalte ich S3-Zugangsdaten, wenn Sie diese noch nicht haben? Das Portal bietet einen “Access”- und “Secret”-Schlüssel. Verwenden Sie die Tasten mit ‘s3cmd’, ‘awscli’oder anderen Tools, um auf S3 zuzugreifen. Für Google Storage lädt das Portal eine Datei mit Zugangsdaten zur Verwendung mit dem Tool ‘gsutil’herunter.

Wie verwende ich die Zugriffs- und geheimen Schlüssel mit s3cmd, um Protokolle und Berichte aus dem S3-Bucket herunterzuladen? Zuerst müssen Sie `s3cmd` von https://s3tools.org/download herunterladen und installieren. Informationen zur Verwendung, Optionen und Befehle finden Sie unter https://s3tools.org/usage. Führen Sie dann den folgenden Befehl aus:

```
s3cmd --access_key=[access key] --secret_key=[secret key] ls s3://
    cedexis-netscope/<customer id>/radar/
<!--NeedCopy-->
```

Führen Sie den folgenden Befehl aus, um die Dateien herunterzuladen:

```
s3cmd --access_key=[access_key] --secret_key=[secret_key] get s3://
    cedexis-netscope/<customer id>/radar/[the_filename_to_download] [
    the_name_of_the_local_file]
<!--NeedCopy-->
```

So verwenden Sie die s3cmd-Konfiguration, um Dateien im S3-Bucket aufzulisten Der erste Schritt ist die Installation `s3cmd`. Sie können es installieren von http://s3tools.org/download

Führen Sie den folgenden Befehl aus, um s3cmd zu konfigurieren

```
s3cmd ls s3://cedexis-netscope/[customer id]/
<!--NeedCopy-->
```

Wenn Sie bereits`s3cmd` mit einem anderen Satz von Zugriffs- und geheimen Schlüsseln verwenden, gehen Sie folgendermaßen vor:

Wenn Sie bereits verwenden `s3cmd`, erstellen Sie eine Kopie der Standardkonfiguration unter `~/.s3cfg`. Erstellen Sie beispielsweise eine Kopie und nennen Sie sie als `~/.s3cfg_netscope`. Ersetzen Sie die Access- und Secret-Key-Einträge in `~/.s3cfg_netscope` durch die von uns bereitgestellten.
Verwenden Sie die neue Konfiguration anstelle der Standardkonfiguration (die Ihres Unternehmens), um mit folgendem Befehl auf den S3-Bucket zuzugreifen:

```
s3cmd -c ~/.s3cfg_netscope ls s3://cedexis-netscope/[customer id]/
<!--NeedCopy-->
```

Der Hauptunterschied ist, dass Sie eine`-c` und wo sich die Konfigurationsdatei mit den von Citrix bereitgestellten Zugriffs- und geheimen Schlüsseln befindet.

Wenn Sie zwischen den Schlüsseln wechseln möchten, betten Sie sie in eine Datei ein. Beziehen Sie sich auf die Datei mit der Option `-c`, um anzugeben, welches Schlüsselpaar Sie verwenden.

> **HINWEIS:** `-c` Parameter gibt an, wo die Konfigurationsdatei ist, die den Zugriff und die geheimen Schlüssel enthält.

So verwenden Sie die Schlüsseldatei mit gsutil oder gcloud zum Herunterladen von Protokolldateien Sobald Sie die JSON-Schlüsseldatei des Google-Dienstkontos heruntergeladen haben, können Sie sie verwenden, um die Anmeldeinformationen Ihres Google-Kontos zu authentifizieren, Ihre Protokolldateien anzuzeigen oder herunterzuladen. Hier ist zum Beispiel eine Möglichkeit, dies mit den Befehlszeilenprogrammen von Google `gcloud` und `gsutil` zu tun:

Schritt 1: Schlüsseldatei aktivieren

Die Authentifizierungsbefehle `gcloud auth activate-` oder `gsutil config -e` sind erforderlich, um die Schlüsseldatei für die Ausführung von gcloud- oder gsutil-Befehlen zu authentifizieren.

Für gcloud:

Führen Sie den folgenden Befehl mit der heruntergeladenen Schlüsseldatei aus:

```
gcloud auth activate-service-account --key-file [downloaded config file
    ]
<!--NeedCopy-->
```

Oder

```
gcloud auth activate-service-account --key-file=[path and file name of
    key file]
<!--NeedCopy-->
```

Für Gsutil:

Führen Sie den folgenden Befehl mit der heruntergeladenen Konfigurationsdatei aus:

```
gsutil config -e
<!--NeedCopy-->
```

Schritt 2: Listen Sie die Dateien im GCS (Google Cloud Storage) Bucket auf

Nachdem Sie die Dienstkontoschlüsseldatei wie im vorherigen Schritt beschrieben aktiviert haben, führen Sie den folgenden Befehl aus, um die Dateien im GCS-Bucket aufzulisten:

```
gsutil ls gs://cedexis-netscope-<customer id>
<!--NeedCopy-->
```

Schritt 3 (falls erforderlich): Wiederherstellen der ursprünglichen Anmeldeinformationen (oder Wechseln zwischen Konten)

Gehen Sie wie folgt vor, um zwischen dem NetScaler ITM-Konto und anderen von Ihnen authentifizierten Google Cloud-Anmeldeinformationen zu wechseln.

Führen Sie zunächst den folgenden Befehl aus, um alle Ihre Konten aufzulisten:

```
gcloud auth list
<!--NeedCopy-->
```


Verwenden Sie dann den folgenden Befehl, um zu einem anderen Konto zu wechseln:

```
gcloud config set account [email of the account to switch to as shown
    in gcloud auth list]
<!--NeedCopy-->
```

Sie können mit demselben Befehl zwischen Konten hin- und herwechseln, indem Sie die E-Mail durch die Konto-E-Mail ersetzen, zu der Sie wechseln möchten.

Wie sieht der Dateiname aus? Legacy Täglich:

Die ShareFile-Namen des täglichen Radarprotokolls haben diese Struktur:

`<prefix><date: YYYY-MM-DD>.<customer_id>.part<uniq_id>.kr.txt.gz`

Zum Beispiel`Cedexis_Daily-2017-11-07.21222.part-cc901e1dd55eal4e.kr.txt.gz` (nicht standardmäßiges Beispiel)

Legacy-Echtzeit-Version:

Die ShareFile-Namen des Radar-Echtzeitprotokolls haben diese Struktur:

`<prefix><customer_id>-YYYY-MM-DDTHH:MM<uniq_id>.txt.gz`

Zum Beispiel `Cedexis_3-32291-2017-11-08T20:56-cc907e8fd71eaf4e.txt.gz`

Netscope NEM-Format:

Das Netscope NEM-Format für tägliche und Echtzeit-Protokollfreigabedateien hat folgende Struktur:

`<freq><log_type><prefix><id_type><id><iso_dt><uniq_id>.<line_format>.gz`

Hierbei gilt:

- `freq: "daily"| "rt"| "hr"`
- `log_type: "radar"| "opx"| "hopx"`
- `prefix: log_share.prefix`
- `id_type: "customer"| "provider"| "asn"`
- `id: log_share.match_id`
- `iso_dt: iso 8601 Date_time "YYYYMMDDTHHMMSSZ"`
- `uniq_id: hash(UUID)`
- `line_format: "tsv"| "json"`

Zum Beispiel `rt-radar-TestRadar1-provider-20363-20171209183034Z-cc907e8fd71eaf4e.tsv.gz`

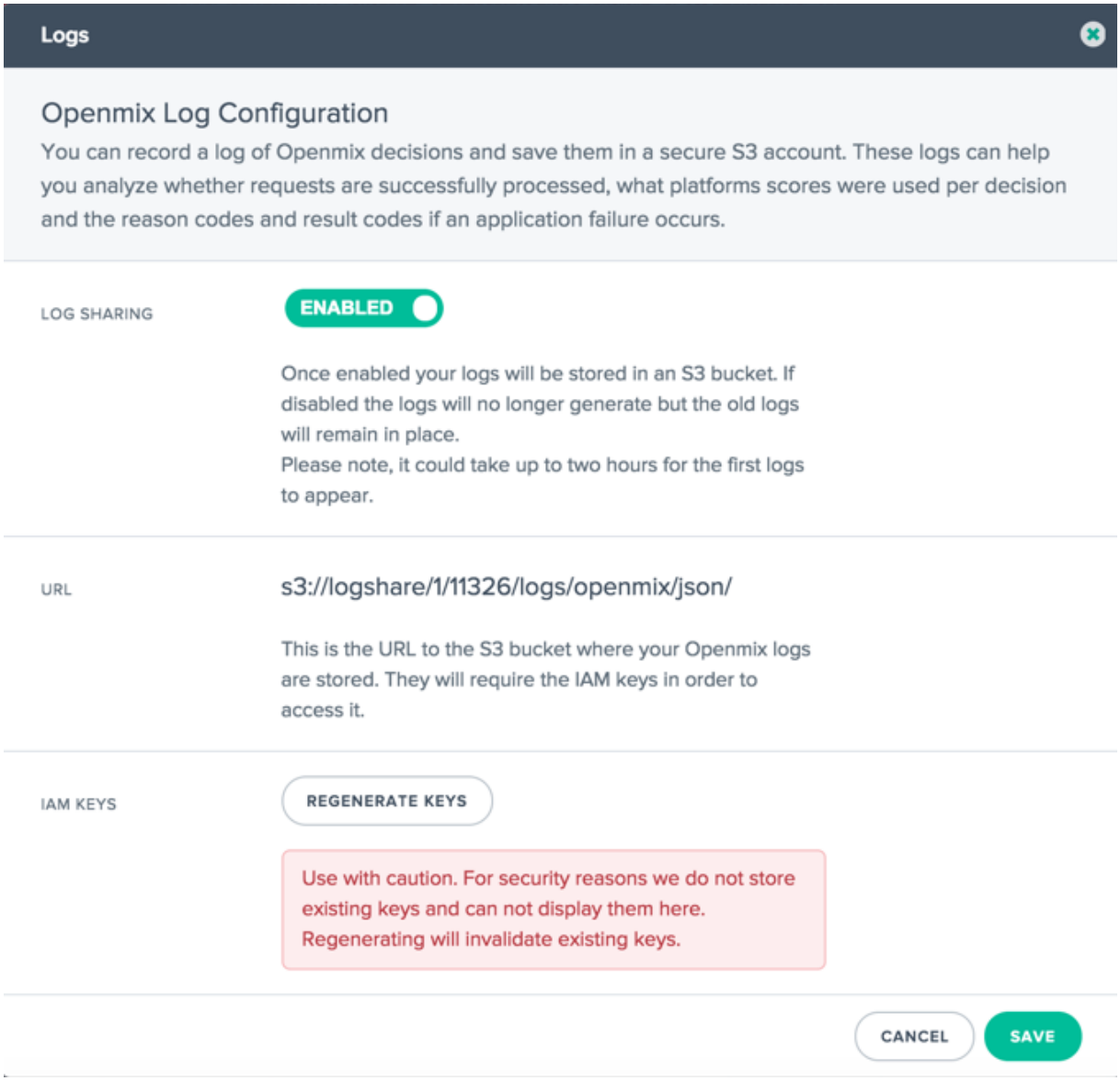
Was ist das Format der Ausgabedatei? Für Radar ist das Ausgabedateiformat TSV (tabulatorgetrennter Wert), gzipped.

Openmix und Openmix HTTP API

Wie oft werden Dateien auf S3 übertragen? Die Häufigkeit der Dateieinlagen beträgt einmal pro Minute für Openmix und HTTP Openmix.

Was ist, wenn Sie die Option zur Konfiguration der Echtzeit-Logfreigabe von Openmix und Openmix HTTP API nicht sehen können? Ihr Account Manager kann die erforderliche Rolle für die Konfiguration und Aktivierung von Openmix und Openmix HTTP API in Echtzeit Log Sharing aktivieren.

Wie aktiviert man Openmix und eine Openmix HTTP API Echtzeit-Log-Sharing und greift auf Dateien zu? Sobald die Rolle in Ihrem Konto aktiviert ist, wird das Symbol **"Protokolle verwalten** "angezeigt. Klicken Sie hier, um den Dialog **Logs** zu öffnen, in dem Sie auf die Einstellungen der Openmix Log Diese Einstellungen sind im Grunde alles, was Sie benötigen, um Openmix und HTTP Openmix in Echtzeit Log-Sharing einzuschalten und auf Dateien zuzugreifen.



Was ist der Back-End-Prozess? Das Aktivieren der Openmix-Logfreigabe ermöglicht auch die Openmix HTTP-API-Protokollfreigabe. Die Openmix- und Openmix-HTTP-API-Log-Sharing-Dienste müssen innerhalb von 10 Minuten mit der Ausgabe von Protokollen für den Kunden beginnen.

Wo werden die Openmix- und HTTP-Openmix-Berichte gespeichert? S3 Legacy (Standort 1):

```
s3://logshare/[zone ID]/[customer ID]/logs/openmix/json/[YYYY]/[MM]/[DD]/[HH]/.
```

S3 (Standort 2):

```
s3://cedexis-netscope/[customer id]/
```


GCS (Standort 3):

```
gs://cedexis-netscope-[customer id]/
```

Wie sieht der Dateiname aus? Die Dateinamenstruktur für Openmix und HTTP Openmix sieht normalerweise wie folgt aus:

Legacy-Echtzeit-Version:

```
[zone ID, 1][customerID]-openmix-json[YYYY][MM][DD][HH][mm][ss]Z-m1-w9-c0.gz
```

Netscope NEM-Format:

Das Netscope NEM-Format für tägliche und Echtzeit-Protokollfreigabedateien hat folgende Struktur:

```
<freq><log_type><prefix><id_type><id><iso_dt><uniq_id>.<line_format>.gz
```

Hierbei gilt:

- `freq`: `"daily"| "rt"| "hr"`
- `log_type`: `"radar"| "opx"| "hopx"`
- `prefix`: `log_share.prefix`
- `id_type`: `"customer"| "provider"| "asn"`
- `idv`: `log_share.match_id`
- `iso_dt`: `iso 8601 Date_time "YYYYMMDDTHHMMSSZ"`
- `uniq_id`: `hash(UUID)`
- `line_format`: `"tsv"| "json"`

Zum Beispiel `hr-opx-TestOpenmix1-provider-20363-20171209183034Z-cc907e8fd71eaf4e.tsv.gz`

Was ist das Ausgabedateiformat? Das Dateiformat für Openmix und eine Openmix HTTP API ist JSON (gzipped).

Verwaltung

September 14, 2023

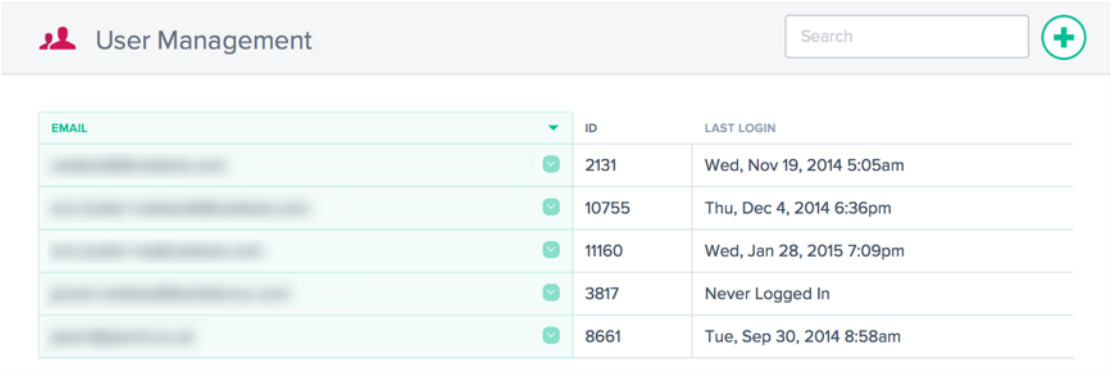
Im Bereich **Mein Konto** können der Endbenutzer das Konto verwalten, die Benutzer, die auf das Konto zugreifen können, und die Benutzer, die auf die Funktionen von Fusion Purge zugreifen können.

Darüber hinaus können Sie im Menü fällige Rechnungen einsehen und die OAuth-API-Anmeldeinformationen verwalten.

Nutzer verwalten

Im Benutzermenü können Sie Benutzer hinzufügen/entfernen und den Passwortzugriff auf das Konto zurücksetzen.

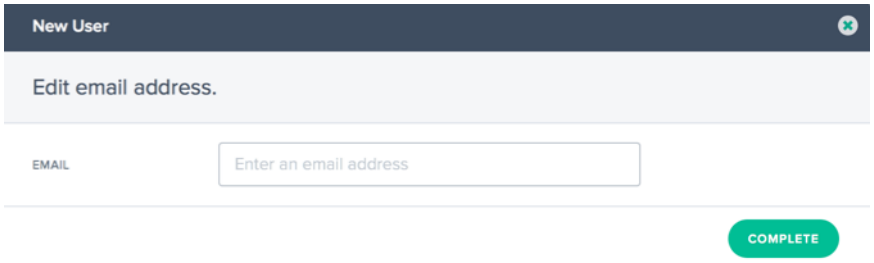
Zusätzlich zur Benutzerverwaltung können Sie E-Mail-Adressen für Service-Benachrichtigungen eingeben und sehen, wann sich ein Benutzer zuletzt angemeldet hat.



Benutzer hinzufügen oder entfernen und Passwörter zurücksetzen

Achten Sie beim Erstellen oder Hinzufügen von Benutzern darauf, dass Sie eine gültige E-Mail-Adresse verwenden. Passwörter werden automatisch erstellt und per E-Mail an die E-Mail-Adresse gesendet, die als Benutzername eingegeben wurde.

Um einen neuen Benutzer hinzuzufügen, klicken Sie auf das **+** in der oberen rechten Ecke. Geben Sie eine gültige E-Mail-Adresse ein und klicken Sie auf **Abschließen**.



Um das Passwort für einen Benutzer zurückzusetzen, klicken Sie auf den Abwärtspfeil rechts neben der E-Mail-Adresse des Benutzers, wählen Sie **Passwort zurücksetzen**und bestätigen Sie die Aktion

im Dialogfeld, indem Sie auf **Ja**klicken. Eine E-Mail zum Zurücksetzen des Passworts wird an den Benutzer gesendet.

Ein Benutzer kann aus dem System entfernt werden, indem Sie auf den Abwärtspfeil rechts neben der E-Mail-Adresse des Benutzers klicken und **Löschen**wählen. Bestätigen Sie die Aktion und der Benutzer wird aus dem System gelöscht.

Einmaliges Anmelden

Wir unterstützen die Verwendung von Identitätsanbietern von Drittanbietern für die Single Sign On-Anmeldung am Portal über SAML 2.0.

Single Sign On wird für die Authentifizierung von Benutzeranmeldungen verwendet. Derzeit geben wir keine Autorisierungsinformationen über SAML SSO weiter. Um sich anmelden zu können, muss ein Benutzer im NetScaler Intelligent Traffic Management Portal mit derselben E-Mail-Adresse wie ein Benutzer im SSO-Identitätsanbieter vorhanden sein.

Single Sign On wird pro Konto verwaltet. Sobald SSO für ein Konto aktiviert ist, müssen alle Benutzer eine SSO-Anmeldung verwenden, um auf das Portal zuzugreifen.

Sie finden die SAML-Konfigurationsinformationen im Menüpunkt **SSO-Konfiguration** . Die Informationen sind kontospezifisch und ermöglichen es Ihnen, SSO in Ihrem Identitätsanbieter zu konfigurieren. Wenn Sie das **SSO-Konfigurationsmenü** nicht finden, wenden Sie sich bitte an das Support-Team .

Die Einrichtung ist für jeden Identitätsanbieter unterschiedlich, Sie benötigen jedoch die folgenden Informationen, die auf der SSO-Konfigurationsseite angezeigt werden:

- URL des Assertion Consumer Service (ACS)
- Entitäts-ID
- Abmelde-URL (optional, je nach Anbieter)
- Start-URL (optional, je nach Anbieter)
- Namensformat: E-Mail
- Signierte Antwort: Nein

Single Sign On aktivieren

Allgemeine Schritte zum Hinzufügen von SSO zum NetScaler Intelligent Traffic Management Portal:

1. Richten Sie den Identitätsanbieter mithilfe der Daten im SSO-Konfigurationsbildschirm ein
2. Laden Sie die SSO-IDP-Metadatendatei vom Identitätsanbieter herunter
3. Laden Sie die Datei auf die SSO-Konfigurationsseite hoch
4. Wenn Sie bereit sind, SSO zu aktivieren, klicken Sie auf **Aktivieren**
5. Benutzer müssen sich jetzt über die SSO-Anmeldeseite anmelden.

Single Sign On ausschalten

Wenn SSO konfiguriert und aktiviert ist, klicken Sie auf die Schaltfläche **Deaktivieren** .

Jeder Benutzer des Kontos, der sich anmelden möchte, muss jetzt auf dem Standardanmeldebildschirm ein Citrix-Passwort verwenden. Wenn ein Benutzer sein Passwort nicht kennt, kann ein Kontoadministrator eine E-Mail zum Zurücksetzen des Passworts senden oder der Benutzer kann vom Anmeldebildschirm aus eine E-Mail zum Zurücksetzen des Passworts anfordern.

Konfigurationsschritte für Google G Suite

Die folgenden Schritte sind erforderlich, um Single Sign On mit Google G Suite-Logins zu verwenden:

In der Google G Suite:

1. Öffnen Sie in der G Suite-Verwaltungskonsole den Bereich Apps
2. Klicken Sie auf die **Kategorie SAML-Apps**
3. Klicken Sie auf die Schaltfläche **SSO für eine SAML-Anwendung aktivieren**
4. Wählen Sie unten im Dialog **SETUP MY OWN CUSTOM APP**
5. Laden Sie im Dialogfeld Google IDP-Informationen die IDP-Metadatendatei unter Option 2 herunter.
6. In den Basisinformationen für Ihre benutzerdefinierte App kann der Anwendungsname „NetScaler Intelligent Traffic Management“lauten.
7. Geben Sie die folgenden Informationen aus der SSO-Konfiguration im Portal ein:
   - ACS-URL: aus den SSO-Konfigurationsinformationen
   - Entitäts-ID: aus den SSO-Konfigurationsinformationen
   - Start-URL: aus den SSO-Konfigurationsinformationen (optional)
   - Namens-ID-Format: E-MAIL
8. Lassen Sie das Dialogfeld „Attribut-Mapping“leer und klicken Sie auf **FINISH**, um die SAML-App zu erstellen
9. Klicken Sie in der Apps-Liste auf die vertikalen Punkte rechts neben dem Portal-Element und wählen Sie **ON for everyone**

Im Portal:

1. Laden Sie auf der SSO-Konfigurationsseite die IDP-Metadatendatei hoch. Klicken Sie auf die Schaltfläche **Datei auswählen** , um den Dateibrowser zu öffnen, und wählen Sie die von G Suite heruntergeladene IDP-Metadatendatei aus.

2. Wenn die Metadatendatei korrekt validiert wurde, wird ein grünes Häkchen angezeigt.
3. Klicken Sie auf **Aktivieren**, um SSO für alle Benutzer im Konto zu aktivieren.

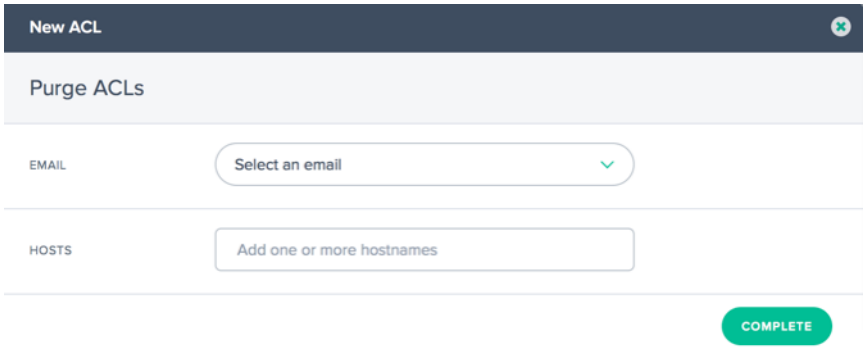
Benutzer können sich jetzt über die SSO-Anmeldeseite oder das **Apps-Menü** in **G**Suite beim NetScaler Intelligent Traffic Management Portal anmelden.

Weitere Informationen zu Google G Suite SSO finden Sie in der Google-Hilfe.

Purge-ACLs einrichten

Im Menü **Zugriffssteuerungslisten löschen** können Benutzer Einschränkungen für die Ausführung der Funktion "Fusion Purge"festlegen. Standardmäßig können Benutzer eine Bereinigung auf jedem Host ausführen, der in den **Fusion Purge**-Einstellungen konfiguriert ist. Die Purge-ACLs werden verwendet, um Benutzer darauf zu beschränken, eine Bereinigung nur auf bestimmten Hosts zuzulassen.

Fügen Sie neue Einschränkungen für einen Benutzer hinzu, indem Sie auf die Schaltfläche **„+“** in der oberen rechten Ecke klicken. Das folgende Dialogfeld wird angezeigt:



Feld	Beschreibung
E-Mail	Wählen Sie die E-Mail-Adresse für den Benutzer aus, für den Sie den eingeschränkten Löschzugriff konfigurieren möchten.
Hosts	Geben Sie die Hostnamen für den Benutzer ein, der Säuberungen ausführen soll. Hostnamen, die nicht in der Liste für den Benutzer enthalten sind, können vom Benutzer nicht gelöscht werden.

Rechnungen

Die Menüoption **Rechnungen** enthält alle Rechnungen für die NetScaler Intelligent Traffic Management-Services, die Sie genutzt haben. Wenn es Probleme mit den Rechnungen gibt, wenden Sie sich an Ihren Vertriebsmitarbeiter oder wenden Sie sich alternativ an das Support-Team .

API

OAuth verwalten

Die **API-Menüoption** enthält Details zu den authentifizierten OAuth-API-Token, die Sie möglicherweise verwenden möchten. Wenn Sie diese Funktion nutzen möchten, wenden Sie sich an Ihren Kundenbetreuer.

REST-API-Ratenbegrenzungen

REST-APIs können verwendet werden, um auf Daten und Einstellungen zuzugreifen, die auf der Plattform gespeichert sind. Wir begrenzen jedoch die Anzahl der Anfragen (um auf diese Daten zuzugreifen), indem wir ihnen ein Ratenlimit auferlegen, d. h. wir begrenzen die Anzahl der API-Aufrufe, die ein Kunde in einem bestimmten Zeitraum tätigen kann. Dies geschieht, um die Last auf dem System auszugleichen.

Attribute für Ratenbegrenzungen Ratenlimits haben die folgenden Eigenschaften:

- Zeitbereich (in Minuten)
- Anzahl der erlaubten Anfragen
- Gleichzeitige Anforderungen

Kunden können für ihren spezifischen Anwendungsfall eine Erhöhung ihrer Ratenlimits beantragen.

Standard-Ratenlimits In der folgenden Tabelle sind verschiedene Arten von API-Aufrufen und die für jeden von ihnen geltenden Standardratenlimits aufgeführt.

API-Typen	Standard-Ratenlimits
Endpunkte melden	**GET**

API-Typen	Standard-Ratenlimits

`/v2/reporting/radar.json`
`/v2/reporting/plt.json`
`/v2/reporting/openmix.json`
`/v2/reporting/sonar.json`
	15 Anfragen pro 15 Minuten. 3 gleichzeitige Anfragen

Anwendungen aktualisieren	**STELLEN, POSTEN**
`/v2/config/applications/dns.json`	10 Anfragen pro Minute. 3 gleichzeitige Anfragen
Fusion Purge	**GET**
`/v2/actions/fusion/purge.json`	150 Anfragen pro Minute
Fusion Purge	**POST**
`/v2/actions/fusion/purge.json`	1 Anfrage pro Minute. 3 Hintergrundprozesse