Red Hat 3scale API Management 2.9

API ゲートウェイの管理

3scale インストール環境のより詳細な設定方法

Last Updated: 2022-11-13

Red Hat 3scale API Management 2.9 API ゲートウェイの管理

3scale インストール環境のより詳細な設定方法

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Administering_the_API_Gateway.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

本ガイドでは、基本インストールの後に実施する設定タスクについて説明します。

目次

前書き 7

パート I. API ゲートウェイ 8

第1章 APICAST の運用 9
1.1. 公開ベース URL 9
1.2. マッピングルール 9
1.2.1. プロダクトおよびバックエンドにおけるマッピングルール 10
1.2.2. マッピングルールの照合 11
1.2.3. マッピングルールのワークフロー 12
1.3. HOST ヘッダー 13
1.4. API バックエンドの保護 13
1.5. プライベート API を扱う APICAST の使用 13
1.6. APICAST への OPENTRACING の設定 14
1.6.1. 前提条件 14
1.6.2. 手順 14
1.6.3. 補足情報 14
1.6.4. OpenShift インスタンスへの Jaeger のインストール 15

第2章 DOCKER コンテナー環境の操作 17
2.1. DOCKER コンテナー環境上の APICAST に関するトラブルシューティング 17
2.1.1. Cannot connect to the Docker daemon エラー 17
2.1.2. 基本的な Docker コマンドラインインターフェイスコマンド 17

第3章 高度な APICAST 設定 18
3.1. シークレットトークンの定義 18
3.2. クレデンシャル 18
3.3. エラーメッセージの設定 19
3.4. 設定履歴 20
3.5. デバッグ 20
3.6. パスルーティング 21

第4章 APICAST ポリシー 22
4.1. APICAST 標準ポリシー 22
4.1.1. 3scale Auth Caching 23
4.1.2. 3scale Batcher 25
4.1.3. 3scale Referrer 26
4.1.4. Anonymous Access 26
4.1.5. Camel Service 27
4.1.5.1. 設定 28
4.1.5.1.1. ユースケースの例 29
4.1.6. Conditional ポリシー 29
4.1.6.1. 条件 30
4.1.6.1.1. Liquid でサポートされている変数 31
4.1.7. Content Caching 31
4.1.7.1. サポートされる設定 32
4.1.7.2. アップストリームレスポンスヘッダー 32
4.1.8. CORS Request Handling 32
4.1.9. Custom metrics 34
4.1.9.1. Custom metrics の制限 34
4.1.9.2. リクエストフローの例 34
4.1.9.3. 設定例 34

4.1.10. Echo 35
4.1.11. Edge Limiting 36
4.1.11.1. 制限のタイプ 36
4.1.11.2. 制限の定義 37
4.1.11.3. Liquid テンプレート 38
4.1.11.4. 条件の適用 38
4.1.11.5. 流量制御カウンター用ストレージの設定 39
4.1.11.6. エラー処理 39
4.1.12. Header Modification 39
4.1.13. IP Check 40
4.1.14. JWT Claim Check 42
4.1.14.1. JWT Claim Check ポリシーの概要 42
4.1.14.2. ポリシーチェーンへの JWT Claim Check ポリシーの設定 42
4.1.14.2.1. ポリシーの設定 43
4.1.15. Liquid Context Debug 43
4.1.16. Logging 44
4.1.16.1. すべての API に対するグローバル設定 44
4.1.16.2. 例 45
4.1.16.3. カスタムロギングに関する補足情報 47
4.1.17. Maintenance Mode 47
4.1.18. OAuth 2.0 Mutual TLS Client Authentication 48
4.1.19. OAuth 2.0 Token Introspection 48
4.1.20. Proxy Service 51
4.1.20.1. 設定 52
4.1.20.1.1. ユースケースの例 52
4.1.21. Rate Limit Headers 52
4.1.21.1. RateLimit ヘッダー 52
4.1.22. Retry 53
4.1.23. RH-SSO/Keycloak Role Check 53
4.1.24. Routing 56
4.1.24.1. ルーティングルール 56
4.1.24.2. リクエストパスルール 56
4.1.24.3. ヘッダールール 57
4.1.24.4. クエリー引数ルール 57
4.1.24.5. JWT クレームルール 58
4.1.24.6. 複数演算ルール 58
4.1.24.7. ルールの結合 59
4.1.24.8. キャッチオールルール 60
4.1.24.9. サポートされる操作 61
4.1.24.10. Liquid テンプレート 62
4.1.24.11. host_header で使用されるホストの設定 62
4.1.25. SOAP 63
4.1.26. TLS Client Certificate Validation 64
4.1.26.1. TLS Client Certificate Validation ポリシーに対応する APIcast の設定 64
4.1.26.1.1. ポリシーに対応する APIcast のセットアップ 64
4.1.26.2. ポリシーチェーンへの TLS Client Certificate Validation ポリシーの設定 65
4.1.26.2.1. ポリシーの設定 65
4.1.26.3. TLS Client Certificate Validation ポリシー機能の確認 66
4.1.26.3.1. ポリシー機能の確認 66
4.1.26.4. ホワイトリストからの証明書の削除 66
4.1.26.4.1. 証明書の削除 67
4.1.26.5. リファレンス資料 67
4.1.27. TLS Termination 67

4.1.27.1. ポリシーチェーンへの TLS Termination ポリシーの設定 67
4.1.27.1.1. ポリシーの設定 67
4.1.27.2. TLS Termination ポリシー機能の確認 68
4.1.27.2.1. ポリシー機能の確認 68
4.1.27.3. TLS Termination ポリシーからのファイルの削除 68
4.1.27.3.1. 証明書の削除 68
4.1.28. Upstream 69
4.1.29. Upstream Connection 70
4.1.29.1. ポリシーチェーンへの Upstream Connection ポリシーの設定 70
4.1.29.1.1. ポリシーの設定 70
4.1.30. Upstream Mutual TLS 70
4.1.30.1. ポリシーチェーンへの Upstream Mutual TLS ポリシーの設定 70
4.1.31. URL Rewriting 71
4.1.31.1. パスを書き換えるためのコマンド 71
4.1.31.2. クエリー文字列を書き換えるためのコマンド 72
4.1.32. URL Rewriting with Captures 74
4.2. 管理ポータルでのポリシーの有効化 74
4.3. カスタム APICAST ポリシーの作成 75
4.4. APICAST へのカスタムポリシーの追加 75
4.4.1. APIcast デプロイメントへのカスタムポリシーの追加 75
4.4.2. Embedded APIcast へのカスタムポリシーの追加 75
4.4.3. 別の OpenShift Container Platform 上の APIcast へのカスタムポリシーの追加 77
4.5. 3SCALE でのポリシーチェーンの作成 78
4.6. ポリシーチェーン JSON 設定ファイルの作成 78

第5章 ポリシーチェーンと APICAST ネイティブデプロイメントのインテグレーション 80
5.1. ポリシーでの変数およびフィルターの使用 80

第6章 FUSE のポリシーエクステンションを使用した 3SCALE メッセージコンテンツの変換 83
6.1. APICAST と FUSE の APACHE CAMEL による変換のインテグレーション 83
6.2. FUSE ON OPENSHIFT の APACHE CAMEL を使用して作成された APICAST ポリシーエクステンションの設定 85

第7章 APICAST の環境変数 88
all_proxy、ALL_PROXY 89
APICAST_ACCESS_LOG_FILE 89
APICAST_BACKEND_CACHE_HANDLER 90
APICAST_CACHE_MAX_TIME 90
APICAST_CACHE_STATUS_CODES 90
APICAST_CONFIGURATION_CACHE 90
APICAST_CONFIGURATION_LOADER 90
APICAST_CUSTOM_CONFIG 91
APICAST_ENVIRONMENT 91
APICAST_EXTENDED_METRICS 91
APICAST_HTTPS_CERTIFICATE 91
APICAST_HTTPS_CERTIFICATE_KEY 91
APICAST_HTTPS_PORT 91
APICAST_HTTPS_VERIFY_DEPTH 91
APICAST_LOAD_SERVICES_WHEN_NEEDED 92
APICAST_LOG_FILE 92
APICAST_LOG_LEVEL 92
APICAST_MANAGEMENT_API 92
APICAST_MODULE 93
APICAST_OIDC_LOG_LEVEL 93

APICAST_PATH_ROUTING 93
APICAST_PATH_ROUTING_ONLY 93
APICAST_POLICY_LOAD_PATH 93
APICAST_PROXY_HTTPS_CERTIFICATE 94
APICAST_PROXY_HTTPS_CERTIFICATE_KEY 94
APICAST_PROXY_HTTPS_PASSWORD_FILE 94
APICAST_PROXY_HTTPS_SESSION_REUSE 94
APICAST_REPORTING_THREADS 94
APICAST_RESPONSE_CODES 94
APICAST_SERVICE_CACHE_SIZE 95
APICAST_SERVICE_${ID}_CONFIGURATION_VERSION 95
APICAST_SERVICES_LIST 95
APICAST_SERVICES_FILTER_BY_URL 95
APICAST_UPSTREAM_RETRY_CASES 96
APICAST_WORKERS 96
BACKEND_ENDPOINT_OVERRIDE 96
HTTP_KEEPALIVE_TIMEOUT 96
http_proxy、HTTP_PROXY 96
https_proxy、HTTPS_PROXY 96
no_proxy、NO_PROXY 96
OPENSSL_VERIFY 96
OPENTRACING_CONFIG 97
OPENTRACING_HEADER_FORWARD 97
OPENTRACING_TRACER 97
RESOLVER 97
THREESCALE_CONFIG_FILE 97
THREESCALE_DEPLOYMENT_ENV 98
THREESCALE_PORTAL_ENDPOINT 98

第8章 パフォーマンスを向上させるための APICAST 設定 99
8.1. 全般的なガイドライン 99
8.2. デフォルトのキャッシング 99
8.3. 非同期レポートスレッド 101
8.4. 3SCALE BATCHER ポリシー 102

第9章 PROMETHEUS への 3SCALE APICAST メトリクスの公開 104
9.1. PROMETHEUS の概要 104
9.1.1. Prometheus クエリー 104
9.2. APICAST と PROMETHEUS のインテグレーション 104
9.2.1. 追加オプション 105
9.3. 3SCALE APICAST 用 OPENSHIFT 環境変数 105
9.4. PROMETHEUS に公開される 3SCALE APICAST メトリクス 106

パート II. API のバージョン管理 109

第10章 API のバージョン管理 110
10.1. 目的 110
10.2. 前提条件 110
10.3. URL によるバージョン管理 110
10.4. エンドポイントによるバージョン管理 113
10.5. カスタムヘッダーによるバージョン管理 113

パート III. API の認証 115

第11章 認証パターン 116

11.1. サポートされる認証パターン 116
11.2. 認証パターンのセットアップ 116
11.2.1. サービスに設定する認証モードの選択 116
11.2.2. 使用する認証モードの選択 117
11.2.3. API が正しいクレデンシャルタイプを受け入れることの確認 117
11.2.4. クレデンシャルをテストするためのアプリケーションの作成 117
11.3. 標準の認証パターン 117
11.3.1. API キー 117
11.3.2. App_ID と App_Key のペア 118
11.3.3. OpenID Connect 118
11.4. 参照元フィルター機能 118

第12章 OPENID CONNECT インテグレーション 122
12.1. APICAST による JWT の検証および解析 122
12.2. ZYNC-QUE によるクライアントクレデンシャルの同期 123
12.3. RED HAT SINGLE SIGN-ON インテグレーションの設定 123
12.3.1. カスタム CA 証明書を使用するための zync-que の設定 123
12.3.2. Red Hat Single Sign-On の設定 124
12.3.3. 3scale の設定 125
12.4. サードパーティーアイデンティティープロバイダーとの HTTP インテグレーションの設定 126
12.4.1. 前提条件 126
12.4.2. 手順 126
12.4.3. Zync REST API の例 126
12.4.3.1. 前提条件 126
12.4.3.2. クライアントの作成、更新、および削除 127
12.4.3.3. Payload 127
12.4.3.4. OAuth2 認証の使用 127
12.5. OAUTH 2.0 SUPPORTED FLOWS 127
12.5.1. OAuth 2.0 対応の認証フローの仕組み 128
12.5.2. OAuth 2.0 対応の認証フローの設定 128
12.6. インテグレーションのテスト 128
12.6.1. クライアントの同期に関するテスト 128
12.6.2. API 承認フローのテスト 129
12.7. インテグレーションの例 129

前書き

本ガイドは、3scale インストール環境により詳細な設定を適用するのに役立ちます。インストールに関する基本的な情報は、3scale のインストールを参照してください。

パート I. API ゲートウェイ

第1章 APICAST の運用

本セクションでは、高度な APIcast 設定を使用する際に考慮すべき概念について説明します。

1.1. 公開ベース URL

公開ベース URL は開発者がご自分の API 製品にリクエストを行うのに使用する URL で、3scale により公開されます。これは、ご自分の APIcast インスタンスの URL になります。

Self-managed デプロイメントオプションのいずれかを使用している場合には、それぞれの環境 (ステージングおよび実稼働環境) について、ご自分の管理するドメインに属する専用の公開ベース URL を選択することができます。この URL はご自分の API バックエンドの URL とは別で、たとえば **https://api.yourdomain.com:443** のようになります。ここで、**yourdomain.com** はご自分のドメインです。公開ベース URL を設定したら必ず変更を保存し、必要に応じてステージング環境の変更を実稼働環境にプロモートしてください。

注記

指定する公開ベース URL は、OpenShift クラスターで利用可能なポートを使用する必要があります。デフォルトでは、OpenShift のルーターは標準の HTTP および HTTPS ポート (80 および 443) の接続しかリッスンしません。ユーザーに他のポート経由で API に接続してもらう場合は、OpenShift の管理者と連携してそのポートを有効にします。

APIcast は公開ベース URL で指定したホスト名に対する呼び出ししか受け付けません。**Echo API** を例に取ると、公開ベース URL を **https://echo-api.3scale.net:443** と指定した場合には、正しい呼び出しは以下のようになります。

```
curl "https://echo-api.3scale.net:443/hello?user_key=YOUR_USER_KEY"
```

API に公開ドメインがない場合には、リクエストに APIcast の IP アドレスを使用することができます。ただし、実際のドメインではなくても良いので、**Public Base URL** フィールドには値を指定する必要があります。その場合には、Host ヘッダーでホストを指定するようにしてください。以下に例を示します。

```
curl "http://192.0.2.12:80/hello?user_key=YOUR_USER_KEY" -H "Host: echo-api.3scale.net"
```

ローカルマシンにデプロイしている場合には、ドメインに localhost を使用することもできます。この場合には公開ベース URL は **http://localhost:80** のようになり、以下のようにリクエストを行うことができます。

```
curl "http://localhost:80/hello?user_key=YOUR_USER_KEY"
```

API プロダクトが複数ある場合には、それぞれのプロダクトについてこの公開ベース URL を適切に設定します。APIcast はホスト名に基づきリクエストをルーティングします。

1.2. マッピングルール

API に対するリクエストに応じて、マッピングルールにより報告するメトリクスまたはメソッドを定義します。マッピングルールの例を以下に示します。

Mapping Rules

Verb	Pattern	+	Metric or Method	Last?	Position	Add Mapping Rule
	Search for Pattern					Search
GET	/▲	1	hits	false	1	

このルールは、/ で始まるすべての **GET** リクエストがメトリクス **hits** のカウントを 1 つ増やす、という意味です。このルールは API に対するすべてのリクエストにマッチします。ただし、このルールは一般的すぎるので、通常は変更されます。そうしないと、より具体的なルールが追加された時に、2 倍にカウントされることになります。

より具体的な Echo API ルールの例を以下に示します。

Mapping Rules

Verb	Pattern	+	Metric or Method	Last?	Position	Add Mapping Rule
	Search for Pattern					Search
GET	/hello	1	get_hello	false	1	
GET	/goodbye	1	get_goodbye	false	2	

1.2.1. プロダクトおよびバックエンドにおけるマッピングルール

マッピングルールは、API プロダクトレベルおよび API バックエンドレベルで機能します。本セクションでは、各レベルにおけるマッピングルールの動作を説明すると共に、マッピングルールが機能する仕組みを例を用いて説明します。

プロダクトレベルでのマッピングルール

- このマッピングルールは、バックエンドレベルのマッピングルールに優先します。つまり、プロダクトレベルのマッピングルールが先に評価されます。
- どのバックエンドがリダイレクトされたトラフィックを受信するかにかかわらず、このマッピングルールは常に評価されます。

バックエンドレベルでのマッピングルール

- バックエンドにマッピングルールを追加すると、それらのマッピングルールはそのバックエンドと結び付くすべてのプロダクトに追加されます。
- このマッピングルールは、プロダクトレベルで定義されたマッピングルールの後に評価されます。
- このマッピングルールは、マッピングルールが設定されたバックエンドにトラフィックがリダイレクトされた場合にのみ評価されます。
- プロダクトに結び付けられるバックエンドのパスが、バックエンドの各マッピングルールの前に自動的に追加されます。

プロダクトレベルおよびバックエンドレベルのマッピングルールの例

この例では、バックエンドから説明を始め、続いてプロダクトに移ります。

- Echo API バックエンド:
  - プライベートエンドポイント: **https://echo-api.3scale.net**
  - 以下のパターンの 2 つのマッピングルールが含まれる

```
/hello
/bye
```

- Cool API プロダクト:
  - 公開エンドポイント: **https://cool.api**
  - ルーティングパス **/echo** により Echo API バックエンドを使用する
- Cool API プロダクトには、自動的に以下のパターンのマッピングルールが含まれます。

```
/echo/hello
/echo/bye
```

- これは、公開 URL **https://cool.api/echo/hello** に送信されたリクエストが、**https://echo-api.3scale.net/hello** にリダイレクトされることを意味します。
- 同様に、**https://cool.api/echo/bye** に送信されたリクエストは、**https://echo-api.3scale.net/bye** にリダイレクトされます。

ここで、同じ Echo API バックエンドを使用する Tools For Devs というプロダクトを追加することを考えてみます。

- Tools For Devs プロダクト:
  - 公開エンドポイント: **https://dev-tools.api**
  - ルーティングパス **/tellmeback** により Echo API バックエンドを使用する
- Tools For Devs プロダクトには、自動的に以下のパターンのマッピングルールが含まれます。

```
/tellmeback/hello
/tellmeback/bye
```

  - したがって、公開 URL **https://dev-tools.api/tellmeback/hello** に送信されたリクエストは、**https://echo-api.3scale.net/hello** にリダイレクトされます。
  - 同様に、**https://dev-tools.api/tellmeback/bye** に送信されたリクエストは、**https://echo-api.3scale.net/bye** にリダイレクトされます。
- パターン **/ping** のマッピングルールを Echo API バックエンドに追加すると、Cool API プロダクトおよび Tools For Devs プロダクトの両方に変更が加えられます。
  - Cool API には、**/echo/ping** というパターンのマッピングルールが含まれます。
  - Tools For Devs には、**/tellmeback/ping** というパターンのマッピングルールが含まれます。

1.2.2. マッピングルールの照合

マッピングルールは前方一致で照合され、複雑な設定が可能です。表記法は OpenAPI および ActiveDocs の仕様に準じます。

- マッピングルールは、スラッシュ (/) で始める必要があります。
- 文字列 (例: **/hello**) を使用してパスの照合を行うことができます。
- マッピングルールでは、クエリー文字列またはボディーにパラメーターを含めることができます (例: **/{word}?value={value}**)。APIcast は以下のようにパラメーターを取得します。
  - **GET** メソッド: クエリー文字列から。
  - **POST**、**DELETE**、または **PUT** メソッド: ボディーから。
- マッピングルールには名前付きワイルドカードを含めることができます (例: **/{word}**)。このルールは、プレースホルダー **{word}** で定義する任意の文字にマッチします。たとえば、**/morning** のようなリクエストがルールにマッチします。ワイルドカードは、スラッシュとスラッシュの間またはスラッシュとピリオドの間に使用することができます。パラメーターにもワイルドカードを含めることができます。
- デフォルトでは、指定したソート法に従ってすべてのマッピングルールが順番に評価されます。ルール **/v1** を追加した場合には、パスが **/v1** で始まるリクエストにマッチします (例: **/v1/word** または **/v1/sentence**)。
- パターンの最後にドル記号 (**$**) を追加して、完全一致を指定することができます。たとえば、**/v1/word$** は、**/v1/word** のリクエストにだけマッチし、**/v1/word/hello** のリクエストにはマッチしません。完全一致を指定する場合には、すべてにマッチするデフォルトのマッピングルール (/) を必ず無効にする必要があります。
- 複数のマッピングルールがリクエストのパスにマッチする場合がありますが、マッチするルールがなければ、リクエストは無視され HTTP 404 ステータスコードが返されます。

1.2.3. マッピングルールのワークフロー

マッピングルールに関するワークフローを以下に示します。

- 新たなマッピングルールを定義することができます (マッピングルールの追加 を参照)。
- 誤って変更されないように、次回のリロード時にマッピングルールはグレーアウト表示されます。
- 既存のマッピングルールを編集するには、右側にある鉛筆アイコンをクリックして、まずそのルールを有効にする必要があります。
- ルールを削除するには、ゴミ箱アイコンをクリックします。
- **Integration > Configuration** で変更をプロモートすると、すべての変更および削除が保存されます。

マッピングルールの追加

新たなマッピングルールを追加するには、以下の手順を実施します。

1. **Add Mapping Rule** をクリックします。
2. 以下の設定を指定します。
   - **Verb**: HTTP リクエストの動詞 (**GET**、**POST**、**DELETE**、または **PUT**)。

- **Pattern**: 照合するパターン (例: **/hello**)。
- **Metric or method to increment** メトリクスまたはメソッドの名前。
- **Increment by**: メトリクスのカウントを増やす数 (例: **1**)。
- **Last?**: このマッピングルールを最後のルールとして、他のマッピングルールの処理を停止するかどうかを定義します。
- **Position**: マッピングルール実行の順番を表す数字。マッピングルールの並べ替えに使用します。

3. **Create Mapping Rule** をクリックして、変更を適用します。

他のマッピングルールの停止

他のマッピングルールの処理を停止するには、新規マッピングルールの作成時に **Last?** を選択します。たとえば、**API Integration Settings** で以下のマッピングルールを定義し、それぞれのルールに異なるメトリクスが関連付けられている場合には、

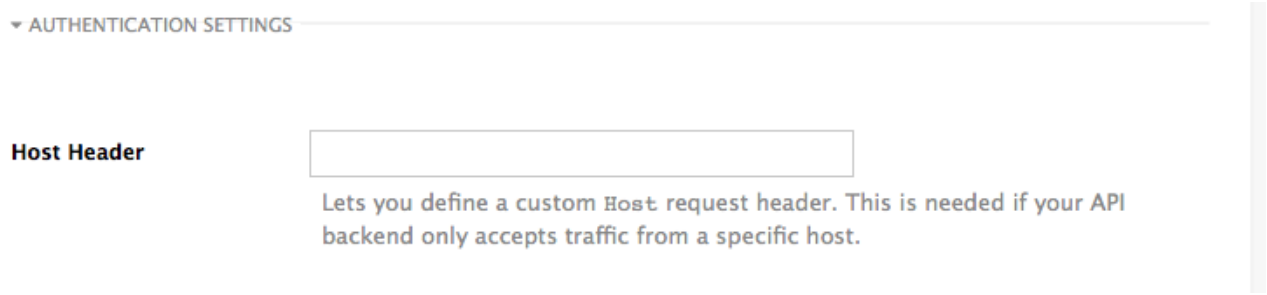
```
(get) /path/to/example/search
(get) /path/to/example/{id}
```

(get) /path/to/example/search の呼び出しを行う場合、APIcast は、残りのマッピングルールを処理してルールがマッチした際にそのメトリクスのカウントを増やすのを停止します。

1.3. HOST ヘッダー

このオプションは、**Host** ヘッダーが指定した値にマッチしない限りトラフィックを拒否する API プロダクトにのみ必要です。このような場合には、**Host** がゲートウェイの 1 つなので、ゲートウェイが API プロダクトの前にあると問題が生じます (例: **xxx-yyy.staging.apicast.io**)。

この問題を避けるには、AUTHENTICATION SETTINGS の **Host Header** フィールドで API プロダクトが想定するホストを定義します。これにより、Hosted APIcast インスタンスはホストを書き換えます。



1.4. API バックエンドの保護

APIcast が実稼動環境で動作するようになったら、クレデンシャルが提供されない API プロダクトへの直接アクセスを制限することが望まれる場合があります。そのための最も簡単な方法は、APIcast が設定するシークレットトークンを使用することです。シークレットトークンの設定方法については、高度な APIcast 設定 を参照してください。

1.5. プライベート API を扱う APICAST の使用

APIcast を使用して、インターネット上に公開されていない API を保護することができます。そのための条件は以下のとおりです。

- デプロイメントオプションとして、Self-managed APIcast を使用している。
- 一般のインターネットから APIcast へのアクセスが可能で、APIcast が 3scale Service Management API に発信の呼び出しを行うことができる。
- APIcast が API プロダクトにアクセスすることができる。

この場合には、**Private Base URL** フィールドに API の内部ドメイン名または IP アドレスを設定し、他の手順は通常どおりに実施することができます。ただし、ステージング環境のメリットが得られない点およびテストコールが成功しない点に注意して下さい。ステージング用 APIcast インスタンスは 3scale がホストし、プライベート API のバックエンドにはアクセスすることができないためです。しかし、APIcast を実稼働環境にデプロイして正しく設定すれば、APIcast は想定どおりに機能します。

1.6. APICAST への OPENTRACING の設定

OpenTracing は API の仕様でマイクロサービスのプロファイリングおよびモニターリングに使用されるメソッドです。バージョン 3.3 以降の APIcast には、OpenTracing ライブラリーおよび Jaeger Tracer ライブラリー が含まれています。

1.6.1. 前提条件

APIcast デプロイメントに分散トレーシング機能を追加するには、以下の前提条件が満たされている必要があります。

- それぞれの外部リクエストに、固有のリクエスト ID がアタッチされている (通常は HTTP ヘッダー経由)。
- それぞれのサービスがリクエスト ID を他のサービスに転送する。
- それぞれのサービスがリクエスト ID をログに出力する。
- それぞれのサービスがリクエストの開始/終了時刻等の補足情報を記録する。
- ログが集約され、HTTP リクエスト ID を使用して解析する手段を提供する。

1.6.2. 手順

OpenTracing を設定するには、以下の環境変数を使用します。

- OPENTRACING_TRACER: 使用するトレーサーの実装を定義します。現在、利用することができるのは Jaeger だけです。
- OPENTRACING_CONFIG: 使用するトレーサーのデフォルト設定ファイルを指定します。ここに例を示します。
- OPENTRACING_HEADER_FORWARD: オプション。実際の OpenTracing 設定に応じて、この環境変数を設定することができます。

これらの変数に関する詳細は、APIcast の環境変数 を参照してください。

インテグレーションが適切に機能しているかどうかをテストするには、トレースが Jaeger トレースインターフェイスで報告されるかどうかを確認する必要があります。

1.6.3. 補足情報

OpenTracing および Jaeger インテグレーションは、アップストリームプロジェクト (https://github.com/3scale/apicast) で公開されています。

1.6.4. OpenShift インスタンスへの Jaeger のインストール

本セクションでは、実行中の OpenShift インスタンスへの Jaeger のインストールについて説明します。

> **警告**
>
> Jaeger はサードパーティーコンポーネントであり、APIcast と共に使用する場合を除き 3scale はサポートを提供しません。以下の手順は参考例としてのみ提供され、実稼働環境での使用には適しません。

1. 現在の namespace に Jaeger オールインワンをインストールします。

```
oc process -f https://raw.githubusercontent.com/jaegertracing/jaeger-openshift/master/all-in-one/jaeger-all-in-one-template.yml | oc create -f -
```

2. 以下の内容で Jaeger 設定ファイル **jaeger_config.json** を作成します。

```
{
   "service_name": "apicast",
   "disabled": false,
   "sampler": {
     "type": "const",
     "param": 1
   },
   "reporter": {
     "queueSize": 100,
     "bufferFlushInterval": 10,
     "logSpans": false,
     "localAgentHostPort": "jaeger-agent:6831"
   },
   "headers": {
     "jaegerDebugHeader": "debug-id",
     "jaegerBaggageHeader": "baggage",
     "TraceContextHeaderName": "uber-trace-id",
     "traceBaggageHeaderPrefix": "testctx-"
   },
   "baggage_restrictions": {
      "denyBaggageOnInitializationFailure": false,
      "hostPort": "127.0.0.1:5778",
      "refreshInterval": 60
   }
}
```

- すべてのリクエストをサンプリングするために、**sampler** 定数を 1 に設定します。
- **reporter** の場所およびキューサイズを設定します。

- リクエストを追跡するのに使用する **TraceContextHeaderName** を含め、**headers** を設定します。

3. Jaeger 設定ファイルから ConfigMap を作成し、それを APIcast にマウントします。

```
oc create configmap jaeger-config --from-file=jaeger_config.json
oc set volumes dc/apicast --add -m /tmp/jaeger/ --configmap-name jaeger-config
```

4. 前のステップで追加した設定で、OpenTracing および Jaeger を有効にします。

```
oc set env deploymentConfig/apicast OPENTRACING_TRACER=jaeger
OPENTRACING_CONFIG=/tmp/jaeger/jaeger_config.json
```

5. Jaeger インターフェイスが動作している URL を確認します。

```
oc get route
(…) jaeger-query-myproject.127.0.0.1.nip.io
```

6. 前のステップで確認した URL から Jaeger インターフェイスを開きます。Openshift のヘルスチェックから読み込まれているデータが表示されます。

7. 最後のステップは、リクエストのトレースをすべて表示できるように、OpenTracing および Jaeger のサポートをバックエンド API に追加することです。この操作は、使用されるフレームワークおよび言語に応じてバックエンドごとに異なります。例として Using OpenTracing with Jaeger to collect Application Metrics in Kubernetes を参照してください。

Jaeger の設定に関する詳細は、以下のドキュメントを参照してください。

- Jaeger OpenShift Templates の Development setup
- Jaeger on OpenShift Production setup
- Distributed tracing on OpenShift Service Mesh

第2章 DOCKER コンテナー環境の操作

2.1. DOCKER コンテナー環境上の APICAST に関するトラブルシューティング

本セクションでは、Docker コンテナー環境上で APIcast を使用する際に直面する、もっとも典型的な問題について説明します。

2.1.1. Cannot connect to the Docker daemon エラー

docker: Cannot connect to the Docker daemon.Is the docker daemon running on this host?というエラーメッセージが表示された場合には、Docker サービスが起動していない可能性があります。**sudo systemctl status docker.service** コマンドを実行して、Docker デーモンのステータスを確認することができます。

RHEL で Docker コンテナー環境の操作を行う場合、デフォルトでは root 権限が必要なので、このコマンドは必ず **root** ユーザーとして実行してください。詳細については、このドキュメント を参照してください。

2.1.2. 基本的な Docker コマンドラインインターフェイスコマンド

デタッチモードでコンテナーを起動し (**-d** オプション)、実行中の APIcast インスタンスのログを確認する場合には、**log** コマンド (**sudo docker logs <container>**) を使用することができます。ここで、**<container>** はコンテナー名 (上記の例ではapicast) またはコンテナー ID です。**sudo docker ps** コマンドを使用して、実行中のコンテナーならびにその ID および名前を一覧表示することができます。

コンテナーを停止するには、**sudo docker stop <container>** コマンドを実行します。**sudo docker rm <container>** コマンドを実行して、コンテナーを削除することもできます。

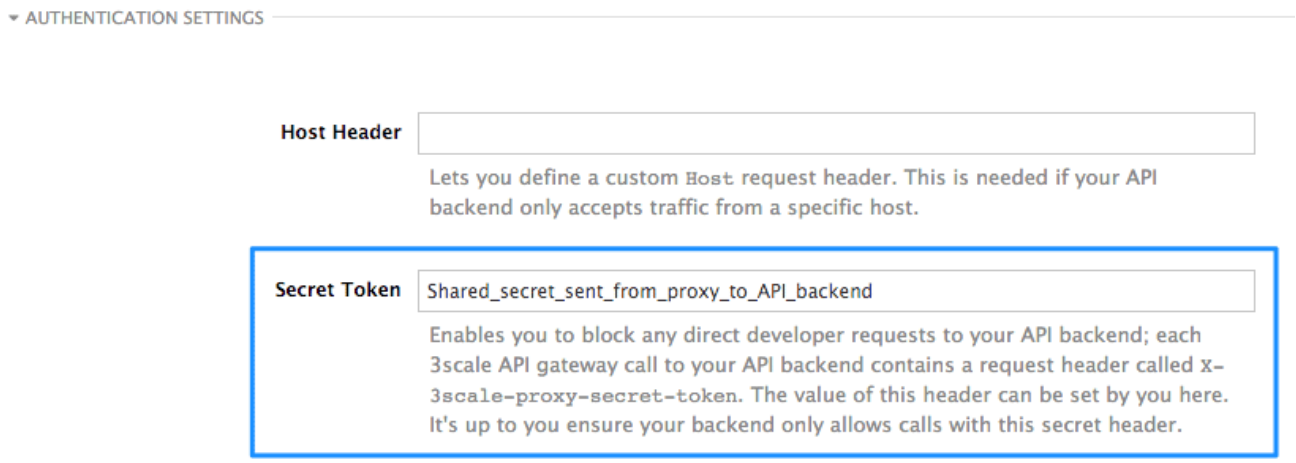
使用できるコマンドの詳細は、Docker コマンドのリファレンス を参照してください。

第3章 高度な APICAST 設定

本セクションでは、ステージング環境における 3scale の API ゲートウェイの高度な設定オプションについて説明します。

3.1. シークレットトークンの定義

セキュリティー上の理由から、3scale ゲートウェイから API バックエンドに送信されるすべてのリクエストには、**X-3scale-proxy-secret-token** というヘッダーが含まれます。Integration ページの **AUTHENTICATION SETTINGS** で、このヘッダーの値を設定することができます。



設定したシークレットトークンは、プロキシーと API 間の共有シークレットとして機能し、ゲートウェイから送信されていない API リクエストを拒否したい場合には、すべてブロックすることができます。これにより、サンドボックスゲートウェイを使用してトラフィック管理ポリシーをセットアップする際に、公開エンドポイントを保護するための新たなセキュリティーレイヤーを追加することができます。

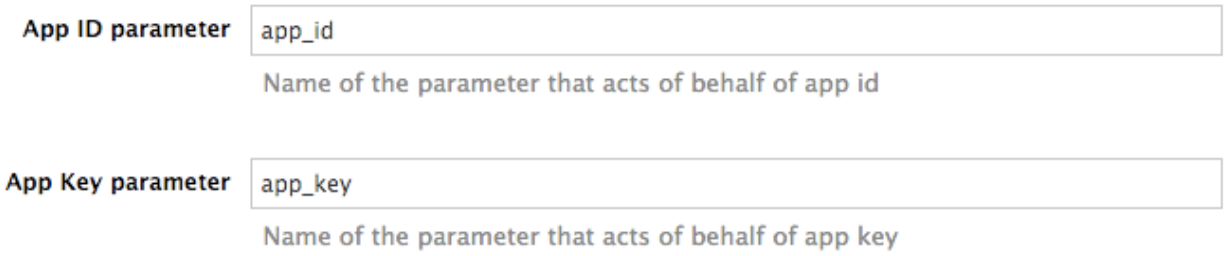
ゲートウェイが機能するためには、API バックエンドには公開されている解決可能なドメインが必要です。したがって、API バックエンドを知っていれば、誰でもクレデンシャルの確認を迂回することができます。ステージング環境の API ゲートウェイは実稼働環境での使用を想定していないので、このことが問題になることはありません。ただし、アクセスを防げるようにしておいた方が望ましいと言えます。

3.2. クレデンシャル

3scale における API クレデンシャルは、**user_key** または **app_id/app_key** のどちらかです (使用する認証モードによります)。ステージング環境の API ゲートウェイでは OpenID Connect が有効です。ただし、Integration ページでテストすることはできません。

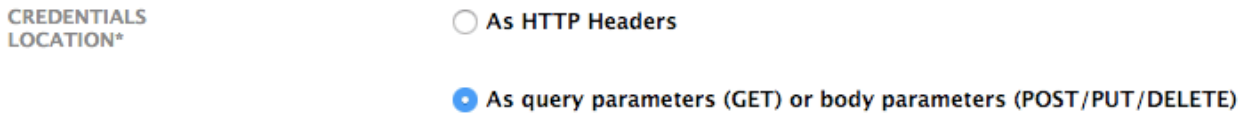
なお、API で異なるクレデンシャル名を使用することが望ましい場合もあります。この場合、API キーモードを使用していれば **user_key** にカスタムな名前を設定する必要があります。

あるいは、以下のように **app_id** および **app_key** を設定します。



たとえば、**app_id** を **key** に変えることが API にとってより適切であれば、名前を変更することができます。ゲートウェイは名前 **key** を取得し、3scale バックエンドに対して承認呼び出しを行う前に **app_id** に変換します。新しいクレデンシャル名には、英数字を使用しなければならない点に注意してください。

API がクレデンシャルを渡す際に、クエリー文字列 (GET 以外ではボディー) またはヘッダーのどちらを使用するかを定義することができます。



注記

クレデンシャルを抽出する際に、APIcast はヘッダー名を正規化します。つまり、大文字と小文字の区別をなくし、アンダースコアとハイフンを等価に扱います。たとえば、アプリケーションキーのパラメーターを **App_Key** と設定した場合には、**app-key** 等の他の値も有効なアプリケーションキーヘッダーとして受け入れられます。

3.3. エラーメッセージの設定

本セクションでは、APIcast のエラーメッセージを設定する方法について説明します。

プロキシーとして、3scale APIcast はリクエストを以下のように管理します。

- エラーがなければ、APIcast はクライアントからのリクエストを API バックエンドサーバーに渡し、API のレスポンスを変更せずにクライアントに返します。レスポンスを変更する場合には、Header Modification ポリシー を使用することができます。
- API のレスポンスが **404 Not Found** または **400 Bad Request** 等のエラーメッセージの場合には、APIcast はそのメッセージをクライアントに返します。ただし、APIcast が **Authentication missing** 等の他のエラーを検出した場合には、APIcast はエラーメッセージを送信してリクエストを終了させます。

したがって、APIcast がこれらのエラーメッセージを返すように設定することができます。

- Authentication failed: このエラーは、クレデンシャルが偽造されているか、アプリケーションが一時的に保留されているかのいずれかにより、API リクエストに有効なクレデンシャルが含まれていないことを意味します。また、このエラーはメトリクスが無効 (その値が **0**) な場合に生成されます。
- Authentication missing: API リクエストにクレデンシャルが含まれていない場合には、必ずこのエラーが生成されます。ユーザーが API リクエストにクレデンシャルを追加しなかった場合に起こります。

- No match: このエラーは、リクエストがどのマッピングルールにもマッチしなかったため、メトリクスが更新されないことを意味します。この状況は必ずしもエラーとは限りませんが、ユーザーが無効なパスを試みているか、マッピングルールが正当なケースに対応していないかのいずれかを意味します。

- Usage limit exceeded: このエラーは、リクエストしたエンドポイントに関して、クライアントが流量制御の上限に達したことを意味します。リクエストが複数のマッピングルールにマッチする場合には、クライアントは複数の流量制御の上限に達する可能性があります。

エラーを設定するには、以下の手順に従います。

1. **[Your_product_name] > Integration > Settings**から操作を行います。

2. **GATEWAY RESPONSE** セクションで設定するエラーのタイプを選択します。

3. 以下のフィールドの値を指定します。

   - Response Code: 3 桁の HTTP レスポンスコード

   - Content-type: **Content-Type** ヘッダーの値

   - Response Body: レスポンスメッセージのボディーの値

4. 変更を保存するには、**Update Product** をクリックします。

3.4. 設定履歴

Promote v.[n] to Staging APIcastをクリックするたびに (**[n]** はバージョン番号を表します)、その時点での設定が JSON ファイルに保存されます。ステージング環境のゲートウェイは、新規リクエストのたびに最新の設定を取得します。それぞれの環境 (ステージングまたは実稼働環境) について、それまでの設定ファイルの履歴をすべて確認することができます。

1. **[Your_product_name] > Integration > Configuration**から操作を行います。

2. 該当する環境 (**Staging APIcast** または **Production APIcast**) の横にある **Configuration history** のリンクをクリックします。

以前のバージョンに自動的にロールバックすることはできない点に注意してください。その代わりに、対応する JSON ファイルによりすべての設定バージョンの履歴にアクセスすることができます。これらのファイルを使用して、それぞれの時点でデプロイした設定を確認することができます。必要であれば、どのデプロイメントでも手動で作成し直すことができます。

3.5. デバッグ

ゲートウェイ設定のセットアップは簡単ですが、それでもエラーが発生する可能性があります。そのような状況のために、ゲートウェイはエラーを追跡するのに有用なデバッグ情報を返すことができます。

APIcast からデバッグ情報を取得するには、アクセスする API サービスに対応するサービストークンを指定して、ヘッダー **X-3scale-debug: {SERVICE_TOKEN}** を API リクエストに追加する必要があります。

ヘッダーが検出されサービストークンが有効であれば、ゲートウェイはレスポンスヘッダーに以下の情報を追加します。

```
X-3scale-matched-rules: /v1/word/{word}.json, /v1
X-3scale-credentials: app_key=APP_KEY&app_id=APP_ID
X-3scale-usage: usage%5Bversion_1%5D=1&usage%5Bword%5D=1
```

X-3scale-matched-rules には、リクエストにマッチしているマッピングルールのコンマ区切りリストが表示されます。

ヘッダー **X-3scale-credentials** は、3scale バックエンドに渡されたクレデンシャルを返します。

X-3scale-usage には、3scale バックエンドに報告された使用状況が表示されます。**usage%5Bversion_1%5D=1&usage%5Bword%5D=1** は **usage[version_1]=1&usage[word]=1** を URL エンコードしたもので、API リクエストによりメソッド (メトリクス) **version_1** および **word** のカウントがそれぞれ 1 増えたこと意味します。

3.6. パスルーティング

APIcast は、3scale アカウント (または **APICAST_SERVICES_LIST** 環境変数が設定されている場合にはサービスのサブセット) で設定されているすべての API サービスを処理します。通常、APIcast はリクエストのホスト名に基づいて API リクエストを適切な API サービスにルーティングします。そのために、**公開ベース URL** との照合を行います。最初にマッチしたサービスが承認に使用されます。

パスルーティング機能により、複数のサービスで同じ **公開ベース URL** を使用することができ、リクエストはリクエストのパスによりルーティングされます。この機能を有効にするには、**APICAST_PATH_ROUTING** 環境変数を **true** または **1** に設定します。有効にすると、APIcast はホスト名とパスの両方に基づいて受信したリクエストをサービスにマッピングします。

同じ **公開ベース URL** を使用して 1 つのゲートウェイを通じて異なるドメインでホストされる複数のバックエンドサービスを公開する場合に、この機能を使用することができます。そのためには、API バックエンド (つまり **プライベートベース URL**) ごとに複数の API サービスを設定し、パスルーティング機能を有効にします。

たとえば、3 つのサービスが以下のように設定されている場合、

- サービス A 公開ベース URL: **api.example.com** マッピングルール: **/a**
- サービス B 公開ベース URL: **api2.example.com** マッピングルール: **/b**
- サービス C 公開ベース URL: **api.example.com** マッピングルール: **/c**

パスルーティングが **無効** な場合には (**APICAST_PATH_ROUTING=false**)、**api.example.com** に対するすべての呼び出しはサービス A との照合を試みます。したがって、呼び出し **api.example.com/c** および **api.example.com/b** は**No Mapping Rule matched**エラーと共に失敗します。

パスルーティングが **有効** な場合には (**APICAST_PATH_ROUTING=true**)、呼び出しはホストおよびパスの両方に照合されます。したがって、

- **api.example.com/a** はサービス A にルーティングされます。
- **api.example.com/c** はサービス C にルーティングされます。
- **api.example.com/b** は No Mapping Rule matched エラーと共に失敗します。つまり、 **公開ベース URL** がマッチしないので、サービス B とはマッチしません。

パスルーティングを使用する場合には、同じ **公開ベース URL** を使用する複数のサービスにおいて、マッピングルールが競合しないようにする必要があります。つまり、メソッドとパスパターンの組み合わせは、それぞれ 1 つのサービスでしか使用することはできません。

第4章 APICAST ポリシー

APIcast ポリシーとは、APIcast の動作を変更する機能の単位です。ポリシーを有効、無効、および設定して、APIcast 動作の変更を制御することができます。ポリシーを使用して、デフォルトの APIcast デプロイメントでは利用することのできない機能を追加します。自分専用のポリシーを作成することや、Red Hat 3scale の提供する 標準ポリシー を使用することができます。

以下のトピックでは、標準 APIcast ポリシー、専用のカスタム APIcast ポリシーの作成、およびポリシーチェーンの作成について説明します。

- APIcast 標準ポリシー
- カスタム APIcast ポリシーの作成
- 3scale でのポリシーチェーンの作成

ポリシーチェーンを使用して、サービスに対するポリシーを制御します。ポリシーチェーンの機能を以下に示します。

- APIcast が使用するポリシーを指定する
- 3scale が使用するポリシーの設定情報を提供する
- 3scale がポリシーを読み込む順番を指定する

注記

Red Hat 3scale でカスタムポリシーを追加することは可能ですが、そのカスタムポリシーはサポートの対象ではありません。

カスタムポリシーを使用して APIIcast の動作を変更するには、以下の操作が必要です。

- カスタムポリシーを APIcast に追加する
- APIcast ポリシーを設定するポリシーチェーンを定義する
- ポリシーチェーンを APIcast に追加する

4.1. APICAST 標準ポリシー

3scale では、以下の標準ポリシーが利用可能です。

- 「3scale Auth Caching」
- 「3scale Batcher」
- 「3scale Referrer」
- 「Anonymous Access」
- 「Camel Service」
- 「Conditional ポリシー」
- 「Content Caching」

- 「CORS Request Handling」
- 「Custom metrics」
- 「Echo」
- 「Edge Limiting」
- 「Header Modification」
- 「IP Check」
- 「JWT Claim Check」
- 「Liquid Context Debug」
- 「Logging」
- 「Maintenance Mode」
- 「OAuth 2.0 Mutual TLS Client Authentication」
- 「OAuth 2.0 Token Introspection」
  注記: Prometheus についての詳細は、*9章Prometheus への 3scale APIcast メトリクスの公開* を参照してください。
- 「Proxy Service」
- 「Rate Limit Headers」
- 「Retry」
- 「RH-SSO/Keycloak Role Check」
- 「Routing」
- 「SOAP」
- 「TLS Client Certificate Validation」
- 「TLS Termination」
- 「Upstream」
- 「Upstream Connection」
- 「Upstream Mutual TLS」
- 「URL Rewriting」
- 「URL Rewriting with Captures」

3scale の標準ポリシーを 有効化および設定する ことができます。

4.1.1. 3scale Auth Caching

3scale Auth Caching ポリシーは、APIcast に送信された認証呼び出しをキャッシュします。動作モードを選択して、キャッシュ操作を設定することができます。

3scale Auth Caching では、以下のモードを使用することができます。

1.strict: 承認された呼び出しだけをキャッシュします。

strict モードでは、承認された呼び出しだけがキャッシュされます。ポリシーを strict モードで実行中に呼び出しが失敗または拒否されると、ポリシーはキャッシュエントリーを無効にします。バックエンドにアクセスできなくなると、キャッシュステータスにかかわらず、キャッシュされたすべての呼び出しが拒否されます。

2.resilient: バックエンドの機能が停止している場合には、最後のリクエストに基づいて承認します。

resilient モードでは、承認された呼び出しおよび拒否された呼び出しの両方がキャッシュされます。ポリシーを resilient モードで実行中は、呼び出しに失敗しても既存のキャッシュエントリーは無効になりません。バックエンドにアクセスできなくなると、キャッシュにヒットする呼び出しは、キャッシュステータスに応じて承認/拒否の状態を維持します。

3.allow: バックエンドの機能が停止している場合には、過去に拒否されていない限りすべてを許可します。

allow モードでは、承認された呼び出しおよび拒否された呼び出しの両方がキャッシュされます。ポリシーを allow モードで実行中は、キャッシュされた呼び出しはキャッシュステータスに応じて拒否/許可の状態を維持します。ただし、新規の呼び出しは承認された呼び出しとしてキャッシュされます。

重要

allow モードで運用した場合には、セキュリティーの低下が懸念されます。これらの懸念に念頭に置き、注意した上で allow モードを使用してください。

4.none: キャッシュを無効にします。

none モードでは、キャッシュが無効になります。ポリシーを有効にしたままキャッシュの使用を止める場合に、このモードが役立ちます。

設定プロパティー

プロパティー	説明	値	必須/任意
caching_type	**caching_type** プロパティーにより、キャッシュの動作モードを定義することができます。	データタイプ: 列挙文字列 [resilient, strict, allow, none]	必須

ポリシーオブジェクトの例

```
{
  "name": "caching",
  "version": "builtin",
  "configuration": {
    "caching_type": "allow"
  }
}
```

ポリシーの設定方法に関する情報は、本書の 3scale でのポリシーチェーンの作成 セクションを参照してください。

4.1.2. 3scale Batcher

標準の APIcast 承認メカニズムでは、APIcast が API リクエストを受け取るたびに、3scale バックエンド (Service Management API) に対して 1 回呼び出しが行われます。3scale Batcher ポリシーは、この標準メカニズムの代替手段を提供します。

3scale Batcher ポリシーを使用すると、承認ステータスがキャッシュされ使用状況レポートがバッチ処理されます。これにより、3scale バックエンドへのリクエスト数が大幅に削減されます。3scale Batcher ポリシーにより、レイテンシーを短縮しスループットを増やすことで、API キャストのパフォーマンスを改善できます。

3scale Batcher ポリシーが有効な場合には、APIcast は以下のフローを使用して承認を行います。

1. それぞれのリクエストにおいて、ポリシーはクレデンシャルがキャッシュされているかどうかを確認します。
   - クレデンシャルがキャッシュされている場合には、ポリシーは 3scale バックエンドに呼び出しを行う代わりに、キャッシュされた承認ステータスを使用します。
   - クレデンシャルがキャッシュされていない場合には、ポリシーはバックエンドに呼び出しを行い、残存期間 (TTL) を設定して承認ステータスをキャッシュします。
2. リクエストに対応する使用状況を直ちに 3scale バックエンドに報告する代わりに、ポリシーは使用状況のカウンターを累積して、バックエンドにバッチで報告します。累積した使用状況のカウンターは、独立したスレッドにより 1 回の呼び出しで 3scale バックエンドに報告されます (報告の頻度は設定が可能です)。

3scale Batcher ポリシーではスループットが向上しますが、精度は低下します。使用上限および現在の使用状況は 3scale に保存され、APIcast は 3scale バックエンドに呼び出しを行う時にのみ正しい承認ステータスを取得することができます。3scale Batcher ポリシーが有効な場合には、APIcast が 3scale に呼び出しを送信しない期間があります。この期間中に、呼び出しを行うアプリケーションが定義された限度を超える可能性があります。

流量制御の精度よりもスループットが重要な場合には、高負荷の API に対してこのポリシーを使用します。報告頻度および承認の TTL が流量制御の期間よりはるかに短い場合には、3scale Batcher ポリシーにより優れた精度が得られます。たとえば、流量制御が 1 日あたりで、報告頻度および承認の TTL が数分に設定されている場合などです。

3scale Batcher ポリシーでは、以下の設定設定がサポートされます。

- **auths_ttl**: 承認キャッシュの有効期限が切れる TTL を秒単位で設定します。
  - 現在の呼び出しの承認がキャッシュされている場合には、APIcast はキャッシュされた値を使用します。**auths_ttl** パラメーターで設定した時間が経過すると、APIcast はキャッシュを削除し、3scale バックエンドに呼び出しを行い承認のステータスを取得します。
  - **auths_ttl** パラメーターを **0** 以外の値に設定します。**auths_ttl** の値を **0** に設定すると、リクエストの初回キャッシュ時に承認カウンターが更新されます。その結果、流量制御が有効になりません。
- **batch_report_seconds**: APIcast が 3scale バックエンドにバッチレポートを送信する頻度を設定します。デフォルト値は **10** 秒です。

重要

このポリシーを使用するには、ポリシーチェーンで **3scale APIcast** および **3scale Batcher** ポリシーの両方を有効にします。

4.1.3. 3scale Referrer

3scale Referrer ポリシーを使用すると、**参照元フィルター** 機能が有効になります。サービスポリシーチェーンでこのポリシーが有効な場合には、APIcast は上流への **AuthRep** コールとして 3scale Referrer ポリシーの値を**Service Management API** に送信します。3scale Referrer ポリシーの値は、呼び出しの **referrer** パラメーターで送信されます。

参照元フィルター機能の仕組みの詳細については、**認証パターン**の 参照元フィルター セクションを参照してください。

4.1.4. Anonymous Access

Anonymous Access ポリシーでは、認証をせずにサービスが公開されます。このポリシーは、認証パラメーターを送信するように変更することのできないレガシーアプリケーション等の場合に有用です。Anonymous ポリシーは、API キーおよびアプリケーション ID/アプリケーションキーによる認証オプションを使用するサービスしかサポートしません。クレデンシャルをまったく持たない API リクエストに対してこのポリシーを有効にした場合には、APIcast はポリシーで設定されたデフォルトのクレデンシャルを使用して呼び出しを承認します。API の呼び出しが承認されるためには、クレデンシャルが設定されたアプリケーションが存在しアクティブでなければなりません。

アプリケーションプランを使用して、デフォルトのクレデンシャルに使用されるアプリケーションに流量制御を設定することができます。

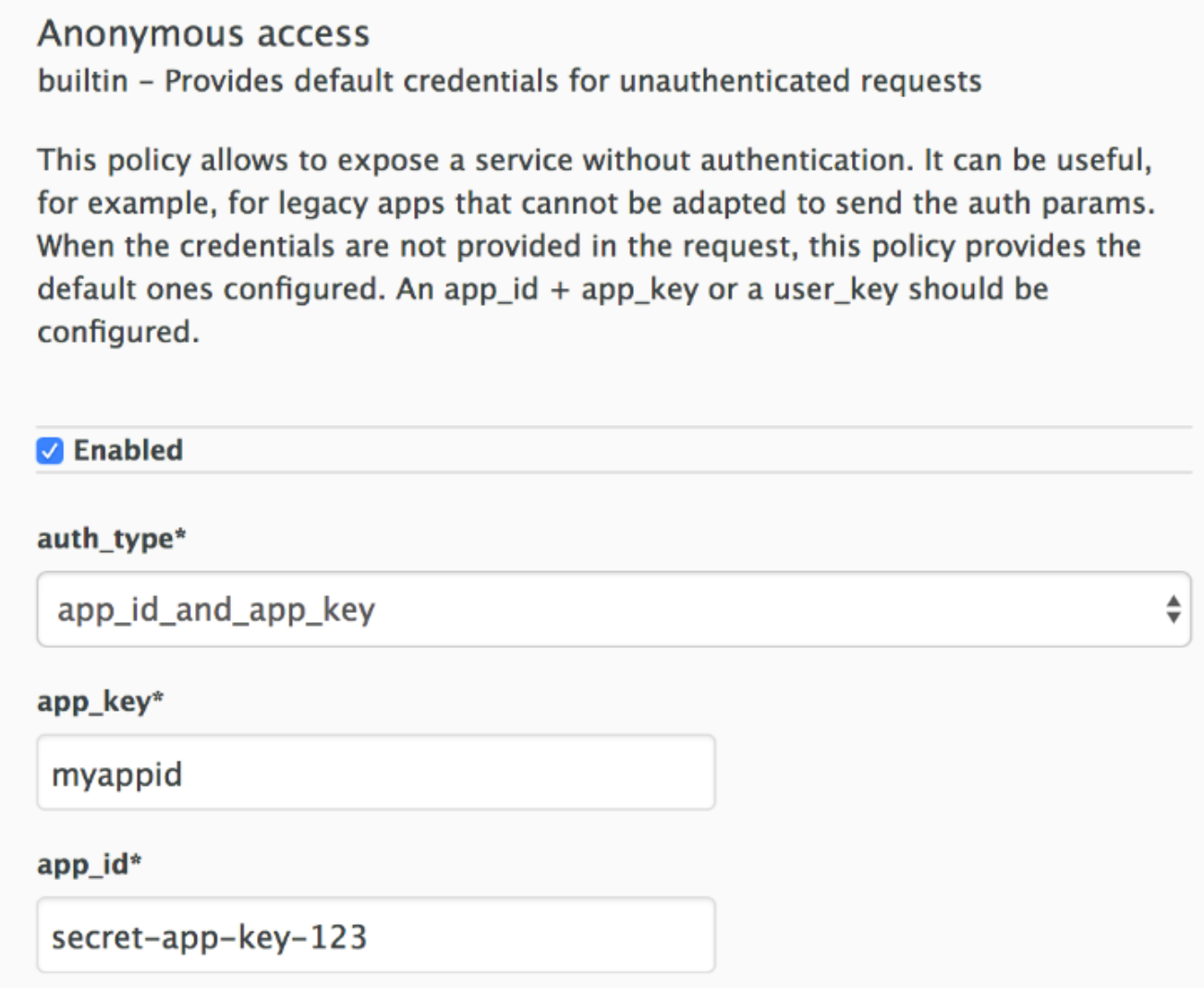
注記

APIcast ポリシーおよび Anonymous Access ポリシーをポリシーチェーンで併用する場合には、APIcast ポリシーの前に Anonymous Access ポリシーを設定する必要があります。

ポリシーに必要な設定プロパティーを以下に示します。

- **auth_type**: 以下に示す選択肢のいずれかの値を選択し、プロパティーが API に設定された認証オプションに対応している状態にします。
  - **app_id_and_app_key**: アプリケーション ID/アプリケーションキーによる認証オプション用
  - **user_key**: API キーによる認証オプション用
- **app_id** (**app_id_and_app_key** 認証タイプにのみ有効): API の呼び出しにクレデンシャルが提供されていない場合に、承認に使用するアプリケーションのアプリケーション ID。
- **app_key** (**app_id_and_app_key** 認証タイプにのみ有効): API の呼び出しにクレデンシャルが提供されていない場合に、承認に使用するアプリケーションのアプリケーションキー。
- **user_key** (**user_key** 認証タイプにのみ有効): API の呼び出しにクレデンシャルが提供されていない場合に、承認に使用するアプリケーションの API キー。

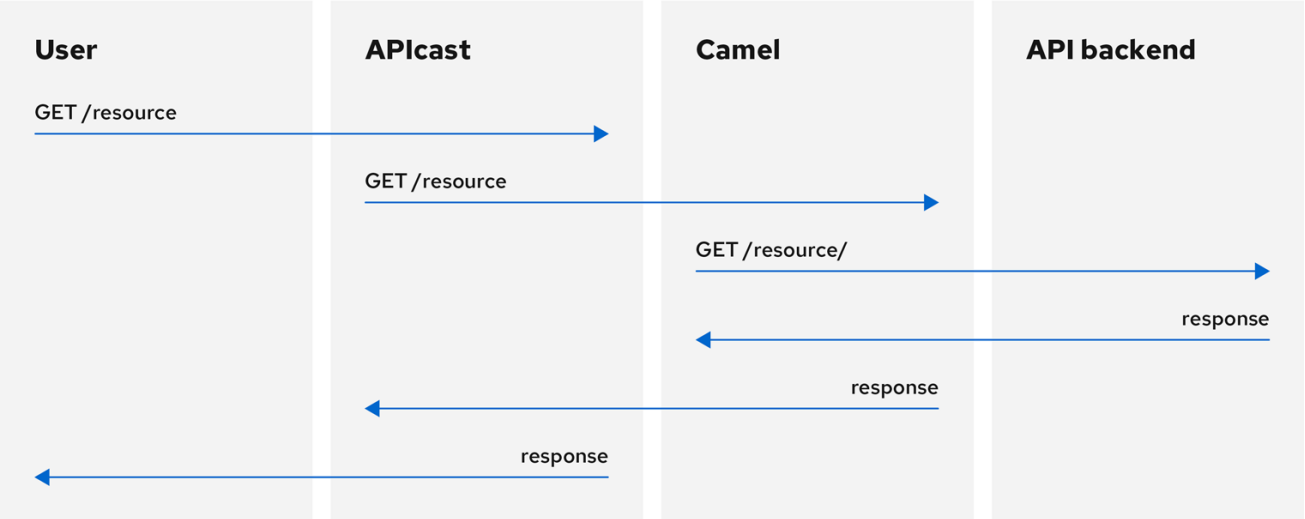
図4.1 Anonymous Access ポリシー



4.1.5. Camel Service

Camel Service ポリシーを使用して、定義した Apache Camel プロキシーを使用して 3scale のトラフィックを送信する **HTTP プロキシー** を定義することができます。この場合、Camel はリバース HTTP プロキシーとして機能し、APIcast は Camel にトラフィックを送信し、Camel がそのトラフィックを API バックエンドに送信します。

トラフィックフローの例を以下に示します。



3scale バックエンドに送信された APIcast トラフィックは、すべて Camel プロキシーを使用しません。このポリシーは、Camel プロキシーおよび APIcast と API バックエンド間の通信にのみ適用されます。

すべてのトラフィックをプロキシー経由で送信するには、**HTTP_PROXY** 環境変数を使用する必要があります。

注記

- Camel Service ポリシーはすべての負荷分散ポリシーを無効にし、トラフィックは Camel プロキシーに送信されます。
- **HTTP_PROXY**、**HTTPS_PROXY**、または **ALL_PROXY** パラメーターが定義されている場合には、このポリシーによりこれらのパラメーターの値が上書きされます。
- プロキシー接続では、認証はサポートされません。認証には Header Modification ポリシーを使用します。

4.1.5.1. 設定

ポリシーチェーンの設定例を以下に示します。

```
"policy_chain": [
  {
    "name": "apicast.policy.apicast"
  },
  {
    "name": "apicast.policy.camel",
    "configuration": {
        "all_proxy": "http://192.168.15.103:8080/",
        "http_proxy": "http://192.168.15.103:8080/",
        "https_proxy": "http://192.168.15.103:8443/"
    }
  }
]
```

http_proxy または **https_proxy** が定義されていない場合は、**all_proxy** の値が使用されます。

4.1.5.1.1. ユースケースの例

Camel Service ポリシーは、Apache Camel を使用して、3scale でより粒度の細かいポリシーおよび変換を適用できるように作られています。このポリシーは、HTTP および HTTPS を使用した Apache Camel とのインテグレーションをサポートします。詳細は、*6章Fuse のポリシーエクステンションを使用した 3scale メッセージコンテンツの変換*を参照してください。

一般的な HTTP プロキシーポリシー使用の詳細は、「Proxy Service」を参照してください。

プロジェクトの例

GitHub の Camel proxy policy で **camel-netty-proxy** の例を参照してください。このプロジェクト例には、API バックエンドからのレスポンスボディーを大文字に変換する HTTP プロキシーが示されています。

4.1.6. Conditional ポリシー

Conditional ポリシーは、ポリシーチェーンが含まれるため、他の APIcast ポリシーとは異なります。このポリシーは、**access**、**rewrite**、**log** など、各 **nginx フェーズ** で評価される条件を定義します。条件が true の場合には、Conditional ポリシーは、チェーンに含まれるポリシーごとにフェーズを実行します。

重要

APIcast の Conditional ポリシーはテクノロジープレビュー機能です。テクノロジープレビューの機能は、Red Hat の実稼働環境のサービスレベルアグリーメント (SLA) の対象外であり、機能的に完全ではないことがあります。Red Hat は実稼働環境でこれらを使用することを推奨していません。テクノロジープレビューの機能は、最新の製品機能をいち早く提供して、開発段階で機能のテストを行いフィードバックを提供していただくことを目的としています。Red Hat のテクノロジープレビュー機能のサポート範囲に関する詳細は、テクノロジープレビュー機能のサポート範囲 を参照してください。

以下の例では、Conditional ポリシーが **the request method is POST** の条件を定義していると仮定しています。

```
APIcast --> Caching --> Conditional --> Upstream

                |
                v

            Headers

                |
                v

          URL Rewriting
```

今回の例では、リクエストが **POST** の場合に、各フェーズの実行順序は以下のようになります。

1. APIcast
2. Caching

3. Headers
4. URL Rewriting
5. Upstream

リクエストが **POST** でない場合には、各フェーズの実行順序は以下のようになります。

1. APIcast
2. Caching
3. Upstream

4.1.6.1. 条件

Conditional ポリシーチェーンでポリシーを実行するかどうかを判断する条件は、**JSON** を使用して表現でき、Liquid テンプレートを使用します。

以下の例では、リクエストパスが **/example_path** かどうかを確認します。

```
{
  "left": "{{ uri }}",
  "left_type": "liquid",
  "op": "==",
  "right": "/example_path",
  "right_type": "plain"
}
```

左側のオペランドと右のオペランドの両方を Liquid または plain 文字列として評価できます。デフォルトは、Plain 文字列です。

and または **or** を使用した操作を組み合わせることができます。この設定では、以前の例の内容に加え、**Backend** ヘッダーの値を確認します。

```
{
  "operations": [
    {
      "left": "{{ uri }}",
      "left_type": "liquid",
      "op": "==",
      "right": "/example_path",
      "right_type": "plain"
    },
    {
      "left": "{{ headers['Backend'] }}",
      "left_type": "liquid",
      "op": "==",
      "right": "test_upstream",
      "right_type": "plain"
    }
  ],
  "combine_op": "and"
}
```

詳細は、policy config schema を参照してください。

4.1.6.1.1. Liquid でサポートされている変数

- uri
- host
- remote_addr
- headers['Some-Header']

変数の更新リストは ngx_variable.lua を参照してください。

以下の例では、リクエストの **Backend** ヘッダーが **staging** の場合に、アップストリームポリシーを実行します。

```
{
  "name":"conditional",
  "version":"builtin",
  "configuration":{
    "condition":{
      "operations":[
        {
          "left":"{{ headers['Backend'] }}",
          "left_type":"liquid",
          "op":"==",
          "right":"staging"
        }
      ]
    },
    "policy_chain":[
      {
        "name":"upstream",
        "version": "builtin",
        "configuration":{
          "rules":[
            {
              "regex":"/",
              "url":"http://my_staging_environment"
            }
          ]
        }
      }
    ]
  }
}
```

4.1.7. Content Caching

Content Caching ポリシーにより、カスタムの条件に基づいてキャシングを有効および無効にすることができます。アップストリームレスポンスをポリシーに使用することができないクライアントリクエストにのみ、これらの条件を適用することができます。

cache-control ヘッダーが送付される場合は、APIcast が設定するタイムアウトに優先します。

以下の設定例の場合、メソッドが GET の場合にレスポンスがキャッシュされます。

設定例

```
{
  "name": "apicast.policy.content_caching",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "cache": true,
        "header": "X-Cache-Status-POLICY",
        "condition": {
          "combine_op": "and",
          "operations": [
            {
              "left": "{{method}}",
              "left_type": "liquid",
              "op": "==",
              "right": "GET"
            }
          ]
        }
      }
    ]
  }
}
```

4.1.7.1. サポートされる設定

- **POST**、**PUT**、または **DELETE** メソッドのいずれかについて、Content Caching ポリシーを disabled に設定します。
- あるルールがマッチし、そのルールがキャッシュを有効にする場合、実行は停止しキャッシングは無効になりません。ここでは、優先度の順に設定することが重要です。

4.1.7.2. アップストリームレスポンスヘッダー

NGINX の **proxy_cache_valid** ディレクティブ情報は、**APICAST_CACHE_STATUS_CODES** および **APICAST_CACHE_MAX_TIME** ではグローバルにしか設定することができません。タイムアウトに関してアップストリームが異なる動作を要求する場合は、**Cache-Control** ヘッダーを使用します。

4.1.8. CORS Request Handling

Cross Origin Resource Sharing (CORS) Request Handling ポリシーを使用すると、以下の項目を指定することができるので CORS の動作の制御が可能です。

- 許可されるヘッダー
- 許可されるメソッド
- 許可されるクレデンシャル
- 許可されるオリジンヘッダー

CORS Request Handling ポリシーにより、指定されていない CORS リクエストはすべてブロックされます。

注記

APIcast ポリシーおよび CORS Request Handling ポリシーをポリシーチェーンで併用する場合には、APIcast ポリシーの前に CORS Request Handling ポリシーを設定する必要があります。

設定プロパティー

プロパティー	説明	値	必須/任意
allow_headers	**allow_headers** プロパティーでは、APIcast が許可する CORS ヘッダーを配列として指定することができます。	データタイプ: 文字列の配列 (CORS ヘッダーでなければなりません)	任意
allow_methods	**allow_methods** プロパティーでは、APIcast が許可する CORS メソッドを配列として指定することができます。	データタイプ: 列挙文字列の配列 [GET, HEAD, POST, PUT, DELETE, PATCH, OPTIONS, TRACE, CONNECT]	任意
allow_origin	**allow_origin** プロパティーでは、APIcast が許可するオリジンのドメインを指定することができます。	データタイプ: 文字列	任意
allow_credentials	**allow_credentials** プロパティーでは、APIcast がクレデンシャルの設定された CORS リクエストを許可するかどうかを指定することができます。	データタイプ: ブール値	任意

ポリシーオブジェクトの例

```
{
  "name": "cors",
  "version": "builtin",
  "configuration": {
    "allow_headers": [
      "App-Id", "App-Key",
      "Content-Type", "Accept"
    ],
    "allow_credentials": true,
    "allow_methods": [
      "GET", "POST"
    ],
```

```
    "allow_origin": "https://example.com"
  }
}
```

ポリシーの設定方法に関する情報は、本書の 3scale でのポリシーチェーンの作成 セクションを参照してください。

4.1.9. Custom metrics

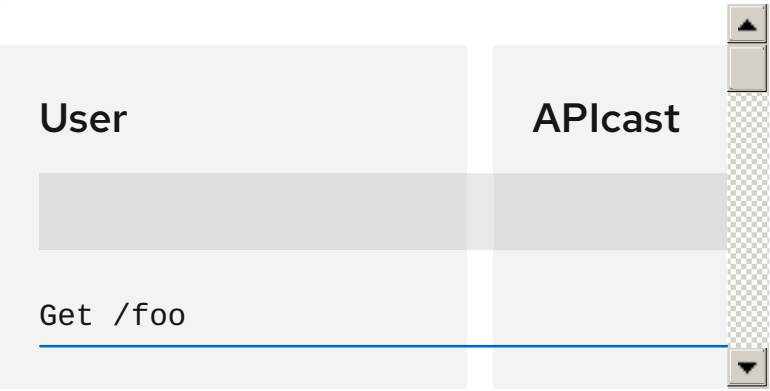
Custom metrics ポリシーにより、アップストリーム API によって送信されるレスポンスの後にメトリクスを追加することができます。このポリシーの主なユースケースは、レスポンスコードのステータス、ヘッダー、またはさまざまな NGINX 変数に基づいてメトリクスを追加する場合です。

4.1.9.1. Custom metrics の制限

- リクエストがアップストリーム API に送信される前に認証が行われると、新しいメトリクスをアップストリーム API に報告するために、バックエンドに 2 番目の呼び出しが行われます。
- このポリシーは、バッチ処理のポリシーとは機能しません。
- ポリシーがメトリクスの値をプッシュする前に、管理ポータルでメトリクスを作成する必要があります。

4.1.9.2. リクエストフローの例

以下のチャートは、認証がキャッシュされていない場合のリクエストフローの例と、認証がキャッシュされている場合のフローを示しています。



4.1.9.3. 設定例

このポリシーは、アップストリーム API が 400 のステータスを返すと、ヘッダーインクリメントだけメトリクス error のカウントを増やします。

```
{
  "name": "apicast.policy.custom_metrics",
  "configuration": {
    "rules": [
      {
        "metric": "error",
        "increment": "{{ resp.headers['increment'] }}",
        "condition": {
          "operations": [
            {
```

```
            "right": "{{status}}",
            "right_type": "liquid",
            "left": "400",
            "op": "=="
          }
        ],
        "combine_op": "and"
      }
    }
  ]
}
}
```

このポリシーは、アップストリーム API が 200 のステータスを返すと、status_code 情報により hits メトリクスのカウントを増やします。

```
{
  "name": "apicast.policy.custom_metrics",
  "configuration": {
    "rules": [
      {
        "metric": "hits_{{status}}",
        "increment": "1",
        "condition": {
          "operations": [
            {
              "right": "{{status}}",
              "right_type": "liquid",
              "left": "200",
              "op": "=="
            }
          ],
          "combine_op": "and"
        }
      }
    ]
  }
}
```

4.1.10. Echo

Echo ポリシーは、受信したリクエストを出力してクライアントに返します。また、オプションで任意の HTTP ステータスコードを返します。

設定プロパティー

プロパティー	説明	値	必須/任意
status	Echo ポリシーがクライアントに返す HTTP ステータスコード	データタイプ: 整数	任意

プロパティー	説明	値	必須/任意
exit	Echo ポリシーが使用する終了モードを指定します。**request** 終了モードは、受信したリクエストの処理を停止します。**set** 終了モードは書き換えフェーズを省略します。	データタイプ: 列挙文字列 [request, set]	必須

ポリシーオブジェクトの例

```
{
  "name": "echo",
  "version": "builtin",
  "configuration": {
    "status": 404,
    "exit": "request"
  }
}
```

ポリシーの設定方法に関する情報は、本書の 3scale でのポリシーチェーンの作成 セクションを参照してください。

4.1.11. Edge Limiting

Edge Limiting ポリシーの目的は、バックエンド API に送信されるトラフィックに対する柔軟な流量制御を提供することで、このポリシーをデフォルトの 3scale 承認メカニズムと共に使用することができます。このポリシーでサポートされるユースケースの例を以下に示します。

- エンドユーザーの流量制御: リクエストの認証ヘッダーで渡される JWT トークンの **sub** (subject) クレームの値による流量制御。**{{ jwt.sub }}** として設定されます。
- 1 秒あたりのリクエスト数 (RPS) 流量制御
- サービスごとのグローバル流量制御: アプリケーションごとではなく、サービスごとに流量制御を適用します。
- 同時接続上限: 許容される同時接続の数を設定します。

4.1.11.1. 制限のタイプ

このポリシーでは、lua-resty-limit-traffic ライブラリーにより提供される以下の制限タイプがサポートされます。

- **leaky_bucket_limiters**: 平均リクエスト数および最大バーストサイズをベースとする、リーキーバケットアルゴリズムに基づきます。
- **fixed_window_limiters**: 特定の期間に基づきます (最後の n 秒) 。

- **connection_limiters**: 同時接続の数に基づきます。

すべての制限をサービスごとまたはグローバルに適用することができます。

4.1.11.2. 制限の定義

リミッターはキーを持ち、制限を定義するのに使用するエンティティーをこのキーでエンコードします (IP アドレス、サービス、エンドポイント、ID、特定ヘッダーの値、その他のエンティティー等)。このキーは、リミッターの **key** パラメーターで指定します。

key は以下のプロパティーで定義されるオブジェクトです。

- **name**: キーの名前を定義します。スコープ内で一意でなければなりません。
- **scope**: キーのスコープを定義します。サポートされるスコープは以下のとおりです。
  - **service**: 1 つのサービスに影響を及ぼすサービスごとのスコープ
  - **global**: すべてのサービスに影響を及ぼすグローバルスコープ
- **name_type**: **name** の値がどのように評価されるかを定義します。
  - **plain**: プレーンテキストとして評価される。
  - **liquid**: Liquid として評価される。

それぞれの制限は、そのタイプに応じたパラメーターも持ちます。

- **leaky_bucket_limiters**: **rate** および **burst**
  - **rate**: 遅延を生じることなく実行できる 1 秒あたりのリクエスト数を定義します。
  - **burst**: 許容レートを超えることのできる 1 秒あたりのリクエスト数を定義します。**rate** で指定される許容レートを超えるリクエストには、人為的な遅延が適用されます。1 秒あたりのリクエスト数が **burst** で定義されるレートを超えると、リクエストは拒否されます。
- **fixed_window_limiters**: **count**、**window**。**count** は、**window** で定義される秒数あたりに実行できるリクエスト数を定義します。
- **connection_limiters**: **conn**、**burst**、および **delay**
  - **conn**: 許容される同時接続の最大数を定義します。**burst** で定義される 1 秒あたりの接続数までこの値を超えることができます。
  - **delay**: 制限を超えた接続を遅延させる秒数を定義します。

例

- service_A に対するリクエストを毎分 10 回許可します。

```
{
  "key": { "name": "service_A" },
  "count": 10,
  "window": 60
}
```

- burst を 10、delay を 1 秒に設定して、100 の同時接続を許可します。

```
{
  "key": { "name": "service_A" },
  "conn": 100,
  "burst": 10,
  "delay": 1
}
```

サービスごとにさまざまな制限を定義することができます。複数の制限を定義した場合には、少なくとも 1 つの制限に達すると、リクエストは拒否または遅延されます。

4.1.11.3. Liquid テンプレート

Edge Limiting ポリシーではキーに Liquid 変数がサポートされるので、動的なキーに制限を指定することができます。そのためには、キーの **name_type** パラメーターを **liquid** に設定する必要があります。これにより、**name** パラメーターに Liquid 変数を使用することができます。たとえば、クライアント IP アドレスの場合は **{{ remote_addr }}**、JWT トークンの **sub** クレームの場合は **{{ jwt.sub }}** を設定します。

例

```
{
  "key": { "name": "{{ jwt.sub }}", "name_type": "liquid" },
  "count": 10,
  "window": 60
}
```

Liquid のサポートに関する詳細な情報は、「ポリシーでの変数およびフィルターの使用」を参照してください。

4.1.11.4. 条件の適用

各リミッターには、リミッターが適用されるタイミングを定義する条件がなければなりません。条件は、リミッターの **condition** プロパティーで指定します。

以下のプロパティーで **condition** を定義します。

- **combine_op**: 演算の一覧に適用されるブール演算子です。**or** および **and** の値がサポートされます。
- **operations**: 評価する必要がある条件のリストです。各演算は、以下のプロパティーを持つオブジェクトにより表されます。
  - **left**: 演算の左側部分
  - **left_type**: **left** プロパティーがどのように評価されるか (plain または liquid)。
  - **right**: 演算の右側部分
  - **right_type**: **right** プロパティーがどのように評価されるか (plain または liquid)。
  - **op**: 左右の部分の間に適用される演算子。**==** (等しい) および **!=** (等しくない) の 2 つの値がサポートされます。

例

```
"condition": {
  "combine_op": "and",
  "operations": [
    {
      "op": "==",
      "right": "GET",
      "left_type": "liquid",
      "left": "{{ http_method }}",
      "right_type": "plain"
    }
  ]
}
```

4.1.11.5. 流量制御カウンター用ストレージの設定

デフォルトでは、Edge Limiting ポリシーは流量制御カウンターに OpenResty 共有ディクショナリーを使用します。ただし、共有ディクショナリーの代わりに外部の Redis サーバーを使用することができます。この設定は、複数の APIcast インスタンスがデプロイされている場合に役立ちます。**redis_url** パラメーターを使用して Redis サーバーを設定することができます。

4.1.11.6. エラー処理

リミッターでは、エラーの処理方法を設定するために以下のパラメーターがサポートされます。

- **limits_exceeded_error**: 設定した上限を超えた際にクライアントに返されるエラーステータスコードおよびメッセージを指定します。以下のパラメーターを設定する必要があります。
  - **status_code**: 上限を超えた際のリクエストのステータスコード。デフォルトは **429** です。
  - **error_handling**: 以下のオプションを使用して、エラーの処理方法を指定します。
    - **exit**: リクエストの処理を中止し、エラーメッセージを返します。
    - **log**: リクエストの処理を完了し、出力ログを返します。
- **configuration_error**: 設定が正しくない場合にクライアントに返されるエラーステータスコードおよびメッセージを指定します。以下のパラメーターを設定する必要があります。
  - **status_code**: 設定に問題がある場合のステータスコード。デフォルトは **500** です。
  - **error_handling**: 以下のオプションを使用して、エラーの処理方法を指定します。
    - **exit**: リクエストの処理を中止し、エラーメッセージを返します。
    - **log**: リクエストの処理を完了し、出力ログを返します。

4.1.12. Header Modification

Header Modification ポリシーを使用すると、受信したリクエストまたはレスポンスに関して、既存のヘッダーを変更する、補足のヘッダーを定義して追加する、またはヘッダーを削除することができます。レスポンスヘッダーおよびリクエストヘッダーの両方を変更することができます。

Header Modification ポリシーでは、以下の設定パラメーターがサポートされます。

- **request**: リクエストヘッダーに適用する操作のリスト

- **response**: レスポンスヘッダーに適用する操作のリスト

それぞれの操作は、以下のパラメーターで設定されます。

- **op**: 適用する操作を指定します。**add** 操作は既存のヘッダーに値を追加します。**set** 操作はヘッダーおよび値を作成し、既存のヘッダーの値が既に存在する場合はその値を上書きします。**push** 操作はヘッダーおよび値を作成しますが、既存のヘッダーの値が既に存在していてもその値を上書きしません。その代わりに、**push** は既存のヘッダーに値を追加します。**delete** 操作はヘッダーを削除します。

- **header**: 作成または変更するヘッダーを指定します。ヘッダー名には任意の文字列を使用することができます (例: **Custom-Header**)。

- **value_type**: ヘッダーの値がどのように評価されるかを定義します。プレーンテキストの場合の **plain** または Liquid テンプレートとして評価する場合の **liquid** いずれかに設定します。詳細は、「ポリシーでの変数およびフィルターの使用」 を参照してください。

- **value**: ヘッダーに使用される値を指定します。値のタイプが liquid の場合には、値は **{{ variable_from_context }}** の形式にする必要があります。削除する場合には不要です。

ポリシーオブジェクトの例

```
{
  "name": "headers",
  "version": "builtin",
  "configuration": {
    "response": [
      {
        "op": "add",
        "header": "Custom-Header",
        "value_type": "plain",
        "value": "any-value"
      }
    ],
    "request": [
      {
        "op": "set",
        "header": "Authorization",
        "value_type": "plain",
        "value": "Basic dXNlcm5hbWU6cGFzc3dvcmQ="
      },
      {
        "op": "set",
        "header": "Service-ID",
        "value_type": "liquid",
        "value": "{{service.id}}"
      }
    ]
  }
}
```

ポリシーの設定方法に関する情報は、本書の 3scale でのポリシーチェーンの作成 セクションを参照してください。

4.1.13. IP Check

IP Check ポリシーは、IP のリストに基づいてリクエストを拒否または許可するために使用します。

設定プロパティー

プロパティー	説明	データタイプ	必須/任意
check_type	**check_type** プロパティーには、**whitelist** または **blacklist** の 2 つの値を指定することができます。**blacklist** は、リスト上の IP からのリクエストをすべて拒否します。**whitelist** は、リスト上に **ない** IP からのリクエストをすべて拒否します。	文字列 (**whitelist** または **blacklist** のどちらかでなければなりません)	必須
ips	**ips** プロパティーでは、ホワイトリストまたはブラックリストに登録する IP アドレスのリストを指定することができます。個別の IP および CIDR 範囲の両方を使用することができます。	文字列の配列 (有効な IP アドレスでなければなりません)	必須
error_msg	**error_msg** プロパティーを使用して、リクエストが拒否された時に返されるエラーメッセージを設定することができます。	文字列	任意
client_ip_sources	**client_ip_sources** プロパティーでは、クライアント IP の取得方法を設定することができます。デフォルトでは、最後に呼び出しを実施した IP が使用されます。これ以外のオプションは、**X-Forwarded-For** および **X-Real-IP** です。	文字列の配列。有効なオプションは、**X-Forwarded-For**、**X-Real-IP**、および **last_caller** です (複数の選択が可能です)。	任意

ポリシーオブジェクトの例

```
{
  "name": "ip_check",
  "configuration": {
    "ips": [ "3.4.5.6", "1.2.3.0/4" ],
    "check_type": "blacklist",
```

```
    "client_ip_sources": ["X-Forwarded-For", "X-Real-IP", "last_caller"],
    "error_msg": "A custom error message"
  }
}
```

ポリシーの設定方法に関する情報は、本書の 3scale でのポリシーチェーンの作成 セクションを参照してください。

4.1.14. JWT Claim Check

JWT Claim Check ポリシーを使用すると、JSON Web Token (JWT) クレームに基づきリソースターゲットおよびメソッドをブロックする、新たなルールを定義することができます。

4.1.14.1. JWT Claim Check ポリシーの概要

JWT クレームの値に基づいてルーティングするためには、ポリシーチェーンには、ポリシーが共有するコンテキストで JWT を検証してクレームを格納するポリシーが必要です。

JWT Claim Check ポリシーがリソースおよびメソッドをブロックしている場合には、ポリシーは JWT 操作も検証します。一方、メソッドおよびリソースがマッチしない場合には、リクエストはバックエンド API に送信されます。

以下の GET リクエストの例では、JWT には管理者として role クレームが必要です。もしなければ、リクエストは拒否されます。一方、GET 以外のリクエストは JWT 操作を検証しないため、POST リソースは JWT の制約なしに許可されます。

```
{
  "name": "apicast.policy.jwt_claim_check",
  "configuration": {
      "error_message": "Invalid JWT check",
      "rules": [
          {
              "operations": [
                  {"op": "==", "jwt_claim": "role", "jwt_claim_type": "plain", "value": "admin"}
              ],
              "combine_op":"and",
              "methods": ["GET"],
              "resource": "/resource",
              "resource_type": "plain"
          }
      ]
  }
}
```

4.1.14.2. ポリシーチェーンへの JWT Claim Check ポリシーの設定

ポリシーチェーンで JWT Claim Check ポリシーを設定するには、以下を行います。

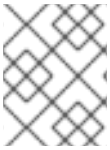
前提条件:

- 3scale システムにアクセスできること。
- すべてのデプロイメントが完了していること。

4.1.14.2.1. ポリシーの設定

1. 管理ポータルでのポリシーの有効化 に記載の手順に従って JWT Claim Check を選択し、API に JWT Claim Check ポリシーを追加します。
2. **JWT Claim Check**のリンクをクリックします。
3. **Enabled** のチェックボックスを選択し、ポリシーを有効にします。
4. ルールを追加するには、プラス (**+**) アイコンをクリックします。
5. **resource_type** を指定します。
6. 演算子を選択します。
7. ルールによって制御される **resource** を指定します。
8. 許可されるメソッドを追加するには、プラス (**+**) アイコンをクリックします。
9. トラフィックがブロックされた時にユーザーに表示するエラーメッセージを入力します。
10. API への JWT Claim Check ポリシーの設定が完了したら、**Update Policy** をクリックします。
    - 該当するセクションのプラス (**+**) アイコンをクリックして、さらにリソースタイプおよび許可されるメソッドを追加することができます。
11. **Update Policy Chain** をクリックして変更を保存します。

4.1.15. Liquid Context Debug



注記

Liquid Context Debug ポリシーの想定は、開発環境でのデバッグ用途のみで、実稼働環境での使用は意図されていません。

このポリシーは **JSON** を使用して API リクエストに応答します。コンテキストで利用可能なオブジェクトおよび値を含み、Liquid テンプレートの評価に使用することができます。3scale APIcast または Upstream ポリシーと組み合わせる場合には、正常な動作のためにポリシーチェーンではこれらのポリシーの前に Liquid Context Debug ポリシーを設定する必要があります。循環参照を避けるために、ポリシーには重複するオブジェクトは 1 回だけ含め、それをスタブ値で置き換えます。

このポリシーが有効な時に APIcast が返す値の例を以下に示します。

```
{
  "jwt": {
    "azp": "972f7b4f",
    "iat": 1537538097,
    ...
    "exp": 1537574096,
    "typ": "Bearer"
  },
  "credentials": {
    "app_id": "972f7b4f"
  },
  "usage": {
    "deltas": {
```

```
        "hits": 1
      },
      "metrics": [
        "hits"
      ]
    },
    "service": {
      "id": "2",
      ...
    }
    ...
  }
```

4.1.16. Logging

Logging ポリシーには 2 つの目的があります。

- アクセスログの出力を有効および無効にする。
- それぞれのサービスごとにカスタムアクセスログのフォーマットを作成し、カスタムアクセスログ書き込みの条件を設定できるようにする。

Logging ポリシーとアクセスログの場所のグローバル設定を組み合わせることができます。APIcast アクセスログの場所を設定するには、**APICAST_ACCESS_LOG_FILE** 環境変数を設定します。デフォルトでは、この変数は標準出力デバイスの **/dev/stdout** に設定されています。グローバル APIcast パラメーターに関する詳細な情報は、???を参照してください。

また、Logging ポリシー機能に関する補足情報を以下に示します。

- このポリシーは、**enable_access_logs** 設定パラメーターしかサポートしません。
- アクセスログを有効にするには、**enable_access_logs** パラメーターを選択するか、Logging ポリシーを無効にします。
- API のアクセスログを無効にするには、以下の手順を実施します。
  1. ポリシーを有効にします。
  2. **enable_access_logs** パラメーターの選択を解除します。
  3. **Submit** ボタンをクリックします。
- デフォルトでは、このポリシーはポリシーチェーンで有効になっていません。

4.1.16.1. すべての API に対するグローバル設定

Logging オプションは、API でログが正しくフォーマットされない問題を避けるのに役立ちます。カスタム APIcast 環境変数を設定して、すべての API に Logging ポリシーを実装することができます。すべてのサービスに読み込まれるポリシーの例を以下に示します (**custom_env.lua**)。

```
local cjson = require('cjson')
local PolicyChain = require('apicast.policy_chain')
local policy_chain = context.policy_chain

local logging_policy_config = cjson.decode([[
{
```

```
  "enable_access_logs": false,
  "custom_logging": "\"{{request}}\" to service {{service.id}} and {{service.name}}"
}
]])

policy_chain:insert( PolicyChain.load_policy('logging', 'builtin', logging_policy_config), 1)

return {
  policy_chain = policy_chain,
  port = { metrics = 9421 },
}
```

この特定の環境を指定して APIcast を実行するには、以下のコマンドを実行します。

```
docker run --name apicast --rm -p 8080:8080 \
   -v $(pwd):/config \
   -e APICAST_ENVIRONMENT=/config/custom_env.lua \
   -e THREESCALE_PORTAL_ENDPOINT=https://ACCESS_TOKEN@ADMIN_PORTAL_DOMAIN \
   quay.io/3scale/apicast:master
```

考慮すべき Docker コマンドの重要な概念を以下に示します。

- 有効な Lua ファイルをコンテナーに共有する必要がある (**-v $(pwd):/config**)。
- APICAST_ENVIRONMENT 変数を **/config** ディレクトリーに保存される Lua ファイルに設定する必要がある。

4.1.16.2. 例

本セクションでは、Logging ポリシーを使用した例について説明します。ここに示す例では、以下の条件を考慮しています。

- **custom_logging** または **enable_json_logs** プロパティーが有効な場合には、デフォルトのアクセスログは無効になる。
- **enable_json_logs** が有効な場合には、**custom_logging** フィールドは省略される。

アクセスログの無効化

```
{
  "name": "apicast.policy.logging",
  "configuration": {
    "enable_access_logs": false
  }
}
```

カスタムアクセスログの有効化

```
{
  "name": "apicast.policy.logging",
  "configuration": {
    "enable_access_logs": false,
    "custom_logging": "[{{time_local}}] {{host}}:{{server_port}} {{remote_addr}}:{{remote_port}} \"
```

```
{{request}}\" {{status}} {{body_bytes_sent}} ({{request_time}}) {{post_action_impact}}",
  }
}
```

サービスを識別した上でのカスタムアクセスログの有効化

```
{
  "name": "apicast.policy.logging",
  "configuration": {
    "enable_access_logs": false,
    "custom_logging": "\"{{request}}\" to service {{service.id}} and {{service.name}}",
  }
}
```

JSON 形式でのアクセスログの設定

```
{
  "name": "apicast.policy.logging",
  "configuration": {
    "enable_access_logs": false,
    "enable_json_logs": true,
    "json_object_config": [
      {
        "key": "host",
        "value": "{{host}}",
        "value_type": "liquid"
      },
      {
        "key": "time",
        "value": "{{time_local}}",
        "value_type": "liquid"
      },
      {
        "key": "custom",
        "value": "custom_method",
        "value_type": "plain"
      }
    ]
  }
}
```

正常なリクエストのみに対するカスタムアクセスログの設定

```
{
  "name": "apicast.policy.logging",
  "configuration": {
    "enable_access_logs": false,
    "custom_logging": "\"{{request}}\" to service {{service.id}} and {{service.name}}",
    "condition": {
      "operations": [
        {"op": "==", "match": "{{status}}", "match_type": "liquid", "value": "200"}
      ],
      "combine_op": "and"
```

```
    }
  }
}
```

レスポンスのステータスが 200 または 500 のいずれかにマッチする場合のアクセスログのカスタマイズ

```
{
  "name": "apicast.policy.logging",
  "configuration": {
    "enable_access_logs": false,
    "custom_logging": "\"{{request}}\" to service {{service.id}} and {{service.name}}",
    "condition": {
      "operations": [
        {"op": "==", "match": "{{status}}", "match_type": "liquid", "value": "200"},
        {"op": "==", "match": "{{status}}", "match_type": "liquid", "value": "500"}
      ],
      "combine_op": "or"
    }
  }
}
```

4.1.16.3. カスタムロギングに関する補足情報

カスタムロギングでは、エクスポートした変数と共に Liquid テンプレートを使用することができます。この変数の例を以下に示します。

- NGINX デフォルトディレクティブ変数: log_format。たとえば **{{remote_addr}}**。
- レスポンスおよびリクエストヘッダー:
  - **{{req.headers.FOO}}**: リクエストの FOO ヘッダーを取得する。
  - **{{res.headers.FOO}}**: レスポンスの FOO ヘッダーを取得する。
- サービス情報 (例: **{{service.id}}**)、および以下のパラメーターにより提供されるすべてのサービスプロパティー:
  - THREESCALE_CONFIG_FILE
  - THREESCALE_PORTAL_ENDPOINT

4.1.17. Maintenance Mode

Maintenance Mode ポリシーを使用すると、指定したステータスコードおよびメッセージと共に受信したリクエストを拒否することができます。このポリシーは、メンテナーンス期間または API を一時的にブロックする場合に役立ちます。

設定プロパティー

設定可能なプロパティーおよびデフォルト値を、以下のリストに示します。

プロパティー	値	デフォルト	説明
status	整数 (**オプション**)	503	レスポンスコード
message	文字列 (**オプション**)	503 Service Unavailable - Maintenance	レスポンスのメッセージ

Maintenance Mode ポリシーの例

```
{
  "policy_chain": [
    {"name": "maintenance-mode", "version": "1.0.0",
    "configuration": {"message": "Be back soon..", "status": 503} },
  ]
}
```

ポリシーの設定方法に関する情報は、本書の 3scale でのポリシーチェーンの作成 セクションを参照してください。

4.1.18. OAuth 2.0 Mutual TLS Client Authentication

このポリシーは、全 API コールに対して OAuth 2.0 相互 TLS クライアント認証を実行します。

OAuth 2.0 Mutual TLS Client Authentication ポリシーの **JSON** の例を以下に示します。

```
{
  "$schema": "http://apicast.io/policy-v1/schema#manifest#",
  "name": "OAuth 2.0 Mutual TLS Client Authentication",
  "summary": "Configure OAuth 2.0 Mutual TLS Client Authentication.",
  "description": ["This policy executes OAuth 2.0 Mutual TLS Client Authentication ",
    "(https://tools.ietf.org/html/draft-ietf-oauth-mtls-12) for every API call."
  ],
  "version": "builtin",
  "configuration": {
    "type": "object",
    "properties": { }
  }
}
```

4.1.19. OAuth 2.0 Token Introspection

OAuth 2.0 Token Introspection ポリシーを使用すると、OpenID Connect (OIDC) 認証オプションを用いるサービスに使用される JSON Web Token (JWT) トークンを検証することができます。この場合、トークン発行者 (Red Hat Single Sign-On) のトークンイントロスペクションエンドポイントを使用します。

トークンイントロスペクションエンドポイントおよびそのエンドポイントに呼び出しを行う際に APIcast が使用するクレデンシャルを定義する場合、**auth_type** フィールドでは以下の認証タイプがサポートされます。

- **use_3scale_oidc_issuer_endpoint**: APIcast は、クライアントのクレデンシャル (**クライアント ID** および **クライアントシークレット**) ならびに Service Integration ページで定義した OIDC

発行者設定からのトークンイントロスペクションエンドポイントを使用します。APIcast は、**token_introspection_endpoint** フィールドからトークンイントロスペクションエンドポイントを検出します。このフィールドは、OIDC 発行者が返す **.well-known/openid-configuration** エンドポイントにあります。

例4.1 use_3scale_oidc_issuer_endpoint に設定された認証タイプ

```
"policy_chain": [
…
  {
    "name": "apicast.policy.token_introspection",
    "configuration": {
      "auth_type": "use_3scale_oidc_issuer_endpoint"
    }
  }
…
],
```

- **client_id+client_secret**: このオプションでは、APIcast がトークン情報を要求するのに使用する **クライアント ID** および **クライアントシークレット** と共に、異なるトークンイントロスペクションエンドポイントを指定することができます。このオプションを使用する場合には、以下の設定パラメーターを定義します。
  - **client_id**: トークンイントロスペクションエンドポイント用のクライアント ID を設定します。
  - **client_secret**: トークンイントロスペクションエンドポイント用のクライアントシークレットを設定します。
  - **introspection_url**: イントロスペクションエンドポイントの URL を設定します。

例4.2 client_id+client_secret に設定された認証タイプ

```
"policy_chain": [
…
  {
    "name": "apicast.policy.token_introspection",
    "configuration": {
      "auth_type": "client_id+client_secret",
      "client_id": "myclient",
      "client_secret": "mysecret",
      "introspection_url": "http://red_hat_single_sign-on/token/introspection"
    }
  }
…
],
```

auth_type フィールドの設定にかかわらず、APIcast は Basic 認証を使用してトークンイントロスペクションの呼び出しを承認します (**Authorization: Basic <token>** ヘッダー、ここで **<token>** は Base64 でエンコードされた **<client_id>:<client_secret>** 設定です)。

Edit Policy

Cancel

OAuth 2.0 Token Introspection

builtin – Configures OAuth 2.0 Token Introspection.

This policy executes OAuth 2.0 Token Introspection (https://tools.ietf.org/html/rfc7662) for every API call.

Enabled

max_ttl_tokens

Max TTL for cached tokens

max_cached_tokens

Max number of tokens to cache

auth_type*

client_id+client_secret

introspection_url*

Introspection Endpoint URL

client_id*

Client ID for the Token Introspection Endpoint

client_secret*

Client Secret for the Token Introspection Endpoint

トークンイントロスペクションエンドポイントのレスポンスには、**active** 属性が含まれます。APIcast はこの属性の値を確認します。属性の値に応じて、APIcast は呼び出しを承認または拒否します。

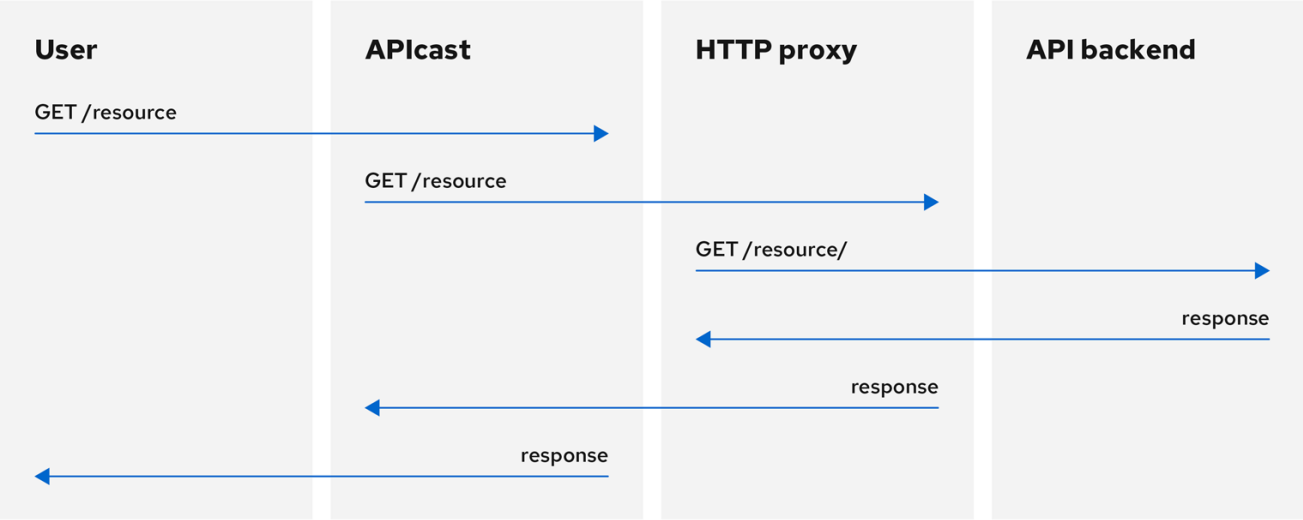
- **true**: 呼び出しを承認します
- **false**: **Authentication Failed** エラーと共に呼び出しを拒否します

このポリシーを使用すると、トークンのキャッシュを有効にして、同じ JWT トークンに対する呼び出しのたびにトークンイントロスペクションエンドポイントに呼び出しを行うのを避けることができます。Token Introspection ポリシーのトークンキャッシュを有効にするには、**max_cached_tokens** フィールドを **0** (機能は無効) から **10000** までの値に設定します。さらに、**max_ttl_tokens** フィールドで、トークンの残存期間 (TTL) の値を **1** から **3600** 秒に設定することができます。

4.1.20. Proxy Service

Proxy Service ポリシーを使用して、定義したプロキシーを使用して 3scale のトラフィックを送信する一般的な **HTTP プロキシー** を定義することができます。この場合、プロキシーサービスはリバース HTTP プロキシーとして機能し、APIcast は HTTP プロキシーにトラフィックを送信し、プロキシーがそのトラフィックを API バックエンドに送信します。

トラフィックフローの例を以下に示します。



3scale バックエンドに送信された APIcast トラフィックは、すべてプロキシーを使用しません。このポリシーは、プロキシーおよび APIcast と API バックエンド間の通信にのみ適用されます。

すべてのトラフィックをプロキシー経由で送信するには、**HTTP_PROXY** 環境変数を使用する必要があります。

注記

- Proxy Service ポリシーはすべての負荷分散ポリシーを無効にし、トラフィックはプロキシーに送信されます。
- **HTTP_PROXY**、**HTTPS_PROXY**、または **ALL_PROXY** パラメーターが定義されている場合には、このポリシーによりこれらのパラメーターの値が上書きされます。
- プロキシー接続では、認証はサポートされません。認証には Header Modification ポリシーを使用します。

4.1.20.1. 設定

ポリシーチェーンの設定例を以下に示します。

```
"policy_chain": [
  {
    "name": "apicast.policy.apicast"
  },
  {
    "name": "apicast.policy.http_proxy",
    "configuration": {
        "all_proxy": "http://192.168.15.103:8888/",
        "https_proxy": "https://192.168.15.103:8888/",
        "http_proxy": "https://192.168.15.103:8888/"
    }
  }
]
```

http_proxy または **https_proxy** が定義されていない場合は、**all_proxy** の値が使用されます。

4.1.20.1.1. ユースケースの例

Proxy Service ポリシーは、HTTP を使用した Apache Camel を用いて、3scale でより粒度の細かいポリシーおよび変換を適用できるように作られました。ただし、Proxy Service ポリシーを一般的な HTTP プロキシーサービスとして使用することもできます。HTTPS を使用した Apache Camel とのインテグレーションについては、「Camel Service」を参照してください。

プロジェクトの例

GitHub の camel-netty-proxy の例を参照してください。このプロジェクトには、API バックエンドからのレスポンスボディーを大文字に変換する HTTP プロキシーが示されています。

4.1.21. Rate Limit Headers

アプリケーションが流量制御の設定されたアプリケーションプランにサブスクライブする際に、Rate Limit Headers ポリシーはレスポンスメッセージに **RateLimit** ヘッダーを追加します。これらのヘッダーは、設定されたリクエストクォータ制限、ならびに現在の時間枠での残りのリクエストクォータおよび秒数に関する有用な情報を提供します。

プロダクトのポリシーチェーンで、Rate Limit Headers ポリシーを追加する場合、3scale APIcast ポリシーの前に設定する必要があります。3scale APIcast ポリシーが Rate Limit Headers ポリシーの前にあると、Rate Limit Headers ポリシーは機能しません。

4.1.21.1. RateLimit ヘッダー

以下の **RateLimit** ヘッダーがそれぞれのメッセージに追加されます。

- **RateLimit-Limit**: 設定された時間枠での合計リクエストクォータを表示します (例: **10** リクエスト)。
- **RateLimit-Remaining**: 現在の時間枠での残りのリクエストクォータを表示します (例: **5** リクエスト)。
- **RateLimit-Resett**: 現在の時間枠での残り時間を秒数で表示します (例: **30** 秒)。このヘッダーの動作は、**Retry-After** ヘッダーの **delta-seconds** 表記と互換性があります。

デフォルトでは、Rate Limit Headers ポリシーが設定されていない場合やアプリケーションプランに流量制御が設定されていない場合、レスポンスメッセージには流量制御に関するヘッダーがありません。

注記

流量制御を設定せずに API メトリクスを要求しているが、親メトリクスに制限が設定されている場合、親の制限が適用されるため、流量制御に関するヘッダーがレスポンスに含まれます。

関連情報

- インターネットドラフト: RateLimit Header Fields for HTTP
- 3scale アプリケーションプランおよび流量制御の設定
- 3scale API メトリクスの設定

4.1.22. Retry

Retry ポリシーは、アップストリーム API へのリトライリクエストの回数を設定します。Retry ポリシーはサービスごとに設定されるため、ユーザーは必要な数のサービスに対してリトライを有効にすることができ、またそれぞれのサービスに異なるリトライ数を設定することもできます。

重要

3scale 2.9 では、リトライするケースをポリシーから設定することはできません。この動作を制御する環境変数 **APICAST_UPSTREAM_RETRY_CASES** は、すべてのサービスにリトライリクエストを適用します。この点についての詳細は、APICAST_UPSTREAM_RETRY_CASES をご確認ください。

Retry ポリシー **JSON** の例を以下に示します。

```
{
  "$schema": "http://apicast.io/policy-v1/schema#manifest#",
  "name": "Retry",
  "summary": "Allows retry requests to the upstream",
  "description": "Allows retry requests to the upstream",
  "version": "builtin",
  "configuration": {
    "type": "object",
    "properties": {
      "retries": {
        "description": "Number of retries",
        "type": "integer",
        "minimum": 1,
        "maximum": 10
      }
    }
  }
}
```

4.1.23. RH-SSO/Keycloak Role Check

OpenID Connect 認証オプションと共に使用した場合、このポリシーによりロールの確認機能が追加さ

れます。このポリシーは、Red Hat Single Sign-On (RH-SSO) により発行されたアクセストークンのレルムロールおよびクライアントロールを確認します。レルムロールを指定すると、3scale のすべてのクライアントリソースにロールの確認機能が追加されます。

ポリシー設定の **type** プロパティーで指定するロールの確認には、2 つのタイプがあります。

- **whitelist** (デフォルト): **whitelist** が使用されると、APIcast は指定したスコープが JWT トークンに含まれるかどうかを確認し、JWT にそのスコープがなければ呼び出しを拒否します。
- **blacklist**: **blacklist** が使用された場合には、JWT トークンにブラックリスト登録したスコープが含まれていれば APIcast は呼び出しを拒否します。

同じポリシーに **blacklist** および **whitelist** 両方のチェックを設定することはできませんが、APIcast ポリシーチェーンに複数の **RH-SSO/Keycloak Role Check** ポリシーインスタンスを追加することができます。

ポリシー設定の **scopes** プロパティーを使用して、スコープのリストを設定することができます。

それぞれの **scope** オブジェクトには、以下のプロパティーがあります。

- **resource**: ロールによって制御されるリソース (エンドポイント)。これは、マッピングルールと同じフォーマットです。文字列の先頭からパターンの照合を行います。完全一致の場合には、最後に **$** を追加する必要があります。
- **resource_type**: このプロパティーで、**resource** の値がどのように評価されるかを定義します。
  - プレーンテキストとして (**plain**): **resource** の値をプレーンテキストとして評価します。たとえば **/api/v1/products$**。
  - Liquid テキストとして (**liquid**): **resource** の値に Liquid を使用することを許可します。たとえば、**/resource_{{ jwt.aud }}** は、クライアント ID が含まれるリソースへのアクセスを管理します。
- **methods**: RH-SSO のユーザーロールに基づいて APIcast で許可される HTTP メソッドを一覧表示する場合に、このパラメーターを使用します。たとえば、以下のロールを持つメソッドを許可することができます。
  - **/resource1** にアクセスするための **role1** レルムロール。このレルムロールを持たないメソッドの場合には、**blacklist** を指定する必要があります。
  - **/resource1** にアクセスするための **role1** という **client1** ロール
  - **/resource1** にアクセスするための **role1** および **role2** レルムロール。**realm_roles** でロールを指定します。各ロールのスコープを指定することもできます。
  - **/resource1** にアクセスするための、アプリケーションクライアントの **role1** というクライアントロール (アクセストークンの受領者)。クライアントに JSON Web Token (JWT) 情報を指定するには、**liquid** クライアントタイプを使用します。
  - **/resource1** にアクセスするための、アプリケーションクライアントのクライアント ID が含まれるクライアントロール (アクセストークンの受領者)。クライアントロールの **name** に JWT 情報を指定するには、**liquid** クライアントタイプを使用します。
  - アプリケーションのクライアント ID が含まれるリソースにアクセスするための、**role1** というクライアントロール。**resource** に JWT 情報を指定するには、**liquid** クライアントタイプを使用します。

- **realm_roles**: レルムロールを確認する場合に使用します (Red Hat Single Sign-On のレルムロール に関するドキュメントを参照してください)。
  レルムロールは、Red Hat Single Sign-On により発行された JWT にあります。

```
"realm_access": {
  "roles": [
    "<realm_role_A>", "<realm_role_B>"
  ]
}
```

  実際のロールは、ポリシーで指定する必要があります。

```
"realm_roles": [
  { "name": "<realm_role_A>" }, { "name": "<realm_role_B>" }
]
```

  realm_roles 配列の各オブジェクトでは、以下のプロパティーを使用することができます。

- **name**: ロールの名前を指定します。

- **name_type**: **plain** または **liquid** のどちらかを指定して、name がどのように評価されるかを定義します (**resource_type** の場合と同じように機能します)。

- **client_roles**: クライアント namespace に特定のアクセス出力があるかどうかを確認する場合に、**client_roles** を使用します (Red Hat Single Sign-On のクライアントロール に関するドキュメントを参照してください)。
  クライアントロールは、JWT の **resource_access** クレームのセクションにあります。

```
"resource_access": {
  "<client_A>": {
    "roles": [
      "<client_role_A>", "<client_role_B>"
    ]
  },
  "<client_B>": {
    "roles": [
      "<client_role_A>", "<client_role_B>"
    ]
  }
}
```

  ポリシーでクライアントロールを指定します。

```
"client_roles": [
  { "name": "<client_role_A>", "client": "<client_A>" },
  { "name": "<client_role_B>", "client": "<client_A>" },
  { "name": "<client_role_A>", "client": "<client_B>" },
  { "name": "<client_role_B>", "client": "<client_B>" }
]
```

  client_roles 配列の各オブジェクトでは、以下のプロパティーを使用することができます。

- **name**: ロールの名前を指定します。

- **name_type**: **plain** または **liquid** のどちらかを指定して、**name** の値がどのように評価されるかを定義します (**resource_type** の場合と同じように機能します)。
- **client**: ロールのクライアントを指定します。定義しなければ、このポリシーはクライアントに **aud** クレームを使用します。
- **client_type**: **plain** または **liquid** のどちらかを指定して、**client** の値がどのように評価されるかを定義します (**resource_type** の場合と同じように機能します)。

4.1.24. Routing

Routing ポリシーを使用すると、リクエストをさまざまなターゲットエンドポイントにルーティングすることができます。ターゲットエンドポイントを定義すると、正規表現を使用して UI から受信したリクエストをターゲットエンドポイントにルーティングできるようになります。

ルーティングは、以下のルールに基づきます。

- リクエストパスルール
- ヘッダールール
- クエリー引数ルール
- JSON Web Token (JWT) クレームルール

APIcast ポリシーと組み合わせる場合には、ポリシーチェーンでは APIcast ポリシーの前に Routing ポリシーを設定する必要があります。2 つのポリシーのうち始めのポリシーがレスポンスにコンテンツを出力するためです。2 番目のポリシーにコンテンツフェーズを実行する変更が加えられても、リクエストはすでにクライアントに送信されるため、レスポンスには何も出力されません。

4.1.24.1. ルーティングルール

- 複数のルールが存在する場合には、Routing ポリシーは最初のマッチに適用されます。これらのルールは並べ替えることができます。
- マッチするルールがなければ、ポリシーはアップストリームを変更せず、サービス設定で定義済みのプライベートベース URL を使用します。

4.1.24.2. リクエストパスルール

以下の設定では、パスが **/accounts** の場合に **http://example.com** にルーティングします。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://example.com",
        "condition": {
          "operations": [
            {
              "match": "path",
              "op": "==",
              "value": "/accounts"
```

```
            }
          ]
        }
      }
    ]
  }
}
```

4.1.24.3. ヘッダールール

以下の設定では、ヘッダー **Test-Header** の値が **123** の場合に **http://example.com** にルーティングします。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://example.com",
        "condition": {
          "operations": [
            {
              "match": "header",
              "header_name": "Test-Header",
              "op": "==",
              "value": "123"
            }
          ]
        }
      }
    ]
  }
}
```

4.1.24.4. クエリー引数ルール

以下の設定では、クエリー引数 **test_query_arg** の値が **123** の場合に **http://example.com** にルーティングします。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://example.com",
        "condition": {
          "operations": [
            {
              "match": "query_arg",
              "query_arg_name": "test_query_arg",
              "op": "==",
              "value": "123"
```

```
            }
          ]
        }
      }
    ]
  }
}
```

4.1.24.5. JWT クレームルール

JWT クレームの値に基づいてルーティングするためには、ポリシーチェーンには、ポリシーが共有するコンテキストで JWT を検証して格納するポリシーが必要です。

以下の設定では、JWT クレーム **test_claim** の値が **123** の場合に **http://example.com** にルーティングします。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://example.com",
        "condition": {
          "operations": [
            {
              "match": "jwt_claim",
              "jwt_claim_name": "test_claim",
              "op": "==",
              "value": "123"
            }
          ]
        }
      }
    ]
  }
}
```

4.1.24.6. 複数演算ルール

ルールに複数の演算を設定し、すべてが true と評価される場合にだけ (and**combine_op** を使用) 指定したアップストリームにルーティングすることや、少なくとも 1 つが true と評価される場合に (or**combine_op** を使用) 指定したアップストリームにルーティングすることができます。**combine_op** のデフォルト値は and です。

以下の設定では、リクエストのパスが **/accounts** で、かつヘッダー **Test-Header** の値が **123** の場合に、**http://example.com** にルーティングします。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
```

```
        "url": "http://example.com",
        "condition": {
          "combine_op": "and",
          "operations": [
            {
              "match": "path",
              "op": "==",
              "value": "/accounts"
            },
            {
              "match": "header",
              "header_name": "Test-Header",
              "op": "==",
              "value": "123"
            }
          ]
        }
      }
    ]
  }
}
```

以下の設定では、リクエストのパスが **/accounts** であるか、またはヘッダー **Test-Header** の値が **123** の場合に、**http://example.com** にルーティングします。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://example.com",
        "condition": {
          "combine_op": "or",
          "operations": [
            {
              "match": "path",
              "op": "==",
              "value": "/accounts"
            },
            {
              "match": "header",
              "header_name": "Test-Header",
              "op": "==",
              "value": "123"
            }
          ]
        }
      }
    ]
  }
}
```

4.1.24.7. ルールの結合

ルールを組み合わせることができます。複数のルールがある場合、選択されるアップストリームは、true と評価される最初のルールです。

複数のルールで設定される設定を以下に示します。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://some_upstream.com",
        "condition": {
          "operations": [
            {
              "match": "path",
              "op": "==",
              "value": "/accounts"
            }
          ]
        }
      },
      {
        "url": "http://another_upstream.com",
        "condition": {
          "operations": [
            {
              "match": "path",
              "op": "==",
              "value": "/users"
            }
          ]
        }
      }
    ]
  }
}
```

4.1.24.8. キャッチオールルール

演算のないルールは常にマッチします。これは、キャッチオールルールを定義するのに役立ちます。

以下の設定では、パスが **/abc** の場合にはリクエストを **http://some_upstream.com** にルーティングし、パスが **/def** の場合には **http://another_upstream.com** にルーティングし、上記ルールのどちらも true と評価されない場合には **http://default_upstream.com** にルーティングします。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://some_upstream.com",
        "condition": {
          "operations": [
```

```
            {
              "match": "path",
              "op": "==",
              "value": "/abc"
            }
          ]
        }
      },
      {
        "url": "http://another_upstream.com",
        "condition": {
          "operations": [
            {
              "match": "path",
              "op": "==",
              "value": "/def"
            }
          ]
        }
      },
      {
        "url": "http://default_upstream.com",
        "condition": {
          "operations": []
        }
      }
    ]
  }
}
```

4.1.24.9. サポートされる操作

サポートされる演算は、**==**、**!=**、および **matches** です。最後の演算は正規表現を使用する文字列との照合を行い、ngx.re.match を使用して実装されます。

以下の設定では、**!=** が使用されています。パスが **/accounts** ではない場合に **http://example.com** にルーティングします。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://example.com",
        "condition": {
          "operations": [
            {
              "match": "path",
              "op": "!=",
              "value": "/accounts"
            }
          ]
        }
      }
```

```
      ]
    }
  }
```

4.1.24.10. Liquid テンプレート

設定の値に liquid テンプレートを使用することができます。これにより、チェーン内のポリシーがコンテキストにキー **my_var** を保存する場合には、動的な値を使用してルールを定義することができます。

以下の設定では、リクエストをルーティングするのにその値が使用されています。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://example.com",
        "condition": {
          "operations": [
            {
              "match": "header",
              "header_name": "Test-Header",
              "op": "==",
              "value": "{{ my_var }}",
              "value_type": "liquid"
            }
          ]
        }
      }
    ]
  }
}
```

4.1.24.11. host_header で使用されるホストの設定

リクエストがルーティングされる際に、デフォルトでは、ポリシーはマッチしたルールの URL のホストを使用して Host ヘッダーを設定します。**host_header** 属性を使用して別のホストを指定することができます。

以下の設定では、Host ヘッダーのホストに **some_host.com** が指定されています。

```
{
  "name": "routing",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "url": "http://example.com",
        "host_header": "some_host.com",
        "condition": {
          "operations": [
            {
              "match": "path",
```

```
                "op": "==",
                "value": "/"
              }
            ]
          }
        }
      ]
    }
  }
```

4.1.25. SOAP

SOAP ポリシーでは、ポリシーで指定したマッピングルールを使用して、HTTP リクエストの SOAPAction または Content-Type ヘッダーにより提供される SOAP アクション URI との照合を行います。

設定プロパティー

プロパティー	説明	値	必須/任意
pattern	**pattern** プロパティーにより、APIcast がマッチを探す SOAPAction URI の文字列を指定することができます。	データタイプ: 文字列	必須
metric_system_name	**metric_system_name** プロパティーを使用して、マッチしたパターンがヒットを登録する 3scale バックエンドメトリクスを指定することができます。	データタイプ: 文字列 (有効な メトリクス でなければなりません)	必須

ポリシーオブジェクトの例

```
{
  "name": "soap",
  "version": "builtin",
  "configuration": {
    "mapping_rules": [
      {
        "pattern": "http://example.com/soap#request",
        "metric_system_name": "soap",
        "delta": 1
      }
    ]
  }
}
```

ポリシーの設定方法に関する情報は、本書の 3scale でのポリシーチェーンの作成 セクションを参照してください。

4.1.26. TLS Client Certificate Validation

TLS Client Certificate Validation ポリシーでは、APIcast は TLS ハンドシェイクを実装し、ホワイトリストに対してクライアント証明書を検証します。ホワイトリストには、認証局 (CA) によって署名された証明書、または単なるクライアント証明書が含まれます。証明書の有効期限が切れている、または証明書が無効な場合には、リクエストは拒否され他のポリシーは処理されません。

クライアントは APIcast に接続してリクエストを送信し、クライアント証明書を提供します。APIcast は、ポリシー設定に従って受信したリクエストで提供された証明書の信ぴょう性を検証します。アップストリームに接続する際に独自のクライアント証明書を使用するように、APIcast を設定することもできます。

4.1.26.1. TLS Client Certificate Validation ポリシーに対応する APIcast の設定

TLS を終端するように APIcast を設定する必要があります。以下の手順に従って、Client Certificate Validation ポリシーが設定された APIcast でユーザーが提供するクライアント証明書を検証するように設定します。

前提条件:

- 3scale システムにアクセスできること。
- すべてのデプロイメントが完了していること。

4.1.26.1.1. ポリシーに対応する APIcast のセットアップ

APIcast をセットアップし TLS を終端するように設定するには、以下の手順に従います。

1. 3scale のインストールの OpenShift テンプレートを使用した APIcast のデプロイ に記載の手順に従って、アクセストークンを取得し Self-managed APIcast をデプロイする必要があります。

注記

ゲートウェイ全体で特定の証明書を使用するように APIcast インスタンスを再設定しなければならないので、Self-managed APIcast のデプロイメントが必要です。

2. テストを簡素化するために、**--param** フラグを指定してレイジーローダー、キャッシュなし、およびステージング環境を使用することができます (ただし、テスト目的の場合のみ)。

```
oc new-app -f https://raw.githubusercontent.com/3scale/3scale-amp-openshift-
templates/master/apicast-gateway/apicast.yml --param CONFIGURATION_LOADER=lazy --
param DEPLOYMENT_ENVIRONMENT=staging --param CONFIGURATION_CACHE=0
```

3. テスト用途の証明書を生成します。なお、実稼働環境のデプロイメントの場合には、認証局から提供された証明書を使用することができます。

4. TLS 証明書を使用してシークレットを作成します。

```
oc create secret tls apicast-tls
--cert=ca/certs/server.crt
--key=ca/keys/server.key
```

5. APIcast デプロイメント内にシークレットをマウントします。

```
oc set volume dc/apicast --add --name=certificates --mount-path=/var/run/secrets/apicast --
secret-name=apicast-tls
```

6. HTTPS 用ポート 8443 のリッスンを開始するように APIcast を設定します。

```
oc set env dc/apicast APICAST_HTTPS_PORT=8443
APICAST_HTTPS_CERTIFICATE=/var/run/secrets/apicast/tls.crt
APICAST_HTTPS_CERTIFICATE_KEY=/var/run/secrets/apicast/tls.key
```

7. サービスでポート 8443 を公開します。

```
oc patch service apicast -p '{"spec":{"ports":[{"name":"https","port":8443,"protocol":"TCP"}]}}'
```

8. デフォルトルートを削除します。

```
oc delete route api-apicast-staging
```

9. **apicast** サービスをルートとして公開します。

```
oc create route passthrough --service=apicast --port=https --hostname=api-3scale-apicast-
staging.$WILDCARD_DOMAIN
```

注記

このステップは、使用するすべての API で実施する必要があります (それぞれの API のドメインに変更してください)。

10. プレースホルダーの [Your_user_key] に実際のキーを指定して、上記のステップでデプロイしたゲートウェイが機能し、設定が保存されていることを確認します。

```
curl https://api-3scale-apicast-staging.$WILDCARD_DOMAIN?user_key=[Your_user_key] -v
--cacert ca/certs/ca.crt
```

4.1.26.2. ポリシーチェーンへの TLS Client Certificate Validation ポリシーの設定

ポリシーチェーンで TLS Client Certificate Validation を設定するには、以下を行います。

前提条件

- 3scale へのログインクレデンシャルが必要です。
- TLS Client Certificate Validation ポリシーに対応するように APIcast を設定 している必要があります。

4.1.26.2.1. ポリシーの設定

1. 管理ポータルでのポリシーの有効化 に記載の手順に従って TLS Client Certificate Validation を選択し、API に TLS Client Certificate Validation ポリシーを追加します。
2. **TLS Client Certificate Validation** のリンクをクリックします。
3. **Enabled** のチェックボックスを選択し、ポリシーを有効にします。

4. 証明書をホワイトリストに追加するには、プラス (**+**) アイコンをクリックします。
5. **-----BEGIN CERTIFICATE-----** および **-----END CERTIFICATE-----** を含めて、証明書を指定します。
6. API への TLS Client Certificate Validation ポリシーの設定が完了したら、**Update Policy** をクリックします。

付加手順:

- プラス (**+**) アイコンをクリックして、さらに証明書を追加することができます。
- 上/下矢印を使用して、証明書の順番を入れ替えることもできます。

変更を保存するには、**Update Policy Chain** をクリックします。

4.1.26.3. TLS Client Certificate Validation ポリシー機能の確認

TLS Client Certificate Validation ポリシーの機能を確認するには、以下を実行します。

前提条件:

- 3scale へのログインクレデンシャルが必要です。
- TLS Client Certificate Validation ポリシーに対応するように APIcast を設定 している必要があります。

4.1.26.3.1. ポリシー機能の確認

プレースホルダーの **[Your_user_key]** に実際のキーを指定して、適用したポリシーを確認することができます。

```
curl https://api-3scale-apicast-staging.$WILDCARD_DOMAIN\?user_key\=[Your_user_key] -v --
cacert ca/certs/ca.crt --cert ca/certs/client.crt --key ca/keys/client.key

curl https://api-3scale-apicast-staging.$WILDCARD_DOMAIN\?user_key\=[Your_user_key] -v --
cacert ca/certs/ca.crt --cert ca/certs/server.crt --key ca/keys/server.key

curl https://api-3scale-apicast-staging.$WILDCARD_DOMAIN\?user_key\=[Your_user_key] -v --
cacert ca/certs/ca.crt
```

4.1.26.4. ホワイトリストからの証明書の削除

ホワイトリストから証明書を削除するには、以下を行います。

前提条件

- 3scale へのログインクレデンシャルが必要です。
- TLS Client Certificate Validation ポリシーに対応するように APIcast を設定 している必要があります。
- ポリシーチェーンに TLS Client Certificate Validation ポリシーを設定 して、証明書をホワイトリストに追加している必要があります。

4.1.26.4.1. 証明書の削除

1. **TLS Client Certificate Validation** のリンクをクリックします。
2. **x** アイコンをクリックし、ホワイトリストから証明書を削除します。
3. 証明書の削除が完了したら、**Update Policy** をクリックします。

変更を保存するには、**Update Policy Chain** をクリックします。

4.1.26.5. リファレンス資料

証明書の操作についての詳細は、Red Hat Certificate System のドキュメント を参照してください。

4.1.27. TLS Termination

本セクションでは、Transport Layer Security (TLS) Termination ポリシーに関して、その概要、設定、検証、およびポリシーからのファイル削除について説明します。

TLS Termination ポリシーを使用すると、全 API 用の単一の証明書を使用せずにそれぞれの API ごとに TLS リクエストを終端するように、APIcast を設定することができます。APIcast は、クライアントへの接続を確立する前に設定設定をプルします。このようにして、APIcast はポリシーからの証明書を使用して TLS を終端させます。このポリシーは、以下のソースと共に機能します。

- ポリシー設定内に保管されるソース
- ファイルシステム上に保管されるソース

デフォルトでは、このポリシーはポリシーチェーンで有効になっていません。

4.1.27.1. ポリシーチェーンへの TLS Termination ポリシーの設定

本セクションでは、ポリシーチェーンに TLS Termination ポリシーを設定するための前提条件および手順について説明します。なお、設定には Privacy Enhanced Mail (PEM) 形式の証明書を使用します。

前提条件

- ユーザーの発行した証明書
- PEM 形式のサーバー証明書
- PEM 形式の証明書の秘密鍵

4.1.27.1.1. ポリシーの設定

1. 管理ポータルでのポリシーの有効化 に記載の手順に従って TLS Termination を選択し、API に TLS Termination ポリシーを追加します。
2. **TLS Termination** のリンクをクリックします。
3. **Enabled** のチェックボックスを選択し、ポリシーを有効にします。
4. TLS 証明書をポリシーに追加するには、プラス (**+**) アイコンをクリックします。
5. 証明書のソースを選択します。

- Embedded certificate: サーバー証明書へのパスおよび証明書の秘密鍵へのパスを指定します。
- Certificate from local file system: 証明書の秘密鍵およびサーバー証明書のファイルを参照します。

6. API への TLS Termination ポリシーの設定が完了したら、**Update Policy** をクリックします。

付加手順:

- プラス (**+**) アイコンをクリックして、さらに証明書を追加することができます。
- 上/下矢印を使用して、証明書の順番を入れ替えることもできます。

変更を保存するには、**Update Policy Chain** をクリックします。

4.1.27.2. TLS Termination ポリシー機能の確認

前提条件

- 3scale へのログインクレデンシャルが必要です。
- APIcast に TLS Termination ポリシーを設定 している必要があります。

4.1.27.2.1. ポリシー機能の確認

以下のコマンドを使用して、ポリシーが機能するかどうかをコマンドラインでテストすることができます。

```
curl “${public_URL}:${port}/?user_key=${user_key}" --cacert ${path_to_certificate}/ca.pem -v
```

ここで、

- **public_URL**: ステージング環境用の公開ベース URL
- **port**: ポート番号
- **user_key**: 認証に使用するユーザーキー
- **path_to_certificate**: ローカルファイルシステムに保管された CA 証明書へのパス

4.1.27.3. TLS Termination ポリシーからのファイルの削除

本セクションでは、TLS Termination ポリシーから証明書およびキーファイルを削除する手順について説明します。

前提条件

- 3scale へのログインクレデンシャルが必要です。
- APIcast に TLS Termination ポリシーを設定 して、証明書をポリシーに追加している必要があります。

4.1.27.3.1. 証明書の削除

1. **TLS Termination** のリンクをクリックします。
2. **x** アイコンをクリックして、証明書およびキーを削除します。
3. 証明書の削除が完了したら、**Update Policy** をクリックします。

変更を保存するには、**Update Policy Chain** をクリックします。

4.1.28. Upstream

Upstream ポリシーでは、正規表現を使用して Host リクエストヘッダーを解析し、プライベートベース URL で定義されたアップストリーム URL を別の URL に置き換えることができます。

例:

正規表現 **/foo** および URL フィールド **newexample.com** が設定されたポリシーが、URL **https://www.example.com/foo/123/** を **newexample.com** に置き換える

ポリシーチェーンの参照

プロパティー	説明	値	必須/任意
regex	**regex** プロパティーを使用して、Upstream ポリシーがリクエストパスを照合する際に使用する正規表現を指定することができます。	データタイプ: 文字列 (有効な正規表現の構文でなければなりません)	必須
url	**url** プロパティーを使用して、マッチした場合に置き換える URL を指定することができます。Upstream ポリシーはこの URL が有効かどうかを確認しない点に注意してください。	データタイプ: 文字列 (有効な URL でなければなりません)	必須

ポリシーオブジェクトの例

```
{
  "name": "upstream",
  "version": "builtin",
  "configuration": {
    "rules": [
      {
        "regex": "^/v1/.*",
        "url": "https://api-v1.example.com",

      }
    ]
  }
}
```

ポリシーの設定方法に関する情報は、本書の 3scale でのポリシーチェーンの作成 セクションを参照してください。

4.1.29. Upstream Connection

Upstream Connection ポリシーを使用すると、3scale システムでの API バックエンドサーバーの設定に応じて、API ごとに以下のディレクティブのデフォルト値を変更することができます。

- **proxy_connect_timeout**
- **proxy_send_timeout**
- **proxy_read_timeout**

4.1.29.1. ポリシーチェーンへの Upstream Connection ポリシーの設定

本セクションでは、ポリシーチェーンで Upstream Connection ポリシーを設定する手順を説明します。

前提条件

- 3scale システムにアクセスできること。
- すべてのデプロイメントが完了していること。

4.1.29.1.1. ポリシーの設定

1. 管理ポータルでのポリシーの有効化 に記載の手順に従って **Upstream Connection** を選択し、API に Upstream Connection ポリシーを追加します。
2. **Upstream Connection** のリンクをクリックします。
3. **Enabled** のチェックボックスを選択し、ポリシーを有効にします。
4. アップストリームへの接続に関するオプションを設定します。
   - **send_timeout**
   - **connect_timeout**
   - **read_timeout**
5. API への Upstream Connection ポリシーの設定が完了したら、**Update Policy** をクリックします。

変更を保存するには、**Update Policy Chain** をクリックします。

4.1.30. Upstream Mutual TLS

Upstream Mutual TLS ポリシーを使用すると、設定で指定した証明書に基づいて、APIcast とアップストリーム API との間で相互 TLS 接続を確立することができます。このポリシーは、アップストリーム API に応じて複数の証明書をサポートします。

4.1.30.1. ポリシーチェーンへの Upstream Mutual TLS ポリシーの設定

本セクションでは、ポリシーチェーンで Upstream Mutual TLS ポリシーを設定する手順を説明します。

前提条件

- 3scale システムにアクセスできること。

手順

1. 管理ポータルでのポリシーの有効化 に記載の手順に従って **Upstream Mutual TLS** を選択し、API に Upstream Mutual TLS ポリシーを追加します。
2. **Upstream Mutual TLS** のリンクをクリックします。
3. **Enabled** のチェックボックスを選択し、ポリシーを有効にします。
4. **Certificate type** を選択します。
   - **path**: OpenShift によって生成された証明書などのパスを指定する場合。
   - **embedded**: サードパーティーが生成した証明書をファイルシステムからアップロードして使用する場合。
5. **Certificate** でクライアント証明書を指定します。
6. **Certificate key** でキーを指定します。
7. API への Upstream Mutual TLS ポリシーの設定が完了したら、**Update Policy Chain** をクリックします。

変更をプロモートするには、以下の手順を実施します。

1. **[Your_product] page > Integration > Configuration**の順に移動します。
2. **APIcast Configuration** セクションで、**Promote v# to Staging APIcast**をクリックします。
   - **v#** は、プロモートされる設定のバージョン番号を表します。

4.1.31. URL Rewriting

URL Rewriting ポリシーを使用すると、リクエストのパスおよびクエリー文字列を変更することができます。

3scale APIcast ポリシーと組み合わせる場合には、ポリシーチェーンで URL Rewriting ポリシーを APIcast ポリシーの前に設定すると、APIcast のマッピングルールは変更したパスに適用されます。ポリシーチェーンで URL Rewriting ポリシーを APIcast ポリシーの後に設定すると、マッピングルールは元のパスに適用されます。

このポリシーでは、以下の 2 つの操作セットがサポートされます。

- **commands**: リクエストのパスを書き換えるために適用されるコマンドのリスト。
- **query_args_commands**: リクエストのクエリー文字列を書き換えるために適用されるコマンドのリスト。

4.1.31.1. パスを書き換えるためのコマンド

commands リストの各コマンドは、以下の設定パラメーターで設定されます。

- **op**: 適用される操作。設定可能なオプションは **sub** および **gsub** です。**sub** 操作では、指定した正規表現との最初のマッチだけが置き換えられます。**gsub** 操作では、指定した正規表現とのマッチがすべて置き換えられます。sub および gsub 操作に関するドキュメントを参照してください。
- **regex**: 照合される Perl 互換の正規表現
- **replace**: マッチした際に置き換えられる文字列
- **options** (オプション): 正規表現との照合がどのように行われるかを定義するオプション。設定可能なオプションに関する情報は、OpenResty Lua モジュールプロジェクトのドキュメントの ngx.re.match セクションを参照してください。
- **break** (オプション): true に設定すると (チェックボックスを選択する)、コマンドが URL を書き換えた場合、それが適用される最後のコマンドになります (リスト内の後続コマンドはすべて破棄されます)。

4.1.31.2. クエリー文字列を書き換えるためのコマンド

query_args_commands リストの各コマンドは、以下の設定パラメーターで設定されます。

- **op**: クエリー引数に適用される操作。以下のオプションを設定することができます。
  - **add**: 既存の引数に値を追加します。
  - **set**: 引数が設定されていなければ作成し、設定されていればその値を置き換えます。
  - **push**: 引数が設定されていなければ作成し、設定されていれば値を追加します。
  - **delete**: 引数を削除します。
- **arg**: 操作が適用されるクエリー引数の名前
- **value**: クエリー引数に使用される値を指定します。値のタイプが liquid の場合には、値は **{{ variable_from_context }}** の形式にする必要があります。**delete** 操作の場合には、値を考慮する必要はありません。
- **value_type** (オプション): クエリー引数の値がどのように評価されるかを定義します。プレーンテキストの場合の **plain** または Liquid テンプレートとして評価する場合の **liquid** いずれかに設定します。詳細は、「ポリシーでの変数およびフィルターの使用」 を参照してください。指定しなければ、デフォルトではタイプ plain が使用されます。

例

URL Rewriting ポリシーは、以下のように設定します。

```
{
  "name": "url_rewriting",
  "version": "builtin",
  "configuration": {
    "query_args_commands": [
      {
        "op": "add",
        "arg": "addarg",
        "value_type": "plain",
```

```
        "value": "addvalue"
      },
      {
        "op": "delete",
        "arg": "user_key",
        "value_type": "plain",
        "value": "any"
      },
      {
        "op": "push",
        "arg": "pusharg",
        "value_type": "plain",
        "value": "pushvalue"
      },
      {
        "op": "set",
        "arg": "setarg",
        "value_type": "plain",
        "value": "setvalue"
      }
    ],
    "commands": [
      {
        "op": "sub",
        "regex": "^/api/v\\d+/",
        "replace": "/internal/",
        "options": "i"
      }
    ]
  }
```

APIcast に送信される元のリクエスト URI:

```
https://api.example.com/api/v1/products/123/details?
user_key=abc123secret&pusharg=first&setarg=original
```

URL の書き換えを適用した後に APIcast が API バックエンドに送信する URI:

```
https://api-backend.example.com/internal/products/123/details?
pusharg=first&pusharg=pushvalue&setarg=setvalue
```

以下の変換が適用されます。

1. サブストリング **/api/v1/** はパス書き換えコマンドだけにマッチし、**/internal/** に置き換えられます。
2. **user_key** クエリー引数は削除されます。
3. 値 **pushvalue** は追加の値として **pusharg** クエリー引数に追加されます。
4. クエリー引数 **setarg** の値 **original** は、設定した値 **setvalue** に置き換えられます。
5. クエリー引数 **addarg** は元の URL に存在しないため、コマンド **add** は適用されませんでした。

ポリシーの設定方法に関する情報は、本書の 3scale でのポリシーチェーンの作成 セクションを参照してください。

4.1.32. URL Rewriting with Captures

URL Rewriting with Captures ポリシーは「URL Rewriting」ポリシーの代替で、API リクエストの URL を API バックエンドに渡す前に書き換えることができます。

URL Rewriting with Captures ポリシーは URL の引数を取得し、その値を書き換えられる URL で使用します。

このポリシーでは **transformations** 設定パラメーターがサポートされます。これは、リクエスト URL に適用される変換を定義するオブジェクトのリストです。それぞれの変換オブジェクトは、以下の 2 つのプロパティーで設定されます。

- **match_rule**: このルールは受信したリクエストの URL と照合されます。このルールには **{nameOfArgument}** 形式の名前付き引数を含めることができ、これらの引数を書き換えられる URL で使用することができます。URL は正規表現として **match_rule** と比較されます。名前付き引数と照合する値には、**[\w-.~%!$&'()*+,;=@:]+** の文字しか使用することができません (PCRE 正規表現表記)。他の正規表現トークンを **match_rule** の表記で使用することができます。たとえば、文字列先頭の **^** および文字列末尾の **$** 等です。

- **template**: URL のテンプレートで、これにより元の URL が書き換えられます。 **match_rule** からの名前付き引数を使用することができます。

元の URL のクエリーパラメーターは、**template** で指定したクエリーパラメーターとマージされます。

例

URL Rewriting with Captures ポリシーは、以下のように設定します。

```
{
  "name": "rewrite_url_captures",
  "version": "builtin",
  "configuration": {
    "transformations": [
      {
        "match_rule": "/api/v1/products/{productId}/details",
        "template": "/internal/products/details?id={productId}&extraparam=anyvalue"
      }
    ]
  }
}
```

APIcast に送信される元のリクエスト URI:

```
https://api.example.com/api/v1/products/123/details?user_key=abc123secret
```

URL の書き換えを適用した後に APIcast が API バックエンドに送信する URI:

```
https://api-backend.example.com/internal/products/details?
user_key=abc123secret&extraparam=anyvalue&id=123
```

4.2. 管理ポータルでのポリシーの有効化

管理ポータルでポリシーを有効にするには、以下の手順を実施します。

1. 3scale にログインします。
2. ポリシーを有効にするプロダクト API を選択します。
3. **[your_product_name]** から **Integration** > **Policies** の順に移動します。
4. **POLICIES** セクションで **Add policy** をクリックします。
5. 追加するポリシーを選択し、必須フィールドに入力します。
6. **Update Policy Chain** ボタンをクリックし、ポリシーチェーンを保存します。

4.3. カスタム APICAST ポリシーの作成

カスタム APIcast ポリシーを新規に作成することや、標準ポリシーを変更することができます。

カスタムポリシーを作成するには、以下の点を理解している必要があります。

- ポリシーは Lua で記述される。
- ポリシーは適切なファイルディレクトリーに保管しなければならない。
- ポリシーチェーン内での設定場所により、ポリシーの動作が異なる。
- カスタムポリシーを追加するインターフェイスは完全にサポートされているが、カスタムポリシー自体はサポートされていない。

4.4. APICAST へのカスタムポリシーの追加

本項では、さまざまな APIcast デプロイメントについて、カスタムポリシーを追加する方法の要点を説明します。

4.4.1. APIcast デプロイメントへのカスタムポリシーの追加

カスタムポリシーを作成したら、それを APIcast に追加する必要があります。その手順は、APIcast がデプロイされている場所により異なります。

- OpenShift および Docker コンテナー環境の APIcast 等の Self-managed APIcast デプロイメントに、カスタムポリシーを追加することができます。
- カスタムポリシーを Hosted APIcast に追加することはできません。

警告

決して、実稼働環境のゲートウェイで直接ポリシーを変更しないでください。変更を必ずテストしてください。

4.4.2. Embedded APIcast へのカスタムポリシーの追加

オンプレミスデプロイメントにカスタム APIcast ポリシーを追加するには、カスタムポリシーが含まれる OpenShift イメージをビルドし、それをデプロイメントに追加する必要があります。3scale では、サンプルリポジトリーを提供しています。このリポジトリーを、カスタムポリシーを作成してオンプレミスデプロイメントに追加するためのフレームワークとして使用することができます。

このサンプルリポジトリーには、カスタムポリシー用の正しいディレクトリー構造に加えて、イメージストリームを作成するテンプレート、および作成するカスタムポリシーが含まれる新しい APIcast OpenShift イメージをビルドするための BuildConfigs が含まれています。

警告

apicast-custom-policies をビルドすると、ビルドプロセスは新しいイメージを **amp-apicast:latest** タグにプッシュします。このイメージストリームタグ (**:latest**) でイメージが変更されると、デフォルトでは **apicast-staging** および **apicast-production** タグの両方が自動的に新しいデプロイメントを開始するように設定されています。実稼働環境 (あるいは、必要であればステージング環境) のサービスが中断されるのを避けるためには、自動デプロイメントを無効にするか (**Automatically start a new deployment when the image changes** チェックボックス) か、実稼働環境用に別のイメージストリームタグ (例: **amp-apicast:production**) を設定することをお勧めします。

カスタムポリシーをオンプレミスデプロイメントに追加するには、以下の手順を実施します。

1. レジストリーサービスアカウントの作成 で作成したクレデンシャルを使用して、**docker-registry** シークレットを作成します。その際に、以下の点に留意してください。

   - **your-registry-service-account-username** を 12345678|username のフォーマットで作成したユーザー名に置き換えてください。
   - **your-registry-service-account-password** を **Token Information** タブでユーザー名の下に表示されるパスワードの文字列に置き換えてください。
   - イメージストリームが存在し **registry.redhat.io** を使用するすべての新規 **namespace** について、**docker-registry** シークレットを作成します。
     以下のコマンドを実行して **docker-registry** シークレットを作成します。

     ```
     oc create secret docker-registry threescale-registry-auth \
       --docker-server=registry.redhat.io \
       --docker-username="your-registry-service-account-username" \
       --docker-password="your-registry-service-account-password"
     ```

2. https://github.com/3scale/apicast-example-policy (ポリシーの例が含まれる公開リポジトリー) をフォークするか、そのコンテンツが含まれるプライベートリポジトリーを作成します。OpenShift がイメージをビルドするには、Git リポジトリーでカスタムポリシーのコードが必要です。プライベート Git リポジトリーを使用するには、OpenShift でシークレットを設定する必要がある点に注意してください。

3. リポジトリーをローカルにクローンし、ポリシーの実装を追加し、変更をご自分の Git リポジトリーにプッシュします。

4. **openshift.yml** テンプレートを更新します。具体的には、以下のパラメーターを変更します。

a. **spec.source.git.uri: https://github.com/3scale/apicast-example-policy.git** (ポリシーの BuildConfig): ご自分の Git リポジトリーの場所に変更します。

b. **spec.source.images[0].paths.sourcePath: /opt/app-root/policies/example** (カスタムポリシーの BuildConfig): **example** をリポジトリーの **policies** ディレクトリーに追加したカスタムポリシーの名前に変更します。

c. オプションで、OpenShift オブジェクト名およびイメージタグを更新します。ただし、変更の一貫性が維持されるようにする必要があります (例: **apicast-example-policy** BuildConfig が **apicast-policy:example** イメージをビルドおよびプッシュし、それを **apicast-custom-policies** BuildConfig がソースとして使用する。これによりダグの一貫性が維持されます)。

5. 以下のコマンドを実行して OpenShift オブジェクトを作成します。

```
oc new-app -f openshift.yml --param AMP_RELEASE=2.9
```

6. ビルドが自動的に開始されない場合には、以下の 2 つのコマンドを実行します。**apicast-example-policy** を変更している場合には、ご自分の BuildConfig 名に置き換えます (例: **apicast-<name>-policy**)。最初のコマンドが完了するのを待ってから、2 番目のコマンドを実行してください。

```
oc start-build apicast-example-policy
oc start-build apicast-custom-policies
```

Embedded APIcast のイメージに **amp-apicast:latest** イメージストリームの変更を追跡するトリガーがある場合には、APIcast の新しいデプロイメントが開始されます。**apicast-staging** が再開されたら **Integration > Policies** の順に移動し、**Add Policy** ボタンをクリックしてご自分のカスタムポリシーがリストに表示されるのを確認します。カスタムポリシーを選択して設定したら、**Update Policy Chain** をクリックし、カスタムポリシーをステージング APIcast で動作状態にします。

4.4.3. 別の OpenShift Container Platform 上の APIcast へのカスタムポリシーの追加

カスタムポリシーを OpenShift Container Platform (OCP) 上の APIcast に追加することができます。そのためには、ご自分のカスタムポリシーが含まれる APIcast イメージを 統合 OpenShift Container Platform レジストリー から取得します。

別の OpenShift Container Platform 上の APIcast にカスタムポリシーを追加します

1. Embedded APIcast にポリシーを追加します。

2. APIcast ゲートウェイをメインの OpenShift クラスターにデプロイしていない場合には、メインの OpenShift クラスター上の内部レジストリーへの アクセスを確立します。

3. 3scale 2.9 APIcast OpenShift テンプレートを ダウンロードします。

4. テンプレートを変更するには、デフォルトの **image** ディレクトリーを内部レジストリーの完全なイメージ名に置き換えます。

```
image: <registry>/<project>/amp-apicast:latest
```

5. カスタマイズしたイメージを指定し、OpenShift テンプレートを使用して APIcast をデプロイします。

```
oc new-app -f customizedApicast.yml
```

注記

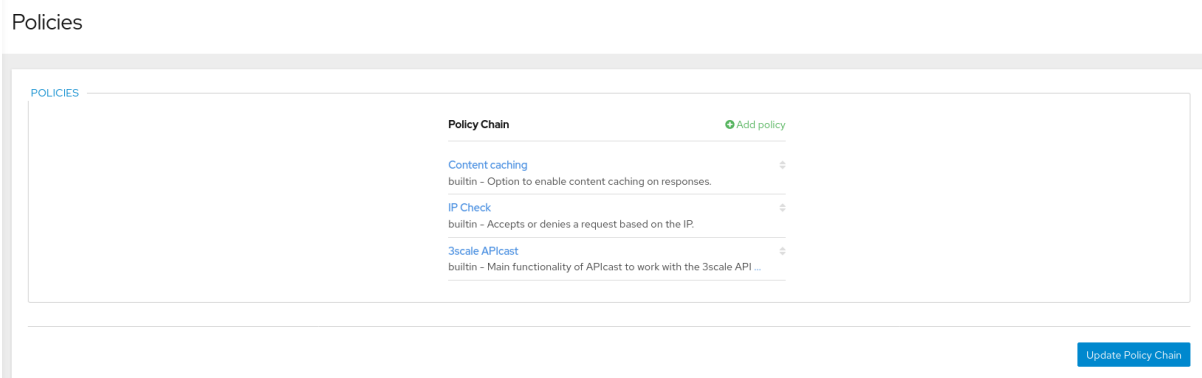
カスタムポリシーが APIcast に追加されて新しいイメージがビルドされ、そのイメージを使用して APIcast がデプロイされると、管理ポータルではそれらのポリシーが利用可能なポリシーとして自動的に表示されます。既存のサービスはこの新しいポリシーを利用可能なポリシーリストで認識できるので、任意のポリシーチェーンで使用することができます。

カスタムポリシーがイメージから削除され、APIcast が再起動されると、そのポリシーはリスト上で利用可能なポリシーとは表示されなくなるので、ポリシーチェーンに追加することができなくなります。

4.5. 3SCALE でのポリシーチェーンの作成

APIcast ゲートウェイ設定の一部として、3scale でポリシーチェーンを作成します。管理ポータルでポリシーチェーンを変更するには、以下の手順に従います。

1. 3scale にログインします。
2. ポリシーチェーンを設定する API プロダクトに移動します。
3. **[your_product_name] > Integration > Policies**の順に移動し、**Add policy** をクリックします。
4. **Policy Chain** セクションで、矢印アイコンを使用してポリシーチェーン内のポリシーの順番を変更します。必ず **3scale APIcast** ポリシーをポリシーチェーンの最後に設定します。



5. **Update Policy Chain** ボタンをクリックし、ポリシーチェーンを保存します。

4.6. ポリシーチェーン JSON 設定ファイルの作成

APIcast のネイティブデプロイメントを使用している場合には、JSON 設定ファイルを作成して、AMP の外部でポリシーチェーンを制御することができます。

ポリシーチェーン JSON 設定ファイルには、以下の情報で設定される JSON 配列が含まれます。

- **services** オブジェクト (**id** の値 (ポリシーチェーンが適用されるサービスを指定する数字) が含まれる)
- **proxy** オブジェクト (policy_chain オブジェクトおよび下位オブジェクトが含まれる)
- **policy_chain** オブジェクト (ポリシーチェーンを定義する値が含まれる)
- 個々の **policy** オブジェクト (ポリシーを識別しポリシーの動作を設定するのに必要な **name** および **configuration** データの両方を指定する)

カスタムポリシー **sample_policy_1** および標準の API イントロスペクションポリシー **token_introspection** で設定されるポリシーチェーンの例を、以下に示します。

```
{
  "services":[
    {
      "id":1,
      "proxy":{
        "policy_chain":[
          {
            "name":"sample_policy_1", "version": "1.0",
            "configuration":{
              "sample_config_param_1":["value_1"],
              "sample_config_param_2":["value_2"]
            }
          },
          {
            "name": "token_introspection", "version": "builtin",
            "configuration": {
              introspection_url:["https://tokenauthorityexample.com"],
              client_id:["exampleName"],
              client_secret:["secretexamplekey123"]
          },
          {
             "name": "apicast", "version": "builtin",
          }
        ]
      }
    }
  ]
}
```

すべてのポリシーチェーンには、内蔵のポリシー **apicast** を含める必要があります。APIcast をポリシーチェーンのどこに設定したかによって、ポリシーの動作が変わります。

第5章 ポリシーチェーンと APICAST ネイティブデプロイメントのインテグレーション

ネイティブ APIcast デプロイメントの場合、**THREESCALE_CONFIG_FILE** 環境変数を使用して設定ファイルを指定することにより、カスタムポリシーチェーン を統合することができます。以下の例では、設定ファイル **example.json** を指定しています。

```
THREESCALE_CONFIG_FILE=example.json bin/apicast
```

5.1. ポリシーでの変数およびフィルターの使用

一部の「APIcast 標準ポリシー」では Liquid テンプレートがサポートされます。Liquid テンプレートにより、通常の文字列値だけでなくリクエストのコンテキストに存在する変数も使用することができます。

コンテキスト変数を使用するには、その名前を **{{** および **}}** で囲みます (例: **{{ uri }}**)。変数がオブジェクトの場合には、その属性にもアクセスすることができます (例: **{{ somevar.attr }}**)。

すべてのポリシーで使用することのできる標準の変数を以下に示します。

- **uri**: クエリーパラメーターを除外したリクエストのパス。組み込まれた NGINX 変数 **$uri** の値
- **host**: リクエストのホスト (組み込まれた NGINX 変数 **$host** の値)
- **remote_addr**: クライアントの IP アドレスト (組み込まれた NGINX 変数 **$remote_addr** の値)
- **headers**: リクエストヘッダーが含まれるオブジェクト。特定のヘッダーの値を取得するには、**{{headers['Some-Header']}}** を使用します。
- **http_method**: リクエストのメソッド (GET、POST 等)

これらの標準変数はリクエストのコンテキストで使用されますが、ポリシーではコンテキストにさらに変数を追加することができます。なお、ここで使われるフェーズとは、APIcast のすべての実行ステップを指します。以下に示す状況では、ポリシーチェーンのすべてのポリシーで変数を使用することができます。

- 同一フェーズ内 (ポリシーで変数が追加され、追加後に次のポリシーで使用される)。
- 次フェースで (あるフェーズで変数が追加され、その変数が次のフェーズで使用される)。

標準の 3scale APIcast ポリシーでコンテキストに追加される変数の例を以下に示します。

- **jwt**: 解析された JWT トークンの JSON ペイロード (OpenID Connect 認証用)
- **credentials**: アプリケーションのクレデンシャルを保持するオブジェクト。たとえば **"app_id": "972f7b4f"**、**"user_key": "13b668c4d1e10eaebaa5144b4749713f"** 等。
- **service**: 現在のリクエストが処理されるサービスの設定を保持するオブジェクト。たとえば、サービス ID は {{ service.id }} として利用可能です。

コンテキストで使用することのできるオブジェクトおよび値の完全なリストは、「Liquid Context Debug」を参照してください。

変数は Liquid テンプレートの機能を活用して使用されます。たとえば **{{ remote_addr }}**、**{{ headers['Some-Header'] }}**、**{{ jwt.aud }}** 等。値に変数をサポートするポリシーは、**_type** 接尾辞が

付く特殊なパラメーターを持ちます (例: **value_type**、**name_type** 等)。このパラメーターには、2 つの値を設定することができます (プレーンテキストの場合の plain および liquid テンプレートの場合の liquid)。

APIcast では、変数の値に適用することのできる Liquid フィルターもサポートされます。フィルターは Liquid 変数の値に NGINX 関数を適用します。

フィルターは変数出力タグ **{{ }}** で囲み、変数の名前または実際の値、パイプ記号 |、およびフィルター名の順に定義します。以下に例を示します。

- **{{ 'username:password' | encode_base64 }}** (ここで **username:password** が変数)
- **{{ uri | escape_uri }}**

パラメーターを必要としないフィルターもあります。この場合には、変数の代わりに空の文字列を使用することができます。たとえば、**{{ '' | utctime }}** は現在の時刻を TUC タイムゾーンで返します。

フィルターは、**{{ variable | function1 | function2 }}** のようにつなげることができます。たとえば **{{ '' | utctime | escape_uri }}**。

利用可能な関数のリストを以下に示します。

- escape_uri
- unescape_uri
- encode_base64
- decode_base64
- crc32_short
- crc32_long
- hmac_sha1
- md5
- md5_bin
- sha1_bin
- quote_sql_str
- today
- time
- now
- localtime
- utctime
- cookie_time
- http_time

- parse_http_time

第6章 FUSE のポリシーエクステンションを使用した 3SCALE メッセージコンテンツの変換

Red Hat Fuse を使用して、Red Hat 3scale API Management 用の非常に柔軟なポリシーエクステンションを作成することができます。そのためには、Fuse on OpenShift でポリシーエクステンションを作成し、それらを 3scale 管理ポータルでポリシーとして設定します。APIcast Camel プロキシーポリシーを使用して、リクエストおよびレスポンスのメッセージコンテンツの複雑な変換を実施することができます (例: XML から JSON への変換)。この変換は、Apache Camel インテグレーションのフレームワークに実装されます。

さらに、静的な APIcast コンテナーイメージを再ビルドして再デプロイする代わりに、Camel でカスタムポリシーエクステンションを動的に追加または変更することができます。Camel Domain Specific Language (DSL) で書かれた任意の Camel Enterprise Integration Pattern (EIP) を使用して、APIcast ポリシーエクステンションを実装することができます。これにより、Java や XML 等の使い慣れたプログラミング言語を使用して、ポリシーエクステンションを作成することができます。本トピックの例では、Camel Netty4 HTTP コンポーネントを使用して、HTTP プロキシーを Java で実装しています。

注記

3scale API バックエンドですでに Fuse Camel アプリケーションを使用している場合は、この機能は必要ありません。この場合は、既存の Fuse Camel アプリケーションを使用して変換を実施することができます。

必要なソフトウェアコンポーネント

以下の Red Hat Integration コンポーネントを同じ OpenShift クラスターにデプロイしている必要があります。

- Fuse on OpenShift 7.7
- オンプレミス型 3scale 2.9
- Embedded APIcast (ステージングおよび実稼働環境用のデフォルトゲートウェイ)、または Self-managed APIcast

カスタム Fuse ポリシーを 3scale とは別の OpenShift プロジェクトにデプロイすることができますが、これは必須の要件ではありません。ただし、両プロジェクト間で通信ができるようにしてください。詳細については、Networking の Configuring network policy with OpenShift SDN を参照してください。

関連情報

- Fuse on OpenShift ガイド

6.1. APICAST と FUSE の APACHE CAMEL による変換のインテグレーション

APIcast と Fuse on OpenShift で Apache Camel アプリケーションとして記述された変換を統合することができます。ポリシーエクステンションによる変換が 3scale に設定およびデプロイされると、3scale トラフィックは Camel ポリシーエクステンションを通過し、メッセージのコンテンツが変換されます。この場合、Camel はリバース HTTP プロキシーとして機能し、APIcast は Camel に 3scale トラフィックを送信し、Camel がそのトラフィックを API バックエンドに送信します。

本トピックの例では、Camel Netty4 HTTP コンポーネントを使用して HTTP プロキシーを作成しています。

- HTTP プロキシープロトコルを通じて受け取ったリクエストは、HTTP ボディーが大文字に変換されて目的のサービスに転送されます。
- 目的のサービスからのレスポンスは大文字への変換処理を受け、続いてクライアントに戻されます。
- 以下の例で、HTTP および HTTPS のユースケースに必要な設定を説明します。

前提条件

- Fuse on OpenShift 7.7 および 3scale 2.9 を、同じ OpenShift クラスターにデプロイしている必要があります。インストールの詳細については、以下のドキュメントを参照してください。
  - Fuse on OpenShift ガイド
  - 3scale のインストール
- Fuse on OpenShift および 3scale をインストールしてプロジェクトを作成するには、クラスターの管理者権限が必要です。ただし、プロジェクトごとの編集アクセス権限で、デプロイ設定の作成、Pod のデプロイ、およびサービスの作成が可能です。

手順

1. Camel **netty4-http** コンポーネントを使用して Java で Apache Camel アプリケーションを作成し、HTTP プロキシーを実装します。これにより、任意の Camel コンポーネントを使用して、メッセージを変換することができます。
   以下に示す簡単な例では、リクエストおよびサービスからのレスポンスを大文字に変換します。

```
import java.nio.file.Files;
import java.nio.file.Path;
import java.util.Locale;

import org.apache.camel.Exchange;
import org.apache.camel.Message;
import org.apache.camel.builder.RouteBuilder;
import org.apache.camel.model.RouteDefinition;

public class ProxyRoute extends RouteBuilder {

    @Override
    public void configure() throws Exception {
        final RouteDefinition from;
        if (Files.exists(keystorePath())) {
            from = from("netty4-http:proxy://0.0.0.0:8443?
ssl=true&keyStoreFile=/tls/keystore.jks&passphrase=changeit&trustStoreFile=/tls/keystore.jks"
); (1)
        } else {
            from = from("netty4-http:proxy://0.0.0.0:8080");
        }

        from
            .process(ProxyRoute::uppercase)
            .toD("netty4-http:"
                + "${headers." + Exchange.HTTP_SCHEME + "}://" (2)
                + "${headers." + Exchange.HTTP_HOST + "}:"
```

```
                + "${headers." + Exchange.HTTP_PORT + "}"
                + "${headers." + Exchange.HTTP_PATH + "}")
            .process(ProxyRoute::uppercase);
    }

    Path keystorePath() {
        return Path.of("/tls", "keystore.jks");
    }

    public static void uppercase(final Exchange exchange) { (3)
        final Message message = exchange.getIn();
        final String body = message.getBody(String.class);
        message.setBody(body.toUpperCase(Locale.US));
    }

}
```

1. この簡単な例では、Java キーストアファイルが **/tls/keystore.jks** にマウントされている場合、リスニングポートは **8443** に設定されます。
2. 3scale により Camel プロキシーポリシーが呼び出されると、**HTTP_SCHEME**、**HTTP_HOST**、**HTTP_PORT**、および **HTTP_PATH** ヘッダーの値は、3scale のバックエンド API に設定された値を元に自動的に設定されます。
3. この簡単な例では、メッセージの内容が大文字に変換されます。Camel エンタープライズ統合パターンを使用して、リクエストおよびレスポンスメッセージの内容のより複雑な変換を実施することができます (例: XML から JSON への変換)。

2. Camel アプリケーションを OpenShift にデプロイし、それをサービスとして公開します。詳細は、Fuse on OpenShift でのアプリケーションの作成およびデプロイ を参照してください。

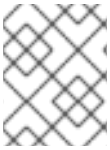
関連情報

- Apache Camel Component Reference の Netty4 HTTP Component

6.2. FUSE ON OPENSHIFT の APACHE CAMEL を使用して作成された APICAST ポリシーエクステンションの設定

Fuse on OpenShift を使用した Apache Camel による変換を実装したら、3scale 管理ポータルを使用して APIcast ポリシーチェーンのポリシーエクステンションとして設定することができます。

ポリシーエクステンションにより、Camel HTTP プロキシーを使用するように 3scale プロダクトを設定することができます。このサービスを使用して HTTP プロキシー経由で 3scale トラフィックを送信し、サードパーティープロキシーでリクエスト/レスポンスの変更を実施します。ここでは、サードパーティープロキシーは Fuse on OpenShift を使用して実装された Apache Camel です。TLS を使用して Camel HTTP プロキシーサービスにセキュアに接続するように、APIcast を設定することもできます。



注記

ポリシーエクステンションコードは Fuse on OpenShift の Apache Camel アプリケーションで実装されており、3scale から変更したり削除したりすることはできません。

前提条件

- Fuse on OpenShift 7.7 および 3scale 2.9 を、同じ OpenShift クラスターにデプロイしている必要があります。インストールの詳細については、以下のドキュメントを参照してください。
  - Fuse on OpenShift ガイド
  - 3scale のインストール
- Fuse on OpenShift の Apache Camel アプリケーションを使用して、APIcast ポリシーエクステンションを実装している必要があります。「APIcast と Fuse の Apache Camel による変換のインテグレーション」を参照してください。
- OpenShift Pod に Apache Camel アプリケーションをデプロイし、それをサービスとして公開している必要があります。詳細は、Fuse on OpenShift ガイドの Fuse on OpenShift でのアプリケーションの作成およびデプロイ を参照してください。

手順

1. 3scale 管理ポータルで **Integration** > **Policies** の順に選択します。
2. **POLICIES** > **Add policy** > **Camel Service** の順に選択します。
3. 適切なフィールドに、Camel HTTP プロキシーサービスに接続するための OpenShift ルートを入力します。
   - **https_proxy**: **http** プロトコルおよび TLS ポートを使用して、Camel HTTPS プロキシーに接続します。以下に例を示します。

     ```
     http://camel-proxy.my-3scale-management-project.svc:8443
     ```

   - **http_proxy**: **http** プロトコルおよびポートを使用して、Camel HTTP プロキシーに接続します。以下に例を示します。

     ```
     http://camel-proxy.my-3scale-management-project.svc:8080
     ```

   - **all_proxy**: プロトコルが指定されない場合に、**http** プロトコルおよびポートを使用して、Camel HTTP プロキシーに接続します。以下に例を示します。

     ```
     http://camel-proxy.my-3scale-management-project.svc:8080
     ```

4. 更新されたポリシー設定をステージング環境または実稼働環境にプロモートします。たとえば、**Promote v.3 to Staging APIcast**をクリックします。
5. 3scale **curl** コマンドを使用して、APIcast ポリシーの設定をテストします。以下に例を示します。

   ```
   curl "https://testapi-3scale-apicast-staging.myuser.app.dev.3sca.net:443/?
   user_key=MY_USER_KEY" -k
   ```

   APIcast は、Camel HTTP プロキシーへの接続に新しい TLS セッションを確立します。
6. メッセージのコンテンツが変換されていることを確認します。この例では大文字に変換されます。

7. APIcast をバイパスし、TLS を使用して直接 Camel HTTP プロキシーをテストする場合は、カスタム HTTP クライアントを使用する必要があります。たとえば、**netcat** コマンドを使用することができます。

```
$ print "GET https://mybackend.example.com HTTP/1.1\nHost:
mybackend.example.com\nAccept: */*\n\n" | ncat --no-shutdown --ssl my-camel-proxy 8443
```

この例では、**GET** の後に完全な URL を使用して HTTP プロキシーリクエストを作成し、 **ncat --ssl** パラメーターを使用してポート **8443** の **my-camel-proxy** ホストへの TLS 接続を指定しています。

注記

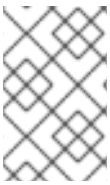
プロキシーは **CONNECT** メソッドを使用した HTTP トンネリングをサポートしないため、**curl** またはその他の一般的な HTTP クライアントを使用して Camel HTTP プロキシーを直接テストすることはできません。**CONNECT** で HTTP トンネリングを使用する場合、トランスポートはエンドツーエンドで暗号化され、Camel HTTP プロキシーはペイロードを仲介することはできません。

関連情報

- 「Camel Service」

第7章 APICAST の環境変数

APIcast の環境変数を使用すると、APIcast の動作を変更することができます。サポートされている環境変数の値を以下に示します。



注記

- サポートされていない環境変数および非推奨の環境変数は記載されていません
- 一部の環境変数の機能は、APIcast ポリシーに移されています

- all_proxy、ALL_PROXY
- APICAST_ACCESS_LOG_FILE
- APICAST_BACKEND_CACHE_HANDLER
- APICAST_CACHE_MAX_TIME
- APICAST_CACHE_STATUS_CODES
- APICAST_CONFIGURATION_CACHE
- APICAST_CONFIGURATION_LOADER
- APICAST_CUSTOM_CONFIG
- APICAST_ENVIRONMENT
- APICAST_EXTENDED_METRICS
- APICAST_HTTPS_CERTIFICATE
- APICAST_HTTPS_CERTIFICATE_KEY
- APICAST_HTTPS_PORT
- APICAST_HTTPS_VERIFY_DEPTH
- APICAST_LOAD_SERVICES_WHEN_NEEDED
- APICAST_LOG_FILE
- APICAST_LOG_LEVEL
- APICAST_MANAGEMENT_API
- APICAST_MODULE
- APICAST_OIDC_LOG_LEVEL
- APICAST_PATH_ROUTING
- APICAST_PATH_ROUTING_ONLY
- APICAST_POLICY_LOAD_PATH

- APICAST_PROXY_HTTPS_CERTIFICATE
- APICAST_PROXY_HTTPS_CERTIFICATE_KEY
- APICAST_PROXY_HTTPS_PASSWORD_FILE
- APICAST_PROXY_HTTPS_SESSION_REUSE
- APICAST_REPORTING_THREADS
- APICAST_RESPONSE_CODES
- APICAST_SERVICE_CACHE_SIZE
- APICAST_SERVICE_${ID}_CONFIGURATION_VERSION
- APICAST_SERVICES_LIST
- APICAST_SERVICES_FILTER_BY_URL
- APICAST_UPSTREAM_RETRY_CASES
- APICAST_WORKERS
- BACKEND_ENDPOINT_OVERRIDE
- HTTP_KEEPALIVE_TIMEOUT
- http_proxy HTTP_PROXY
- https_proxy HTTPS_PROXY
- no_proxy NO_PROXY
- OPENSSL_VERIFY
- OPENTRACING_CONFIG
- OPENTRACING_HEADER_FORWARD
- OPENTRACING_TRACER
- RESOLVER
- THREESCALE_CONFIG_FILE
- THREESCALE_DEPLOYMENT_ENV
- THREESCALE_PORTAL_ENDPOINT

all_proxy、ALL_PROXY

デフォルト: 値なし **値**: 文字列 **例**: **http://forward-proxy:80**

プロトコル固有のプロキシーが指定されていない場合に、サービスへの接続に使用される HTTP プロキシーを定義します。認証機能はサポートされていません。

APICAST_ACCESS_LOG_FILE

デフォルト: stdout

アクセスログを保存するファイルを定義します。

APICAST_BACKEND_CACHE_HANDLER

値: strict | resilient

デフォルト: strict

非推奨: この環境変数の代わりに、Caching ポリシーを使用してください。

バックエンドにアクセスすることができない場合に、承認キャッシュがどのように動作するかを定義します。strict に設定すると、バックエンドにアクセスすることができない場合にキャッシュされたアプリケーションを削除します。resilient に設定すると、バックエンドから承認が拒否された場合にのみキャッシュされたアプリケーションを削除します。

APICAST_CACHE_MAX_TIME

デフォルト: 1m

値: 文字列

レスポンスがシステムにキャッシュされる設定の場合、この変数の値はキャッシュされる最大の時間を示します。cache-control ヘッダーが設定されていない場合、キャッシュされる時間はここで定義される時間になります。

この値のフォーマットは、**proxy_cache_valid** NGINX ディレクティブ で定義されます。

このパラメーターは、コンテンツキャッシュポリシーを使用している API によってのみ使用され、リクエストのキャッシュが可能です。

APICAST_CACHE_STATUS_CODES

デフォルト: 200、302

値: 文字列

アップストリームからのレスポンスコードがこの環境変数で定義されるステータスコードのいずれかと一致する場合、レスポンスの内容が NGINX にキャッシュされます。キャッシュされる時間は、ヘッダーキャッシュ時間の値または **APICAST_CACHE_MAX_TIME** 環境変数で定義される最大時間のいずれかに依存します。

このパラメーターは、コンテンツキャッシュポリシーを使用している API によってのみ使用され、リクエストのキャッシュが可能です。

APICAST_CONFIGURATION_CACHE

値: 数字

デフォルト: 0

設定を保存する間隔 (秒単位) を指定します。0 (ブート値の **APICAST_CONFIGURATION_LOADER** との互換性はない) または 60 より大きい値を設定する必要があります。たとえば、**APICAST_CONFIGURATION_CACHE** を 120 に設定すると、ゲートウェイは 2 分 (120 秒) ごとに設定を API Manager から読み込み直します。負の値を設定すると、再読み込みは無効になります。

APICAST_CONFIGURATION_LOADER

値: boot | lazy

デフォルト: lazy

設定の読み込み方法を定義します。boot に設定すると、ゲートウェイの起動時に API Manager に設定

を要求します。lazy に設定すると、リクエストを受信するたびに設定を読み込みます (リクエストのたびに完全にリフレッシュするには、**APICAST_CONFIGURATION_CACHE** を 0 に設定する必要があります)。

APICAST_CUSTOM_CONFIG

非推奨: この環境変数の代わりに、policies を使用してください。

既存の APIcast ロジックをオーバーライドするカスタムロジックを実装する Lua モジュールの名前を定義します。

APICAST_ENVIRONMENT

デフォルト:

値: 文字列[:]

例: production:cloud-hosted

APIcast は、環境 (またはパス) のリストをコンマ (**:**) 区切りで読み込む必要があります。このリストは、CLI の **-e** または **--environment** パラメーターの代わりに使用することができ、たとえばデフォルト環境としてコンテナーイメージに保存されます。CLI で渡される値は、常にこの変数に優先します。

APICAST_EXTENDED_METRICS

デフォルト: false

値: ブール値

例:true

Prometheus メトリクスに関する追加情報を有効にします。以下のメトリクスでは **service_id** および **service_system_name** ラベルを使用することができ、APIcast をより詳細に設定することができます。

- **total_response_time_seconds**
- **upstream_response_time_seconds**
- **upstream_status**

APICAST_HTTPS_CERTIFICATE

デフォルト: 値なし

HTTPS 接続用 X.509 証明書が含まれる PEM 形式ファイルへのパス

APICAST_HTTPS_CERTIFICATE_KEY

デフォルト: 値なし

X.509 証明書の秘密鍵が含まれる PEM 形式ファイルへのパス

APICAST_HTTPS_PORT

デフォルト: 値なし

HTTPS 接続用に APIcast がリッスンを開始するポートを制御します。この設定が HTTP 用ポートと競合する場合には、HTTPS 用にだけ使用されます。

APICAST_HTTPS_VERIFY_DEPTH

デフォルト:1

値: 正の整数

クライアント証明書チェーンの最大長を定義します。このパラメーターの値が **1** の場合は、クライアント証明書チェーンに追加の証明書を含めることができます。たとえば、ルート認証局などです。

APICAST_LOAD_SERVICES_WHEN_NEEDED

値:

- **真** の場合には **true** または **1**
- **偽** の場合には **false**、**0**、または空欄

デフォルト: false

多くのサービスが設定されている場合に、このオプションを使用することができます。ただし、そのパフォーマンスは、サービスの数、APIcast と 3scale 管理ポータル間のレイテンシー、設定の残存期間 (TTL) など、他の要素に依存します。

デフォルトでは、APIcast が管理ポータルから設定をダウンロードするたびに、すべてのサービスが読み込みます。このオプションを有効にすると、設定にレイジーローディングが使用されます。APIcast は、リクエストの Host ヘッダーで指定したホストに設定されたサービスだけを読み込みます。

注記

- **APICAST_CONFIGURATION_CACHE** で定義されたキャッシュ動作が適用されます。
- **APICAST_CONFIGURATION_LOADER** が **boot** に設定されている場合には、このオプションは無効になります。
- **APICAST_PATH_ROUTING** との互換性はありません。

APICAST_LOG_FILE

デフォルト: stderr

OpenResty エラーログが含まれるファイルを定義します。このファイルは、**bin/apicast** の **error_log** ディレクティブで使用されます。ファイルパスは、絶対パスまたは APIcast プリフィックスディレクトリーへの相対パスのいずれかで指定します。デフォルトの接頭辞ディレクトリーは APIcast である点に注意してください。詳細は、NGINX のドキュメント を参照してください。

APICAST_LOG_LEVEL

値: debug | info | notice | warn | error | crit | alert | emerg

デフォルト: warn

OpenResty ログのログレベルを指定します。

APICAST_MANAGEMENT_API

値:

- **disabled**: 完全に無効で、ポートをリッスンするだけの状態
- **status**: ヘルスチェック用に、/status/ エンドポイントだけが有効な状態
- **debug**: API 全体がオープンな状態

Management API の機能は強力で、APIcast の設定を制御することができます。debug レベルは、デバッグ用途にのみ有効にしてください。

APICAST_MODULE

デフォルト: apicast

非推奨: この環境変数の代わりに、policies を使用してください。

API ゲートウェイロジックを実装するメインの Lua モジュール名を指定します。カスタムモジュールは、デフォルトの **apicast.lua** モジュールの機能に優先します。モジュールの使用方法の 例 を参照してください。

APICAST_OIDC_LOG_LEVEL

値: debug | info | notice | warn | error | crit | alert | emerg

デフォルト: err

OpenID Connect インテグレーションに関するログのログレベルを設定することができます。

APICAST_PATH_ROUTING

値:

- 真の場合には **true** または **1**
- 偽の場合には **false**、**0**、または空欄

このパラメーターを **true** に設定すると、ゲートウェイはデフォルトのホストベースのルーティングに加えて、パスベースのルーティングを使用します。API リクエストは、リクエストの **Host** ヘッダーの値が **Public Base URL** にマッチするサービスの中で、マッピングルールが最初にマッチするサービスにルーティングされます。

APICAST_PATH_ROUTING_ONLY

値:

- 真の場合には **true** または **1**
- 偽の場合には **false**、**0**、または空欄

このパラメーターを **true** に設定すると、ゲートウェイはパスベースのルーティングを使用し、デフォルトのホストベースのルーティングにはフォールバックしません。API リクエストは、リクエストの **Host** ヘッダーの値が **公開ベース URL** にマッチするサービスの中で、マッピングルールが最初にマッチするサービスにルーティングされます。

このパラメーターは、APICAST_PATH_ROUTING に優先します。**APICAST_PATH_ROUTING_ONLY** が有効な場合は、APIcast は **APICAST_PATH_ROUTING** の値に関わらずパスベースのルーティングだけを実施します。

APICAST_POLICY_LOAD_PATH

デフォルト: **APICAST_DIR/policies**

値: 文字列[:]

例: **~/apicast/policies:$PWD/policies**

APIcast がポリシーを探すパスのコロン (**:**) 区切りリスト。開発用ディレクトリーから最初にポリシーを読み込む場合や、例を読み込む場合に使用することができます。

APICAST_PROXY_HTTPS_CERTIFICATE

デフォルト:

値: 文字列

例: /home/apicast/my_certificate.crt

APIcast がアップストリームと接続する際に使用するクライアント SSL 証明書へのパス。この証明書が設定内のすべてのサービスに使用される点に注意してください。

APICAST_PROXY_HTTPS_CERTIFICATE_KEY

デフォルト:

値: 文字列

例: /home/apicast/my_certificate.key

クライアント SSL 証明書の鍵へのパス

APICAST_PROXY_HTTPS_PASSWORD_FILE

デフォルト:

値: 文字列

例: /home/apicast/passwords.txt

APICAST_PROXY_HTTPS_CERTIFICATE_KEY で指定する SSL 証明書の鍵のパスフレーズが含まれるファイルへのパス

APICAST_PROXY_HTTPS_SESSION_REUSE

デフォルト: on

値:

- **on**: SSL セッションを再利用します。
- **off**: SSL セッションを再利用しません。

APICAST_REPORTING_THREADS

デフォルト: 0

値: 0 または正の整数

実験的機能: 負荷が極端に大きい場合のパフォーマンスは予測が不可能で、レポートが失われる可能性があります。

0 より大きい値を設定すると、バックエンドへの非同期のレポートが有効になります。これは、パフォーマンスを向上させるための新たな **実験的** 機能です。クライアントにはバックエンドのレイテンシーは適用されず、すべてが非同期状態で処理されます。この値により、同時に実行することのできる非同期レポートの数を決定します。レポート数がこの値を超えると、クライアントにスロットリングが適用され、レイテンシーが追加されます。

APICAST_RESPONSE_CODES

値:

- 真の場合には **true** または **1**

- 偽の場合には **false**、**0**、または空欄

デフォルト: 空欄 (**false**)

true に設定すると、APIcast は API バックエンドから返されたレスポンスのレスポンスコードを 3scale に記録します。レスポンスコード機能の詳細は、3scale カスタマーポータル を参照してください。

APICAST_SERVICE_CACHE_SIZE

値: 0 または正の整数

デフォルト: 1000

APIcast が内部キャッシュに保存することのできるサービスの数を指定します。Lua の **lru** キャッシュによりすべてのエントリーが初期化されるので、大きな値を設定するとパフォーマンスに影響が出ます。

APICAST_SERVICE_${ID}_CONFIGURATION_VERSION

${ID} を実際のサービス ID に置き換えてください。値は、管理ポータルの設定履歴に表示される設定バージョンにする必要があります。特定のバージョンに設定すると自動更新されなくなり、常にそのバージョンが使用されます。

APICAST_SERVICES_LIST

値: サービス ID のコンマ区切りリスト

APICAST_SERVICES_LIST 環境変数を使用して、3scale API Manager で設定されているサービスにフィルターを適用します。この環境変数は、ゲートウェイの特定サービスの設定にだけ適用され、リストで指定されていないサービス ID は無視されます。プロダクトのサービス識別子は、管理ポータルの **Products > [Your_product_name] > Overview**に移動し、続いて、**Configuration, Methods and Settings** および **ID for API calls**を参照して確認することができます。

APICAST_SERVICES_FILTER_BY_URL

値: **.*.example.com** 等の PCRE (Perl 互換正規表現)

3scale API Manager で設定されているサービスにフィルターを適用します。

このフィルターは、公開ベース **URL** を照合します。フィルターにマッチしないサービスは、無視されます。正規表現をコンパイルすることができない場合には、サービスは読み込まれません。

注記

フィルターにはマッチしないが「APICAST_SERVICES_LIST」に **含まれる** サービスは、無視されません。

例7.1 例を示します。

正規表現フィルター **http://.*.foo.dev** が以下のバックエンドのエンドポイントに適用される。

1. http://staging.foo.dev
2. http://staging.bar.dev
3. http://prod.foo.dev
4. http://prod.bar.dev

この場合、**1** および **3** は Embedded APIcast に設定され、 **2** および **4** は無視されます。

I

APICAST_UPSTREAM_RETRY_CASES

値: error | timeout | invalid_header | http_500 | http_502 | http_503 | http_504 | http_403 | http_404 | http_429 | non_idempotent | off

注記

この環境変数は Retry ポリシーが設定されている場合にのみ使用され、いつアップストリーム API へのリクエストを再試行するかを指定します。Nginx の PROXY_NEXT_UPSTREAM モジュール と同じ値を設定することができます。

APICAST_WORKERS

デフォルト: auto

値: **数字** | auto

この値は、nginx の **worker_processes** ディレクティブ で使用されます。**1** が使用される開発環境を除き、デフォルトの APIcast では **auto** が使用されます。

BACKEND_ENDPOINT_OVERRIDE

設定からのバックエンドエンドポイントをオーバーライドする URI。OpenShift がデプロイした AMP の外部にデプロイする際に役立ちます。**例**: **https://backend.example.com**。

HTTP_KEEPALIVE_TIMEOUT

デフォルト: 75 **値**: 正の整数 **例**: 1

このパラメーターにより、キープアライブ用のクライアント接続がタイムアウトする期間を設定します。この間、サーバー側では接続が開き続けます。値にゼロを設定すると、キープアライブ用のクライアント接続は無効になります。

デフォルトでは、ゲートウェイは HTTP_KEEPALIVE_TIMEOUT を無効にした状態に維持します。この設定により、NGINX からのキープアライブのタイムアウト (デフォルト値は 75 秒) を使用することができます。

http_proxy、HTTP_PROXY

デフォルト: 値なし **値**: 文字列 **例**: **http://forward-proxy:80**

HTTP サービスへの接続に使用される HTTP プロキシーを定義します。認証機能はサポートされていません。

https_proxy、HTTPS_PROXY

デフォルト: 値なし **値**: 文字列 **例**: **https://forward-proxy:443**

HTTPS サービスへの接続に使用される HTTP プロキシーを定義します。認証機能はサポートされていません。

no_proxy、NO_PROXY

デフォルト: 値なし **値**: string\[,<string>\]; * **例**: **foo,bar.com,.extra.dot.com**

リクエストをプロキシーすべきではないホスト名およびドメイン名のコンマ区切りリストを定義します。*1 文字 (すべてのホストとマッチする) を設定すると、実質的にプロキシーは無効になります。

OPENSSL_VERIFY

値:

- **0**、**false**: ピア検証を無効にします
- **1**、**true**: ピア検証を有効にします

OpenSSL ピア検証を制御します。OpenSSL はシステム証明書ストアを使用することができないため、デフォルトではオフになっています。カスタム証明書バンドルを信頼済み証明書に追加する必要があります。

lua_ssl_trusted_certificate を使用して、 export-builtin-trusted-certs により生成される証明書バンドルをポイントすることを推奨します。

OPENTRACING_CONFIG

この環境変数は、OpenTracing トレーサーの設定ファイルを定義するのに使用されます。**OPENTRACING_TRACER** が設定されていない場合には、この変数は無視されます。

それぞれのトレーサーには、デフォルトの設定ファイル * **jaeger: conf.d/opentracing/jaeger.example.json** があります。

この変数を使用してファイルパスを設定することにより、デフォルトで提供されるものとは異なる設定をマウントすることができます。

例: **/tmp/jaeger/jaeger.json**

OPENTRACING_HEADER_FORWARD

デフォルト: **uber-trace-id**

この環境変数は、OpenTracing の情報を転送するのに使用される HTTP ヘッダーを制御します。この HTTP ヘッダーは、アップストリームサーバーに転送されます。

OPENTRACING_TRACER

例: **jaeger**

この環境変数は、読み込むトレースライブラリーを制御します。現時点では、OpenTracing のトレーサーとして利用可能なのは **jaeger** だけです。

空欄の場合には、OpenTracing のサポートは無効です。

RESOLVER

OpenResty で使用されるカスタム DNS リゾルバーを指定することができます。**RESOLVER** パラメーターが空欄の場合には、DNS リゾルバーは自動検出されます。

THREESCALE_CONFIG_FILE

ゲートウェイの設定が含まれる JSON ファイルへのパス。ゲートウェイが正常に動作するには、THREESCALE_PORTAL_ENDPOINT または **THREESCALE_CONFIG_FILE** のどちらかを指定する必要があります。これら 2 つの環境変数のうち、**THREESCALE_CONFIG_FILE** が優先されます。

Proxy Config Show および **Proxy Config Show Latest** エンドポイントは、サービスによって範囲が限定され、**Proxy Configs List** サービスも対象となります。サービスの ID を知っている必要があります。以下のオプションを使用します。

- **Proxy Configs List** プロバイダーエンドポイントを使用します: **<schema>://<admin-portal-domain>/admin/api/account/proxy_configs/<env>.json**
  - エンドポイントは、各サービスの最新のものだけでなく、プロバイダーの保存されているすべてのプロキシー設定を返します。JSON で返された **proxy_configs** の配列を繰り返し処理し、同じ **proxy_config.content.id** (サービスの ID) を持つすべてのプロキシー設定の中で **proxy_config.version** が最も高い **proxy_config.content** を選択します。

- Service List エンドポイントの使用: **/admin/api/services.json**
  - エンドポイントには、プロバイダーのすべてのサービスが一覧表示されます。サービスの配列を繰り返し処理し、サービスごとに、サービスによってスコープが設定された **Proxy Config Show Latest** エンドポイントを消費します。

コンテナーイメージを使用してゲートウェイをデプロイする場合:

1. イメージへのファイルを読み取り専用ボリュームとして設定します。
2. ボリュームをマウントした場所を示すパスを指定します。

設定ファイルの例については、examples フォルダーを参照してください。

THREESCALE_DEPLOYMENT_ENV

値: staging | production

デフォルト: production

この環境変数の値を使用して、新しい APIcast を使用する際に設定をダウンロードする環境 (3scale ステージングまたは実稼働環境) を定義します。

この値は、3scale Service Management API への承認/レポートリクエストのヘッダー **X-3scale-User-Agent** でも使用されます。この値は、3scale では統計のためだけに使用されます。

THREESCALE_PORTAL_ENDPOINT

パスワードおよびポータルエンドポイントが含まれる、以下の形式の URI。

<schema>://<password>@<admin-portal-domain>

ここで、

- **<password>** は、プロバイダーキーまたは 3scale Account Management API のアクセストークンのいずれかです。
- **<admin-portal-domain>** は、3scale 管理ポータルにログインするための URL アドレスです。

例: **https://access-token@account-admin.3scale.net**

THREESCALE_PORTAL_ENDPOINT 環境変数を指定すると、ゲートウェイは初期化時に 3scale から設定をダウンロードします。この設定には、API の Integration ページで指定したすべての設定が含まれます。

この環境変数を使用して、マスター管理ポータルを使用して単一のゲートウェイを作成する こともできます。

ゲートウェイが正常に動作するには、**THREESCALE_PORTAL_ENDPOINT** または **THREESCALE_CONFIG_FILE** (優先) を指定する **必要があります**。

第8章 パフォーマンスを向上させるための APICAST 設定

本セクションでは、APIcast のパフォーマンスの問題をデバッグする際の全般的なガイドラインについて説明します。また、使用可能なキャッシュモードを紹介しパフォーマンスの向上にどのように役立つかを説明します、さらに、同期モードの詳細についても言及します。コンテンツは、以下のセクションで設定されています。

- 「全般的なガイドライン」
- 「デフォルトのキャッシング」
- 「非同期レポートスレッド」
- 「3scale Batcher ポリシー」

8.1. 全般的なガイドライン

典型的な APIcast デプロイメントで考慮すべき 3 つのコンポーネントを以下に示します。

- APIcast
- リクエストを承認し使用状況を追跡する 3scale バックエンドサーバー
- アップストリーム API

APIcast でパフォーマンスの問題が発生している場合には、以下の手順に従います。

- 問題の原因となっているコンポーネントを特定します。
- アップストリーム API のレイテンシーを測定し、APIcast と 3scale バックエンドサーバーで生じるレイテンシーを把握します。
- ベンチマーク試験を実施するのと同じツールを使用して、新たな計測を実施します。ただし、直接アップストリーム API をポイントするのではなく、APIcast をポイントします。

これらの結果を比較することで、APIcast と 3scale バックエンドサーバーで生じるレイテンシーを把握することができます。

ホスト型 (SaaS) システムと Self-managed APIcast の組み合わせにおいて、APIcast と 3scale バックエンドサーバーで生じるレイテンシーが高い場合には、以下の手順に従います。

1. APIcast がデプロイされているマシンから 3scale バックエンドサーバーにリクエストを送信します。
2. レイテンシーを測定します。

3scale バックエンドサーバーは、バージョンを返すエンドポイント https://su1.3scale.net/status を公開します。それに比べて、承認呼び出しは鍵、制限、およびキューのバックグラウンドジョブを検証するため、より多くのリソースを必要とします。3scale バックエンドサーバーはこれらのタスクを数ミリ秒で実行しますが、これには **/status** エンドポイントが処理するようなバージョン確認よりも多くの作業が必要です。たとえば、ご自分の APIcast 環境から **/status** へのリクエストに約 300 ミリ秒かかるとすると、キャッシュされないすべてのリクエストについて、承認にはより長い時間がかかります。

8.2. デフォルトのキャッシング

キャッシュされていないリクエストの場合には、フローは以下のようになります。

1. APIcast は、マッチするマッピングルールから使用状況のメトリクスを抽出します。
2. APIcast は、メトリクスおよびアプリケーションのクレデンシャルを 3scale バックエンドサーバーに送信します。
3. 3scale バックエンドサーバーは、以下の処理を実施します。
   a. アプリケーションキーおよび報告されたメトリクスの使用状況が定義された制限内であることを確認する。
   b. 報告されたメトリクスの使用状況を増やすバックグラウンドジョブをキューに入れる。
   c. リクエストを承認すべきかどうかを APIcast に応答する。
4. リクエストが承認されると、リクエストがアップストリームに送信されます。

この場合、3scale バックエンドサーバーが応答するまで、リクエストはアップストリームに到着しません。

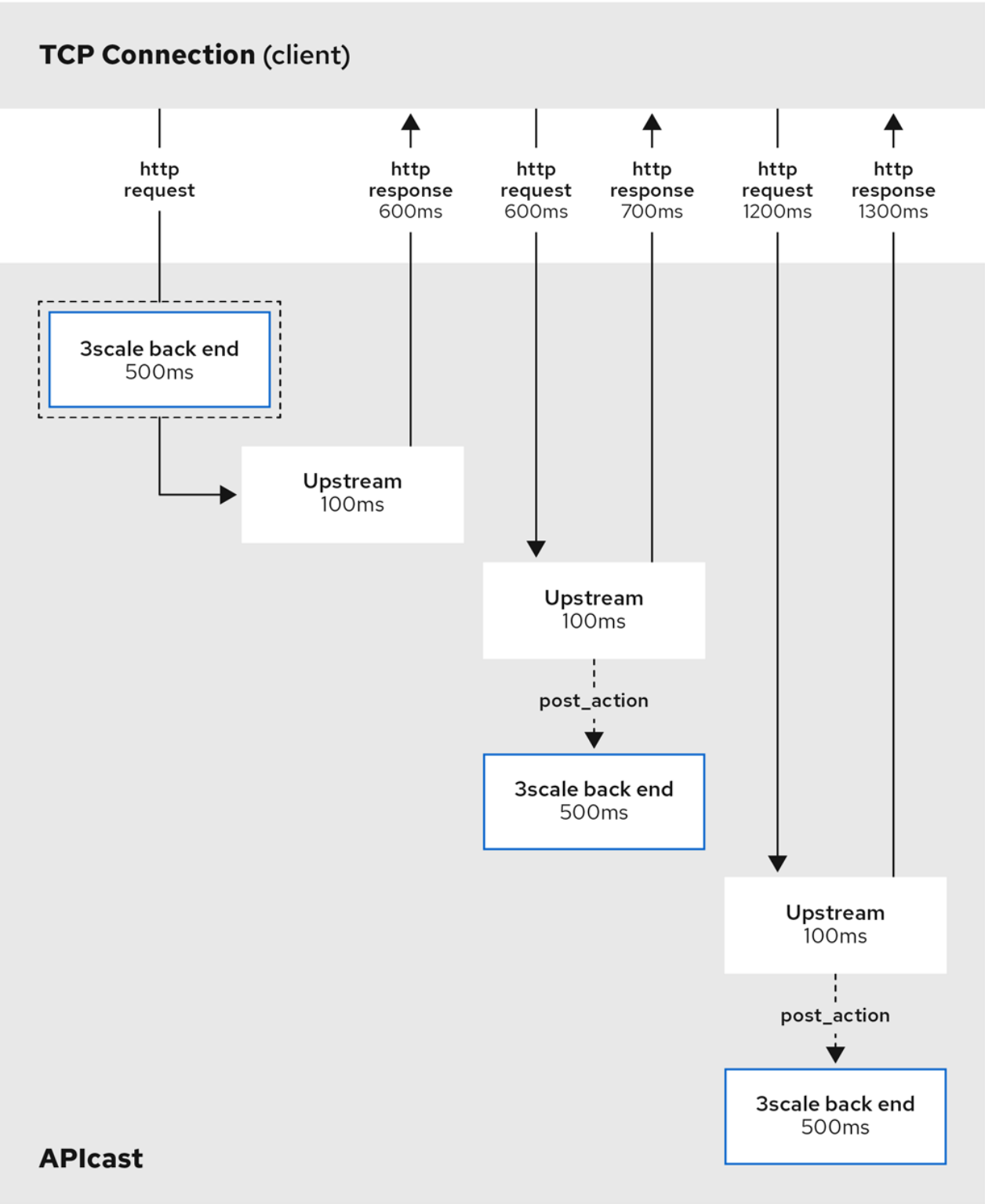
一方、デフォルトで有効になっているキャッシングメカニズムを使用した場合には、フローは以下のようになります。

- 3scale バックエンドサーバーへの承認呼び出しが承認された場合、APIcast はその結果をキャッシュに保存します。
- 同じクレデンシャルおよびメトリクスが使用される次のリクエストは、3scale バックエンドサーバーに照会する代わりに、キャッシュされたその承認を使用します。
- リクエストが承認されなかった場合、または APIcast がそのクレデンシャルを初めて受け取る場合には、APIcast は上述のように同期した状態で 3scale バックエンドサーバーに呼び出しを行います。

認証がキャッシュされている場合には、APIcast はまずアップストリームに呼び出しを行い、続いて **ポストアクション** と呼ばれるフェーズで 3scale バックエンドサーバーに呼び出しを行い、次のリクエスト用に承認をキャッシュに保存します。3scale バックエンドサーバーへの呼び出しはリクエスト時に行われる訳ではないので、レイテンシーが生じない点に注意してください。ただし、同じ接続で送信されたリクエストは、**ポストアクション** フェーズが終了するまで待つ必要があります。

クライアントが **キープアライブ** を使用していて、1 秒ごとにリクエストを送信するシナリオを考えてみます。アップストリームの応答時間が 100 ミリ秒で 3scale バックエンドサーバーへのレイテンシーが 500 ミリ秒の場合、クライアントは毎回 100 ミリ秒でレスポンスを得ます。アップストリームのレスポンスとレポートの合計は 600 ミリ秒かかります。これにより、次のリクエストを受け取るまでにさらに 400 ミリ秒かかります。

以下の図で、上述のデフォルトのキャッシュ動作を説明します。キャッシュメカニズムの動作は、Caching ポリシー を使用して変更することができます。



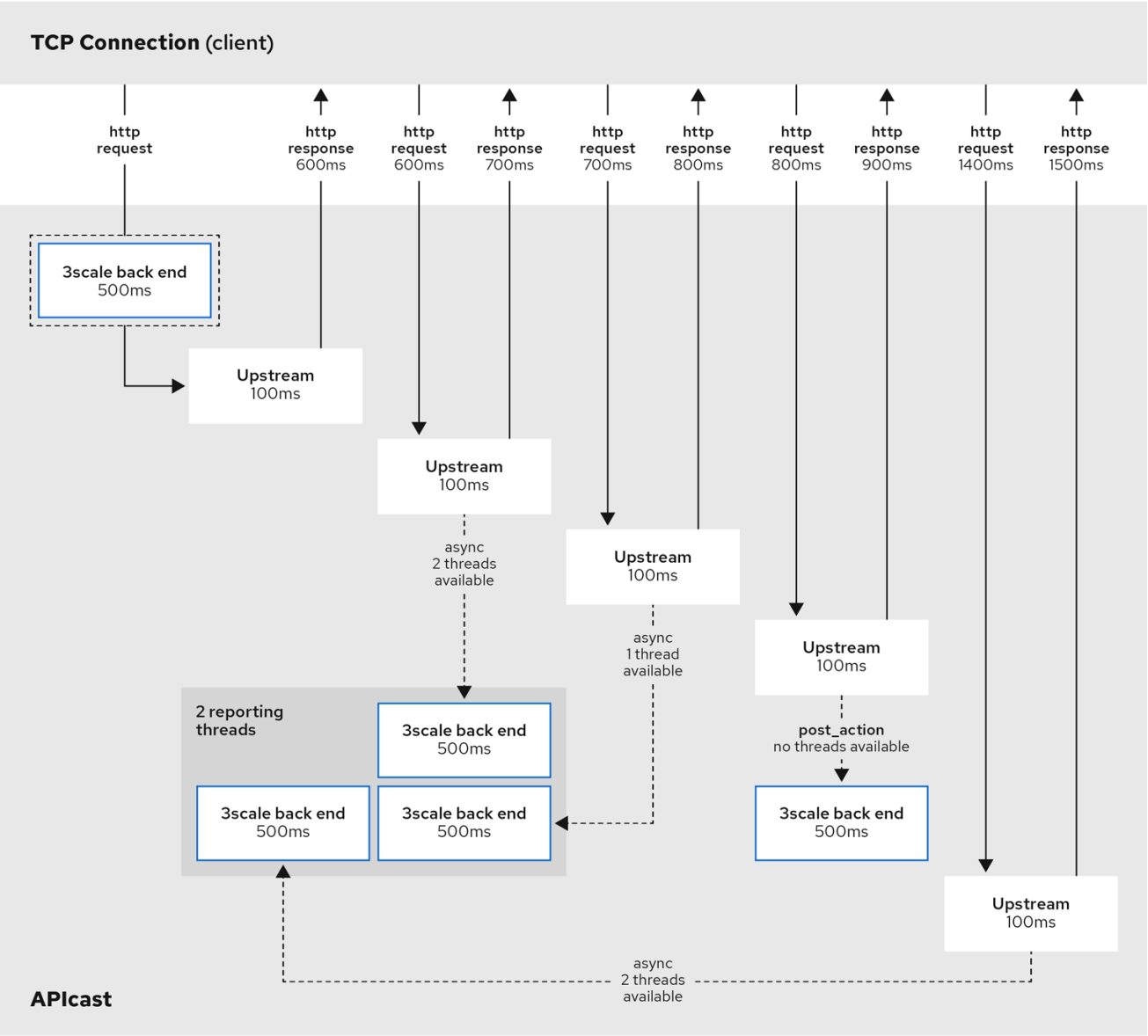
8.3. 非同期レポートスレッド

APIcast には、3scale バックエンドサーバーに対して承認するスレッドのプールを有効にする機能があります。この機能を有効にすると、APIcast はまず同期した状態で 3scale バックエンドサーバーに呼び出しを行い、マッピングルールがマッチするアプリケーションおよびメトリクスを検証します。この動作は、デフォルトで有効になっているキャッシュメカニズムを使用する場合と類似しています。違いは、プール内に空のレポートスレッドがある限り、それ以降の 3scale バックエンドサーバーへの呼び出しが完全に非同期状態で報告されることです。

レポートスレッドはゲートウェイ全体で共通的に使用され、すべてのサービス間で共有されます。2 番目の TCP 接続が確立されると、承認がすでにキャッシュされている限り、完全に非同期になります。空のレポートスレッドがない場合には、同期モードは標準の非同期モードにフォールバックし、ポストアクションフェーズでレポートを行います。

APICAST_REPORTING_THREADS 環境変数を使用して、この機能を有効にすることができます。

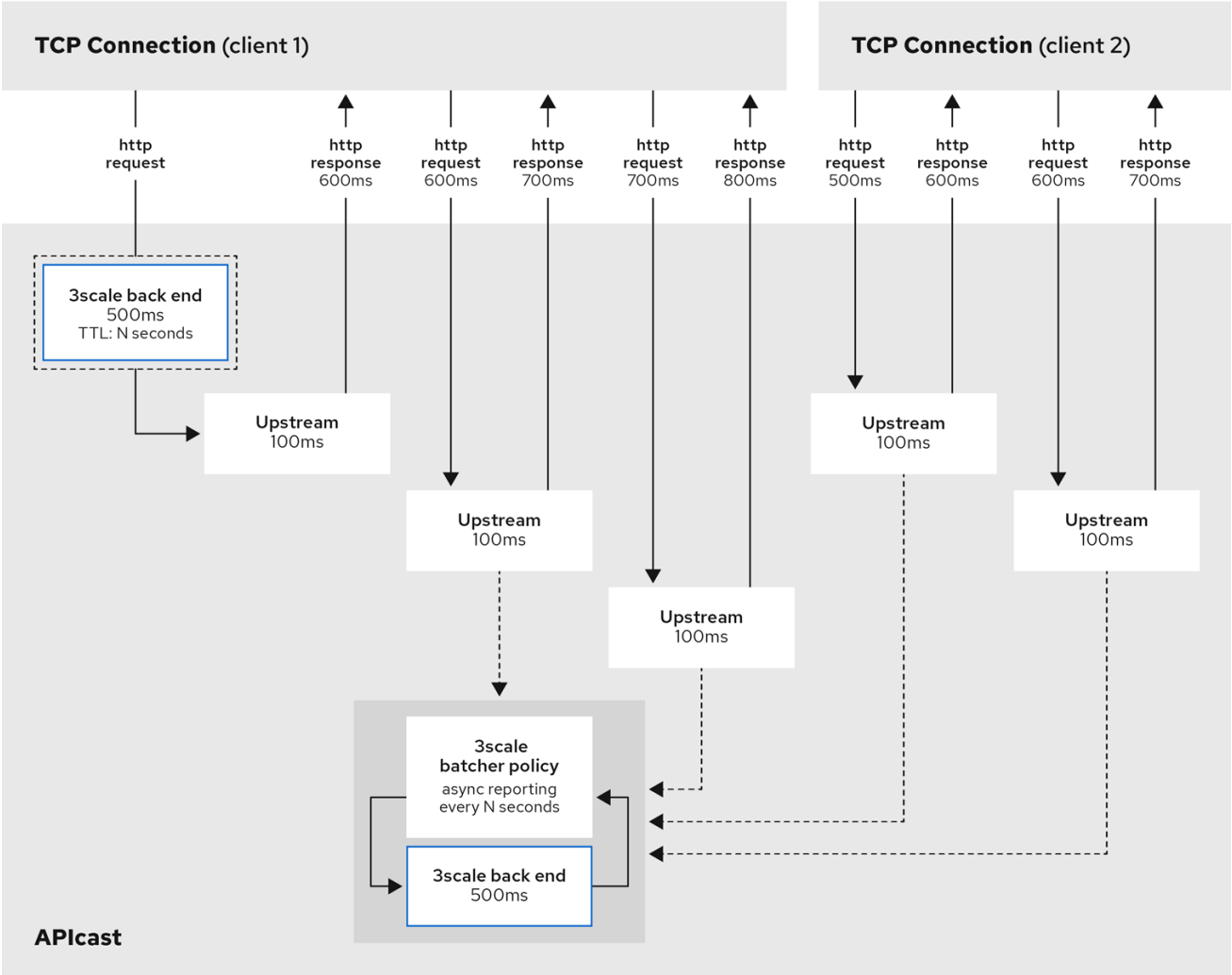
下記の図で、非同期レポートスレッドプールが機能する仕組みを説明します。



8.4. 3SCALE BATCHER ポリシー

デフォルトでは、APIcast はリクエストを受け取るたびに 1 回 3scale バックエンドサーバーに呼び出しを行います。3scale Batcher ポリシーの目的は、3scale バックエンドサーバーに対して行われるリクエストの数を大幅に減らすことにより、レイテンシーを低減しスループットを向上させることです。そのために、このポリシーは承認ステータスをキャッシュし、レポートをバッチ処理します。

「3scale Batcher」に、3scale Batcher ポリシーの詳細を記載しています。以下の図で、このポリシーが機能する仕組みを説明します。



3Scale_38_0819

第9章 PROMETHEUS への 3SCALE APICAST メトリクスの公開

重要

3scale の本リリースでは、Prometheus のインストールおよび設定はサポートされていません。オプションとして、コミュニティーバージョンの Prometheus を使用して、APIcast 管理下の API サービスのメトリクスおよび警告を視覚化することができます。

9.1. PROMETHEUS の概要

Prometheus はオープンソースのシステム監視用ツールキットです。Prometheus を使用して、Red Hat OpenShift 環境にデプロイされた 3scale APIcast のサービスを監視することができます。

Prometheus を使用してサービスを監視するには、サービスは Prometheus エンドポイントを公開する必要があります。このエンドポイントは、メトリクスのリストおよびメトリクスの現在の値を公開する HTTP インターフェイスです。Prometheus は定期的にこれらのターゲット定義のエンドポイントを収集し、収集したデータをそのデータベースに書き込みます。

9.1.1. Prometheus クエリー

Prometheus UI において、Prometheus Query Language (PromQL) でクエリーを作成してメトリクス情報を抽出することができます。PromQL を使用すると、リアルタイムに時系列データを選択して集計することができます。

たとえば、以下のクエリーを使用すると、Prometheus が直近の 5 分間に記録したすべて時系列データから、メトリクス名が **http_requests_total** の値をすべて選択することができます。

```
http_requests_total[5m]
```

メトリックの **ラベル** (キー/値のペア) を指定して、クエリーの結果をさらに定義または絞り込むことができます。たとえば、以下のクエリーを使用すると、Prometheus が直近の 5 分間に記録したすべて時系列データから、メトリクス名が **http_requests_total** でかつ **job** ラベルが **integration** に設定されている値をすべて選択することができます。

```
http_requests_total{job="integration"}[5m]
```

クエリーの結果は、Prometheus の表示ブラウザーでグラフや表として表示したり、Prometheus HTTP API を使用して外部のシステムで処理したりすることができます。Prometheus はデータのグラフィカルビューを提供します。Prometheus メトリクスを表示するより安定したグラフィカルダッシュボードとしては、Grafana を選択するのが一般的です。

PromQL 言語を使用して、Prometheus alertmanager ツールで警告を設定することもできます。

注記

Grafana はコミュニティーがサポートする機能です。Grafana をデプロイして Red Hat 3scale プロダクトを監視する設定は、Red Hat の実稼働環境のサービスレベルアグリーメント (SLA) の対象外です。

9.2. APICAST と PROMETHEUS のインテグレーション

APIcast と Prometheus のインテグレーションは、以下のデプロイメントオプションで利用することができます。

- Self-managed APIcast (ホスト型 API Management およびオンプレミス型 API Management 両方との組み合わせに対応)
- Embedded APIcast (オンプレミス型 API Management)

注記

APIcast と Prometheus のインテグレーションは、ホスト型 API Management と Hosted APIcast の組み合わせでは利用することができません。

デフォルトでは、Prometheus は 表9.2「3scale APIcast 用 Prometheus のデフォルトメトリクス」 に記載された APIcast メトリクスを監視することができます。

9.2.1. 追加オプション

オプションとして、OpenShift クラスターのクラスター管理者アクセス権限があれば、**total_response_time_seconds**、**upstream_response_time_seconds**、および **upstream_status** メトリクスを拡張して **service_id** および **service_system_name** ラベルを含めることができます。これらのメトリクスを拡張するには、以下のコマンドを使用して **APICAST_EXTENDED_METRICS** OpenShift 環境変数を **true** に設定します。

```
oc set env dc/apicast APICAST_EXTENDED_METRICS=true
```

APIcast Batcher ポリシー (「3scale Batcher」に詳細を記載) を使用している場合、Prometheus は 表9.3「3scale APIcast Batch ポリシー用 Prometheus メトリクス」に記載されたメトリクスも監視することができます。

注記

メトリクスに値がない場合、Prometheus はメトリクスを非表示にします。たとえば、**nginx_error_log** に報告するエラーがない場合、Prometheus は **nginx_error_log** メトリクスを表示しません。**Nginx_error_log** メトリクスは、値がある場合にのみ表示されます。

関連情報

Prometheus についての情報は、PROMETHEUS: GETTING STARTED を参照してください。

9.3. 3SCALE APICAST 用 OPENSHIFT 環境変数

Prometheus インスタンスを設定するには、表9.1「3scale APIcast 用 Prometheus 環境変数」 に記載の OpenShift 環境変数を設定します。

表9.1 3scale APIcast 用 Prometheus 環境変数

環境変数	説明	デフォルト

環境変数	説明	デフォルト
APICAST_EXTENDED_METRICS	Prometheus メトリクスに関する追加情報を有効にするブール値。以下のメトリクスでは **service_id** および **service_system_name** ラベルを使用することができ、APIcast をより詳細に設定することができます。 • **total_response_time_seconds** • **upstream_response_time_seconds** • **upstream_status**	**false**

関連情報

環境変数の設定については、該当する OpenShift のガイドを参照してください。

- OpenShift 4: アプリケーション
- OpenShift 3.11: 開発者ガイド

サポート対象設定の情報については、Red Hat 3scale API Management のサポート対象設定 のアーティクルを参照してください。

9.4. PROMETHEUS に公開される 3SCALE APICAST メトリクス

3scale APIcast の監視用に Prometheus を設定すると、デフォルトでは 表9.2「3scale APIcast 用 Prometheus のデフォルトメトリクス」に記載されたメトリクスを監視することができます。

表9.3「3scale APIcast Batch ポリシー用 Prometheus メトリクス」 に記載されたメトリクスは、「3scale Batcher」を使用する場合にのみ利用することができます。

表9.2 3scale APIcast 用 Prometheus のデフォルトメトリクス

メトリクス	説明	タイプ	ラベル
nginx_http_connections	HTTP 接続の数	ゲージ	state (accepted、active、handled、reading、total、waiting、writing)
nginx_error_log	APIcast エラー	カウンター	**level (debug、info、notice、warn、error、crit、alert、emerg)**

メトリクス	説明	タイプ	ラベル
openresty_shdict_capacity	ワーカー間で共有されるディクショナリーの容量	ゲージ	**dict** (すべてのディクショナリーで共通)
openresty_shdict_free_space	ワーカー間で共有されるディクショナリーの空き容量	ゲージ	**dict** (すべてのディクショナリーで共通)
nginx_metric_errors_total	メトリクスを管理する Lua ライブラリーのエラーの数	カウンター	none
total_response_time_seconds	クライアントにレスポンスを送信するのに必要な時間 (秒単位) **注記**: **service_id** および **service_system_name** ラベルにアクセスするためには、「APIcast と Prometheus のインテグレーション」に記載のとおり **APICAST_EXTENDED_METRICS** 環境変数を true に設定する必要があります。	ヒストグラム	**service_id**、**service_system_name**
upstream_response_time_seconds	アップストリームサーバーからの応答時間 (秒単位) **注記**: **service_id** および **service_system_name** ラベルにアクセスするためには、「APIcast と Prometheus のインテグレーション」に記載のとおり **APICAST_EXTENDED_METRICS** 環境変数を true に設定する必要があります。	ヒストグラム	**service_id**、**service_system_name**

メトリクス	説明	タイプ	ラベル
upstream_status	アップストリームサーバーからの HTTP ステータス 注記: **service_id** および **service_system_name** ラベルにアクセスするためには、「APIcast と Prometheus のインテグレーション」に記載のとおり **APICAST_EXTENDED_METRICS** 環境変数を **true** に設定する必要があります。	counter	**status**、**service_id**、**service_system_name**
threescale_backend_calls	3scale バックエンド (Apisonator) に対する承認および報告リクエスト	カウンター	**endpoint** (**authrep**、**auth**、**report**)、**status** (**2xx**、**4xx**、**5xx**)

表9.3 3scale APIcast Batch ポリシー用 Prometheus メトリクス

メトリクス	説明	タイプ	ラベル
batching_policy_auths_cache_hits	3scale Batcher ポリシーの承認キャッシュのヒット数	カウンター	none
batching_policy_auths_cache_misses	3scale Batcher ポリシーの承認キャッシュのミス数	カウンター	none

パート II. API のバージョン管理

第10章 API のバージョン管理

Red Hat 3scale API Management では、API のバージョン管理が可能です。3scale で API を管理する際、3 とおりの方法でご自分の API のバージョンを正しく管理することができます。3scale ゲートウェイで API のバージョンを管理する方法の例を以下に示します。3scale ゲートウェイは、3scale アーキテクチャーにより新たな機能を提供します。

10.1. 目的

本項では、3scale に API バージョン管理システムを実装するための詳細な情報を説明します。

あなたは楽曲を検索するための API を所有しているとします。ユーザーは、さまざまなキーワード (例: アーティスト、作詞家、曲のタイトル、アルバムタイトル等) を使用して好みの楽曲を検索することができます。API の初期バージョン (v1) があり、新たな改良バージョン (v2) を開発したと仮定します。

以降のセクションで、3scale を使用して API バージョン管理システムを実装する最も一般的な方法を 3 とおり説明します。

- URL によるバージョン管理
- エンドポイントによるバージョン管理
- カスタムヘッダーによるバージョン管理

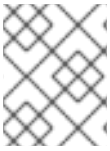
10.2. 前提条件

以下に示すクイックスタートガイドを使用する前に、API を 3scale に接続する ための基本手順を完了してください。

10.3. URL によるバージョン管理

楽曲の検索用に異なるエンドポイントがある場合には (アーティストで検索、曲のタイトルで検索など)、URL によるバージョン管理では URI の一部に API バージョンを含めてください。以下に例を示します。

1. api.songs.com/v1/songwriter
2. api.songs.com/v2/songwriter
3. api.songs.com/v1/song
4. api.songs.com/v2/song
5. 以下、同様



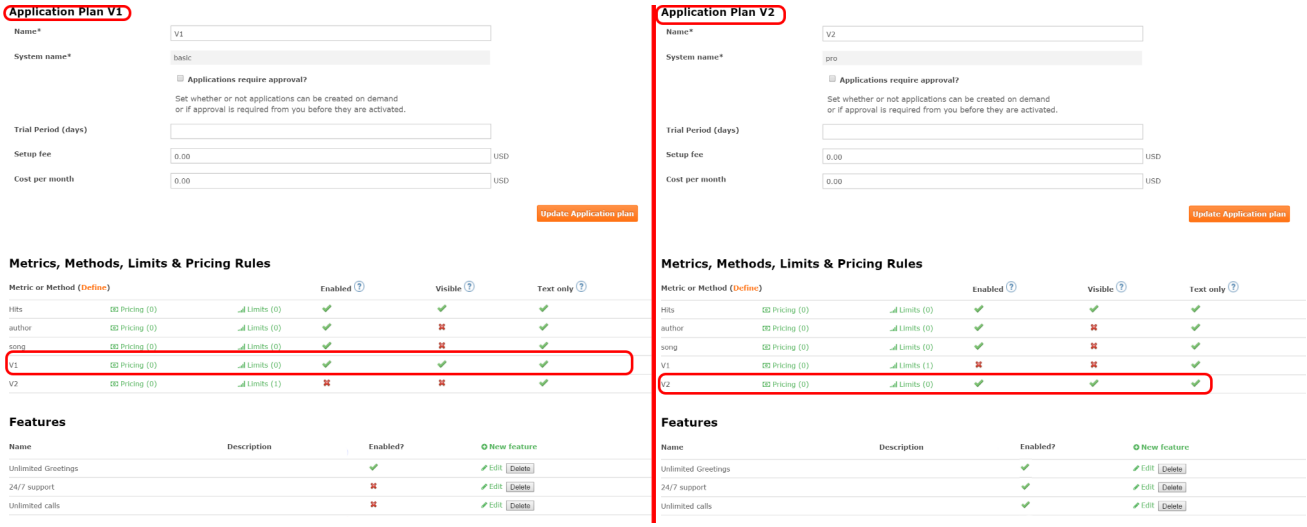
注記

この手法を用いる場合には、v1 の時点で API のバージョン管理を行うことを計画している必要があります。

この場合、3scale ゲートウェイは URI からエンドポイントおよびバージョンを抽出します。このアプローチでは、バージョンとエンドポイントの任意の組み合わせで、アプリケーションプランを設定することができます。続いて、メトリクスをこれらのプランおよびエンドポイントに関連付け、それぞれのエンドポイントおよびバージョンごとに、使用状況を把握することができます。

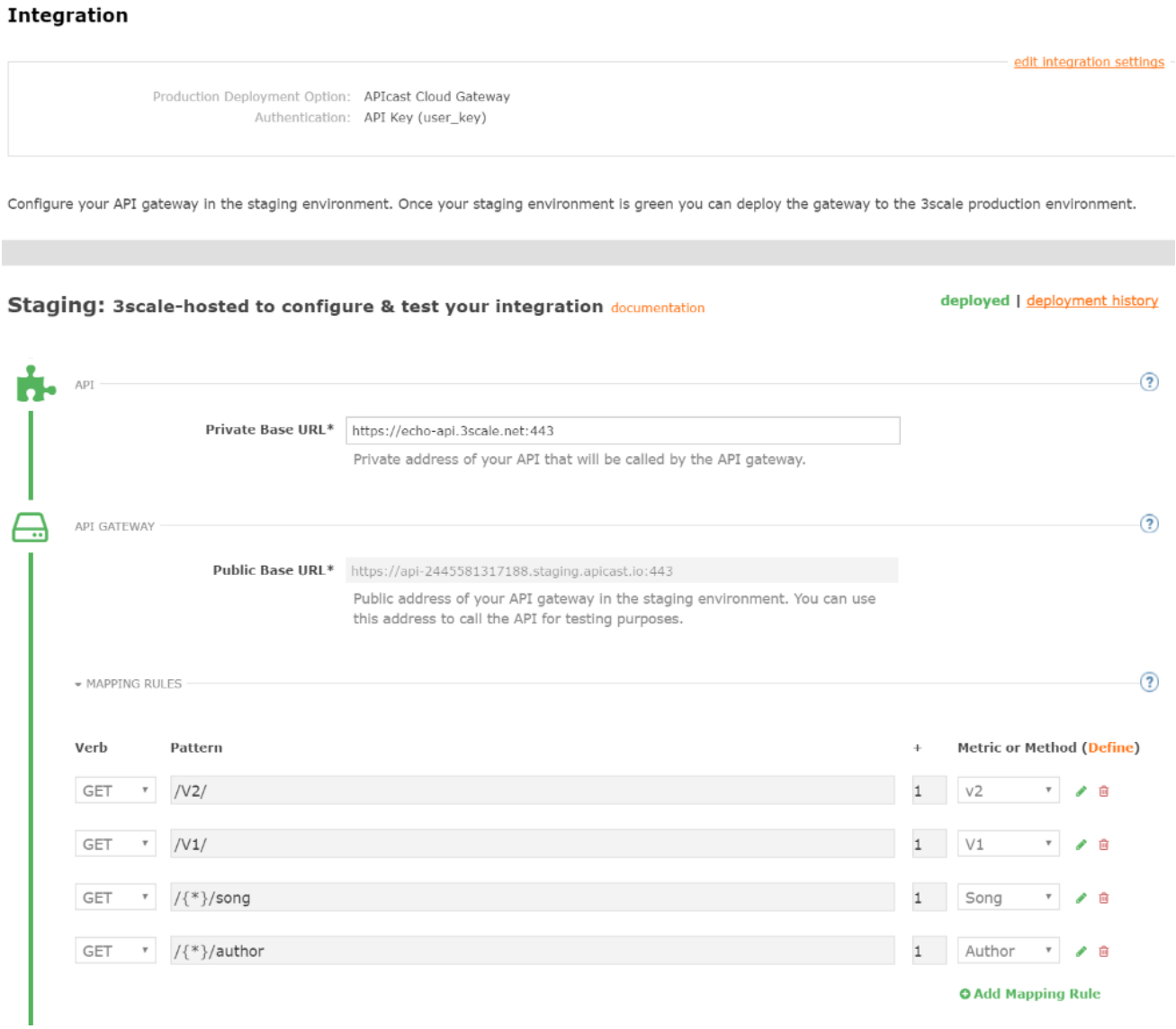
3scale 機能の柔軟性を以下のスクリーンショットに示します。

図10.1 バージョン管理計画機能



後は、以下の図に示すように、3scale 管理ポータルの **[your_API_name] > Integration > Configuration** の順に移動し、URI をメトリクスにマッピングするだけです。

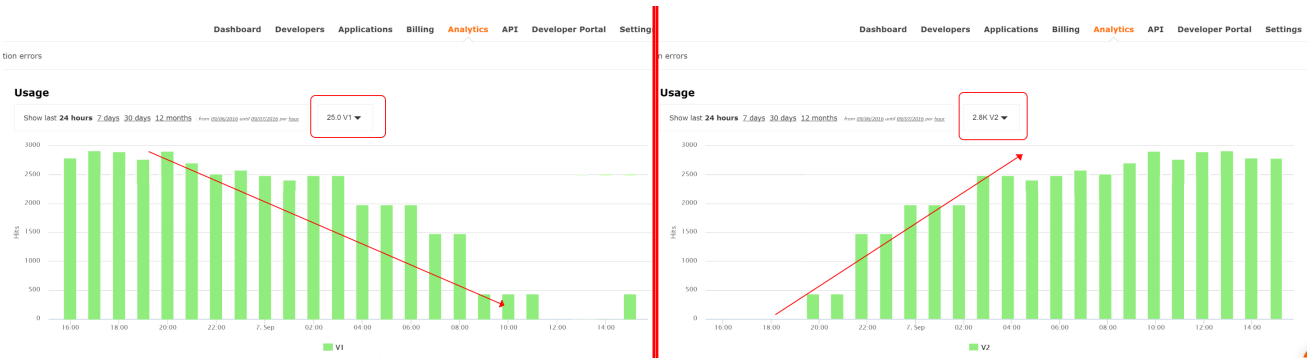
図10.2 メトリクスへの URI のマッピング



これで、異なる機能が有効になった 2 つの異なる API バージョンを使用することができます。それぞれの API の使用状況を、完全に管理し把握することができます。

API v2 に移行する必要があることをすべてのユーザーに伝える場合には、移行を依頼するメッセージを送信することができます。どのユーザーが移行したかを監視し、v1 の使用が減少して v2 の使用が増加する様子を確認することができます。3scale への承認呼び出しにメトリクスを追加して、v1 エンドポイントと v2 エンドポイントにアクセスする全トラフィック量を比較し、v1 を廃止しても問題ない時期を判断することができます。

図10.3 バージョン管理



一部のユーザーが v1 を使用し続けている場合には、それらのユーザーを絞り込み、v2 への切り替えに関する新たなメッセージを送信することができます。

3scale では、3 段階のステップにより廃止の通知を送信することができます。

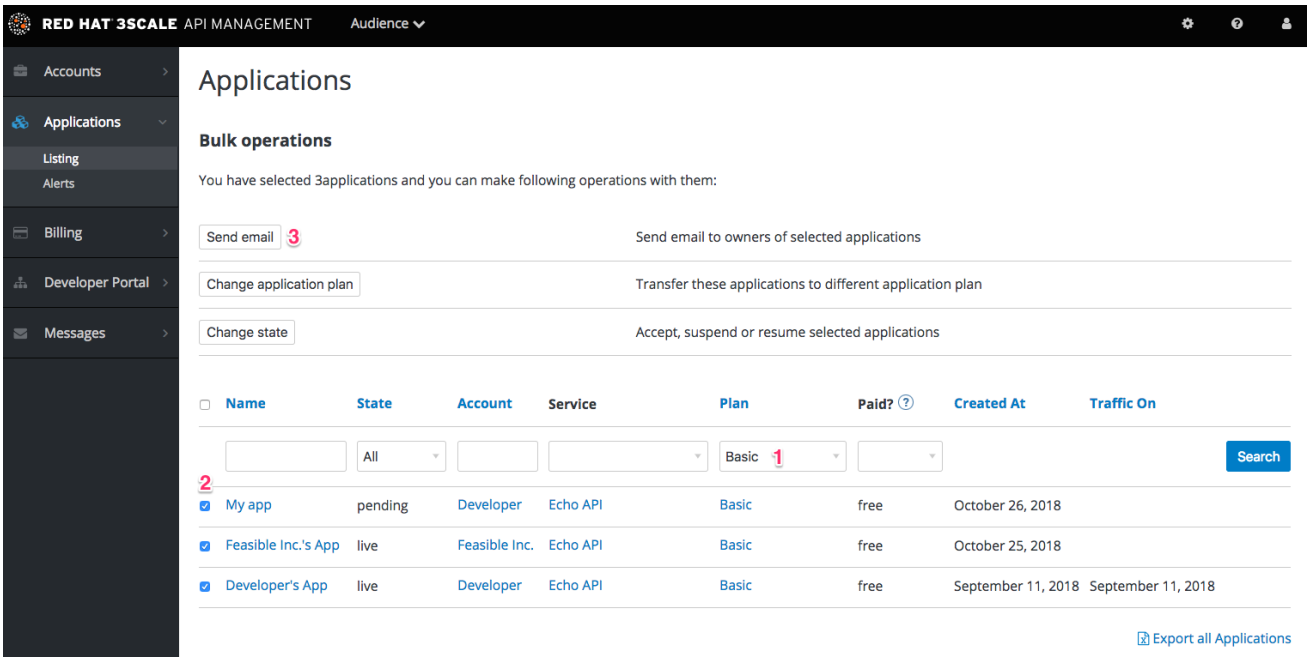
1. **Audience** > **Applications** > **Listing**の順に移動し、廃止の通知を送信するアプリケーションプランを選択して **Search** をクリックし、リストを絞り込みます。

2. チェックボックスをクリックし (複数選択可能)、問題の特定バージョンのアプリケーションをすべて選択します。新たなオプションが表示され、一括操作 (**電子メールの送信**、**アプリケーションプランの変更**、および **ステータスの変更**) を行うことができます。

3. **Send email** をクリックし、手順に従って選択したアプリケーションのオーナーに廃止の通知を送信します。

以下の図を参照してください。

図10.4 廃止通知の送信



エンドポイントに authrep 呼び出しが行われるたびに、認証は 1 度だけですが報告は 2 度行われます (エンドポイント用と API バージョン用にそれぞれ 1 度ずつ)。呼び出しは 1 度しか認証されないので、二重に請求することはありません。ある API バージョンの任意のエンドポイントに呼び出しを行うたびに、バージョン番号 (v1、v2 等) から名前を取ったメトリクスのヒット数が積算されます。これを使用して、バージョンごとの全トラフィックを相互に比較することができます。

10.4. エンドポイントによるバージョン管理

エンドポイントによるバージョン管理では、API のバージョンごとに異なるエンドポイントを設定することができます (例: **api.cons.com/author_v1**)。ゲートウェイは、エンドポイントそのものからエンドポイントおよびバージョンを抽出します。本手法および前項の手法では、API プロバイダーは外部 URL を内部 URL にマッピングすることができます。

エンドポイントによるバージョン管理手法は、オンプレミスデプロイメントでのみ実施することができます。この手法に必要な URL の書き換えに使用する LUA スクリプトが、オンプレミス設定の一環として提供されるためです。

外部 URL		内部 URL
api.songs.com/songwriter_v1	は、次のように書き換えられます。	internal.songs.com/search_by_songwriter
api.songs.com/songwriter_v2	は、次のように書き換えられます。	internal.songs.com/songwriter

ほとんどすべて (マッピング、アプリケーションプランの機能など) が、前項の手法と全く同じように機能します。

10.5. カスタムヘッダーによるバージョン管理

カスタムヘッダーによるバージョン管理では、バージョンを指定するのに URI ではなくヘッダー (x-api-version) を使用します。

この場合、ゲートウェイはパスからエンドポイントを、ヘッダーからバージョンを、それぞれ抽出します。前述の手法とまったく同様に、パス/バージョンの任意の組み合わせを解析して可視化することができます。このアプローチには、使用する API 管理システムにかかわらず、いくつかのデメリットがあります。詳細については、API versioning methods: A brief reference を参照してください。3scale が機能する仕組みを以下に示します。

- 前項の手法とまったく同様に、カスタムヘッダーによるバージョン管理は、オンプレミスのホスト型 API にのみ適用可能です。authrep 呼び出しを正しくルーティングするには、リクエストヘッダーの解析/処理が必要だからです。このタイプのカスタム処理の実施には、Lua スクリプトの使用が不可欠です。

- この手法では、前項の手法のようなきめ細かな機能分離を実現するのが非常に困難です。

- この手法の最も重要なメリットは、開発者の指定する URL およびエンドポイントが変更されないことです。開発者がある API バージョンから別の API バージョンに切り替える場合、変更する必要があるのはヘッダーだけです。それ以外はすべて同じままで機能します。

パート III. API の認証

第11章 認証パターン

本チュートリアルでは、API に認証パターンを設定する方法、およびアプリケーションと API 間の通信への影響について説明します。

API にアクセスするためのクレデンシャルを発行するのに、API に応じて異なる認証パターンを使用しなければならない場合があります。これには、API キー、penAuth トークン、およびカスタム設定が含まれます。本チュートリアルでは、利用可能な標準的な認証パターンから適切なパターンを選択する方法について説明します。

11.1. サポートされる認証パターン

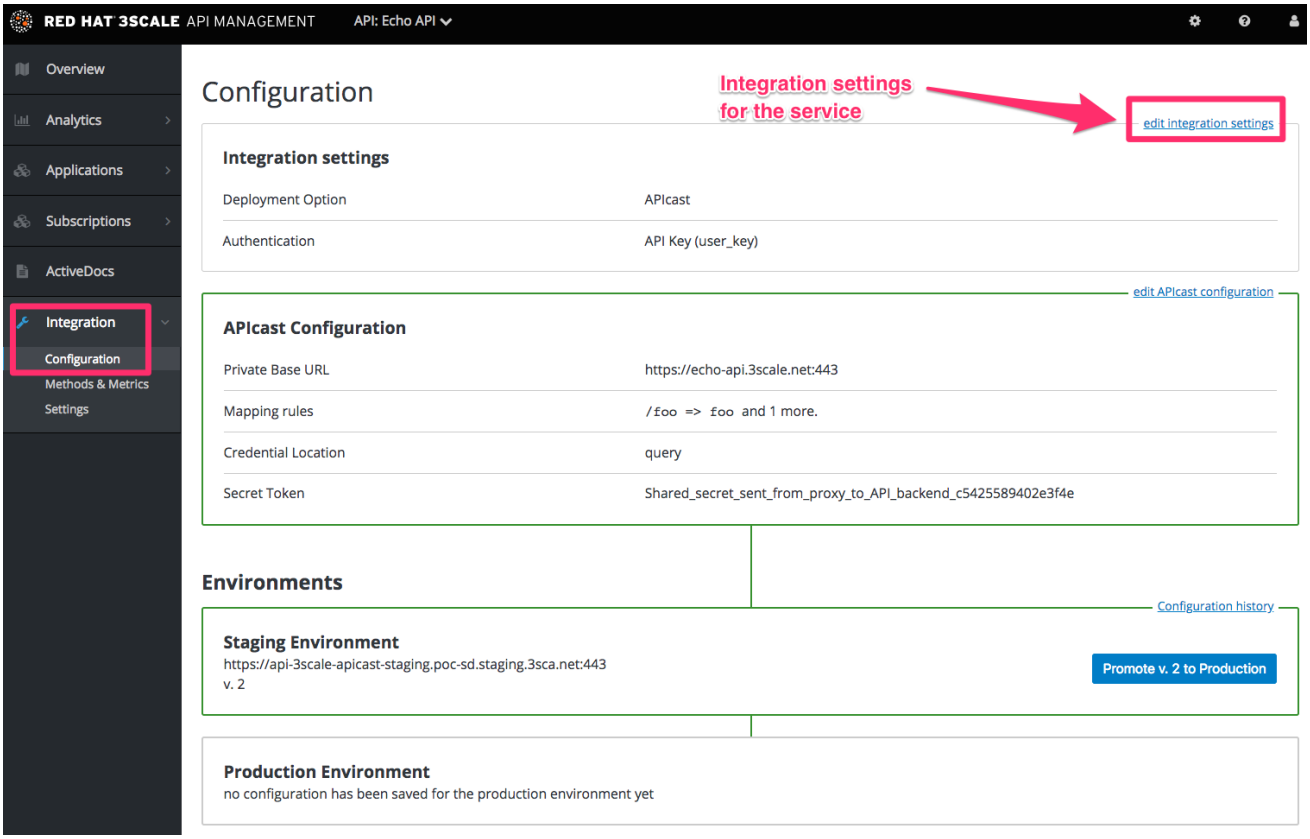
3scale では、以下の認証パターンが標準でサポートされます。

- **標準 API キー**: 識別子およびシークレットトークンとして機能する、1 つの無作為な文字列またはハッシュ
- **アプリケーション ID とキーのペア**: イミュータブルな識別子とミュータブルなシークレットキー文字列
- **OpenID Connect**

11.2. 認証パターンのセットアップ

11.2.1. サービスに設定する認証モードの選択

設定を行う API サービスに移動します (API という名称のサービスが 1 つしかない場合には、それを選択します)。**Integration** セクションに移動します。



運用するサービスごとに異なる認証パターンを使用できますが、1つのサービスに使用することのできるパターンは1つだけです。

重要

サービスの動作が予測不能になる可能性があるため、クレデンシャルを登録したら認証パターンを変更しないでください。認証パターンを変更するには、新しいサービスを作成して顧客を移行することを推奨します。

11.2.2. 使用する認証モードの選択

認証モードを選択するには、AUTHENTICATION セクションまでスクロールします。ここで、以下のオプションのいずれかを選択することができます。

- API Key (user_key)
- App_ID and App_Key Pair
- OpenID Connect

11.2.3. API が正しいクレデンシャルタイプを受け入れることの確認

選択したクレデンシャルのタイプごとに、API の呼び出しで異なるパラメーター (キーフィールド、ID 等) を受け入れなければならない場合があります。これらのパラメーターの名前は、3scale 内部で使用されているものとは異なる場合があります。3scale バックエンドへの呼び出しで正しいパラメーター名が使用されている場合に、3scale の認証は正しく機能します。

11.2.4. クレデンシャルをテストするためのアプリケーションの作成

クレデンシャルセットが機能していることを確認するには、新しいアプリケーションを作成して API を使用するためのクレデンシャルを発行します。管理ポータル Dashboard の Accounts 領域に移動し、使用するアカウントをクリックして **new application** をクリックします。

フォームに入力して save をクリックすると、API を使用するためのクレデンシャルと共に新しいアプリケーションが作成されます。これで、これらのクレデンシャルを使用して API を呼び出すことができ、3scale に登録されたアプリケーションのリストに対して記録が照合されます。

11.3. 標準の認証パターン

3scale でサポートされる認証パターンの詳細を、以下のセクションで説明します。

11.3.1. API キー

サポートされるクレデンシャルの中で最もシンプルな形態は、単一の API モデルです。API へのアクセス権限を持つアプリケーションは、それぞれ1つの (一意の) 長い文字列を持ちます。以下に例を示します。

```
API-key = 853a76f7c8d5f4a1ee8bf10a4e0d1f13
```

デフォルトでは、キーパラメーターの名前は **user_key** です。このラベルを使用するか、**API-key** 等の別のラベルを選択することができます。別のラベルを選択する場合には、3scale への承認呼び出しを行う前に値をマッピングする必要があります。この文字列は、API を使用するための識別子およびシーク

レットトークンの両方として機能します。このパターンは、セキュリティーに対する要件が低い環境または API の呼び出しに SSL セキュリティーが使用される環境でのみ使用することを推奨します。トークンおよびアプリケーションに対して実行される操作は、以下のとおりです。

- アプリケーションの一時中止: アプリケーションの API へのアクセスが一時中止され、実質的に、該当するキーを使用する API への呼び出しがすべて一時中止されます。
- アプリケーションの再開: アプリケーションの一時中止アクションの効力を解除します。
- キーの再生成: アプリケーション用に新しい無作為な文字列キーが生成され、それがアプリケーションに関連付けられます。このアクションが実行されると、直ちに以前のトークンを使用した呼び出しは受け入れられなくなります。

最後のアクションのトリガーとなるのは、管理ポータルでの API 管理および API の開発者ユーザーのコンソール (許可される場合) です。

11.3.2. App_ID と App_Key のペア

API キーの認証パターンでは、アプリケーションの識別子とシークレットトークンが 1 つのトークンに組み合わされます。一方、この認証パターンでは両者が分離されます。

- API を使用する各アプリケーションは、**アプリケーション ID** (App_ID) と呼ばれるイミュータブルな初期 ID を発行します。App_ID は不変で、秘密である場合とそうでない場合があります。
- また、各アプリケーション は 1 つから 5 つまでの数の **アプリケーションキー** (App_Key) を持ちます。それぞれのキーは App_ID に直接関連付けられ、秘密として扱う必要があります。

```
app_id = 80a4e03 app_key = a1ee8bf10a4e0d1f13853a76f7c8d5f4
```

デフォルトの設定では、開発者はアプリケーションごとに最大 5 つのキーを作成することができます。これにより、開発者は新しいキーを作成してコードに追加し、アプリケーションを再デプロイして古いキーを無効にすることができます。そのため、API キーを再生成する場合のようなアプリケーションのダウンタイムが発生することはありません。

統計値および流量制御は、API キーごとではなく、常にアプリケーション ID レベルで維持されます。開発者が 2 組の統計値を追跡するためには、2 つのキーではなく 2 つのアプリケーションを作成する必要があります。

システムのモードを変更し、アプリケーションキーを持たないアプリケーションを作成することもできます。この場合には、3scale システムは App_ID のみに基づいてアクセスを認証します (キーの確認は行われません)。このモードは、ウィジェットタイプのシナリオ、またはアプリケーションではなくユーザーに流量制御が適用される場合に役立ちます。ほとんどの API では、アプリケーションごとに少なくとも 1 つのアプリケーションキーを持つ必要があります。この設定は、**[your_API_name] > Integration > Settings** で可能です。

11.3.3. OpenID Connect

OpenID Connect による認証に関する情報は、OpenID Connect インテグレーション の章を参照してください。

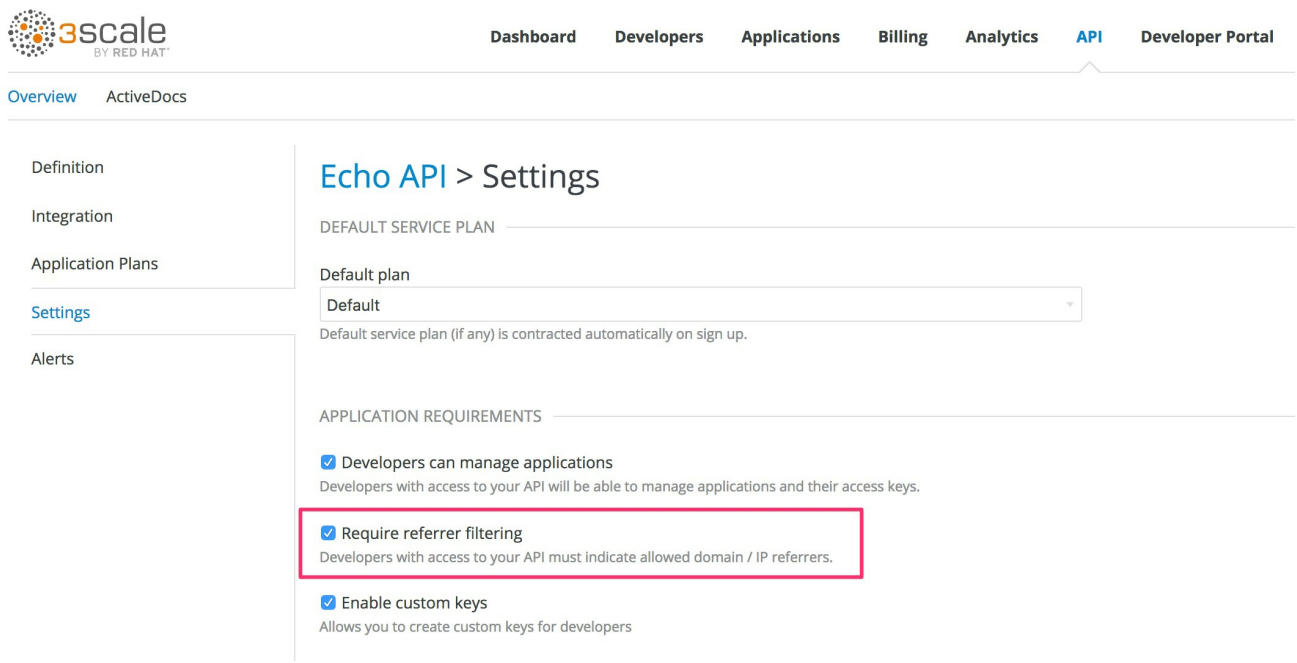
11.4. 参照元フィルター機能

3scale では参照元フィルター機能がサポートされ、API へのアクセスが許可されるアプリケーションの IP アドレスまたはドメイン名をホワイトリストに登録することができます。API クライアントでは、**Referrer** ヘッダーで参照元の値を指定します。Referrer ヘッダーの目的および使用法について

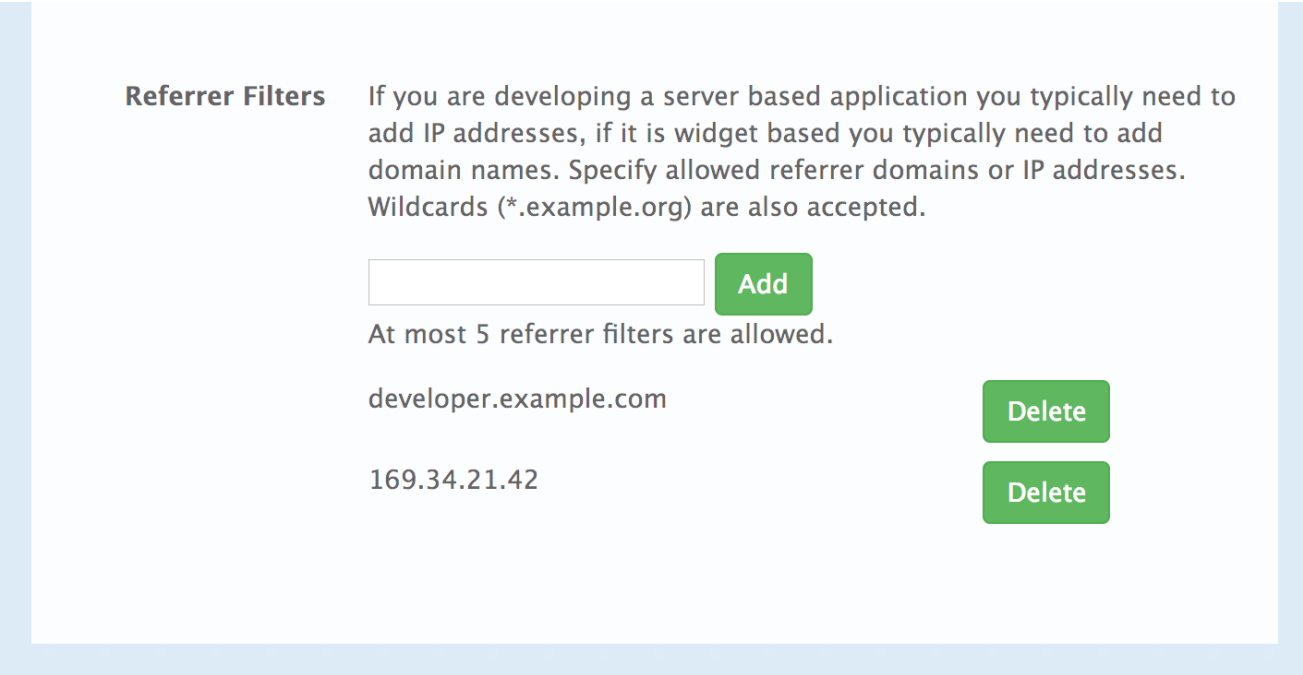
は、RFC 7231 のセクション 5.5.2Referer に説明があります。

参照元フィルター機能が動作するためには、サービスポリシーチェーンで APIcast Referrer ポリシー を有効にする必要があります。

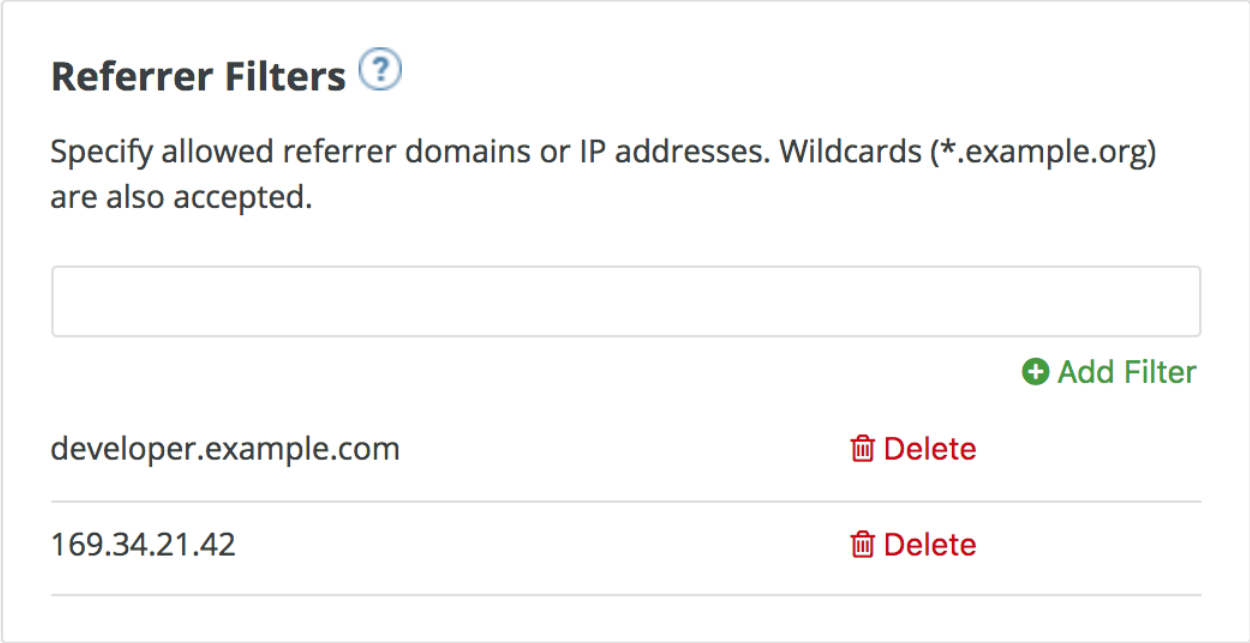
参照元フィルター機能を有効にするには、**[your_API_name] > Applications > Settings > Usage Rules** の順に移動します。**Require referrer filtering** を選択し、**Update Product** をクリックします。



ご自分の API にアクセスする開発者は、デベロッパーポータルから許可される参照元のドメイン/IP を設定する必要があります。



管理ポータルでは、このサービスに属する全アプリケーションの詳細ページに、新たな **Referrer Filters** セクションが表示されます。ここで、管理者は、このアプリケーションの許可される Referrer ヘッダー値のホワイトリストを設定することもできます。



アプリケーションごとに、最大 5 つの参照元の値を設定することができます。

値に使用することができるのは、ラテン文字、数字、ならびに特殊文字 *、.、および - だけです。* はワイルドカードの値として使用することができます。値を * に設定するとあらゆる参照元の値が許可され、参照元の確認はバイパスされます。

Require referrer filtering 機能および **3scale Referrer** ポリシーが有効な場合には、承認は以下のように行われます。

1. 参照元フィルターが指定されていないアプリケーションは、提供されたクレデンシャルだけを使用して通常どおり承認されます。

2. 参照元フィルターの値が設定されたアプリケーションの場合には、APIcast はリクエストの **Referrer** ヘッダーから参照元の値を抽出し、それを AuthRep (承認およびレポート) リクエストの **referrer** パラメーターとして Service Management API に送信します。以下の表は、参照元フィルター機能のパラメーターのさまざまな組み合わせに対する AuthRep の応答をまとめています。

referrer パラメーターが渡されるか	アプリケーションに参照元フィルターが設定されているか	referrer パラメーターの値	HTTP レスポンス	レスポンスのボディー
はい	はい	参照元フィルターと一致する	200 OK	**<status><authorized>true</authorized></status>**
はい	いいえ	参照元フィルターと一致する	200 OK	**<status><authorized>true</authorized></status>**

referrer パラメーターが渡されるか	アプリケーションに参照元フィルターが設定されているか	referrer パラメーターの値	HTTP レスポンス	レスポンスのボディー
はい	はい	参照元フィルターと一致しない	409 Conflict	**<status><authorized>false</authorized><reason>referrer "test.example.com" is not allowed</reason>** (**test.example.com** は例です)
はい	いいえ	参照元フィルターと一致しない	200 OK	**<status><authorized>true</authorized></status>**
はい	はい	*	200 OK	**<status><authorized>true</authorized></status>**
はい	いいえ	*	200 OK	**<status><authorized>true</authorized></status>**
いいえ	はい	–	409 Conflict	**<status><authorized>false</authorized><reason>referrer is missing</reason>**
いいえ	いいえ	–	200 OK	**<status><authorized>true</authorized></status>**

AuthRep により承認されない呼び出しは、APIcast により拒否され Authorization Failed エラーが返されます。サービスの Integration ページで、ステータスコードおよびエラーメッセージを具体的に設定することができます。

第12章 OPENID CONNECT インテグレーション

3scale では、以下の機能を持つOpenID Connect 仕様を使用して、API リクエストの認証用にサードパーティーアイデンティティープロバイダー (IdP) を統合します。

- OpenID Connect は OAuth 2.0 に追加する形で構築され、OAuth 2.0 の承認フレームワークを認証メカニズムにより補完します。
- **OpenID Connect 認証**オプションにより、API リクエストは JSON Web Token (JWT) 形式 (RFC 7519) のアクセストークンを使用して認証されます。

インテグレーションは、以下に示す 2 つの部分で設定されます。

- APIcast による JWT の検証および解析
- **zync-que** によるクライアントクレデンシャルの同期

Red Hat 3scale API Management は、OpenID プロバイダーとして機能する Red Hat Single Sign-On (RH-SSO) により、両方のインテグレーションポイントを完全にサポートしています。サポートされる RH-SSO のバージョンについては、Red Hat 3scale API Management のサポート対象設定 のアーティクルを参照してください。APIcast のインテグレーションは、ForgeRock でもテストされています。

どちらのケースでも、OpenID Connect の認証オプションを使用するサービスの Integration ページにおいて、APIcast Configuration の **OpenID Connect Issuer** フィールドを指定して、インテグレーションを設定することができます。手順については、Red Hat Single Sign-On 統合の設定 を参照してください。

12.1. APICAST による JWT の検証および解析

OpenID Connect の認証モードを使用するサービスに対する API リクエストは、OpenID プロバイダーにより発行された JWT 形式のアクセストークンを提供する必要があります。このトークンは、**Bearer** スキーマを使用して **Authorization** ヘッダーで提供されます。ヘッダーの例を以下に示します。

```
Authorization: Bearer <JWK>
```

例:


```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJodHRwczovL2lkcC5leGFtcGxlLmNvbSIsInN1YiI
6ImFiYzEyMyIsIm5iZiI6MTUzNzg5MjQ5NCwiZXhwIjoxNTM3ODk2MDk0LCJpYXQiOjE1Mzc4OTI0OT
QsImp0aSI6ImlkMTIzNDU2IiwidHlwIjoiQmVhcmVyIn0.LM2PSmQ0k8mR7eDS_Z8iRdGta-Ea-
pJRrf4C6bAiKz-Nzhxpm7fF7oV3BOipFmimwkQ_-mw3kN--
oOc3vU1RE4FTCQGbzO1SAWHOZqG5ZUx5ugaASY-
hUHIohy6PC7dQl0e2NlAeqqg4MuZtEwrpESJW-
VnGdljrAS0HsXzd6nENM0Z_ofo4ZdTKvIKsk2KrdyVBOcjgVjYongtppR0cw30FwnpqfeCkuATeINN5OK
HXOibRA24pQyIF1s81nnmxLnjnVbu24SFE34aMGRXYzs4icMI8sK65eKxbvwV3PIG3mM0C4ilZPO26d
oP0YrLfVwFcqEirmENUAcHXz7NuvA
```


JWT トークンの受領者はトークンに含まれる署名を検証し、トークンが既知の発行者により署名されていること、およびその内容が変更されていないことを確認します。3scale では、公開/秘密鍵のペアに基づく RSA 署名がサポートされます。なお、発行者は秘密鍵を使用して JWT トークンに署名します。APIcast は公開鍵を使用してこのトークンを検証します。

APIcast では、JWT 署名の検証に使用する JSON Web Key (JWK) の取得に、OpenID Connect Discovery が使用されます。

それぞれのリクエストについて、APIcast は以下の処理を行います。

1. 公開鍵を使用して JWT トークンを検証する。
2. クレーム **nbf** および **exp** を検証する。
3. クレーム **iss** (Issuer) で指定される発行者が **OpenID Connect Issuer** フィールドで設定される発行者と同じであることを検証する。
4. **azp** または **aud** クレームの値を抽出し、それをクライアント ID (3scale 内のアプリケーションを識別する) として使用して Service Management API を通じて呼び出しを承認する。

JWT の検証または承認の確認のいずれかが失敗すると、APIcast は Authenication failed エラーを返します。そうでなければ、APIcast は API バックエンドにリクエストをプロキシー処理します。**Authorization** ヘッダーはリクエストにそのまま残るので、API バックエンドは JWT トークンを使用してユーザーおよびクライアントの ID を確認することができます。

12.2. ZYNC-QUE によるクライアントクレデンシャルの同期

zync-que コンポーネントの使用する場合、3scale は 3scale と RH-SSO サーバー間でクライアント (アプリケーション) のクレデンシャルを同期します。**OpenID Connect Issuer** 設定を使用してこれを設定します。

OpenID Connect を使用するように設定されたサービスを作成/更新/削除する場合、**zync-que** は該当するイベントを受け取り、RH-SSO API を使用してその変更を RH-SSO インスタンスに通知します。

Red Hat Single Sign-On 統合の設定 セクションでは、RH-SSO API を使用するための正しい認証情報が **zync-que** にあることを確認するために必要な手順を説明しています。

12.3. RED HAT SINGLE SIGN-ON インテグレーションの設定

次の手順では、カスタム CA 証明書を使用するように **zync-que** を設定する方法を説明します。

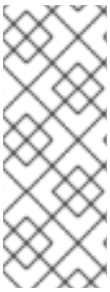
12.3.1. カスタム CA 証明書を使用するための zync-que の設定

前提条件

- **https** で RH-SSO を提供でき、 **zync-que** がアクセス可能であることを確認します。これをテストするには、以下を入力します。

```
curl https://rhsso-fqdn
```

- 3scale 2.2 以降は、**SSL_CERT_FILE** 環境変数により、RH-SSO 用カスタム CA 証明書がサポートされます。この変数は、証明書バンドルのローカルパスをポイントします。



注記

- OpenSSL の一部のバージョンは、 **--showcerts** ではなく、**-showcerts** を受け入れます。使用しているバージョンに合わせて、以下のコマンドを変更します。
- 以下の手順のステップ 1 のコマンドには **<rhsso_fqdn>** が記載されています。完全修飾ドメイン名 (FQDN) は、人間が判読可能なドメイン名 (例: **host.example.com**) です。

手順

1. 以下のコマンドを実行して、適切な証明書チェーンを取得します。

```
echo -n | openssl s_client -connect <rhsso_fqdn>:<rhsso_port> -servername <rhsso_fqdn> --showcerts | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > customCA.pem
```

2. 以下の cURL コマンドを使用して、新しい証明書を検証します。レルムの JSON 設定が返されるはずです。検証の失敗は、証明書が正しくないことを意味します。

```
curl -v https://<secure-sso-host>/auth/realms/master --cacert customCA.pem
```

3. 証明書バンドルを Zync Pod に追加します。

   a. Zync Pod 上の **/etc/pki/tls/cert.pem** ファイルの既存コンテンツを収集します。以下を実行します。

   ```
   oc exec <zync-que-pod-id> cat /etc/pki/tls/cert.pem > zync.pem
   ```

   b. カスタム CA 証明書ファイルの内容を **zync.pem** に追加します。

   ```
   cat customCA.pem >> zync.pem
   ```

   c. 新たなファイルを ConfigMap として Zync Pod に追加します。

   ```
   oc create configmap zync-ca-bundle --from-file=./zync.pem
   ```

   ```
   oc set volume dc/zync-que --add --name=zync-ca-bundle --mount-path /etc/pki/tls/zync/zync.pem --sub-path zync.pem --source='{"configMap":{"name":"zync-ca-bundle","items":[{"key":"zync.pem","path":"zync.pem"}]}}'
   ```

4. デプロイメント後に、証明書が追加され内容が正しいことを確認します。

```
oc exec <zync-pod-id> cat /etc/pki/tls/zync/zync.pem
```

5. 新たな CA 証明書のバンドルをポイントするように、Zync の **SSL_CERT_FILE** 環境変数を設定します。

```
oc set env dc/zync-que SSL_CERT_FILE=/etc/pki/tls/zync/zync.pem
```

12.3.2. Red Hat Single Sign-On の設定

RH-SSO を設定するには、次の手順を実行します。

1. レルム (**<REALM_NAME>**) を作成します。

2. クライアントを作成します。

   a. クライアント ID を指定します。

   b. **Client Protocol** フィールドで、**openid-connect** を選択します。

3. 以下のように値を設定して、クライアントのアクセス権限を設定します。

a. Access Type: **confidential**

b. Standard Flow Enabled: **OFF**

c. Direct Access Grants Enabled: **OFF**

d. Service Accounts Enabled: **ON**

4. クライアントのサービスアカウントロールを設定します。

a. クライアントの **Service Account Roles** タブに移動します。

b. **Client Roles** ドロップダウンリストで、**realm-management** をクリックします。

c. **Available Roles** ペインで **manage-clients** リスト項目を選択し、**Add selected >>** をクリックしてロールを割り当てます。

5. クライアントのクレデンシャルを書き留めます。

a. クライアント ID (**<CLIENT_ID>**) を書き留めます。

b. クライアントの **Credentials** タブに移動し、**Secret** フィールド (**<CLIENT_SECRET>**) の値を書き留めます。

6. レルムにユーザーを追加します。

a. ウィンドウ左側の **Users** メニューをクリックします。

b. **Add user** をクリックします。

c. ユーザー名を入力して **Email Verified** スイッチを **ON** に設定し、**Save** をクリックします。

d. **Credentials** タブでパスワードを設定します。両方のフィールドにパスワードを入力し、**Temporary** スイッチを **OFF** に設定して次回ログイン時のパスワードリセットを回避します。続いて **Reset Password** をクリックします。

e. ポップアップウィンドウが表示されたら、**Change password** をクリックします。

12.3.3. 3scale の設定

RH-SSO でクライアントを作成して設定したら、RH-SSO と連携するように 3scale を設定する必要があります。

3scale を設定するには、以下の手順を実施します。

1. OpenID Connect を有効にします。

a. OpenID Connect による認証を有効にするサービスを選択し、**[your_product_name] > Integration > Settings** の順に移動します。

b. **Authentication** オプションのセクションで、**OpenID Connect Use OpenID Connect for any OAuth 2.0 flow.** を選択します。

2. APIcast の設定を編集します。OpenID Connect のオプションを選択すると、新しいセクション **OpenID Connect (OIDC) Basics** が表示されます。

a. **OpenID Connect Issuer Type** で適切なタイプを選択します。

b. 以下の URL テンプレートに示すように、前項の手順で書き留めたクライアントのクレデンシャルおよび Red Hat Single Sign-On サーバーの URL (ホスト: **<RHSSO_HOST>**、ポート: **<RHSSO_PORT>**) を **OpenID Connect Issuer** フィールドに入力して指定します。

```
https://<CLIENT_ID>:<CLIENT_SECRET>@<RHSSO_HOST>:
<RHSSO_PORT>/auth/realms/<REALM_NAME>
```

c. 設定を保存するには、**Update Product** をクリックします。

12.4. サードパーティーアイデンティティープロバイダーとの HTTP インテグレーションの設定

OpenID Connect (OIDC) の HTTP インテグレーションを設定して、サードパーティーアイデンティティープロバイダー (IdP) とのクレデンシャルの同期を円滑化することができます。つまり、当社の提供する OpenAPI 仕様を実装して、RH-SSO 以外のさまざまな IdP を統合することができます。

12.4.1. 前提条件

- 3scale の設定 に示すように、認証モードとして OIDC を有効にする。
- Zync
- 選択した IdP と 3scale 間でクライアントを同期させるための Zync とのインテグレーション

12.4.2. 手順

サードパーティーアイデンティティープロバイダーとの OIDC の HTTP インテグレーションを設定するには、管理ポータルで以下の手順を実施します。

1. **[Your_product_name] > Integration > Settings**の順に移動します。
2. **AUTHENTICATION** セクションで、**OpenID Connect Use OpenID Connect for any OAuth 2.0 flow.** を選択します。
3. **AUTHENTICATION SETTINGS** セクションに **OPENID CONNECT (OIDC) BASICS** が表示されます。
   a. **OpenID Connect Issuer Type** フィールドで、ご自分の OpenID プロバイダーのタイプを指定します。
   b. **OpenID Connect Issuer** フィールドで、ご自分の OpenID プロバイダーの URL が指定します。
4. 変更を保存するには、**Update Product** をクリックします。

12.4.3. Zync REST API の例

このサンプルプロジェクトでは、Zync REST API プロトコルを実装して OAuth2.0 クライアントを同期します。3scale アプリケーションを作成/更新/削除すると、Zync はその変更を **http://example.com/api** に複製することを試みます。

12.4.3.1. 前提条件

3scale を以下のように設定する必要があります。

- 認証モードに OIDC を使用する
- OpenID Connect Issuer Type に **REST API** を使用する
- **http://id:secret@example.com/api** as OpenID Connect Issuer

12.4.3.2. クライアントの作成、更新、および削除

クライアントを作成、更新、または削除するために、Zync は以下のリクエストを行います。

- 作成および更新: **PUT /clients/:client_id**
- 削除: **DELETE /clients/:client_id**

すべてのエンドポイントは **2xx** のステータスコードを返す必要があります。それ以外の場合、3scale はリクエストを再試行します。

12.4.3.3. Payload

作成および更新の場合のリクエストペイロードは **application/json** です。

```
{
  "client_id": "ee305610",
  "client_secret": "ac0e42db426b4377096c6590e2b06aed",
  "client_name": "oidc-app",
  "redirect_uris": ["http://example.com"],
  "grant_types": ["client_credentials", "password"]
}
```

クライアントを削除するリクエストにペイロードはありません。

12.4.3.4. OAuth2 認証の使用

Zync は GET リクエストを **/.well-known/openid-configuration** エンドポイントに送信し、**application/json** のレスポンスを期待します。レスポンスペイロードには以下の内容が含まれている必要があります。

```
{
  "token_endpoint": "http://idp.example.com/auth/realm/token"
}
```

OAuth2 プロトコル により、Zync は **token_endpoint** を使用して OpenID Connect Issuer アドレスで指定した **client_id** および **client_secret** を変換し、アクセストークンをリクエストします。API が正常ではないレスポンスを返す場合には、Zync は指定されたクレデンシャルを使用する HTTP 基本/ダイジェスト認証にフォールバックします。

12.5. OAUTH 2.0 SUPPORTED FLOWS

API クライアントは、3scale で設定した OpenID Connect (OIDC) 発行者からアクセストークンを取得する必要があります。この場合、その OpenID プロバイダーのサポートする任意の OAuth 2.0 フローが使用されます。RH-SSO の場合には、以下のフローがサポートされます (RH-SSO クライアントで使用される用語をかっこ書きで指定します)。

- 認可コード (**標準フロー**)

- リソースオーナーパスワードクレデンシャル (**直接アクセスグラントフロー**)
- インプリシット (**インプリシットフロー**)
- クライアントクレデンシャル (**サービスアカウントフロー**)

3scale で OIDC による認証を有効にしたクライアントを作成した場合、RH SSO 側で Zync により作成される対応するクライアントでは、認可コードフローだけが有効になります。このフローは、ほとんどすべてのケースについて最もセキュアで適切なフローとして推奨されます。ただし、他のフローを有効にすることが可能です。

12.5.1. OAuth 2.0 対応の認証フローの仕組み

クライアントは、承認リクエストもしくはトークンリクエスト、またはその両方を使用してアクセストークンを取得します。これらのリクエストを受け取る URL は、OpenID プロバイダーの **.well-known/openid-configuration** エンドポイントを使用して把握することができます。それぞれ、**"authorization_endpoint"** および **"token_endpoint"** が該当します。たとえば、**https://<RHSSO_HOST>:<RHSSO_PORT>/auth/realms/<REALM_NAME>/.well-known/openid-configuration** です。

12.5.2. OAuth 2.0 対応の認証フローの設定

管理ポータルで、3scale API 用に許可される OAuth 2.0 フローを設定することができます。新たなアプリケーションを作成する際には、OpenId Connect (OIDC) の設定を含めて、基本的なインテグレーションは完了しています。

OAuth 2.0 対応の認証フローを設定するには、以下の手順を実施します。

1. AUTHENTICATION SETTINGS セクションに移動します (**[Your_product_name] > Integration > Settings**)。
2. **AUTHENTICATION** セクションで、**OpenID Connect Use OpenID Connect for any OAuth 2.0 flow.** を選択します。対応するフローが有効になります。
   - **standardFlowEnabled** (Authorization Code Flow) [デフォルトで選択済み]
   - **implicitFlowEnabled** (Implicit Flow)
   - **serviceAccountsEnabled** (Service Accounts Flow)
   - **directAccessGrantsEnabled** (Direct Access Grant Flow)
3. 1 つまたは複数のフローを選択します。
4. 変更を保存するには、**Update Product** をクリックします。

12.6. インテグレーションのテスト

インテグレーションをテストするには、以降のセクションに記載する手順を実施する必要があります。

12.6.1. クライアントの同期に関するテスト

クライアントの同期をテストするには、以下の手順を実施します。

1. OpenID Connect インテグレーションを設定したサービスにアプリケーションを作成します。

2. 生成したアプリケーションのクライアント ID およびクライアントシークレットを書き留めます。

3. 同じクライアント ID およびクライアントシークレットを持つクライアントが、設定された RH-SSO レルムに存在することを確認します。

4. 3scale Admin Portal でアプリケーションのリダイレクト URL を更新します。リダイレクト用 URL は、可能な限り正確に指定する必要があります。

5. これに対応して、RH-SSO のクライアントの **Valid Redirect URIs** フィールドが更新されることを確認します。

12.6.2. API 承認フローのテスト

API 承認フローをテストするには、以下の手順を実施します。

1. 対応する RH-SSO クライアントで有効な OAuth 2.0 フローを使用して、RH-SSO サーバーからアクセストークンを取得します。

2. **Authorization** ヘッダーで、RH-SSO から取得した **access_token** の値を使用します (例: **Authorization: Bearer <access_token>**)。

トークンが正しく対応する 3scale のアプリケーションが承認されると、APIcast ゲートウェイは 3scale バックエンドからのレスポンスを返します。

12.7. インテグレーションの例

3scale のサービス API は、OpenID Connect による認証を使用するように設定されています。サービス API の **公開ベース URL** は **https://api.example.com** に、**プライベートベース URL** は **https://internal-api.example.com** に、それぞれ設定されています。

API のインテグレーションの **OpenID Connect Issuer** フィールドは **https://zync:41dbb98b-e4e9-4a89-84a3-91d1d19c4207@idp.example.com/auth/realms/myrealm** に設定され、レルム **myrealm** のクライアント **zync** には正しい Service Account ロールが設定されています。

3scale には、クライアント ID、クライアントシークレット、およびリダイレクト URL がそれぞれ **myclientid**、**myclientsecret**、および **https://myapp.example.com** に設定されたアプリケーションがあります。

RH-SSO の **myrealm** レルムには、次の値を持つクライアントも存在します。

- クライアント ID: **myclientid**
- シークレット: **myclientsecret**
- Valid Redirect URIs: **https://myapp.example.com**

このクライアントでは、標準フローが有効になっています。

レルム **myrealm** には 1 人のユーザーが設定され、そのユーザー名およびパスワードは **myuser** および **mypassword** です。

フローは以下のようになります。

1. エンドポイント **https://idp.example.com/auth/realms/myrealm/protocol/openid-connect/auth** を使用して、アプリケーションは RH-SSO に承認リクエストを送信します。こ

のリクエストの中で、アプリケーションは **myclientid** クライアント ID および **https://myapp.example.com** リダイレクト URL をパラメーターとして提供します。

2. RH-SSO はログインウィンドウを表示し、ユーザーはここで自分のクレデンシャル (ユーザー名 **myuser** およびパスワード **mypassword**) を入力する必要があります。

3. 設定およびユーザーがこのアプリケーションで初めて認証されるかどうかに応じて、同意に関するウィンドウが表示されます。

4. ユーザーが認証されると、アプリケーションはエンドポイント **https://idp.example.com/auth/realms/myrealm/protocol/openid-connect/token** を使用して、クライアント ID **myclientid**、クライアントシークレット **myclientsecret**、およびリダイレクト URL **https://myapp.example.com** と共に、トークンリクエストを RH-SSO に送信します。

5. RH-SSO は、access_token フィールドが **eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2Ik…xBArNhqF-A** と設定された JSON を返します。

6. アプリケーションは、ヘッダー **Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2Ik…xBArNhqF-A** と共に API リクエストを **https://api.example.com** に送信します。

7. アプリケーションは、**https://internal-api.example.com** から正常なレスポンスを受け取るはずです。