



OpenShift Container Platform 3.11

Service Mesh リリースノート

OpenShift Container Platform 3.11 Service Mesh リリースノート

OpenShift Container Platform 3.11 Service Mesh リリースノート

OpenShift Container Platform 3.11 Service Mesh リリースノート

法律上の通知

Copyright © 2019 Red Hat, Inc.

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

Service Mesh リリースノート

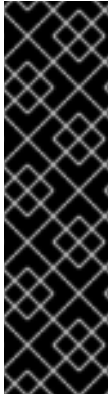
目次

第1章 RED HAT OPENSIFT SERVICE MESH リリースノート	3
1.1. RED HAT OPENSIFT SERVICE MESH 0.12.TECHPREVIEW について	3
1.2. 新機能および変更された機能	4
1.3. 解決済みの問題	5
1.4. 既知の問題	7

第1章 RED HAT OPENSIFT SERVICE MESH リリースノート

1.1. RED HAT OPENSIFT SERVICE MESH 0.12.TECHPREVIEW について

1.1.1. Red Hat OpenShift Service Mesh の概要



重要

Red Hat OpenShift Service Mesh の本リリースはテクノロジープレビューリリースでのみ利用可能です。テクノロジープレビューリリースは、Red Hat 製品のサービスレベルアグリーメント (SLA) ではサポートされておらず、機能的に完全でない可能性があり、Red Hat では実稼働環境での使用を推奨しません。クラスターで Red Hat OpenShift Service Mesh を使用すると、OpenShift 全体がテクノロジープレビューとしてレンダリングされます (サポートされていない状態)。これらの機能は、近々発表予定の製品機能をリリースに先駆けてご提供することにより、お客様は機能性をテストし、開発プロセス中にフィードバックをお寄せいただくことができます。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。

Red Hat OpenShift Service Mesh は動作についての洞察、およびサービスメッシュに対する運用上の制御を提供するプラットフォームであり、マイクロサービスアプリケーションへの接続、そのセキュリティ保護、およびモニターを実行するための統一した方法を提供します。

サービスメッシュ という用語は、分散したマイクロサービスアーキテクチャーの複数のアプリケーションを構成するマイクロサービスのネットワークおよびマイクロサービス間の対話を説明するために使用されます。サービスメッシュのサイズとおよび複雑性が増大すると、これを把握し、管理することがより困難になる可能性があります。

オープンソースの Istio プロジェクトをベースとする Red Hat OpenShift Service Mesh は、サービスコードに変更を加えずに、既存の分散したアプリケーションに透過的な層を追加します。マイクロサービス間のネットワーク通信をすべてインターセプトする環境全体に特別なサイドカープロキシをデプロイすることで、Red Hat OpenShift Service Mesh のサポートをサービスに追加することができます。コントロールプレーンの機能を使用してサービスメッシュを設定し、管理します。

Red Hat OpenShift Service Mesh では、検出、負荷分散、サービス間の認証、障害復旧、メトリクス、およびモニタリングを提供する、デプロイされたサービスのネットワークを簡単に作成できます。サービスメッシュは、A/B テスト、カナリアリリース、レート制限、アクセス制御、エンドツーエンド認証を含む、より複雑な運用機能を提供します。

1.1.2. サポート

本書で説明されている手順で問題が発生した場合は、Red Hat カスタマーポータル (<http://access.redhat.com>) にアクセスしてください。カスタマーポータルでは、次のことができます。

- Red Hat 製品に関する技術サポート記事の Red Hat ナレッジベースの検索またはブラウズ。
- Red Hat グローバルサポートサービス (GSS) へのサポートケースの送信
- その他の製品ドキュメントへのアクセス

本書の改善が提案されている場合やエラーが見つかった場合は、**Documentation** コンポーネントの **Product** に対して、<http://bugzilla.redhat.com> から Bugzilla レポートを送信してください。コンテンツを簡単に見つけられるよう、セクション番号、ガイド名、Service Mesh のバージョンなどの詳細情報を記載してください。

1.2. 新機能および変更された機能

1.2.1. テクノロジープレビューの新機能 12

Red Hat OpenShift Service Mesh の本リリースでは、Istio 1.1.8、Jaeger 1.13.1、Kiali 1.0.0、および 3scale Istio Adapter 0.7.1 のサポートが追加されました。

このリリースにおけるその他の主な変更点は、以下のとおりです。

- Kiali および Jaeger Operator をインストールに統合。
- Kubernetes Container Network Interface (CNI) のサポートを追加。
- Operator Lifecycle Management (OLM) のサポートを追加。
- マルチテナンシー向けに Istio OpenShift ルーターを更新。
- デフォルトで、マルチテナンシー用のコントロールプレーンを設定。ただし、Red Hat OpenShift Service Mesh 0.12.TechPreview では単一テナントのコントロールプレーンを設定できます。



注記

インストールとサポートを単純化するために、今後のリリースは、1つ以上のテナントのマルチテナントコントロールプレーンのみをサポートします。

1.2.2. テクノロジープレビューの新機能 11

Red Hat OpenShift Service Mesh のリリースでは、マルチテナントインストール、Red Hat Enterprise Linux (RHEL) Universal Base Images (UBI8)、OpenSSL 1.1.1、Kiali 0.20.x、3scale Istio Adapter 0.6.0、および Istio 1.1.5 のサポートが追加されました。

1.2.3. テクノロジープレビューの新機能 10

Red Hat OpenShift Service Mesh のリリースでは、Kiali 0.16.x、3scale Istio Adapter 0.5.0、および Istio 1.1 のサポートが追加されました。

1.2.4. テクノロジープレビューの新機能 9



注記

Red Hat OpenShift Service Mesh 0.9.TechPreview 以降、Mixer のポリシーの適用はデフォルトで無効にされていますが、これを有効にしてポリシータスクを実行する必要があります。Mixer ポリシーの適用を有効にする方法については、[Mixer ポリシーの適用の更新](#)について参照してください。

Red Hat OpenShift Service Mesh のリリースでは、Kiali 0.15.x、Jaeger 1.11、3scale Istio Adapter 0.4.1、および Istio 1.1.0-rc.2 のサポートが追加されました。

1.2.5. テクノロジープレビューの新機能 8

Red Hat OpenShift Service Mesh のリリースでは、Kiali 0.14.x および 3scale Istio Adapter 0.3 のサポートが追加されました。

1.2.6. テクノロジープレビューの新機能 7

Red Hat OpenShift Service Mesh のリリースでは、3scale Istio Adapter が追加され、Kiali 0.13.x、Jaeger 1.9.0、および Istio 1.1 のサポートが追加されました。

1.2.7. テクノロジープレビューの新機能 6

Red Hat OpenShift Service Mesh のリリースでは、Kiali 0.11.x および Istio 1.0.5 のサポートが追加されました。

1.2.8. テクノロジープレビューの新機能 5

Red Hat OpenShift Service Mesh のリリースでは、Kiali 0.10.x、Jaeger 1.8.1、および Istio 1.0.4 のサポートが追加されました。

1.2.9. テクノロジープレビューの新機能 4

Red Hat OpenShift Service Mesh のリリースでは、Kiali 0.9.x および Istio 1.0.3 のサポートが追加されました。

1.2.10. テクノロジープレビューの新機能 3

Red Hat OpenShift Service Mesh のリリースでは、OpenShift 3.11、Kiali 0.8.x のサポートと、更新されたベース Ansible インストーラー (3.11.16-3) のサポートが追加されました。

1.2.11. テクノロジープレビューの新機能 2

本リリースで、Kiali の可観測性コンソールが Red Hat OpenShift Service Mesh に追加されました。Kiali では、サービスメッシュを構成するマイクロサービスのトポロジーおよびヘルス状態を確認できるグラフが多数提供されます。着信および発信トラフィックごとに詳細な要求と応答メトリクス (ボリューム、期間、サイズ、TCP トラフィック) を確認できる事前定義ダッシュボードを表示できます。アプリケーション、ワークロードおよびサービスごとにサービスメッシュをブラウズし、各要素の健全性を確認できます。

1.2.12. テクノロジープレビューの新機能 1

Red Hat OpenShift Service Mesh は、サービスのネットワーク全体で多数の主要機能を均一に提供します。

- **トラフィック管理:** サービス間でトラフィックおよび API 呼び出しのフローを制御し、呼び出しの安定度を高め、不利な条件下でもネットワークの堅牢性を維持します。
- **サービス ID とセキュリティー:** メッシュのサービスを検証可能な ID で指定でき、サービスのトラフィックがさまざまな信頼度のネットワークに送られる際にそのトラフィックを保護する機能を提供します。
- **ポリシーの適用:** サービス間の対話に組織のポリシーを適用し、アクセスポリシーが適用され、リソースはコンシューマー間で均等に分散されるようにします。ポリシー変更は、アプリケーションコードを変更するのではなく、メッシュを設定して行います。
- **Telemetry:** サービス間の依存関係やそれらの間のトラフィックの性質やフローを理解するのに役立ち、問題を素早く特定できます。

1.3. 解決済みの問題

1.3.1. 修正された問題

次の問題は、現在のリリースで解決されています。

- [MAISTRA-4](#): アンインストールによってファイルはすべて削除せられず、**customresourcedefinitions.apiextensions.k8s.io "installations.istio.openshift.com"** がすでに存在しているため、`istio-operator` を再インストールするとインストールは失敗します。
- [MAISTRA-5](#): **openshift-ansible-istio-installer-job** Pod は起動を試みますが、エラーが発生します。
- [MAISTRA-13](#): インストーラーはインストールされたコンポーネントのリリースバージョンを判別します。現時点で、インストーラーは yml ファイルをクエリーしますが、yml が変更された場合、インストーラーは古いバージョンを削除できません。
- [MAISTRA-21](#): インストーラーのデフォルトの 512Mi はトレーシングには低い値です。デフォルトの Elasticsearch メモリーが 512 MB から 1 GB に増加しました。
- [MAISTRA-61](#) 該当するすべてのリソースが OpenShift にデプロイされると、Istio サイドカーコンテナはそれらのルートについての情報を失い、次の更新を受け取るまでサービスと通信できなくなる可能性があります。
- [MAISTRA-79](#): **istiooc cluster up** コマンドの実行により、`istio-operator` namespace は Elasticsearch sysctl 要件を継続的に満たす Pod をデプロイします。このループは、クラスターを実行しているシステムの負荷を大幅に発生させます。
- [MAISTRA-110](#) 大規模なクラスターでは、`citadel` がシークレットを作成するためにかなり時間がかかる場合があります。これにより、インストールが失敗する場合があります。
- [MAISTRA-157](#) 条件付きレート制限機能は、アクセスを予想通りに制限しません。
- [MAISTRA-196](#) インストールを編集してパラメーターを変更する (例: 認証を有効にする) 場合には、新しい 1.1 CRD `configmap` が存在することにより、新規インストールが失敗します。
- [MAISTRA-420](#) [マルチテナント実装] Jaeger エージェント Pod は、OpenShift 4.1.rc.5 のマルチテナンシーのデプロイメントでのポート競合が原因でスケジュールされません。
- [MAISTRA-245](#) アップストリームのコミュニティバージョンを実行している場合は、サイドカーインジェクター Pod が起動に失敗します。
- [MAISTRA-462](#) [マルチテナント実装] namespace メンバーを 2 つ目のコントロールプレーンに追加した後、2 つ目のコントロールプレーンの namespace には **maistra.io/member-of** および **istio.openshift.io/member-of** ラベルがないため、Kiali は namespace 一覧に namespace メンバーを表示しません。これは、2 つ目のコントロールプレーンのインストールが、[MAISTRA-464](#) (NodePort が最初のコントロールプレーンですすでに使用されているために 2 つ目のコントロールプレーンで Operator が **istio-ingressgateway** サービスを作成できない問題) によって失敗することによって生じます。回避策としては、(**oc edit svc** を使用して) 最初のコントロールプレーンの namespace の **istio-ingressgateway** サービスのノードポートを手動で変更することができます。その後 Operator は 2 つ目のコントロールプレーンのデプロイメントを完了できます。
- [MAISTRA-466](#) [マルチテナント実装] 複数のコントロールプレーンをインストールする場合、最新のインストールのみが機能するように、Operator は既存の Kiali インストールの Kiali `oauthclient` yml を上書きします。Kiali `oauthclient` (**oc get oauthclients kiali**) には、OpenShift OAuth がリダイレクトする承認された URL の一覧が含まれます。使用する URL がこの一覧に含まれていない場合、`oauth` ログインは失敗し、以下のメッセージが返されます。

```
{"error": "invalid_request", "error_description": "The request is missing a required parameter, includes an invalid parameter value, includes a parameter more than once, or is otherwise malformed."}
```

- [MAISTRA-469](#) ServiceMeshControlPlane を削除する前にプロジェクトを削除すると、クリーンアッププロセスは削除されたプロジェクトのリソースに対して実行されません。SecurityContextConstraints に追加されたサービスアカウントは削除されず、Kiali OAuthClient リソースは適切に更新されません。
- [MAISTRA-470](#) コントロールプレーンの namespace をメンバーロールに含めると、調整プロセスでは、ログを送信し、正常に設定されているメンバーについても configuredMembers 一覧のステータスが更新できないようにするエラーが出されます。
- [KIALI-1284](#) Istio では、ワークロードに、その出所にかかわらず、任意の Pod または Pod のグループを使用することができます。出所は、Kubernetes Deployment、Replica Set、または単一の「孤立」Pod である可能性があります。Kiali では、現時点でワークロードの出所は Deployment であることを前提としています。大半のケースがこれに該当するはずです。
- [KIALI-1570](#) Kiali コンソールでグラフを読み込むと、グラフが読み込まれていることを示すメッセージではなく、グラフが空であることを示すメッセージが表示されます。
- [KIALI-1572](#) Kiali ログを表示する際にこのエラーメッセージが表示されても、これを無視することができます。

```
Failed to determine console version from file [/opt/kiali/console/version.txt]. error=open /opt/kiali/console/version.txt: no such file or directory Kiali: Console version: unknown
```

- [KIALI-1609](#) 非常に小さい値 (例: 0.0.1 rps 未満) を処理する場合、グラフに不整合が生じる可能性があります。現在、非常に小さい値を処理する場合のこの機能の強化に向けて変更を実施できるように取り組んでいます。
- [KIALI-2261](#) Kiali グラフでは、要求トラフィックがなくても、未使用のリンク (トラフィックのないエッジ) には要求トラフィックの 100% のラベルが付けられます。[KIALI-2296](#) も参照してください。
- [KIALI-2403](#) 最新の Istio Pilot は異なるポートでリッスンするようになったため、Istio 1.1.0-snapshot.6 への移行後に Istio バージョンは Kiali About ページに一覧表示されなくなりました。Istio Pilot はポート 8080 でリッスンし、Pilot にアクセスして Istio バージョン (<http://istio-pilot:8080/version>) を判別できます。
- [KIALI-2430](#) TCP エッジをクリックしてから、HTTP エッジをクリックすると、グラフが Kiali でクラッシュします。
- [KIALI-2671](#) コントロールプレーンカスタムリソースでダッシュボードのユーザー/パスワードを指定しない場合、Operator はインストールに OAuth を使用します。OAuth を使用する OpenShift ストラテジーは、Red Hat OpenShift Service Mesh 0.12.TechPreview テクノロジープレビュー 10 では機能しません。回避策として、カスタムリソースにユーザーおよびパスワードを指定するようにしてください。
- [KIALI-2942](#) OpenShift OAuth を使用する場合、ログアウトリンクをクリックすると、Kiali コンソールにログインされます。ログイン URL に移動して、Cookies をチェックし、自動的にログインします。回避策として、Kiali の Cookie を削除します。

1.4. 既知の問題

1.4.1. 既知の問題

現時点で、Red Hat OpenShift Service Mesh には以下のような制限が存在します。

- アップストリームの Istio プロジェクトでサポートされておらず、また OpenShift でも完全にサポートされていないため、Red Hat OpenShift Service Mesh は IPv6 をサポートしていません。
- istio-init コンテナでは、特権付きのセキュリティーコンテキストがあること、または最低でも root として実行され、NET_ADMIN 機能を使用できるようにする必要があります。istio-init コンテナには、ネットワーク接続のインターセプトのために Pod の iptables ルールを適切に設定する必要があるため、特権が設定される必要があります。現時点で、Istio で必要な権限を縮小する方法について調査されています。



注記

Istio CNI プラグインは、各 Pod について追加の権限を要求することなく、Pod がサービスマッシュに参加することを許可します。プラグインを有効にするには、コントロールプレーンカスタムリソースファイルを編集し、**istio_cni** セクションの **enabled** フィールドを **true** に設定します。

- グラフレイアウト: Kiali グラフのレイアウトは、アプリケーションのアーキテクチャーや表示データ (グラフィックノードとその対話の数) によって異なることがあります。すべての状況に適した単一のレイアウトを作成することは不可能ではないにしても困難であるため、Kiali は複数の異なるレイアウトの選択肢を提供します。別のレイアウトを選択するには、**Graph Settings** メニューから異なる **Layout Schema** を選択します。



注記

Kafka パブリッシャーは Jaeger の一部としてリリースに含まれていますが、サポートされていません。

1.4.1.1. Red Hat OpenShift Service Mesh の問題

現時点で、Red Hat OpenShift Service Mesh には次のような既知の問題が存在します。

- [MAISTRA-684 istio-operator](#) のデフォルトの Jaeger バージョンは 1.12.0 で、Red Hat OpenShift Service Mesh 0.12.TechPreview で提供される Jaeger バージョン 1.13.1 と一致しません。

Jaeger バージョンを 1.13.1 に変更せずに Red Hat OpenShift Service Mesh 0.12.TechPreview をインストールすると、**istio-system** で Pod を確認する際に表示される内容が表示されます。

```
$ oc get pods -n istio-system
```

NAME	READY	STATUS	RESTARTS	AGE
elasticsearch-0	1/1	Running	0	16m
grafana-694d54c786-m6dfc	2/2	Running	0	18m
istio-citadel-7658c96954-r8p46	1/1	Running	0	18m
istio-egressgateway-d759556b8-hwc7n	1/1	Running	0	18m
istio-galley-7cf565999f-b729t	1/1	Running	0	18m
istio-ingressgateway-bc97545d5-5mpw4	1/1	Running	0	18m
istio-pilot-dd7c67fb5-r8nbt	2/2	Running	0	29m
istio-policy-b5df8c557-5xbbl	2/2	Running	0	18m
istio-sidecar-injector-5bccb75987-xl6t6	1/1	Running	0	18m
istio-telemetry-7f86b4f6d9-kgl5p	2/2	Running	0	30m
jaeger-collector-85c597698c-54b2c	0/1	ImagePullBackOff	0	18m

```
jaeger-query-59b877c9d9-92vmj    1/3 ImagePullBackOff 0    18m
kiali-54ff784b57-8clh2          1/1 Running             0    18m
prometheus-7b89468cf6-pbnqh     2/2 Running          0    18m
```

このコマンドを実行して **istio-system** イベントを表示します。

```
$ oc get events -n istio-system
```

以下のエラーが表示されます。

```
...
8m50s    Warning Failed                pod/jaeger-query-59b877c9d9-92vmj
Failed to pull image "registry.redhat.io/distributed-tracing-tech-preview/jaeger-agent:1.12.0":
rpc error: code = Unknown desc = Error reading manifest 1.12.0 in
registry.redhat.io/distributed-tracing-tech-preview/jaeger-agent: error parsing HTTP 404
response body: invalid character 'F' looking for beginning of value: "File not found.\'"
...
```

回避策として、以下の変更をカスタムリソースに加え、Jaeger 1.13.1 をインストールします。

```
tracing:
  enabled: true
jaeger:
  tag: 1.13.1
```

- [MAISTRA-622](#) Maistra 0.12.0/TP12 では、パーミッシブモードは機能しません。ユーザーには Plain text モードまたは Mutual TLS モードを使用するオプションがありますが、パーミッシブモードのオプションはありません。
- [MAISTRA-572](#) Jaeger を Kiali と併用できません。本リリースでは、Jaeger は OAuth プロキシを使用するように設定されていますが、ブラウザでのみ機能するようにも設定され、サービスアクセスを許可しません。Kiali は Jaeger エンドポイントと適切に通信できないため、Jaeger が無効であると見なします。[TRACING-591](#) も参照してください。
- [MAISTRA-465](#) Maistra Operator が、Operator メトリクスのサービスの作成に失敗します。
- [MAISTRA-453](#) 新規プロジェクトを作成して Pod を即時にデプロイすると、サイドカーコンテナの挿入は発生しません。この Operator は Pod の作成前に **maistra.io/member-of** を追加できないため、サイドカーコンテナの挿入を発生させるには Pod を削除し、再作成する必要があります。
- [MAISTRA-357](#) AWS の OpenShift 4 Beta では、追加設定なしでポート 80 以外のポートの Ingress ゲートウェイを介して TCP または HTTPS サービスにアクセスすることはできません。AWS ロードバランサーには、サービスエンドポイントのポート 80 がアクティブであるかどうかを検証するヘルスチェックがあります。
ロードバランサーのヘルスチェックは、Istio Ingress ゲートウェイポートの一覧で定義されている最初のポートのみを確認します。このポートは 80/HTTP:31380/TCP として設定されています。サービスがこのポート上で実行されていないと、ロードバランサーのヘルスチェックは失敗します。

Ingress ゲートウェイを使用して HTTPS または TCP トラフィックをチェックするには、既存の HTTP サービスが必要になります (たとえば、Ingress ゲートウェイポート 80 で実行中の Bookinfo サンプルアプリケーション製品ページなど)。または、AWS EC2 コンソールを使用して、ロードバランサーがヘルスチェックを実行するために使用するポートを変更して、80 をサービスが実際に使用するポートに置き換えます。

- [MAISTRA-348](#) 80 または 443 以外のポートでの Ingress ゲートウェイを使用して TCP サービスにアクセスするには、OpenShift ルーターではなく AWS ロードバランサーによって提供されるサービスホスト名を使用します。

istio-ingressgateway ルートホスト名 (例: **istio-ingressgateway-istio-system.apps.[cluster name].openshift.com**) は、ポート 80 またはポート 443 トラフィックで機能します。ただし、そのルートのホスト名は他のポートトラフィックをサポートしません。

Ingress ゲートウェイの TCP ポートで実行しているサービスにアクセスするには、istio-ingressgateway 外部ホスト名 (たとえば、**[uuid].[aws region].elb.amazonaws.com**) を取得し、その外部ホスト名の値を使用してトラフィックをチェックできます。

外部 IP ホスト名の値を取得するには、以下のコマンドを実行します。

```
$ oc -n istio-system get service istio-ingressgateway -o
jsonpath='{.status.loadBalancer.ingress[0].hostname}'
```

- [MAISTRA-193](#) ヘルスチェックが citadel で有効になっていると、予期しないコンソール情報メッセージが表示されます。
- [MAISTRA-158](#) 同じホスト名を参照する複数のゲートウェイを適用すると、すべてのゲートウェイが機能しなくなります。
- [MAISTRA-108](#) OpenShift Container Platform クラスターで Operator Lifecycle Manager (OLM) をインストールするプロセスの一部として、[レジストリー承認 Playbook](#) が実行されますが、エラーが生じるためにプロセスが正常に完了されません。

「openshift_control_plane: Check for file paths outside of /etc/origin/master in master's config」タスクは、master-config.yaml ファイル内に「/dev/null」文字列が見つかったら失敗します。この文字列は、Istio のインストール用にクラスターを準備する際に設定にパッチを適用すると追加されます。

以下は 2 つの Webhook です。

```
MutatingAdmissionWebhook:
configuration:
apiVersion: apiserver.config.k8s.io/v1alpha1
kind: WebhookAdmission
kubeConfigFile: /dev/null
```

```
ValidatingAdmissionWebhook:
configuration:
apiVersion: apiserver.config.k8s.io/v1alpha1s
kind: WebhookAdmission
kubeConfigFile: /dev/null
```

/var/lib/origin/null から **/dev/null** にソフトリンクを作成し、2 つの kubeConfigFile 変数を **/var/lib/origin/null** に置き換えます。これにより、タスクでは **/var/lib/origin/null** が元の "perimeter" のアセットとなり、実行を継続します。

- [MAISTRA-62](#) Istio インストールが正常に実行された後に、OCP クラスターを 3.10 から 3.11 にアップグレードすると、ストレージのアップグレードタスクが失敗し、アップグレードプロセス全体が失敗します。

1.4.1.2. Kiali の問題

- [KIALI-3118](#) ServiceMeshMemberRoll の変更 (namespace の追加または削除などの) 後、Kiali Pod が再起動し、その間にグラフページにエラーが表示されます。
- [KIALI-3096](#) サービスメッシュでラインタイムメトリクスが失敗します。サービスメッシュと Prometheus 間には oauth フィルターがあり、アクセスを付与するにはベアータークンを Prometheus に渡す必要があります。Kiali は Prometheus サーバーと通信する際にこのトークンを使用するように更新されていますが、アプリケーションメトリクスは現在 403 エラーで失敗しています。
- [KIALI-2206](#) 初回の Kiali コンソールへのアクセス時に、Kiali のキャッシュされたブラウザーデータがない場合、Kiali サービスの詳細ページの Metrics タブにある「View in Grafana」リンクは誤った場所にリダイレクトされます。この問題は、Kiali への初回アクセス時にのみ生じます。
- [KIALI-507](#) Kiali は Internet Explorer 11 に対応していません。これは、基礎となるフレームワークが Internet Explorer に対応していないためです。Kiali コンソールにアクセスするには、Chrome、Edge、Firefox、または Safari ブラウザーの最新の 2 バージョンのいずれかを使用します。