OpenShift Dedicated 4

セキュリティーおよびコンプライアンス

OpenShift Dedicated での Security Context Constraints の設定

Last Updated: 2024-10-15

OpenShift Dedicated 4 セキュリティーおよびコンプライアンス

OpenShift Dedicated での Security Context Constraints の設定

法律上の通知

概要

このドキュメントでは、OpenShift Dedicated でセキュリティーコンテキストの制約を設定する手順を説明します。

目次

第1章 監査ログの表示

OpenShift Dedicated 監査は、システムに影響を与えた一連のアクティビティーを個別のユーザー、管理者、またはその他システムのコンポーネント別に記述したセキュリティー関連の時系列のレコードを提供します。

1.1. API の監査ログについて

監査は API サーバーレベルで実行され、サーバーに送られるすべての要求をログに記録します。それぞれの監査ログには、以下の情報が含まれます。

表1.1 監査ログフィールド

フィールド	説明
level	イベントが生成された監査レベル。
auditID	要求ごとに生成される一意の監査 ID。
stage	このイベントインスタンスの生成時の要求処理のステージ。
requestURI	クライアントによってサーバーに送信される要求 URI。
verb	要求に関連付けられる Kubernetes の動詞。リソース以外の要求の場合、これは小文字の HTTP メソッドになります。
user	認証されたユーザーの情報。
impersonatedUser	オプション。偽装ユーザーの情報 (要求で別のユーザーを偽装する場合)。
sourceIPs	オプション。要求の送信元および中間プロキシーからのソース IP。
userAgent	オプション。クライアントが報告するユーザーエージェントの文字列。ユーザーエージェントはクライアントによって提供されており、信頼できないことに注意してください。
objectRef	オプション。この要求のターゲットとなっているオブジェクト参照。これは、**List** タイプの要求やリソース以外の要求には適用されません。
responseStatus	オプション。**ResponseObject** が **Status** タイプでなくても設定される応答ステータス。正常な応答の場合、これにはコードのみが含まれます。ステータス以外のタイプのエラー応答の場合、これにはエラーメッセージが自動的に設定されます。

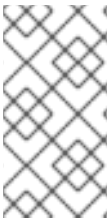
フィールド	説明
requestObject	オプション。JSON 形式の要求からの API オブジェクト。**RequestObject** は、バージョンの変換、デフォルト設定、受付またはマージの前に要求の場合のように記録されます (JSON として再エンコードされる可能性がある)。これは外部のバージョン付けされたオブジェクトタイプであり、それ自体では有効なオブジェクトではない可能性があります。これはリソース以外の要求の場合には省略され、要求レベル以上でのみログに記録されます。
responseObject	オプション。JSON 形式の応答で返される API オブジェクト。**ResponseObject** は外部タイプへの変換後に記録され、JSON としてシリアライズされます。これはリソース以外の要求の場合には省略され、応答レベルでのみログに記録されます。
requestReceivedTimestamp	要求が API サーバーに到達した時間。
stageTimestamp	要求が現在の監査ステージに達した時間。
annotations	オプション。監査イベントと共に保存される構造化されていないキーと値のマップ。これは、認証、認可、受付プラグインなど、要求提供チェーンで呼び出されるプラグインによって設定される可能性があります。これらのアノテーションは監査イベント用のもので、送信されたオブジェクトの **metadata.annotations** に対応しないことに注意してください。キーは、名前の競合が発生しないように通知コンポーネントを一意に識別する必要があります (例: **podsecuritypolicy.admission.k8s.io/policy**)。値は短くする必要があります。アノテーションはメタデータレベルに含まれます。

Kubernetes API サーバーの出力例:


```
{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"Metadata","auditID":"ad209ce1-fec7-4130-8192-c4cc63f1d8cd","stage":"ResponseComplete","requestURI":"/api/v1/namespaces/openshift-kube-controller-manager/configmaps/cert-recovery-controller-lock?timeout=35s","verb":"update","user":{"username":"system:serviceaccount:openshift-kube-controller-manager:localhost-recovery-client","uid":"dd4997e3-d565-4e37-80f8-7fc122ccd785","groups":["system:serviceaccounts","system:serviceaccounts:openshift-kube-controller-manager","system:authenticated"]},"sourceIPs":["::1"],"userAgent":"cluster-kube-controller-manager-operator/v0.0.0 (linux/amd64) kubernetes/$Format","objectRef":{"resource":"configmaps","namespace":"openshift-kube-controller-manager","name":"cert-recovery-controller-lock","uid":"5c57190b-6993-425d-8101-8337e48c7548","apiVersion":"v1","resourceVersion":"574307"},"responseStatus":{"metadata":{},"code":200},"requestReceivedTimestamp":"2020-04-02T08:27:20.200962Z","stageTimestamp":"2020-04-02T08:27:20.206710Z","annotations":{"authorization.k8s.io/decision":"allow","authorization.k8s.io/reason":"RBAC: allowed by ClusterRoleBinding \"system:openshift:operator:kube-controller-manager-recovery\" of ClusterRole \"cluster-admin\" to ServiceAccount \"localhost-recovery-client/openshift-kube-controller-manager\""}}
```


1.2. 監査ログの表示

それぞれのコントロールプレーンノードについて OpenShift API サーバー、Kubernetes API サーバー、OpenShift OAuth API サーバー、および OpenShift OAuth サーバーのログを表示できます。



注記

OpenShift Dedicated デプロイメントでは、Customer Cloud Subscription (CCS) モデルを使用していないお客様は、Red Hat サポートに連絡してクラスターの監査ログのコピーを要求する必要があります。これは、API サーバーの監査ログを表示するには、**cluster-admin** 権限が必要であるためです。

手順

監査ログを表示するには、以下を実行します。

- OpenShift API サーバーの監査ログを表示します。
  a. 各コントロールプレーンノードで利用可能な OpenShift API サーバー監査ログをリスト表示します。

```
$ oc adm node-logs --role=master --path=openshift-apiserver/
```

出力例

```
ci-ln-m0wpfjb-f76d1-vnb5x-master-0 audit-2021-03-09T00-12-19.834.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-0 audit.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-1 audit-2021-03-09T00-11-49.835.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-1 audit.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-2 audit-2021-03-09T00-13-00.128.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-2 audit.log
```

  b. ノード名とログ名を指定して、特定の OpenShift API サーバー監査ログを表示します。

```
$ oc adm node-logs <node_name> --path=openshift-apiserver/<log_name>
```

以下に例を示します。

```
$ oc adm node-logs ci-ln-m0wpfjb-f76d1-vnb5x-master-0 --path=openshift-
apiserver/audit-2021-03-09T00-12-19.834.log
```

出力例

```
{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"Metadata","auditID":"381acf6d-5f30-
4c7d-8175-
c9c317ae5893","stage":"ResponseComplete","requestURI":"/metrics","verb":"get","user":
{"username":"system:serviceaccount:openshift-monitoring:prometheus-
k8s","uid":"825b60a0-3976-4861-a342-3b2b561e8f82","groups":
["system:serviceaccounts","system:serviceaccounts:openshift-
monitoring","system:authenticated"]},"sourceIPs":
["10.129.2.6"],"userAgent":"Prometheus/2.23.0","responseStatus":{"metadata":
{},"code":200},"requestReceivedTimestamp":"2021-03-
08T18:02:04.086545Z","stageTimestamp":"2021-03-
08T18:02:04.107102Z","annotations":
```

```
{"authorization.k8s.io/decision":"allow","authorization.k8s.io/reason":"RBAC: allowed by ClusterRoleBinding \"prometheus-k8s\" of ClusterRole \"prometheus-k8s\" to ServiceAccount \"prometheus-k8s/openshift-monitoring\""}}
```

- Kubernetes API サーバーの監査ログを表示します。

  a. 各コントロールプレーンノードで利用可能な Kubernetes API 監査サーバーログをリスト表示します。

  ```
  $ oc adm node-logs --role=master --path=kube-apiserver/
  ```

  出力例

  ```
  ci-ln-m0wpfjb-f76d1-vnb5x-master-0 audit-2021-03-09T14-07-27.129.log
  ci-ln-m0wpfjb-f76d1-vnb5x-master-0 audit.log
  ci-ln-m0wpfjb-f76d1-vnb5x-master-1 audit-2021-03-09T19-24-22.620.log
  ci-ln-m0wpfjb-f76d1-vnb5x-master-1 audit.log
  ci-ln-m0wpfjb-f76d1-vnb5x-master-2 audit-2021-03-09T18-37-07.511.log
  ci-ln-m0wpfjb-f76d1-vnb5x-master-2 audit.log
  ```

  b. ノード名とログ名を指定して、特定の Kubernetes API 監査サーバーログを表示します。

  ```
  $ oc adm node-logs <node_name> --path=kube-apiserver/<log_name>
  ```

  以下に例を示します。

  ```
  $ oc adm node-logs ci-ln-m0wpfjb-f76d1-vnb5x-master-0 --path=kube-apiserver/audit-2021-03-09T14-07-27.129.log
  ```

  出力例

  ```
  {"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"Metadata","auditID":"cfce8a0b-b5f5-4365-8c9f-79c1227d10f9","stage":"ResponseComplete","requestURI":"/api/v1/namespaces/openshift-kube-scheduler/serviceaccounts/openshift-kube-scheduler-sa","verb":"get","user":{"username":"system:serviceaccount:openshift-kube-scheduler-operator:openshift-kube-scheduler-operator","uid":"2574b041-f3c8-44e6-a057-baef7aa81516","groups":["system:serviceaccounts","system:serviceaccounts:openshift-kube-scheduler-operator","system:authenticated"]},"sourceIPs":["10.128.0.8"],"userAgent":"cluster-kube-scheduler-operator/v0.0.0 (linux/amd64) kubernetes/$Format","objectRef":{"resource":"serviceaccounts","namespace":"openshift-kube-scheduler","name":"openshift-kube-scheduler-sa","apiVersion":"v1"},"responseStatus":{"metadata":{},"code":200},"requestReceivedTimestamp":"2021-03-08T18:06:42.512619Z","stageTimestamp":"2021-03-08T18:06:42.516145Z","annotations":{"authentication.k8s.io/legacy-token":"system:serviceaccount:openshift-kube-scheduler-operator:openshift-kube-scheduler-operator","authorization.k8s.io/decision":"allow","authorization.k8s.io/reason":"RBAC: allowed by ClusterRoleBinding \"system:openshift:operator:cluster-kube-scheduler-operator\" of ClusterRole \"cluster-admin\" to ServiceAccount \"openshift-kube-scheduler-operator/openshift-kube-scheduler-operator\""}}
  ```

- OpenShift OAuth API サーバーの監査ログを表示します。

a. 各コントロールプレーンノードで利用可能な OpenShift OAuth API 監査サーバーログをリスト表示します。

```
$ oc adm node-logs --role=master --path=oauth-apiserver/
```

出力例

```
ci-ln-m0wpfjb-f76d1-vnb5x-master-0 audit-2021-03-09T13-06-26.128.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-0 audit.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-1 audit-2021-03-09T18-23-21.619.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-1 audit.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-2 audit-2021-03-09T17-36-06.510.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-2 audit.log
```

b. ノード名とログ名を指定して、特定の OpenShift OAuth API 監査サーバーログを表示します。

```
$ oc adm node-logs <node_name> --path=oauth-apiserver/<log_name>
```

以下に例を示します。

```
$ oc adm node-logs ci-ln-m0wpfjb-f76d1-vnb5x-master-0 --path=oauth-apiserver/audit-2021-03-09T13-06-26.128.log
```

出力例

```
{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"Metadata","auditID":"dd4c44e2-3ea1-4830-9ab7-c91a5f1388d6","stage":"ResponseComplete","requestURI":"/apis/user.openshift.io/v1/users/~","verb":"get","user":{"username":"system:serviceaccount:openshift-monitoring:prometheus-k8s","groups":["system:serviceaccounts","system:serviceaccounts:openshift-monitoring","system:authenticated"]},"sourceIPs":["10.0.32.4","10.128.0.1"],"userAgent":"dockerregistry/v0.0.0 (linux/amd64) kubernetes/$Format","objectRef":{"resource":"users","name":"~","apiGroup":"user.openshift.io","apiVersion":"v1"},"responseStatus":{"metadata":{},"code":200},"requestReceivedTimestamp":"2021-03-08T17:47:43.653187Z","stageTimestamp":"2021-03-08T17:47:43.660187Z","annotations":{"authorization.k8s.io/decision":"allow","authorization.k8s.io/reason":"RBAC: allowed by ClusterRoleBinding \"basic-users\" of ClusterRole \"basic-user\" to Group \"system:authenticated\""}}
```

- OpenShift OAuth サーバーの監査ログを表示します。

a. 各コントロールプレーンノードで利用可能な OpenShift OAuth サーバーログをリスト表示します。

```
$ oc adm node-logs --role=master --path=oauth-server/
```

出力例

```
ci-ln-m0wpfjb-f76d1-vnb5x-master-0 audit-2022-05-11T18-57-32.395.log
```

```
ci-ln-m0wpfjb-f76d1-vnb5x-master-0 audit.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-1 audit-2022-05-11T19-07-07.021.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-1 audit.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-2 audit-2022-05-11T19-06-51.844.log
ci-ln-m0wpfjb-f76d1-vnb5x-master-2 audit.log
```

b. ノード名とログ名を指定して、特定の OpenShift OAuth サーバーログを表示します。

```
$ oc adm node-logs <node_name> --path=oauth-server/<log_name>
```

以下に例を示します。

```
$ oc adm node-logs ci-ln-m0wpfjb-f76d1-vnb5x-master-0 --path=oauth-server/audit-2022-05-11T18-57-32.395.log
```

出力例

```
{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"Metadata","auditID":"13c20345-f33b-4b7d-b3b6-e7793f805621","stage":"ResponseComplete","requestURI":"/login","verb":"post","user":{"username":"system:anonymous","groups":["system:unauthenticated"]},"sourceIPs":["10.128.2.6"],"userAgent":"Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0","responseStatus":{"metadata":{},"code":302},"requestReceivedTimestamp":"2022-05-11T17:31:16.280155Z","stageTimestamp":"2022-05-11T17:31:16.297083Z","annotations":{"authentication.openshift.io/decision":"error","authentication.openshift.io/username":"kubeadmin","authorization.k8s.io/decision":"allow","authorization.k8s.io/reason":""}}
```

authentication.openshift.io/decision アノテーションに使用できる値は、**allow**、**deny**、または **error** です。

1.3. 監査ログのフィルター

jq または別の JSON 解析ツールを使用して、API サーバー監査ログをフィルターできます。

注記

API サーバー監査ログに記録する情報量は、設定される監査ログポリシーで制御できます。

以下の手順では、**jq** を使用してコントロールプレーンノード **node-1.example.com** で監査ログをフィルターする例を示します。**jq** の使用に関する詳細は、jq Manual を参照してください。

前提条件

- **dedicated-admin** ロールを持つユーザーとしてクラスターにアクセスできる。
- **jq** がインストールされている。

手順

- OpenShift API サーバー監査ログをユーザーでフィルターします。

```
$ oc adm node-logs node-1.example.com  \
  --path=openshift-apiserver/audit.log \
  | jq 'select(.user.username == "myusername")'
```

- OpenShift API サーバー監査ログをユーザーエージェントでフィルターします。

```
$ oc adm node-logs node-1.example.com  \
  --path=openshift-apiserver/audit.log \
  | jq 'select(.userAgent == "cluster-version-operator/v0.0.0 (linux/amd64)
kubernetes/$Format")'
```

- Kubernetes API サーバー監査ログを特定の API バージョンでフィルターし、ユーザーエージェントのみを出力します。

```
$ oc adm node-logs node-1.example.com  \
  --path=kube-apiserver/audit.log \
  | jq 'select(.requestURI | startswith("/apis/apiextensions.k8s.io/v1beta1")) | .userAgent'
```

- 動詞を除外して OpenShift OAuth API サーバー監査ログをフィルターします。

```
$ oc adm node-logs node-1.example.com  \
  --path=oauth-apiserver/audit.log \
  | jq 'select(.verb != "get")'
```

- ユーザー名を識別し、エラーで失敗したイベントで OpenShift OAuth サーバー監査ログをフィルタリングします。

```
$ oc adm node-logs node-1.example.com  \
  --path=oauth-server/audit.log \
  | jq 'select(.annotations["authentication.openshift.io/username"] != null and
.annotations["authentication.openshift.io/decision"] == "error")'
```

1.4. 監査ログの収集

must-gather ツールを使用して、クラスターをデバッグするための監査ログを収集できます。このログは、確認したり、Red Hat サポートに送信したりできます。

注記

OpenShift Dedicated デプロイメントでは、Customer Cloud Subscription (CCS) モデルを使用していないお客様は、Red Hat サポートに連絡してクラスターの監査ログのコピーを要求する必要があります。これは、must-gather ツールを使用するには **cluster-admin** 権限が必要であるためです。

手順

1. **-- /usr/bin/gather_audit_logs** を指定して **oc adm must-gather** コマンドを実行します。

```
$ oc adm must-gather -- /usr/bin/gather_audit_logs
```

2. 作業ディレクトリーに作成された **must-gather** ディレクトリーから圧縮ファイルを作成します。たとえば、Linux オペレーティングシステムを使用するコンピューターで以下のコマンドを実行します。

```
$ tar cvaf must-gather.tar.gz must-gather.local.472290403699006248 1
```

1 **must-gather-local.472290403699006248** は、実際のディレクトリー名に置き換えます。

3. Red Hat カスタマーポータルの **カスタマーサポート** ページ で、圧縮ファイルをサポートケースに添付します。

1.5. 関連情報

- must-gather ツール

第2章 SRE クラスターアクセスに必要な許可リスト IP アドレス

2.1. 概要

Red Hat SRE が OpenShift Dedicated クラスター内の問題をトラブルシューティングするには、許可リスト IP アドレスを介して API サーバーに Ingress アクセスできるようにする必要があります。

2.2. 許可リストに登録された IP アドレスの取得

OpenShift Dedicated ユーザーは、OpenShift Cluster Manager CLI コマンドを使用して、OpenShift Dedicated クラスターへの SRE アクセスに必要な Red Hat マシンの最新の許可リスト IP アドレスを取得できます。

注記

これらの許可リストの IP アドレスは永続的なものではなく、変更される可能性があります。最新の許可リスト IP アドレスについては、API 出力を継続的に確認する必要があります。

前提条件

- OpenShift Cluster Manager API コマンドラインインターフェイス (**ocm**) をインストールしている。
- 許可リストの IP アドレスを含めるようにファイアウォールを設定できます。

手順

1. OpenShift Dedicated クラスターへの SRE アクセスに必要な現在の許可リスト IP アドレスを取得するには、次のコマンドを実行します。

```
$ ocm get /api/clusters_mgmt/v1/trusted_ip_addresses|jq -r '.items[].id'
```

2. 許可リストの IP アドレスへのアクセスを許可するようにファイアウォールを設定します。