OpenShift Dedicated 4

La sécurité et la conformité

Configuration des contraintes de contexte de sécurité dans OpenShift Dedicated

Last Updated: 2025-05-27

OpenShift Dedicated 4 La sécurité et la conformité

Configuration des contraintes de contexte de sécurité dans OpenShift Dedicated

Notice légale

Résumé

Ce document fournit des instructions pour configurer les contraintes de contexte de sécurité dans OpenShift Dedicated.

Table des matières

CHAPITRE 1. AFFICHAGE DES JOURNAUX D'AUDIT

L'audit dédié OpenShift fournit un ensemble chronologique pertinent d'enregistrements documentant la séquence d'activités qui ont affecté le système par des utilisateurs, des administrateurs ou d'autres composants du système.

1.1. À PROPOS DU JOURNAL D'AUDIT API

L'audit fonctionne au niveau du serveur API, enregistrant toutes les demandes venant au serveur. Chaque journal d'audit contient les informations suivantes:

Tableau 1.1. Champs de journal d'audit

Le champ	Description
a) Niveau	Le niveau d'audit auquel l'événement a été généré.
auditID	ID d'audit unique, généré pour chaque demande.
l'étape	L'étape du traitement de la demande lorsque cette instance d'événement a été générée.
demande d'URI	L'URI de requête envoyé par le client à un serveur.
le verbe	Le verbe Kubernetes associé à la requête. Dans le cas des demandes de non-ressource, il s'agit de la méthode HTTP minuscule.
l'utilisateur	Les informations d'utilisateur authentifiées.
identité de l'utilisateur	En option. Les informations personnelles de l'utilisateur, si la demande est l'identité d'un autre utilisateur.
les SourceIPs	En option. Les adresses IP source, d'où provient la demande et tout mandataire intermédiaire.
Agent utilisateur	En option. La chaîne d'agent utilisateur rapportée par le client. A noter que l'agent utilisateur est fourni par le client et ne doit pas faire confiance.
l'objetRef	En option. L'objet référence à cette demande est ciblé. Cela ne s'applique pas aux demandes de type liste, ni aux demandes de non-ressource.
État de réponse	En option. L'état de réponse, peuplé même lorsque l'Objet de Réponse n'est pas un type d'état. Dans le cas des réponses réussies, cela inclura uniquement le code. Dans le cas des réponses d'erreur de type non statutaire, cela sera auto-rempli avec le message d'erreur.

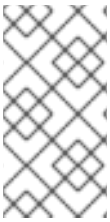
Le champ	Description
demande d'objectif	En option. L'objet API de la requête, au format JSON. L'Objet Demande est enregistré tel qu'il est dans la requête (peut-être ré-encodée en JSON), avant la conversion de la version, le défaut, l'admission ou la fusion. Il s'agit d'un type d'objet versionné externe, et peut ne pas être un objet valide par lui-même. Ceci est omis pour les demandes de non-ressource et n'est enregistré qu'au niveau de la demande et plus haut.
l'objectif de réponse	En option. L'objet API est retourné dans la réponse, au format JSON. L'Objet de Réponse est enregistré après conversion au type externe, et sérialisé comme JSON. Ceci est omis pour les demandes de non-ressource et n'est enregistré qu'au niveau de réponse.
demande reçueTimestamp	L'heure à laquelle la demande a atteint le serveur API.
le stageTimestamp	Le moment où la demande est arrivée à l'étape de la vérification actuelle.
annotations	En option. Carte de valeur clé non structurée stockée avec un événement d'audit qui peut être défini par des plugins invoqués dans la chaîne de service de requête, y compris les plugins d'authentification, d'autorisation et d'admission. A noter que ces annotations sont pour l'événement d'audit et ne correspondent pas aux métadonnées.annotations de l'objet soumis. Les clés doivent identifier de manière unique le composant informatif pour éviter les collisions de noms, par exemple podsecuritypolicy.admission.k8s.io/policy. Les valeurs devraient être courtes. Les annotations sont incluses dans le niveau des métadonnées.

Exemple de sortie pour le serveur API Kubernetes:


```
{"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. AFFICHAGE DES JOURNAUX D'AUDIT

Les journaux pour le serveur API OpenShift, le serveur API Kubernetes, le serveur OpenShift OAuth API et le serveur OpenShift OAuth pour chaque nœud de plan de contrôle peuvent être consultés.



NOTE

Dans les déploiements dédiés à OpenShift, les clients qui n'utilisent pas le modèle Customer Cloud Subscription (CCS) doivent demander une copie des journaux d'audit de votre cluster en contactant Red Hat Support. C'est parce que la visualisation des journaux d'audit de serveur API nécessite des privilèges cluster-admin.

Procédure

Consulter les journaux d'audit:

- Consultez les journaux d'audit du serveur d'API OpenShift:

  a. Liste des journaux d'audit du serveur OpenShift API disponibles pour chaque nœud de plan de contrôle:

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

  Exemple de sortie

  ```
  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. Afficher un journal d'audit spécifique du serveur d'API OpenShift en fournissant le nom du nœud et le nom du journal:

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

  À titre d'exemple:

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

  Exemple de sortie

  ```
  {"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\""}}
```

- Consultez les journaux d'audit du serveur de l'API Kubernetes:

  a. Liste des journaux d'audit du serveur de l'API Kubernetes disponibles pour chaque nœud de plan de contrôle:

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

  Exemple de sortie

  ```
  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. Consultez un journal d'audit spécifique du serveur de l'API Kubernetes en fournissant le nom du nœud et le nom du journal:

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

  À titre d'exemple:

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

  Exemple de sortie

  ```
  {"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\""}}
  ```

- Consultez les journaux d'audit du serveur OpenShift OAuth API:

a. Liste des journaux d'audit du serveur OpenShift OAuth API disponibles pour chaque nœud de plan de contrôle:

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

Exemple de sortie

```
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. Afficher un journal d'audit spécifique du serveur OpenShift OAuth API en fournissant le nom du nœud et le nom du journal:

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

À titre d'exemple:

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

Exemple de sortie

```
{"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\""}}
```

- Consultez les journaux d'audit du serveur OpenShift OAuth:

a. Liste des journaux d'audit du serveur OpenShift OAuth disponibles pour chaque nœud de plan de contrôle:

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

Exemple de sortie

```
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. Afficher un journal d'audit spécifique du serveur OpenShift OAuth en fournissant le nom du nœud et le nom du journal:

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

À titre d'exemple:

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

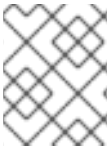
Exemple de sortie

```
{"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":""}}
```

Les valeurs possibles pour l'annotation d'authentification.openshift.io/decision sont autorisées, niées ou erreur.

1.3. FILTRER LES JOURNAUX D'AUDIT

Il est possible d'utiliser jq ou un autre outil d'analyse JSON pour filtrer les journaux d'audit du serveur API.



NOTE

La quantité d'informations enregistrées dans les journaux d'audit du serveur API est contrôlée par la stratégie de journal d'audit qui est définie.

La procédure suivante fournit des exemples d'utilisation de jq pour filtrer les journaux d'audit sur le node de plan de contrôle node-1.example.com. Consultez le manuel jq pour obtenir des informations détaillées sur l'utilisation de jq.

Conditions préalables

- En tant qu'utilisateur, vous avez accès au cluster avec le rôle d'administrateur dédié.
- Jq. Vous avez installé jq.

Procédure

- Filtrer les journaux d'audit du serveur d'API OpenShift par utilisateur:

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

- Filtrer les journaux d'audit du serveur API OpenShift par agent utilisateur:

```
$ 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")'
```

- Filtrer les journaux d'audit du serveur API Kubernetes par une certaine version de l'API et ne produit que l'agent utilisateur:

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

- Filtrer les journaux d'audit du serveur OpenShift OAuth API en excluant un verbe:

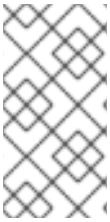
```
$ oc adm node-logs node-1.example.com  \
  --path=oauth-apiserver/audit.log \
  | jq 'select(.verb != "get")'
```

- Filtrer les journaux d'audit du serveur OpenShift OAuth par des événements qui ont identifié un nom d'utilisateur et qui ont échoué avec une erreur:

```
$ 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. COLLECTE DES JOURNAUX D'AUDIT

Il est possible d'utiliser l'outil must-collectther pour collecter les journaux d'audit pour le débogage de votre cluster, que vous pouvez consulter ou envoyer à Red Hat Support.



NOTE

Dans les déploiements dédiés à OpenShift, les clients qui n'utilisent pas le modèle Customer Cloud Subscription (CCS) doivent demander une copie des journaux d'audit de votre cluster en contactant Red Hat Support. C'est parce que l'utilisation de l'outil must-collectther nécessite des privilèges cluster-admin.

Procédure

1. Exécutez la commande oc adm must-collectther avec -- /usr/bin/gather_audit_logs:

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

2. Créez un fichier compressé à partir du répertoire must-collectther qui vient d'être créé dans votre répertoire de travail. À titre d'exemple, sur un ordinateur qui utilise un système d'exploitation Linux, exécutez la commande suivante:

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

1 Il suffit de remplacer must-collectther-local.472290403699006248 par le nom du répertoire.

3. Joindre le fichier compressé à votre dossier d'assistance sur la page Assistance clientèle du portail client Red Hat.

1.5. RESSOURCES SUPPLÉMENTAIRES

- L'outil must-collectther