Entretien de la grappe

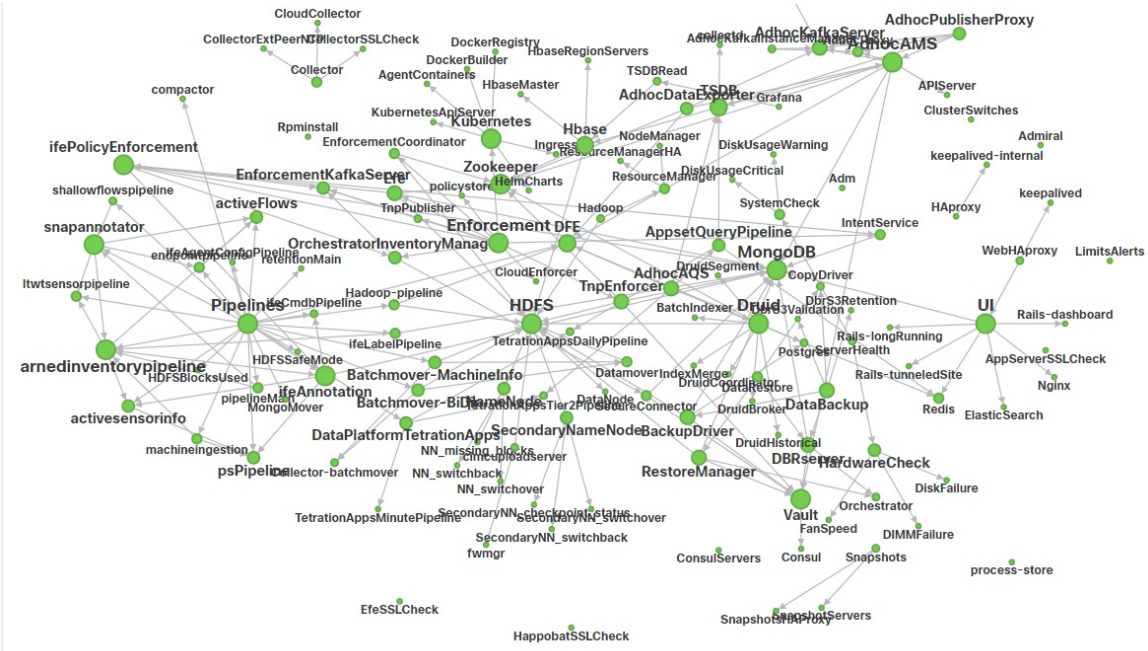
Ce chapitre fournit des détails sur les diverses actions de maintenance de la grappe que vous pouvez effectuer, telles que la mise à niveau, le redémarrage, la planification de sauvegardes de données et la restauration de données. Vous pouvez également afficher l'état du service et de la grappe à partir des options disponibles dans le menu de **dépannage**.

État du service

Dans le volet de navigation de gauche, la page **Troubleshoot (Dépannage)** > **Service Status (État du service)** affiche l'intégrité de tous les services utilisés dans votre grappe Cisco Cisco Secure Workload ainsi que leurs dépendances.

La vue graphique affiche l'intégrité du service, chaque nœud du graphique affiche l'intégrité du service et une périphérie représente la dépendance à l'égard d'autres services. Les services non intègres sont signalés en rouge lorsque le service n'est pas disponible et en orangé lorsque le service est défaillant mais disponible. Un nœud vert indique que le service est intègre. Pour plus d'informations de débogage sur ces nœuds, utilisez l'arborescence qui comporte le bouton **Expand All** (Tout développer) pour afficher tous les nœuds enfants dans l'arborescence des dépendances. « En panne » indique que le service n'est pas fonctionnel et « Non intègre » indique que le service n'est pas entièrement fonctionnel.

Figure 1: Page État du service



Alertes Admiral

Admiral est un système d'alerte intégré. Il traite les alertes en fonction de l'intégrité du service signalée par le État du service (État du service). Ainsi, les utilisateurs disposent d'un moyen unifié de déterminer l'intégrité d'un service ou de la grappe. L'état du service affiche l'intégrité actuelle (à un moment donné) d'un service. Le service est considéré comme en panne lorsqu'il indique l'état du service en rouge, sinon il est considéré comme activé. La disponibilité est le moment où le service est signalé comme opérationnel. Admiral évalue l'intégrité du service signalée par état de service au fil du temps et déclenche une alerte si le pourcentage de disponibilité du service tombe sous un certain seuil. Cette évaluation sur une certaine durée garantit que nous réduisons les faux positifs et que nous alertons uniquement en cas de pannes de service réelles.

Comme les services ont des besoins en alertes différents, ce pourcentage et cet intervalle de temps sont fixés différemment pour chaque service.

Les clients peuvent utiliser les notifications Admiral pour être informés de ces événements. Elles sont également visibles sur la page **Investigate (Enquêter)** > **Alerts (Alertes)** , sous le type PLATFORM (PLATEFORME).

Note Seul un sous-ensemble de services choisi est associé à une alerte Admiral. Si un service ne fait pas partie du sous-ensemble ci-dessus, aucune alerte Admiral ne sera déclenchée lors de sa panne. Ce sous-ensemble de services avec alertes Admiral, leurs pourcentages de seuil d'alerte et leurs intervalles de temps est fixe et n'est pas configurable par l'utilisateur.

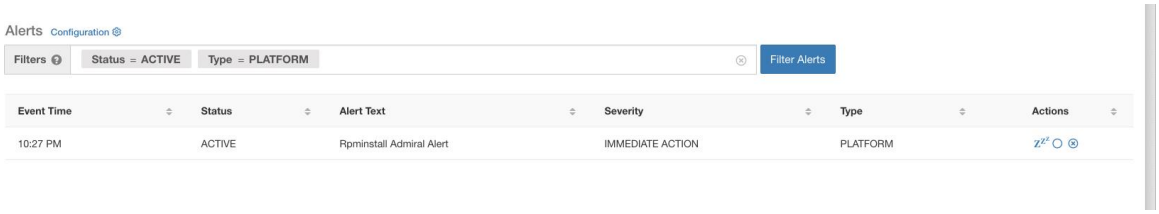
Les sections suivantes décrivent plus en détail les alertes et les notifications Admiral.

Cycle de vie d'une alerte Admiral

L'Admiral vérifie la disponibilité des services sur l'état des services. Il déclenche une alerte lorsque ce temps de disponibilité devient inférieur au seuil d'alerte préconfiguré.

Par exemple, Rpminstall est un service utilisé pour installer les RPM lors des déploiements, des mises à niveau, des correctifs, etc. Il est configuré pour générer une alerte Admiral si son temps de disponibilité est inférieur à 80 % sur une heure. Si le service Rpminstall tombe en panne pendant une durée supérieure au seuil précisé ci-dessus, une alerte Admiral est générée pour Rpminstall avec l'état ACTIVE.

Figure 2: Alerte Admiral active



Lorsque le service se rétablit, son pourcentage de disponibilité commence à augmenter. Lorsque la disponibilité dépasse son seuil, l'alerte se ferme automatiquement et son état passe à CLOSED (FERMÉE). Dans l'exemple Rpminstall décrit ci-dessus, RpminstallAdmiral Alert se ferme automatiquement lorsque son temps de disponibilité dépasse 80 % en une heure.

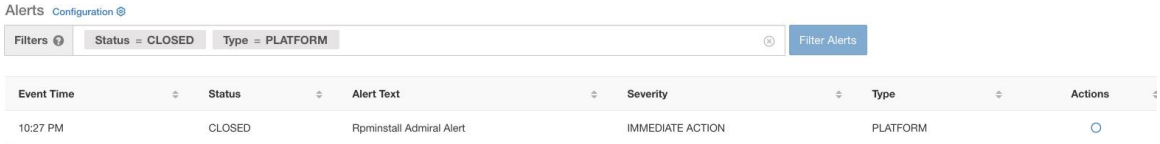
Note La fin de l'alerte est TOUJOURS décalée par rapport au retour à la normale du service. En effet, Admiral examine l'intégrité du service sur une période donnée. Dans l'exemple ci-dessus, puisque le seuil d'alerte Rpminstall est défini à 80 % d'une heure de disponibilité, il doit l'être depuis au moins 48 minutes (80 % d'une heure) avant que l'alerte ne se ferme.

Aucune action n'est requise pour fermer l'alerte. Ainsi, toutes les alertes Admiral ACTIVENT indiquent un problème sous-jacent nécessitant notre attention.

Note Aucune notification dédiée n'est générée à la fermeture des alertes.

Après qu'une alerte soit passée à FERMÉE, elle ne s'affichera plus sous les alertes ACTIVES. Les alertes fermées peuvent toujours être vues sur l'interface utilisateur en utilisant le filtre Status=CLOSED comme indiqué ci-dessous :

Figure 3: Fermeture automatique d'alerte Admiral à la reprise du service



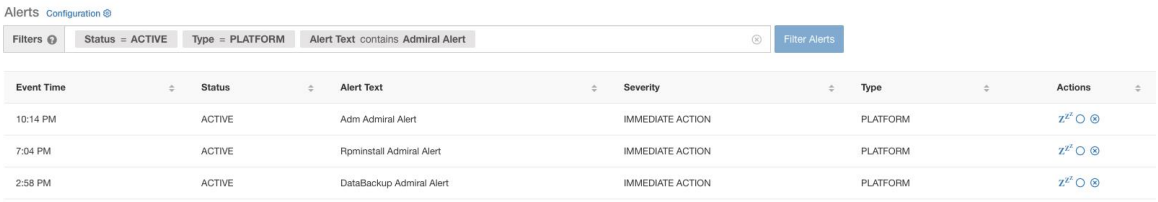
Il existe deux types d'alertes Admiral :

- Alerte Admiral individuelle
- Résumé des alertes Admiral

Alerte Admiral individuelle

Les alertes décrites dans la section précédente, les alertes qui sont déclenchées pour des services individuels, appartiennent à la catégorie d'alerte individuelle Admiral. Le texte de l'alerte contient toujours l <*Service Name*> de l'alerte Admiral. Cela facilite le filtrage des alertes individuelles par service ou par le suffixe **Admiral Alert**.

Figure 4: Filtre de texte d'alerte pour les alertes Admiral individuelles

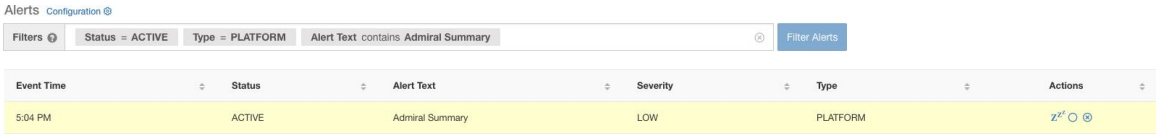


Résumé des alertes Admiral

Admiral génère des alertes résumées quotidiennement à minuit UTC. Elles contiennent une liste des alertes actuellement actives et de toutes les alertes fermées au cours de la dernière journée. Cela permet à l'utilisateur de voir l'intégrité globale de la grappe signalée par Admiral en un seul endroit. C'est également utile pour constater les alertes fermées qui ne génèrent pas de notification dédiée autrement. Si la grappe est intègre et qu'aucune alerte n'a été fermée au cours de la dernière journée, aucune notification récapitulative n'est générée pour ce jour-là. Cela sert à réduire les notifications et le bruit informationnel inutiles.

Le texte des alertes, dans ce cas, est toujours **« Admiral Summary** » . Cela facilite le filtrage des alertes résumées, comme le montre la figure suivante.

Figure 5: Filtre de texte de résumé Admiral



Détails de l'alerte

Alertes individuelles

Lorsque l'on clique sur l'alerte pour une alerte de type Admiral, celle-ci se déploie pour afficher des champs utiles au débogage et à l'analyse de l'alerte.

Figure 6: Détails de l'alerte

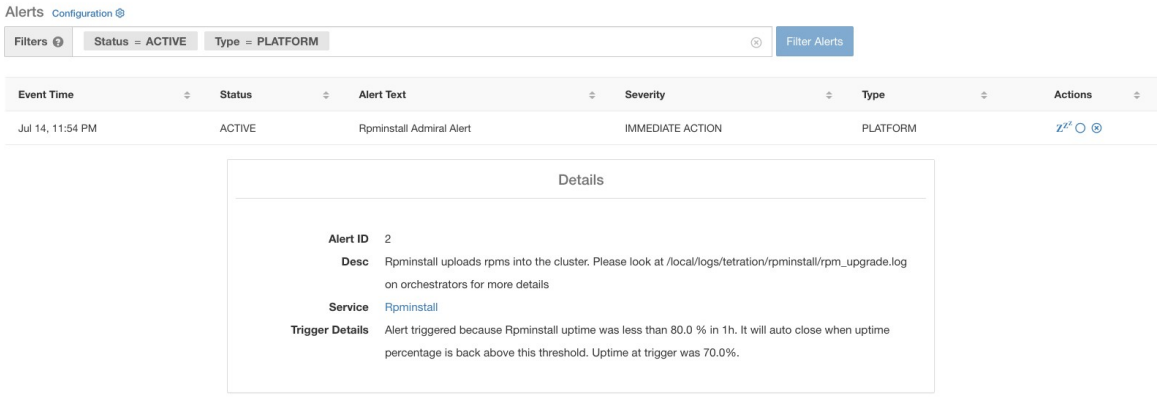


Table 1: Description des champs des détails de l'alerte

Champ	Description
ID d'alerte	Identifiant unique pour les alertes. Cela permet d'identifier un cas particulier de défaillance d'un service. Comme indiqué précédemment, lorsque le temps de fonctionnement sous-jacent du service signalé par l'alerte devient normal, l'alerte se ferme automatiquement. Si le même service tombe en panne ensuite, une nouvelle alerte avec un ID d'alerte différent est générée. L'identifiant de l'alerte permet donc d'identifier chaque cas de déclenchement de l'alerte.
Desc	Le champ de description contient des renseignements supplémentaires sur le problème de service à l'origine de l'alerte.
Service	Celui-ci contient un lien conduisant l'utilisateur à la page d'état du service où ce dernier peut être consulté. L'utilisateur peut également obtenir plus de détails sur les raisons pour lesquelles le service est signalé dans la page d'état du service.
Détails du déclencheur	Ceci contient les détails sur les seuils de déclenchement pour le service. Ces seuils permettent à l'utilisateur de savoir à quel moment l'alerte doit être clôturée après le rétablissement du service sous-jacent. Par exemple, le seuil RPMinstall est indiqué comme suit : 80 % de disponibilité sur une heure. Par conséquent, le service RPMinstall doit être actif depuis au moins 48 minutes (80 % d'une heure) avant que l'alerte ne se ferme automatiquement. Cela affiche également la valeur de disponibilité observée pour le service lorsque l'alerte a été déclenchée.

Voici un exemple de sortie de Kafka JSON :

```
  {
  "severity": "IMMEDIATE_ACTION",
  "tenant_id": 0,
  "alert_time": 1595630519423,
  "alert_text": "Rpminstall Admiral Alert",
  "key_id": "ADMIRAL_ALERT_5",
  "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
location_name='platform', location_grain='MIN',
root_scope_id='5efcfdf5497d4f474f1707c2'}/66eb975f5f987fe9eaefa81cee757c8b6dac5facc26554182d8112a98b35c4ab",

  "root_scope_id": "5efcfdf5497d4f474f1707c2",
  "type": "PLATFORM",
  "event_time": 1595630511858,
  "Check  /local/logs/tetration/rpminstall/rpm_upgrade.log on
orchestrators for more details\",\"Trigger Details\":\"Alert triggered because Rpminstall
uptime was less than 80.0 % in 1h. It will auto close when uptime percentage is back above
this threshold. Uptime at trigger was 65.0%. \"}"
  }
```

Toutes les alertes individuelles respectent le format JSON Kafka. Les services (à partir de l'état du service) qui sont couverts par la surveillance Admiral sont énumérés dans le tableau suivant :

Table 2: Services couverts par la surveillance Admiral

Service	Conditions de déclenchement	Gravité
Serveur API Kubernetes	La disponibilité du service est inférieure à 90 % au cours des 15 dernières minutes	ACTION IMMÉDIATE
Administrateur	La disponibilité du service est inférieure à 90 % au cours de la dernière heure.	ACTION IMMÉDIATE
Sauvegarde des données	La disponibilité du service est inférieure à 90 % au cours des 6 dernières heures.	ACTION IMMÉDIATE
Utilisation disque critique	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
Redémarrage requis	La disponibilité du service est inférieure à 90 % au cours de la dernière heure.	ACTION IMMÉDIATE
RPMinstall	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
SecondaryNN_checkpoint_status	La disponibilité du service est inférieure à 90 % au cours de la dernière heure.	ACTION IMMÉDIATE

Pour les grappes physiques de 8 ou 39 RU, les services suivants sont également surveillés :

Table 3: Services couverts par la surveillance Admiral pour les grappes de 8 ou 39 RU

Service	Conditions de déclenchement	Gravité
Échec DIMM	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
Échec de disque	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
Vitesse du ventilateur	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
Commutateurs en grappe	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE

Note La surveillance Admiral s'appuie sur les mesures de traitement générées par l'état du service pour générer des alertes. Si la récupération de la mesure n'est pas possible pendant une durée prolongée (par exemple, si l'état du service est en panne), une alerte (TSDBOracleConnectivity) est déclenchée pour indiquer que le traitement des alertes en fonction du service est désactivé sur la grappe.

Alertes résumées

Les alertes résumées sont de nature informationnelle et sont toujours définies comme de priorité FAIBLE. Lorsque l'on clique sur un résumé d'alerte Admiral, celui-ci se développe pour afficher divers champs contenant des informations résumées sur les alertes Admiral.

Figure 7: Détails de l'alerte résumée Admiral

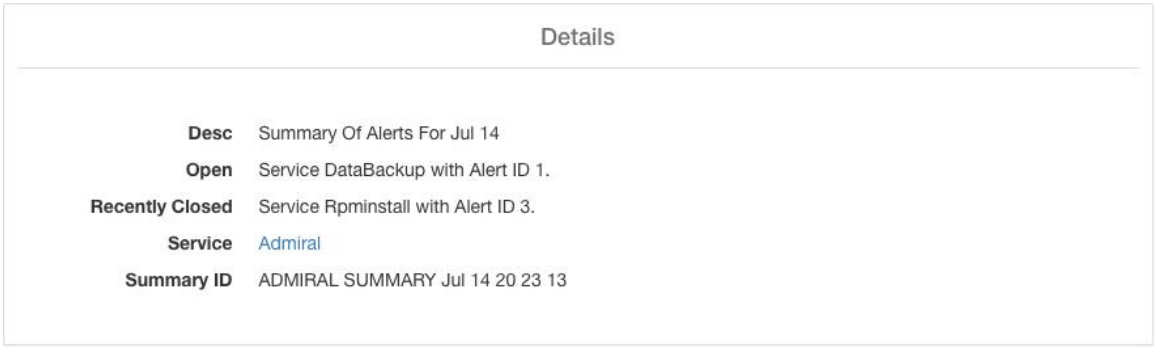


Table 4: Description des champs de l'alerte résumée Admiral

Champ	Description
Desc	Le champ de description contient le jour du résumé quotidien.

Champ	Description
Ouvert	Les alertes ouvertes indiquent quelles alertes étaient actives lorsque le résumé a été généré.
Fermées récemment	Ceci contient les alertes fermées au cours des dernières 24 heures, c'est-à-dire au cours de la journée pour laquelle le résumé a été généré. L'ID de chaque alerte est également inclus. Étant donné que les alertes se ferment automatiquement, un service donné a pu tomber en panne et créer une alerte, puis revenir à la normale et l'alerte se fermer automatiquement. Il aurait pu le faire plusieurs fois par jour, auquel cas la liste des incidents récemment clôturés comprendra chaque incident ainsi que son numéro d'alerte unique. Toutefois, cela ne devrait pas se produire souvent étant donné que chaque service doit être opérationnel pendant un certain temps avant que l'alerte ne soit clôturée. L'utilisateur peut filtrer avec Status = CLOSED pour obtenir plus d'informations sur chaque incident.
Service	Lien vers l'état du service pour Admiral, qui est le service qui traite et génère le résumé quotidien.
ID du résumé	ID de l'alerte résumée.

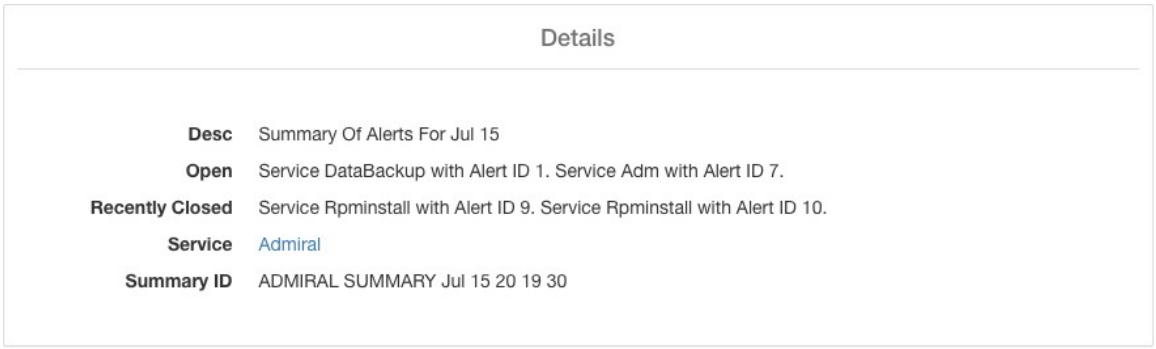
Voici un exemple de sortie de Kafka JSON :


```
  {
    "severity": "LOW",
    "tenant_id": 0,
    "alert_time": 1595721914808,
    "alert_text": "Admiral Summary",
    "key_id": "ADMIRAL_SUMMARY_Jul-26-20-00-04",
    "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
location_name='platform', location_grain='MIN',
root_scope_id='5efcfdf5497d4f474f1707c2'}/e95da4521012a4789048f72a791fb58ab233bbff63e6cbc421525d4272d469aa",

    "root_scope_id": "5efcfdf5497d4f474f1707c2",
    "type": "PLATFORM",
    "event_time": 1595721856303,
    "alert_details": "{\"Desc\":\"Summary of alerts for Jul-26\",\"Recently
Closed\":\"None\",\"Open\":\" Service Rpminstall with Alert ID
5.\",\"Service\":\"Admiral\",\"Summary ID\":\"ADMIRAL_SUMMARY_Jul-26-20-00-04\"}"
  }
```


Un exemple d'alerte résumée dans laquelle un service déclenche plusieurs alertes dans une journée est présenté ci-dessous :

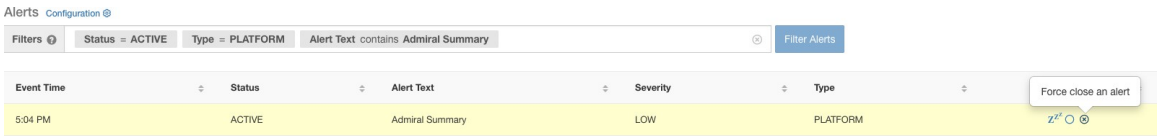
Figure 8: Alertes multiples



Actions des utilisateurs

Puisque les alertes Admiral ne génèrent qu'une seule notification par alerte, l'inclusion, l'exclusion ou la répétition d'alertes précises ne sont pas nécessaires. Les alertes se ferment automatiquement lorsque le service redevient normal pour le seuil de disponibilité, comme décrit ci-dessus. Il existe la possibilité de forcer la fermeture d'une alerte. Normalement, cela ne doit être utilisé que pour supprimer les récapitulatifs des alertes de l'interface utilisateur, car les alertes individuelles se ferment automatiquement.

Figure 9: Forcer la fermeture des alertes

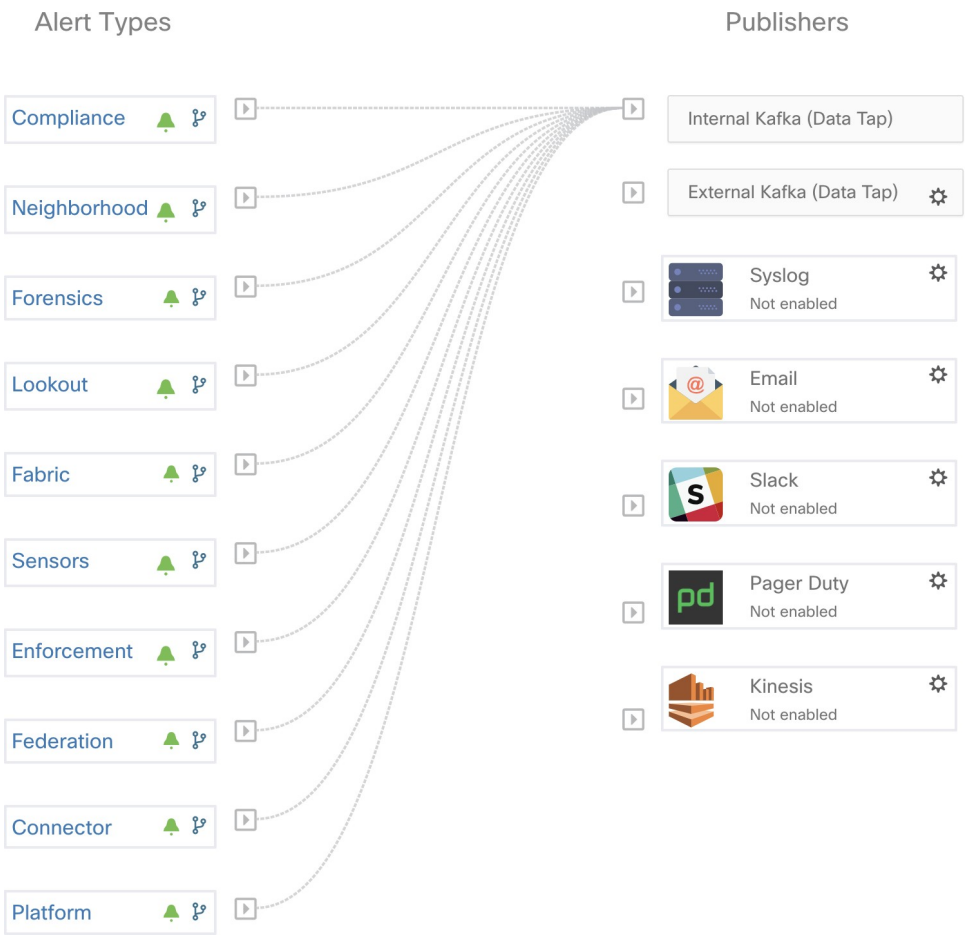


Warning Les alertes individuelles ne doivent pas être fermées de force. Si vous le faites alors que le service sous-jacent est toujours en panne ou que son temps de fonctionnement est inférieur au seuil prévu, une autre alerte sera déclenchée pour le même service lors de la prochaine itération du traitement Admiral.

Notifications Admiral

Les alertes Admiral sont de type PLATFORM. De ce fait, ces alertes peuvent être configurées pour être envoyées à divers annonceurs par les connexions appropriées pour les alertes de plateforme à l'aide de la page de configuration ./configuration. Pour plus de commodité, la connexion est activée entre les alertes de la plateforme et le Kafka interne par défaut, ce qui permet d'afficher les alertes Admiral sur la page Alertes actuelles (aller à **Investigate (Investiguer)** > **Alerts (Alertes)**) sans aucune configuration manuelle.

Figure 10: Configuration des alertes de la plateforme



Les alertes Admiral sont également envoyées à l'adresse courriel configurée sous **Platform (Plateforme)** > **Cluster Configuration (Configuration de la grappe)** > **Admiral Alert Email (Courriel de l'alerte Admiral)**.

Figure 11: Exemple de courriel Admiral

There is a new admiral platform alert on your tetration cluster.
Service: Rpminstall
Start Time: 2020-07-14 23:09 UTC
Alert ID: 3
Description: Rpminstall uploads rpms into the cluster. Please look at /local/logs/tetration/rpminstall/rpm_upgrade.log for more details

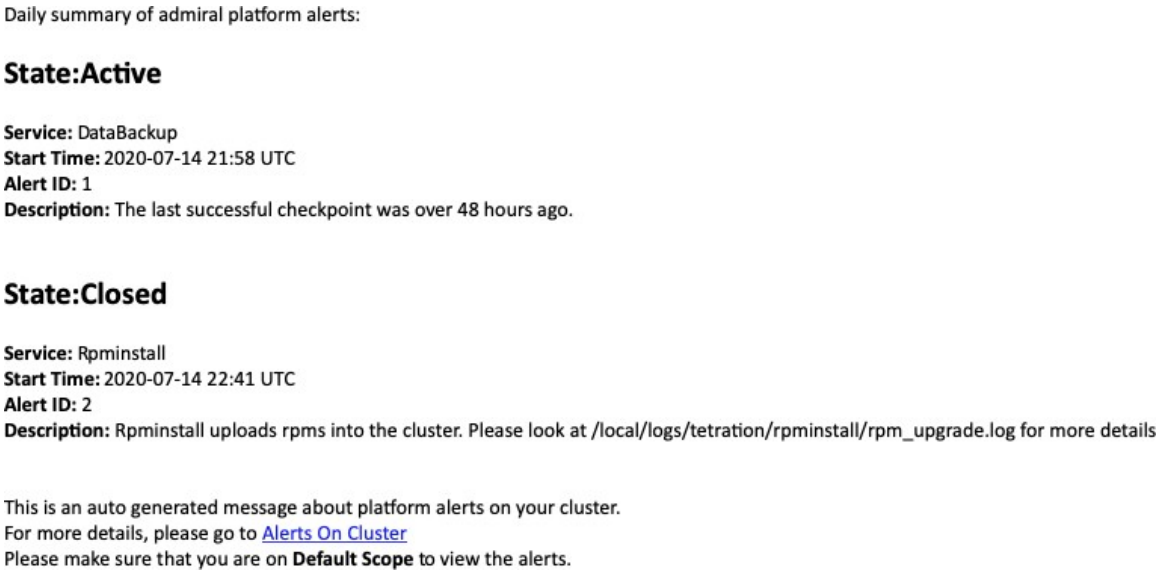
This is an auto generated message about platform alerts on your cluster.
For more details, please go to Alerts On Cluster
Please make sure that you are on **Default Scope** to view the alerts.

Ainsi, les utilisateurs peuvent recevoir des notifications Admiral même s'ils n'ont pas configuré l'appareil TAN Edge. Ce comportement est similaire au comportement du Bosun (maître d'exploitation) dans les versions précédentes.

Figure 12: Adresse courriel de Admiral

Ces notifications par courriel sont générées sur les mêmes déclencheurs que la page Current Alerts (Alertes actuelles). Ainsi, elles sont envoyées lors de la création de l'alerte et lors d'un courriel récapitulatif quotidien à minuit UTC. Le courriel récapitulatif quotidien répertorie toutes les alertes actives et celles fermées au cours des dernières 24 heures.

Figure 13: Exemple de courriel récapitulatif Admiral



Daily summary of admiral platform alerts:

State:Active

Service: DataBackup
Start Time: 2020-07-14 21:58 UTC
Alert ID: 1
Description: The last successful checkpoint was over 48 hours ago.

State:Closed

Service: Rpminstall
Start Time: 2020-07-14 22:41 UTC
Alert ID: 2
Description: Rpminstall uploads rpms into the cluster. Please look at /local/logs/tetration/rpminstall/rpm_upgrade.log for more details

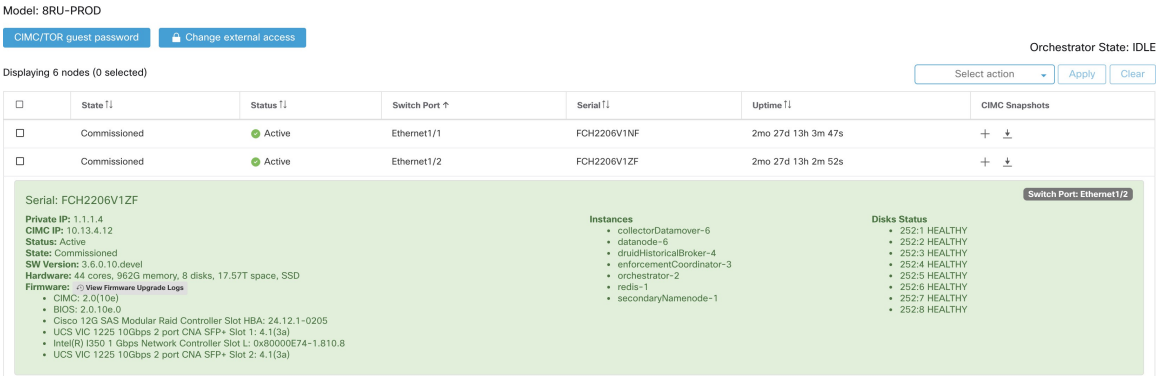
This is an auto generated message about platform alerts on your cluster.
For more details, please go to Alerts On Cluster
Please make sure that you are on **Default Scope** to view the alerts.

S'il n'y a aucune alerte active, ni aucune alerte fermée au cours des dernières 24 heures, les courriels récapitulatifs sont ignorés pour réduire le bruit des courriels.

État de la grappe

La page d' **état de la grappe**, sous le menu **dépannage** dans la barre de navigation de gauche, est accessible aux **administrateurs du site**, mais les actions ne peuvent être effectuées que par les utilisateurs du **service d'assistance à la clientèle**. Il affiche l'état de tous les serveurs physiques du support Cisco Cisco Secure Workload. Chaque ligne du tableau représente un nœud physique avec des détails tels que la configuration de son matériel et de son micrologiciel et l'adresse IP de son contrôleur CIMC (si attribuée). Vous pouvez afficher la vue détaillée du nœud en cliquant sur la ligne . Dans cette page, nous pouvons également modifier le mot de passe CIMC des nœuds et activer ou désactiver l'accès externe. L'état de l'orchestrateur est également affiché sur la page d'état de la grappe pour fournir un contexte au service d'assistance à la clientèle.

Figure 14: État de la grappe



Actions qui affectent tous les nœuds

La modification du mot de passe du contrôleur CIMC et l'activation ou la désactivation de l'accès du contrôleur CIMC externe peuvent être effectuées à l'aide des options **CIMC/TOR guest password** (Mot de passe invité CIMC/TOR) et **Change external access** (modifier l'accès externe). Les actions affectent tous les nœuds de la grappe.

Détails du nœud d'accès du contrôleur CIMC externe

Cliquez sur **Modifier l'accès externe** pour ouvrir une boîte de dialogue qui fournit l'état de l'accès du contrôleur CIMC externe et permet d'activer, de renouveler ou de désactiver l'accès externe à CIMC.

Cliquez sur **Enable** (activer) pour configurer la grappe en arrière-plan pour activer l'accès CIMC externe. Cela peut prendre jusqu'à 60 secondes pour que les tâches soient terminées et que l'accès CIMC externe soit entièrement activé. Lorsque l'accès CIMC externe est activé, une boîte de dialogue s'affiche lorsque l'accès est défini pour expirer automatiquement et **Enable** (activer) passe à **Renew** (Renouveler) pour indiquer que vous pouvez renouveler l'accès CIMC externe. Le renouvellement de l'accès au contrôleur CIMC externe augmente l'heure d'expiration de deux heures par rapport à l'heure actuelle.

Si l'accès CIMC externe est activé, l'adresse IP du contrôleur CIMC dans les détails du nœud (visible en cliquant sur la ligne d'un nœud) devient un lien sur lequel vous pouvez accéder directement à l'interface utilisateur du contrôleur CIMC. Vous devrez peut-être recharger la page d'état de la grappe pour afficher les liens.

Figure 15: Détails du nœud d'accès du contrôleur CIMC externe

L'interface utilisateur du contrôleur CIMC comporte généralement un certificat autosigné. L'accès à l'interface utilisateur du contrôleur CIMC entraînera probablement une erreur dans le navigateur indiquant que le certificat n'est pas valide. Si vous utilisez Google Chrome, vous devrez peut-être taper **`thisisunsafe`** sans guillemets lorsque l'erreur de certificat non valide s'affiche pour contourner la vérification de certificat et accéder à l'interface utilisateur du contrôleur CIMC.

Dans l'interface utilisateur du contrôleur CIMC, l'accès KVM n'est fonctionnel que si la version du contrôleur CIMC est 4.1(1g) ou ultérieure. Une fois l'accès CIMC externe activé, il est automatiquement désactivé au bout de deux heures, sauf si l'accès est renouvelé ou désactivé.

La désactivation de l'accès CIMC externe configure la grappe en arrière-plan pour désactiver l'accès CIMC externe. Cela peut prendre jusqu'à 60 secondes pour que la tâche se termine et que l'accès CIMC externe soit complètement désactivé.

Table 5: Détails du nœud physique

Champ	Description
État	Le champ **Status** (État) indique l'état de l'alimentation du nœud. Les valeurs possibles sont les suivantes : • **Actif** : le nœud est sous tension. • **Inactif** : le nœud n'est pas sous tension ou connecté.
Province	Le champ **State** (État) indique l'état d'appartenance à la grappe du nœud. Les valeurs possibles sont les suivantes : • **Nouveau** : le nœud ne fait pas encore partie de la grappe. • **Initialisé** : le nœud fait partie de la grappe. Cependant, Cisco Secure Workload n'est pas déployé sur le nœud. • **Mis en service** : le nœud est opérationnel et fonctionne sur Cisco Secure Workload. Le champ de version logicielle est également indiqué et devient rouge si un nœud individuel n'a pas la même version que celle de l'ensemble de la grappe. • **Désactivé** : le nœud a été supprimé de la grappe à des fins de dépannage. Le nœud doit être remplacé par du nouveau matériel. Un nœud peut être désactivé à l'aide de l'action de mise hors-service (voir les actions suivantes).
Port de commutation	Désigne le port de commutateur des deux commutateurs sur lesquels le nœud physique est connecté.
Disponibilité	Indique la durée pendant laquelle le nœud a fonctionné sans redémarrage ni arrêt.

Champ	Description
Instantanés du contrôleur CIMC	Peuvent être utilisés pour lancer une collecte d'assistance technique du contrôleur CIMC et télécharger un fichier d'assistance technique du contrôleur CIMC.

Table 6: Actions correctives de la grappe

Action	Description
Mise en service	Sélectionnez cette action pour intégrer de nouveaux nœuds dans la grappe. Seuls les nœuds avec l'état Nouveau peuvent être sélectionnés pour cette action.
Mise hors service	Sélectionnez cette action pour supprimer les nœuds qui font partie de la grappe. Seuls les nœuds avec l'état **Mise en service** ou **Initialisé** peuvent être sélectionnés pour cette action.
Recréation d'image	Sélectionner cette action pour redéployer Cisco Secure Workload. Cela peut effacer toutes les données de la grappe et est particulièrement utile pour la mise à niveau d'une machine sans système d'exploitation à partir d'une version antérieure vers une nouvelle. Cette étape est requise lors de la désactivation d'une machine sans système d'exploitation.
Mise à niveau du micrologiciel	Les informations sur le micrologiciel sont disponibles pour les nœuds pour lesquels l'adresse IP du contrôleur CIMC est accessible. Cette action est utile pour mettre à niveau le micrologiciel sur les nœuds avec des versions plus anciennes.
Mettre hors tension	Sélectionnez cette action pour mettre les nœuds hors tension. **Note** Vous ne pouvez pas mettre hors tension les nœuds avec l'état **Inactive** (Inactif) et **Shutdown in progress** (Arrêt en cours).

Détails des mises à niveau du micrologiciel

La grappe Cisco Secure Workload sur site regroupe un système informatique unifié (UCS) Cisco Integrated Management Controller (CIMC) Host Upgrade Utility (HUU) ISO. L'option de mise à niveau du micrologiciel sur la page d'état de la grappe peut être utilisée pour mettre à jour une version physique sans système d'exploitation vers la version du micrologiciel UCS incluse dans l'image HUU ISO qui a été groupée dans les RPM Cisco Secure Workload.

La mise à jour du micrologiciel peut commencer sur un hôte sans système d'exploitation lorsque l'état est *actif* ou *inactif* , tant que l'état sans système d'exploitation n'est pas *initialisé* ou *Incompatibilité UGS*. Un

seul micrologiciel UCS à la fois peut voir son micrologiciel UCS mis à jour. Pour démarrer la mise à jour du micrologiciel, l'état Cisco Secure Workload de l'orchestrateur doit être *Idle* (inactif). Lorsque la mise à jour du micrologiciel UCS est lancée, certaines des fonctionnalités de l'interface utilisateur spécifiques à la page d'état de la grappe peuvent être temporairement touchées si le consul leader, l'orchestration ou le gestionnaire actif du micrologiciel (fwmgr) doit être commuté vers d'autres hôtes - ces basculements devraient se produire automatiquement . Pendant la mise à jour du micrologiciel, les détails du micrologiciel du système sans système d'exploitation mis à jour ne s'afficheront pas. Après la mise à jour, cela peut prendre jusqu'à 15 minutes avant que les détails du micrologiciel ne s'affichent à nouveau dans la page Cluster Status (État de la grappe). Avant de commencer la mise à jour du micrologiciel, consultez la page Service Status (État des services) pour vérifier que tous les services sont intègres.

Lorsque vous lancez une mise à jour de micrologiciel sur un système sans système d'exploitation, fwmgr vérifie que la mise à jour peut se poursuivre, met hors tension normalement le système sans système d'exploitation si nécessaire, puis se connecte au contrôleur CIMC sur l'environnement sans système d'exploitation et démarre la mise à jour du micrologiciel basée sur HUU. Ce processus de mise à jour du micrologiciel basé sur HUU implique de démarrer le matériel sans système d'exploitation dans HUU ISO, d'effectuer la mise à jour, de redémarrer le contrôleur CIMC pour activer le nouveau micrologiciel, puis de redémarrer la machine sans système d'exploitation dans HUU ISO pour vérifier que la mise à jour a été effectuée. Le processus global de mise à jour peut prendre plus de 2 heures pour un G1 sans système d'exploitation ou plus d'une heure pour un G2 sans système d'exploitation. Lorsque le processus de mise à jour du micrologiciel est lancé, la page Service Status (État du service) peut indiquer que certains services ne sont pas intègres, car les systèmes sans système d'exploitation et toutes les machines virtuelles fonctionnant sur ces services sans système d'exploitation ne sont plus actifs dans la grappe. Lorsque la mise à jour du micrologiciel est terminée, cela peut prendre 30 minutes de plus pour que le système sans système d'exploitation redevienne actif dans la grappe, et il faudra peut-être plus de temps pour que tous les services soient de nouveau intègres. Si les services ne récupèrent pas dans les deux heures suivant une mise à jour du micrologiciel, contactez un représentant du service d'assistance à la clientèle.

Vous pouvez cliquer sur un nœud sans système d'exploitation dans la page Cluster Status (État de la grappe) pour développer les détails de ce nœud. Lorsqu'une mise à jour du micrologiciel est lancée, vous pouvez cliquer sur le bouton *View Firmware Upgrade Logs* (Afficher les journaux de mise à niveau du micrologiciel) pour afficher l'état de la mise à jour du micrologiciel. Le journal contient l'état général de la mise à jour du micrologiciel. L'état peut être :

- **La mise à jour du micrologiciel a été déclenchée** : la mise à jour du micrologiciel a été demandée, mais n'a pas encore commencé. Pendant cet état, fwmgr vérifiera que les services requis pour la mise à jour du micrologiciel sont fonctionnels et que le CIMC peut accéder à ces services.
- **La mise à jour du micrologiciel est en cours d'exécution** : la mise à jour du micrologiciel a été lancée. Lorsqu'une mise à jour de micrologiciel atteint cet état, le contrôleur CIMC et HUU contrôlent la mise à jour, et la grappe Cisco Secure Workload signale l'état que lui fournit CIMC au sujet de la mise à jour.
- **La mise à jour du micrologiciel a expiré** : cela indique qu'un processus de mise à jour du micrologiciel a dépassé le délai attendu. Le processus global de mise à jour du micrologiciel a une limite de 240 minutes lorsqu'il entre dans la phase *de mise à jour du micrologiciel en cours* . Pendant la mise à jour du micrologiciel, CIMC peut devenir inaccessible lors du redémarrage avec la nouvelle version, cet état inaccessible a un délai de 40 minutes avant que la mise à jour du micrologiciel ne soit déclarée expirée. Lorsque la mise à jour du micrologiciel a commencé, la surveillance de cette mise à jour expire après 120 minutes.
- **La mise à jour du micrologiciel a échoué avec une erreur** : ceci indique qu'une erreur est survenue et que la mise à jour du micrologiciel a échoué. Le contrôleur CIMC ne donne généralement pas d'indication de réussite ou d'échec, donc cet état indique généralement qu'une erreur s'est produite avant que la mise à jour du micrologiciel ne soit en cours d'exécution.

- **Fin de la mise à jour du micrologiciel** : la mise à jour du micrologiciel s'est terminée sans erreur ni délai d'expiration. Le contrôleur CIMC ne donne généralement pas d'indication de réussite ou d'échec, il est préférable de vérifier que les versions du micrologiciel UCS sont mises à jour lorsque ces détails deviennent disponibles dans la page Cluster Status (État de la grappe) - cela peut prendre jusqu'à 15 minutes pour que ces détails soient disponibles.

Sous l'état général dans la fenêtre contextuelle *View Firmware Upgrade Logs* (afficher les journaux de mise à niveau du micrologiciel) se trouve une section de *progression de la mise à jour* qui contiendra des messages de journal horodatés indiquant la progression de la mise à jour du micrologiciel. Lorsque l'état de *redémarrage de l'hôte en cours* est affiché dans ces messages de journal, CIMC contrôle la mise à jour et la grappe la surveille. La plupart des messages de journal suivants proviennent directement du CIMC et ne sont ajoutés à la liste des messages de journal que si l'état de la mise à jour change.

Sous la section de *progression de la mise à jour* de la fenêtre contextuelle *View Firmware Upgrade Logs* (Afficher les journaux de mise à jour du micrologiciel), une section *Component update status* (État de mise à jour des composants) s'affichera lorsque CIMC commencera à fournir des états de mise à jour de composant individuel. Cette section résume l'état de la mise à jour des divers composants UCS sur le système sans système d'exploitation.

Sauvegarde et restauration des données

La sauvegarde et la restauration des données sont un mécanisme de reprise après sinistre qui copie les données de la grappe Cisco Secure Workload, des connecteurs et des orchestrateurs externes vers un stockage hors site. En cas de sinistre, les données sont restaurées à partir du stockage hors site vers une grappe de même type de taille. Vous pouvez également basculer entre différents sites de sauvegarde.

- La sauvegarde et la restauration des données sont prises en charge pour les grappes physiques de 8 et 39 RU.
- Les données peuvent être sauvegardées dans n'importe quel stockage d'objets externe compatible avec l'API S3V4.
- Cisco Secure Workload nécessite une bande passante et un stockage suffisants pour sauvegarder les données. Des vitesses de réseau lentes et une latence élevée peuvent faire échouer les sauvegardes.
- Les limites de stockage des données sont basées sur le type de sauvegarde sélectionné.
  - Pour la sauvegarde de données en mode continu, nous vous recommandons de stocker 200 To pour les sauvegardes complètes, y compris les données de flux. Pour déterminer l'espace de stockage réel requis, utilisez l'option du **planificateur de capacité** disponible sur la page de sauvegarde des données. Pour en savoir plus, consultez Utiliser le Planificateur de capacité, on page 22. Le manque d'espace de stockage pour de multiples sauvegardes entraîne la suppression fréquente d'anciennes sauvegardes afin de pouvoir gérer les sauvegardes dans la limite de l'espace de stockage. Il doit y avoir suffisamment de stockage pour au moins une sauvegarde.
  - Pour la sauvegarde des données en mode continu, le stockage minimal requis est de 50 To pour les sauvegardes complètes, y compris les données de flux. Pour déterminer l'espace de stockage réel requis, utilisez l'option du **planificateur de capacité** disponible sur la page de sauvegarde des données. Pour en savoir plus, consultez Utiliser le Planificateur de capacité, on page 22. Le manque d'espace de stockage pour de multiples sauvegardes entraîne la suppression fréquente d'anciennes sauvegardes afin de pouvoir gérer les sauvegardes dans la limite de l'espace de stockage. Il doit y avoir suffisamment de stockage pour au moins une sauvegarde.

  - Pour les sauvegardes en mode allégé, 1 To de stockage est suffisant, car les données de flux, qui constituent la majeure partie des données de sauvegarde, ne sont pas incluses dans la sauvegarde.

- Les données peuvent uniquement être restaurées dans une grappe de taille compatible, exécutant la même version que la grappe principale. Par exemple, vous pouvez restaurer les données d'une grappe de 8 RU uniquement vers une autre de 8 RU.

Sauvegarde des données

Un calendrier pour la sauvegarde des données peut être configuré à l'aide de la section Sauvegarde des données de l'interface utilisateur. Les sauvegardes sont déclenchées une fois par jour et à l'heure programmée en fonction des paramètres configurés ou peuvent être configurées pour s'exécuter en continu. Une sauvegarde réussie s'appelle un *point de contrôle*. Un point de contrôle est un instantané à un point dans le temps des magasins de données principaux de la grappe.

Un point de contrôle réussi peut être utilisé pour restaurer les données sur une autre grappe ou au sein de la même grappe.

Les données de configuration de la grappe sont toujours sauvegardées pour chaque point de contrôle. Le flux et d'autres données constituent la majeure partie des données sauvegardées. Par conséquent, si elles sont configurées correctement, seules les modifications incrémentielles sont sauvegardées. Les sauvegardes incrémentielles permettent de réduire la quantité de données transférées vers le stockage externe, ce qui évite de surcharger le réseau. Si vous le souhaitez, une sauvegarde complète peut être déclenchée selon une planification convenue pour toutes les sources de données lorsque la sauvegarde incrémentielle est configurée. Une sauvegarde complète copie chaque objet d'un point de contrôle, même s'il est déjà copié et que l'objet n'a pas été modifié. Cela peut ajouter une charge importante sur la grappe, sur le réseau entre la grappe et la bibliothèque d'objets, et sur la bibliothèque d'objets elle-même. Une sauvegarde complète peut s'avérer nécessaire en cas de détérioration des objets ou de défaillance matérielle irrémédiable de la bibliothèque d'objets. En outre, si le compartiment fourni pour la sauvegarde change, une sauvegarde complète est automatiquement appliquée, car une sauvegarde complète est nécessaire pour que les sauvegardes incrémentielles soient utiles.

Table 7: Données de grappe sauvegardées dans différents modes

Données de grappe Cisco Secure Workload	Les données sont-elles sauvegardées en mode de sauvegarde complète?	Les données sont-elles sauvegardées en mode allégé?
Configurations de grappe	**Oui**	**Oui**
RPM utilisés pour la création d'image de la grappe	**Oui**	**Oui**
Images de déploiement d'agents logiciels	**Oui**	**Oui**
Base de données de flux	**Oui**	Non
Données requises pour la découverte automatique des politiques	**Oui**	Non

Données de grappe Cisco Secure Workload	Les données sont-elles sauvegardées en mode de sauvegarde complète?	Les données sont-elles sauvegardées en mode allégé?
Données pour faciliter la criminalistique, comme les condensés de fichiers et les modèles de fuites de données.	**Oui**	Non
Données pour faciliter l'analyse de la surface d'attaque	**Oui**	Non
Bases de données CVE.	**Oui**	Non

Note

- Les informations du connecteur sécurisé ne sont pas sauvegardées ou restaurées dans la version sur site de Cisco Secure Workload, mais sont sauvegardées et restaurées dans la version logiciel-service (SaaS) de Cisco Secure Workload.
- Les informations sur les correctifs virtuels des connecteurs FMC ne sont pas restaurées après la restauration des données sauvegardées.

Pre-Requisites for Data Backup

- To obtain an activation key for the Data Backup and Restore (DBR) feature, send an email to taentitlement@cisco.com requesting a DBR activation key and also attach the cluster ID file in the email.

Note The license entitlement is only required for the primary (active) cluster and not by the standby cluster.

- The access and secret keys for the object store are required. The Data backup and restore option does not work with pre-authenticated link for object store.
- Configure any policing to throttle the bandwidth used by the Secure Workload appliance to object store. Note that policing with low bandwidth when volume of data to be backed up is high can cause backup failures.
- Configure the cluster's FQDNs and ensure that software agents can resolve the FQDNs.

Note After you enable data backup and restore, only the current and later software agent versions are available for installation and upgrades. Earlier versions than the current cluster version remain hidden due to incompatibility.

Software agent or Kafka FQDNs Requirements

Software agents use an IP address to get control information from Secure Workload appliance. To enable data backup and restore and allow for seamless failover after a disaster, agents must switch to using FQDN.

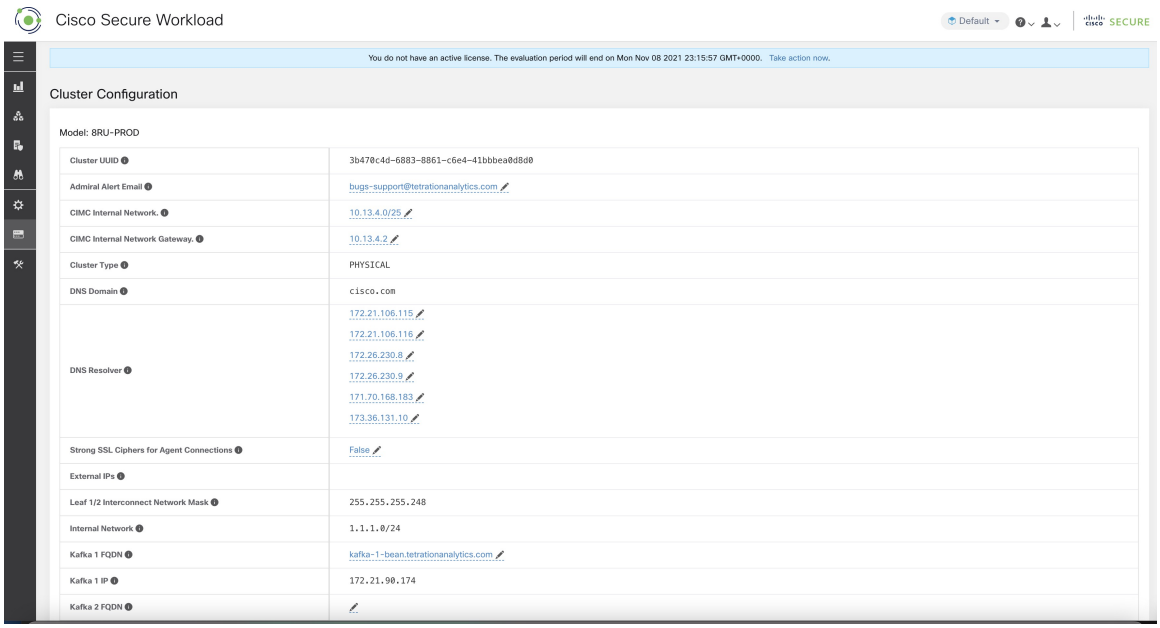
Upgrading Secure Workload cluster is not sufficient for this switch. Software agents support the use of FQDN starting Secure Workload version 3.3 and later. Therefore, to enable agent failover and to ensure that agents are ready for data backup and restore, upgrade the agents to version 3.3 or later.

If FQDNs are not configured, the default FQDNs are:

IP Type	Default FQDN
Sensor VIP	wss{{cluster_ui_fqdn}}
Kafka 1	kafka-1-{{cluster_ui_fqdn}}
Kafka 2	kafka-2-{{cluster_ui_fqdn}}
Kafka 3	kafka-3-{{cluster_ui_fqdn}}

The FQDNs can be changed on the **Platform** > **Cluster Configuration** page.

Figure 16: FQDNs or IP for Data Backup and Restore on Cluster Configuration page



Update the DNS record for the FQDNs with the IPs provided in the same page. The following table lists the mapping of IPs and FQDNs.

Field Name	Corresponding IP Field	Description
Sensor VIP FQDN	Sensor VIP	Update the FQDN to connect to cluster control plane
Kafka 1 FQDN	Kafka 1 IP	Kafka node 1 IP
Kafka 2 FQDN	Kafka 2 IP	Kafka node 2 IP
Kafka 3 FQDN	Kafka 3 IP	Kafka node 3 IP

Note FQDN for sensors VIP and Kafka hosts can only be changed before data backup and restore is configured. After the configuration, FQDN cannot be changed.

Exigences du magasin d'objets

La boutique d'objets doit fournir une interface de plainte S3V4.

Note Quelques stockages d'objets conformes à S3V4 ne prennent pas en charge la fonctionnalité DeleteObjects (SupprimerObjets). La fonctionnalité DeleteObjects est requise pour supprimer les informations de point de contrôle obsolètes. L'absence de cette fonctionnalité peut entraîner des échecs lors de la tentative de suppression des points de contrôle obsolètes du stockage et peut entraîner un manque d'espace du stockage.

- **Site**

  L'emplacement du magasin d'objets est essentiel pour la latence liée à la sauvegarde et à la restauration du magasin. Pour améliorer le temps de restauration, vérifiez que le magasin d'objets est situé plus près de la grappe de secours.

- **Compartiment**

  Créez un nouveau compartiment dédié à Cisco Secure Workload dans le magasin d'objets. Seule la grappe doit avoir un accès en *écriture* à ce compartiment. La grappe écrira les objets et gérera la rétention sur le compartiment. Mettez en service au moins 200 To de stockage pour le compartiment et obtenez un accès et une clé secrète pour ce dernier. La sauvegarde et la restauration des données dans Cisco Secure Workload ne fonctionnent pas avec les liens pré-authentifiés.

Note Si vous utilisez Cohesity comme magasin d'objets, désactivez les chargements en plusieurs parties lors de la planification.

- **HTTPS**

  L'option de sauvegarde de données prend uniquement en charge l'interface HTTPS avec le magasin d'objets. Cela permet de s'assurer que les données en transit vers ce dernier sont chiffrées et sécurisées. Si le certificat de stockage SSL/TSL est signé par une autorité de certification tierce de confiance, la grappe l'utilisera pour authentifier le magasin d'objets. Si le magasin d'objets utilise un certificat autosigné, la clé publique ou l'autorité de certification peut être téléversée en sélectionnant l'option **Use Server CA Certificate** (Utiliser le certificat de l'autorité de certification du serveur).

- **Chiffrement côté serveur**

  Il est fortement recommandé d'activer le chiffrement côté serveur pour le compartiment affecté à la grappe de Cisco Secure Workload. La grappe utilisera HTTPS pour transférer les données vers le magasin d'objets. Cependant, le magasin d'objets doit chiffrer les objets pour s'assurer que les données stockées sont sécurisées.

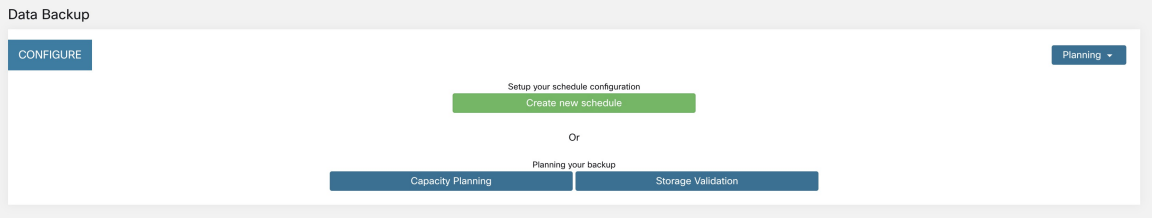
Configuration of Data Backup

To configure data backup in Secure Workload, perform the following:

1. **Planning**—The data backup option provides a planner to test the access to the object store, determine the storage requirement, and the backup duration needed for each day. This can be used to experiment before configuring a schedule.

   To use data backup and restore calculators, navigate to **Platform** > **Data Backup**. If data backup and restore is not configured, this will navigate to the Data Backup landing page.

   Figure 17: Backup Landing Page

   - Utiliser le Planificateur de stockage, on page 21
   - Utiliser le Planificateur de capacité, on page 22

Note If you are unable to view the Data Backup option under Platform, ensure that you have the license to enable data backup and restore.

2. **Configuring and scheduling data backup**—Secure Workload will copy data to object store only in the configured time-window. While configuring backup for the first time, the pre-checks will run to ensure the FQDNs are resolvable and resolves to the right IP. After the initial validation, an update is pushed to registered software agents to switch to using FQDNs. Without FQDN, the agents cannot failover to another cluster after a disaster event. To support this, agents must be upgraded to the latest version supported by the cluster and all the agents should be able to resolve the sensor VIP FQDN. As of Secure Workload release 3.3 and later, only deep visibility and enforcement agents support data backup and restore and will switch to using FQDN.

   To create a schedule and configure data backup, see Configurer la sauvegarde des données, on page 23.

Utiliser le Planificateur de stockage

Procedure

Étape 1 Pour vous assurer que le stockage est compatible avec Cisco Secure Workload, effectuez l'une des actions suivantes :

- Dans la page de destination de la **sauvegarde des données**, cliquez sur **Storage Planning**(planification du stockage).
- Dans le menu déroulant **Planning** (Planification), choisissez **Storage**(stockage).

La page **Storage Planning** (planification du stockage) s'affiche.

Étape 2 Saisissez les informations suivantes :

- Un nom pour le stockage.
- URL d'un point terminal de stockage conforme à S3.

  Note L'adresse IPv6 d'un stockage conforme S3 doit être une URL ou un nom de domaine complet, et pas seulement une adresse IPv6.

- Un nom de compartiment conforme à S3 configuré sur le stockage
- (Facultatif pour certains types de stockage) Région du stockage conforme à S3.
- Clé d'accès au stockage.
- Clé secrète du stockage.

Étape 3 (Facultatif) Si nécessaire, vous pouvez activer le serveur mandataire HTTP.

Étape 4 (Facultatif) Pour utiliser des chargements en plusieurs parties des données sauvegardées, activez **Use Multipart Upload**(utiliser le chargement en plusieurs parties) .

Étape 5 (Facultatif) Si un certificat de l'autorité de certification est requis pour authentifier le serveur de stockage, activez l'option **Use Server CA Certificate** (utiliser le certificat de l'autorité de certification du serveur) et saisissez les détails du certificat.

Étape 6 Cliquez sur **Test**.

La validation du stockage permet de tester :

- L'authentification et l'accès au magasin d'objets et au compartiment.
- Le téléchargement vers et depuis le compartiment configuré.
- Les vérifications de la bande passante.

Le processus de planification du stockage peut prendre environ cinq minutes.

Utiliser le Planificateur de capacité

Procedure

Étape 1 Pour planifier la taille de stockage et les estimations de la fenêtre de sauvegarde, effectuez l'une des actions suivantes :

- Dans la page de destination de **Data Backup** (sauvegarde des données), cliquez sur **Capacity Planning** (Planification de la capacité).
- Dans le menu déroulant **Planning** (Planification), choisissez **Capacity**(capacité).

La page **Planification de la capacité** s'affiche.

Étape 2 Saisissez la limite de bande passante maximale pour sauvegarder les données.

Cette bande passante doit au plus correspondre à la configuration du contrôleur qui limitera les données envoyées au magasin d'objets.

Étape 3 Le nombre d'agents logiciels enregistrés est rempli automatiquement. En fonction des prévisions, vous pouvez modifier le nombre d'agents.

Étape 4 (Facultatif) Activez **Lean Data Mode** (le mode de données allégé) pour exclure les données qui ne font pas partie de la configuration de la sauvegarde. L'utilisation de cette option réduit la limite de stockage de 75 %.

Étape 5 Le stockage maximal configuré pour l'ensemble de stockage. Cela définira automatiquement la période de rétention des sauvegardes.

Une fois les renseignements détaillés requis saisis, la durée estimée de la sauvegarde affiche le temps requis pour la sauvegarde des données d'une journée. Il s'agit d'une estimation basée sur la charge d'agent typique, le nombre d'agents estimatif et la bande passante maximale configurée. L'estimation de la capacité de stockage maximale affiche l'estimation de la capacité de stockage maximale requise par Cisco Secure Workload pour prendre en charge la rétention précisée et le nombre estimatif d'agents.

Configurer la sauvegarde des données

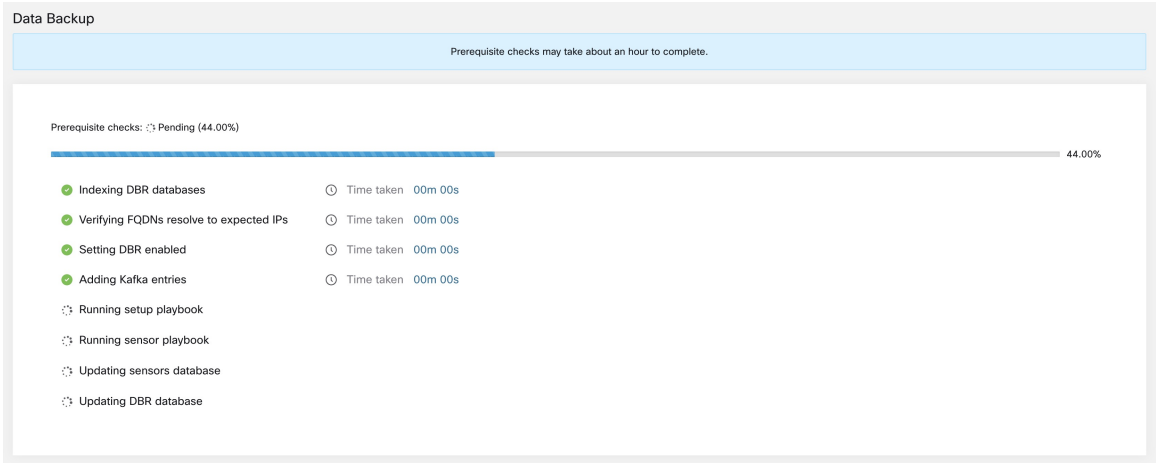
Procedure

Étape 1 Dans la page de destination de la sauvegarde des données, cliquez sur **Create new schedule** (Créer une nouvelle planification).

Étape 2 Pour confirmer les vérifications des préalables à exécuter, cochez les boutons **Approve** (approuver) et cliquez sur **Proceed** (Continuer).

La vérification des préalables prend environ 30 minutes et n'est exécutée que lors de la première configuration d'une planification.

Figure 18: Exécution de la sauvegarde des conditions préalables



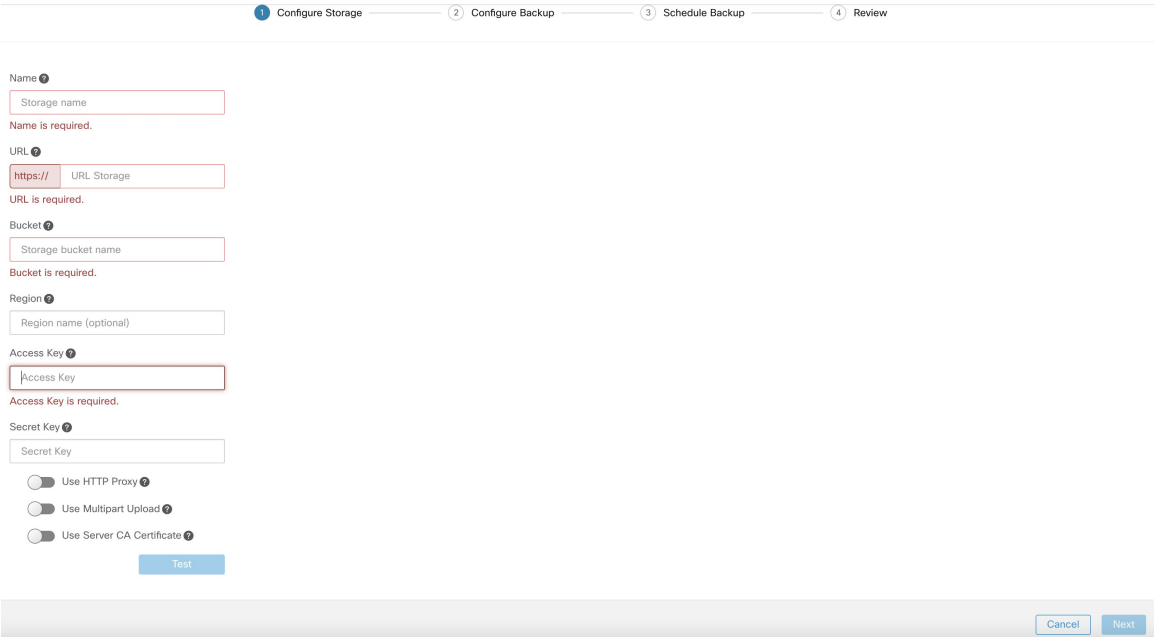
Étape 3 Pour configurer le stockage, entrez les détails suivants et cliquez sur **Test** (Tester).

- Un nom pour le stockage.
- URL d'un point terminal de stockage conforme à S3.

Note L'adresse IPv6 d'un stockage conforme S3 doit être une URL ou un nom de domaine complet, et pas seulement une adresse IPv6.

- Un nom de compartiment conforme à S3 configuré sur le stockage
- (Facultatif pour certains types de stockage) Région du stockage conforme à S3.
- Clé d'accès au stockage.
- Clé secrète du stockage.
- (Facultatif) Activez le serveur mandataire HTTP, si nécessaire.
- (Facultatif) Pour utiliser des chargements en plusieurs parties des données sauvegardées, activez **Use Multipart Upload**(utiliser le chargement en plusieurs parties) .
- (Facultatif) Si un certificat de l'autorité de certification est requis pour authentifier le serveur de stockage, activez l'option **Use Server CA Certificate** (utiliser le certificat de l'autorité de certification du serveur) et saisissez les détails du certificat.

Figure 19: Configuration du stockage.

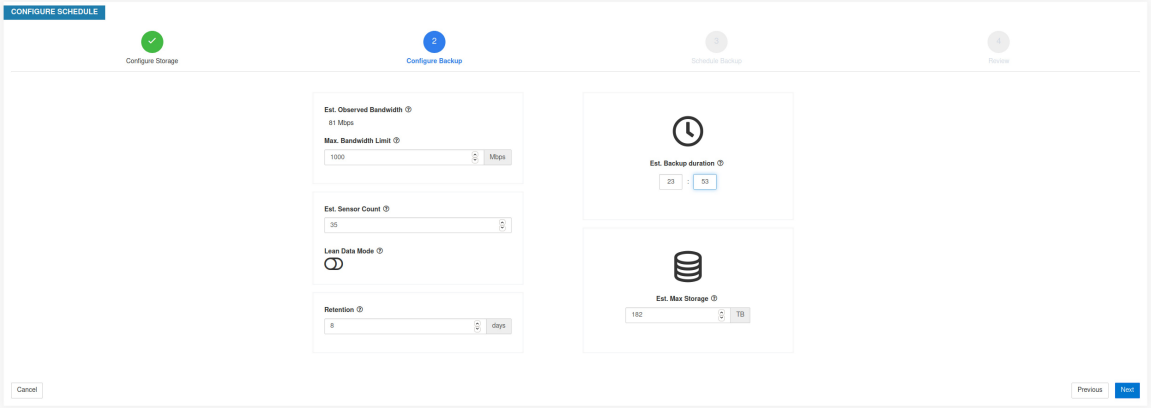


Étape 4 Pour configurer la capacité de stockage, saisissez les informations suivantes :

- La limite de bande passante maximale pour la sauvegarde des données. Cette bande passante doit au plus correspondre à la configuration du contrôleur qui limitera les données envoyées au magasin d'objets.
- Le nombre d'agents logiciels enregistrés est rempli automatiquement. En fonction des prévisions, vous pouvez modifier le nombre d'agents.
- (Facultatif) Activez **Lean Data Mode** (le mode de données allégé) pour exclure les données qui ne font pas partie de la configuration de la sauvegarde. L'utilisation de cette option réduit la limite de stockage de 75 %.

- Le stockage maximal configuré pour l'ensemble de stockage. Cela définira automatiquement la période de rétention des sauvegardes.

Figure 20: Planification de la capacité



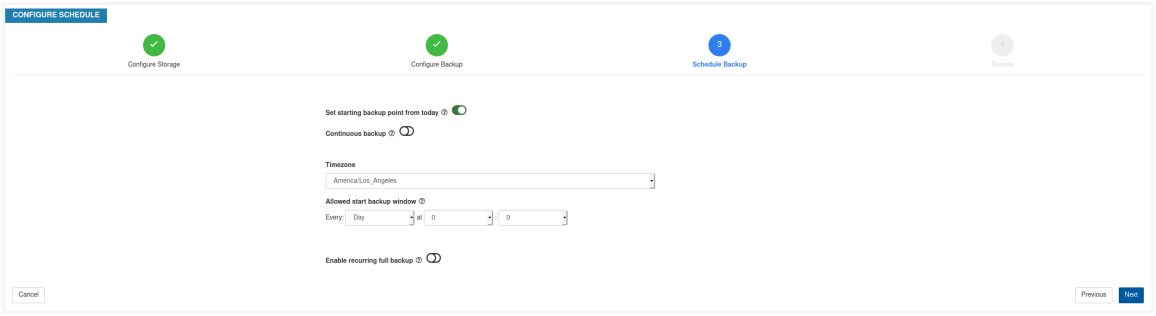
Étape 5 Pour planifier la sauvegarde, activez les éléments suivants :

- Par défaut, l'option **Set starting backup point from today** (Définir le point de sauvegarde de départ à partir d'aujourd'hui) est activée. Cette option ignorera tous les fichiers créés avant minuit UTC le jour de la configuration. Dans une grappe qui fonctionne, il peut y avoir un volume élevé de données à sauvegarder le premier jour et qui risque de surcharger la grappe, le réseau et le magasin d'objets. Si vous souhaitez sauvegarder toutes les données existantes, décochez cette case mais notez l'incidence sur le réseau, le magasin d'objets et la grappe.

  Note Toutes les données de configuration seront sauvegardées, quelle que soit cette option.

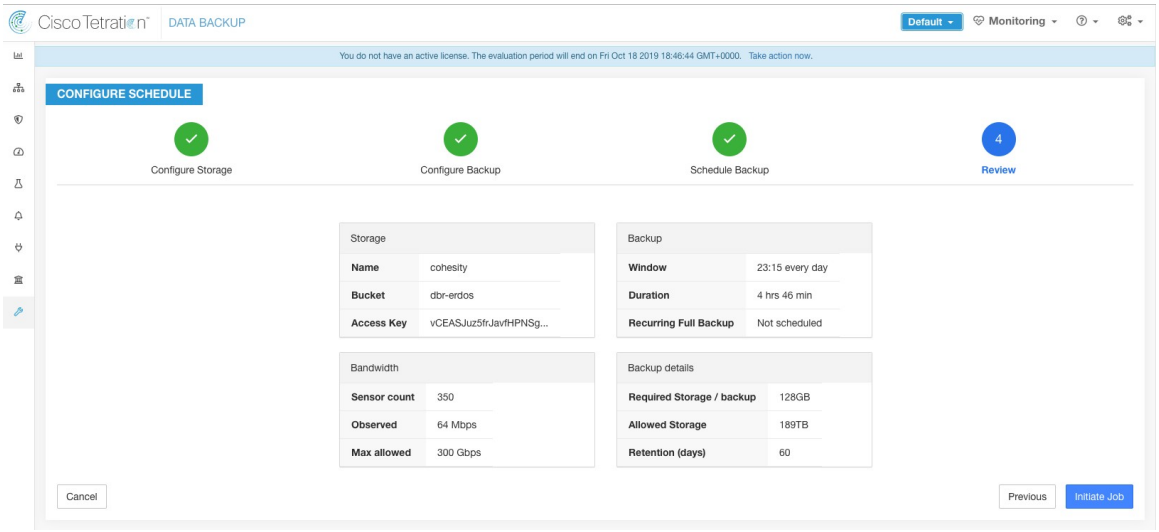
- Sauvegarde continue : si cette option est activée, les données seront sauvegardées 15 minutes après la fin de la sauvegarde précédente. Cette option permet aux sauvegardes de s'exécuter en permanence, au lieu d'être planifiées à une heure précise. Les options de **fuseau horaire** et **de fenêtre de sauvegarde de début autorisée** ne sont pas disponibles lorsque la sauvegarde continue est activée.
- Les deux options suivantes sont utilisées pour configurer la planification de la sauvegarde, si la sauvegarde en continu n'est pas utilisée.
  - Time zone (Fuseau horaire) : utilise par défaut le fuseau horaire du navigateur Web
  - Allowed Start save Window (fenêtre autorisée de démarrage de la sauvegarde) : heure (en heures ou minutes) à laquelle la sauvegarde commencera. L'heure doit être saisie au format 24 heures
  - Activer la sauvegarde complète récurrente (non sélectionnée par défaut) : Si cette option est activée, une planification pour la sauvegarde complète peut être configurée. Par défaut, après la première sauvegarde complète, toutes les sauvegardes sont différentielles. L'activation de cette configuration forcera une sauvegarde complète selon le calendrier spécifié.

Figure 21: Planifier une sauvegarde



Étape 6 Passez en revue la planification et les paramètres de sauvegarde configurés, puis cliquez sur **Initiate Job** (Démarrer a tâche).

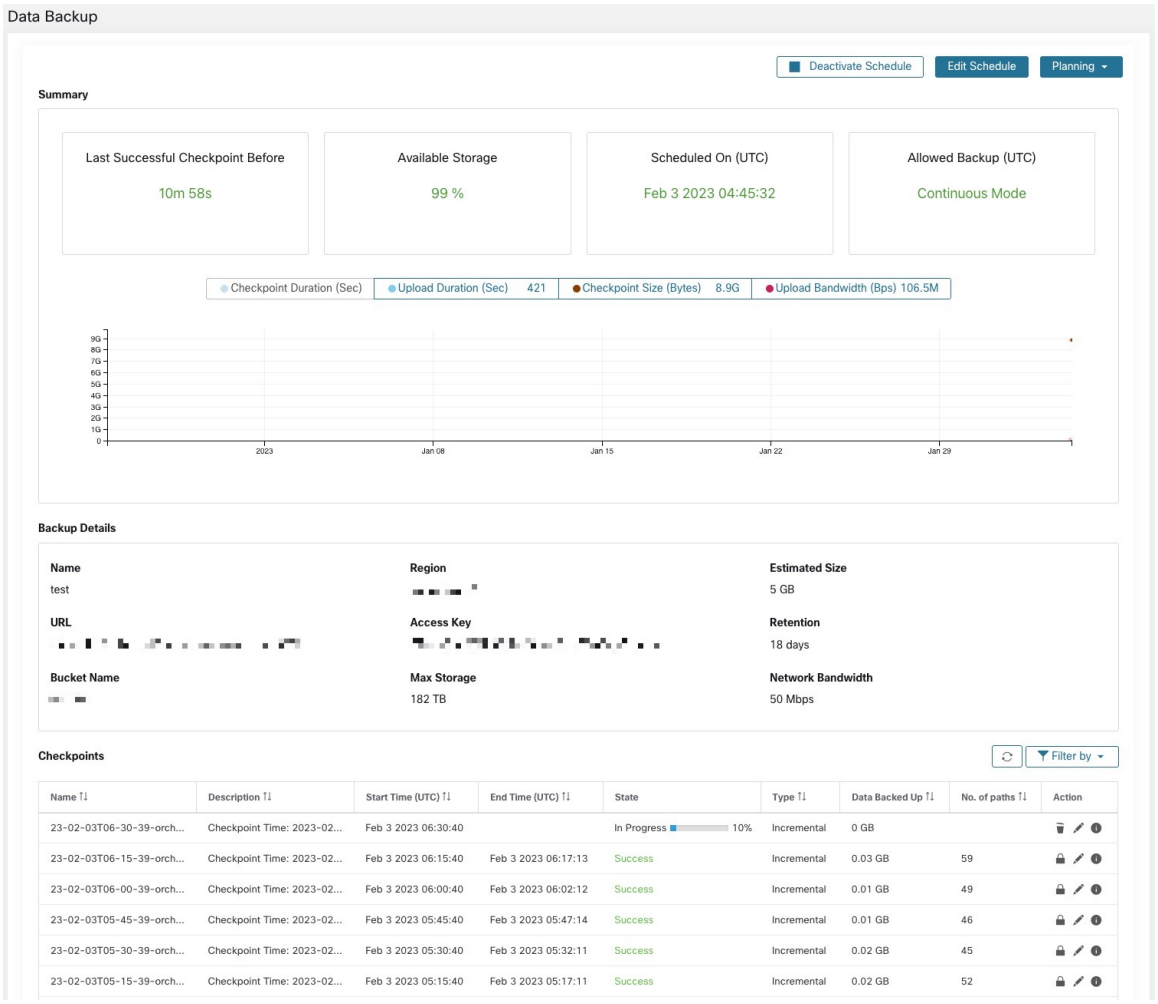
Figure 22: Examiner la configuration de sauvegarde)



État de la sauvegarde

Après la configuration de la sauvegarde des données, elle est déclenchée tous les jours à une heure planifiée, sauf si le mode continu est activé. L'état des sauvegardes peut être consulté sur le tableau de bord de la sauvegarde des données en accédant à **Platform (Plateformes)** > **Data Backup (Sauvegarde des données)**.

Figure 23: État de la sauvegarde



Le temps écoulé depuis le dernier point de contrôle réussi doit être inférieur à 24 heures + le temps nécessaire au point de contrôle. Par exemple, si le point de contrôle + la sauvegarde prennent environ 6 heures, le temps écoulé depuis le dernier point de contrôle réussi doit être inférieur à 30 heures.

Les graphiques suivants fournissent des renseignements supplémentaires :

- Durée du point de contrôle : ce graphique montre la ligne de tendance de la durée du point de contrôle.
- Durée du chargement : ce graphique montre la ligne de tendance pour le temps nécessaire au chargement du point de contrôle vers la base de données de sauvegarde.
- Taille du point de contrôle : ce graphique montre la ligne de tendance pour la taille du point de contrôle.
- Bande passante de téléversement : ce graphique montre la ligne de tendance de la bande passante de téléversement.

Le tableau présente tous les points de contrôle. Les étiquettes de point de contrôle peuvent être modifiées et seront disponibles lors du choix d'un point de contrôle pour restaurer les données sur la grappe de secours.

Un point de contrôle passe par plusieurs états. Voici les états possibles :

- Créé/en attente : le point de contrôle vient d'être créé et en attente de copie.
- En cours d'exécution : les données sont sauvegardées activement sur un stockage externe
- Réussite : le point de contrôle est terminé et a réussi; peut être utilisé pour la restauration des données
- Échec : le point de contrôle est terminé et a échoué; ne peut pas être utilisé pour la restauration des données
- Suppression en cours/Supprimé : un point de contrôle obsolète est en cours de suppression ou est supprimé

Pour modifier la planification ou le regroupement, cliquez sur **Edit Schedule** (Modifier le calendrier). Pour terminer la mise en œuvre de l'assistant, consultez la section Configurer la sauvegarde des données.

Pour résoudre les erreurs lors de la création des points de contrôle, consultez Dépannage : sauvegarde et restauration des données, on page 35.

Désactiver la planification de sauvegarde

Les sauvegardes peuvent être désactivées en cliquant sur le bouton **Deactivate Schedule** (Désactiver la planification). Il est recommandé de désactiver la planification de sauvegarde avant d'y apporter des modifications. Désactivez la planification uniquement lorsqu'aucun point de contrôle n'est en cours. L'exécution d'un test ou la désactivation de la planification alors qu'un point de contrôle est en cours peut entraîner l'échec de ce dernier et un état indéfini du téléchargement.

Rétention du magasin d'objets

La grappe Cisco Secure Workload gère le cycle de vie des objets du compartiment. Vous ne devez pas supprimer ni ajouter d'objets au compartiment. Cela pourrait entraîner des incohérences et endommager les points de contrôle réussis. Dans l'assistant de configuration, la mémoire maximale à utiliser doit être spécifiée. Cisco Secure Workload fait en sorte que l'utilisation du compartiment ne dépasse pas la limite configurée. Il existe un service de conservation du stockage qui élimine les objets après un certain temps et les supprime du compartiment. Une fois que l'utilisation du stockage a atteint un seuil (80 % de la capacité du compartiment) calculé en fonction du stockage maximal configuré et du débit de données entrantes, la fonction de rétention tente de supprimer les points de contrôle *non conservés* pour ramener l'utilisation sous le seuil. La fonction de rétention conservera également un minimum de deux points de contrôle réussis à tout moment et tous les points de contrôle préservés, le nombre le plus élevé des deux situations étant retenu. Si la fonction de rétention ne peut supprimer aucun point de contrôle pour libérer de l'espace, les ***points de contrôle commenceront à générer des échecs***.

Conserver les points de contrôle

À mesure que de nouveaux points de contrôle sont créés, les anciens expirent et sont supprimés. Cependant, les points de contrôle peuvent être conservés, empêchant ainsi leur suppression par la fonction de rétention. Un point de contrôle conservé ne sera pas supprimé. S'il y a plusieurs points de contrôle conservés, à un moment donné, le stockage sera insuffisant pour les nouveaux objets et les points de contrôle périmés ne pourront pas être supprimés parce qu'ils ont été conservés. Une bonne pratique consiste à conserver les points de contrôle en fonction des besoins et à mettre à jour l'étiquette du point de contrôle en indiquant la raison et la validité comme référence. Pour conserver un point de contrôle, cliquez sur l'icône représentant un verrou à côté du point de contrôle requis.

Restaurer les données

- Pour restaurer à l'aide de données sauvegardées, une grappe doit être en **mode d'attente DBR**. Actuellement, vous pouvez définir une grappe en mode veille **uniquement lors de la configuration initiale**.
- Une fois que la grappe est en mode veille, choisissez **Platform** (plateforme) dans le volet de navigation pour accéder à l'option de restauration des données.

Cisco Secure Workload prend en charge les combinaisons suivantes :

Table 8: UGS de grappes principale et secondaire pour la restauration des données

UGS de grappe principale	UGS de grappe en attente
8RU-PROD	8RU-PROD, 8RU-M5, 8RU-M6
8RU-M5	8RU-PROD, 8RU-M5, 8RU-M6
39RU-GEN1	39RU-GEN1, 39RU-M5, 39RU-M6
39RU-M5	39RU-GEN1, 39RU-M5, 39RU-M6
8RU-M6	8RU-PROD, 8RU-M5, 8RU-M6
39RU-M6	39RU-GEN1, 39RU-M5, 39RU-M6

UGS de grappe principale	UGS de grappe en attente
8RU-PROD	8RU-PROD, 8RU-M5
8RU-M5	8RU-PROD, 8RU-M5
39RU-GEN1	39RU-GEN1, 39RU-M5
39RU-M5	39RU-GEN1, 39RU-M5

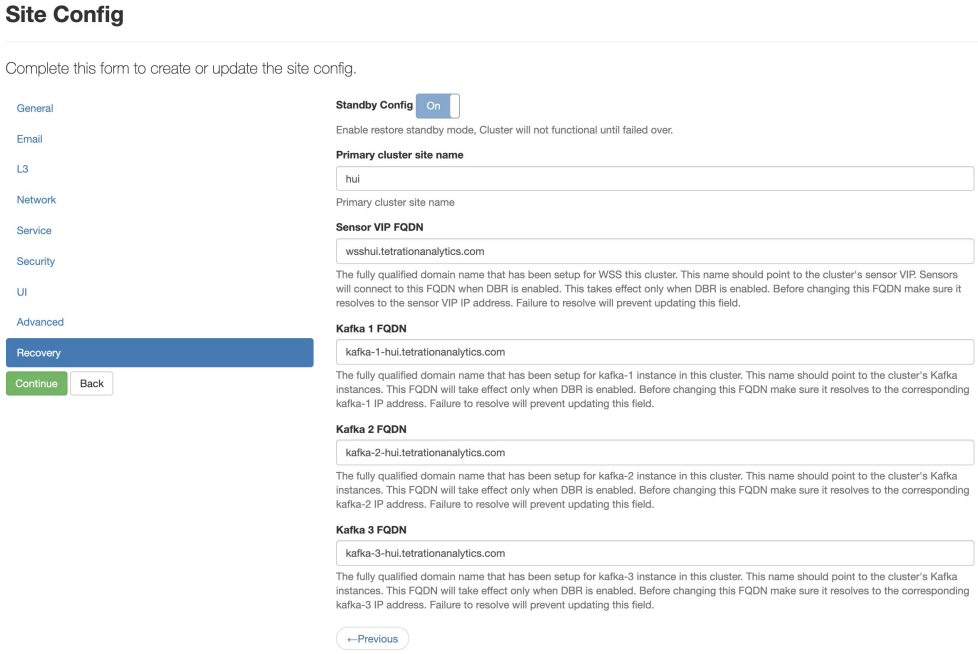
Deploy Cluster in Standby Mode

Contact Cisco to initiate data restore.

A cluster can be deployed in the Standby mode by configuring the recovery options in site information. While configuring site information during deployment, configure the restore details under the **Recovery** tab in the setup UI during deployment.

There are three modes to deploy a standby and for all the three modes, configure these settings:

- Set the **Standby Config** to **On**. This configuration cannot be changed once set until the cluster is redeployed.
- Configure primary cluster name and FQDNs. This configuration can be changed subsequently.



Rest of the deployment is same as a regular deployment of Secure Workload cluster.

A banner is displayed on the Secure Workload UI after the cluster enters the standby mode.

Primary cluster name and FQDNs can be reconfigured after the deployment to enable the standby cluster to track another cluster. This can be reconfigured at a later time before failover is triggered from the Cluster Configuration page.

Standby Deployment Modes

- **Cold Standby**: There is no standby cluster. However, the primary cluster backs the data to S3. During a disaster, a new cluster (or the same cluster as primary) needs to be provisioned, deployed in standby mode and restored.
- **Warm Standby**: A standby cluster is operational and deployed in standby mode. It periodically fetches state from S3 cluster and places it in the ready state to be operational in case of a disaster. During a disaster, log in to this new cluster and trigger a failover.
- **Luke Warm Standby**: Multiple primary clusters are backed by fewer standby clusters. The standby cluster is deployed in standby mode. Only after a disaster, the storage bucket information is configured, data is prefetched, and cluster is restored.

Restore Data to a Secure Workload Cluster

Before you begin

Ensure that the cluster is deployed in standby mode. For more details, see Deploy Cluster in Standby Mode.

Procedure

Étape 1 (Optional) If you have already configured the storage details, go to Step 2. To configure S3 storage, enter the following details:

- A name for the storage.
- The URL of an S3-compliant storage endpoint.

  Note The IPv6 address of an S3-compliant storage must be a URL or FQDN, and not just an IPv6 address.

- An S3-compliant bucket name configured on the endpoint storage.
- (Optional for certain storage) Region of the S3-compliant storage.
- Access key to the storage.
- Secret key of the storage.
- (Optional) Enable HTTP proxy, if necessary.
- (Optional) If a CA certificate is required to authenticate the storage server, enable **Use Server CA Certificate** and enter the certificate details.

Étape 2 Click **Test** to check if the S3 storage is accessible from the Secure Workload cluster.

The status of the tests that are performed are displayed in the table. If there are any errors connecting to the storage, read the description and troubleshoot the errors to continue to the next step.

Étape 3 Click **Next**.

Étape 4 Under **Pre-checks**, the status of the prechecks runs by Secure Workload are displayed. To manually run the prechecks, click **Perform Check**.

The status of all the checks is displayed:

- For the checks that have an error, but do not prevent you from restoring the data, hover your cursor over the warning icon to get the details and a link to navigate to the **Service Status** page to get more details of the service.
- If any of the checks failed, you must troubleshoot the issue to proceed with data restore. Navigate to the **Service Status** page to get more details of the service.

Note Ensure that the checkpoint you are restoring to is the latest with no errors.

Étape 5 Click **Start restore process**.

Under **Restore**, all the data restore jobs that run, the configured S3 storage details, and the status of the data restore prechecks are displayed.

Étape 6 Click **Restore now**.

Étape 7 In the confirmation dialog box, check the check boxes to confirm that you agree to the fact that agent connectivity is lost and data may be lost during the data restore. Click **Confirm** to start the data restore process.

The progress of the data restore process is displayed.

Caution At the **Pre Restore Playbook** stage, all the services within the cluster are reinitialized and there is a downtime of approximately two hours. At this stage, the Secure Workload GUI is not accessible. For more information about the phases that are involved in data restore, see Phases de restauration de la grappe.

If the GUI is rendered inaccessible for an extended period, contact the Cisco Technical Assistance Center to troubleshoot the issue.

Note

After the **Post Restore Playbook** stage, the GUI is accessible and the status of all the jobs are updated. A confirmation message is displayed indicating that the data restore is successful.

What to do next

Update your DNS server to redirect the configured FQDNs to the cluster IP address, which ensures that the software agents communicate with the cluster after the cluster failover is complete.

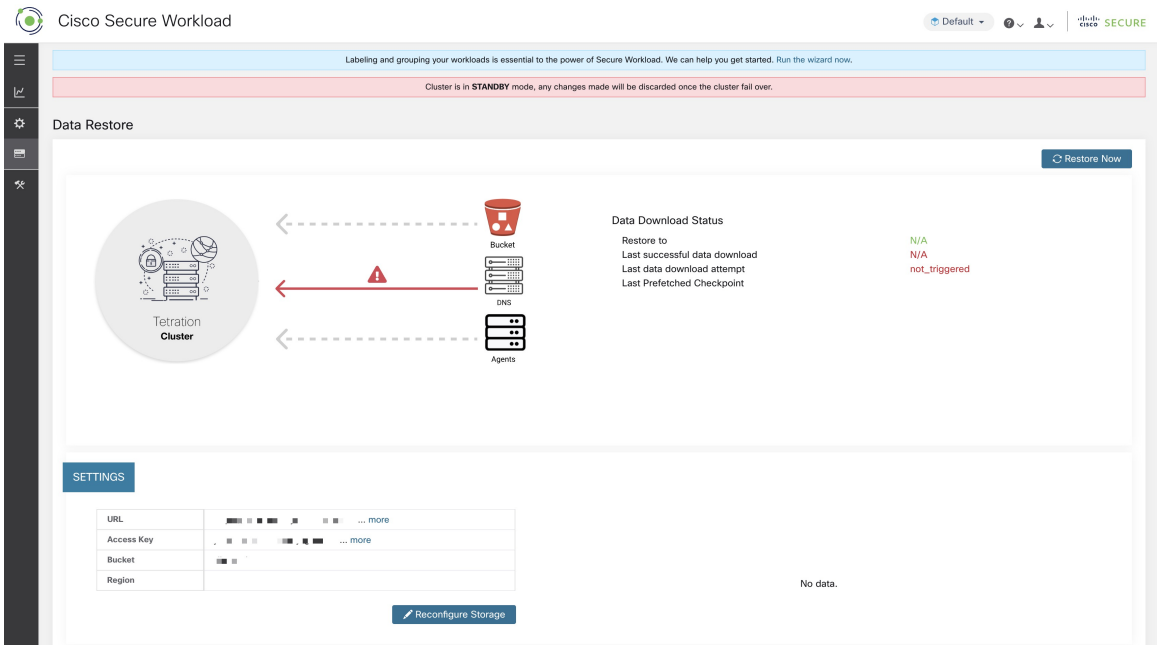
Pré-lecture des données de grappe

Avant de pouvoir restaurer la grappe, elle doit précharger les données. Les données du point de reprise sont prélues à partir du même compartiment de stockage que celui utilisé pour la sauvegarde des données. Des informations d'authentification doivent être fournies pour que le service de sauvegarde puisse être téléchargé à partir du stockage. Si un stockage n'est pas configuré pour la prélecture, l'onglet **Data Restore** (Restauration des données) lance l'assistant de configuration.

Note La grappe de secours interagit uniquement avec le stockage S3. Lorsque la sauvegarde sur la grappe principale est mise à jour pour utiliser un stockage ou un compartiment différent, la grappe de stockage en attente doit être mise à jour.

Une fois les informations validées, le stockage est automatiquement configuré pour la pré-lecture. L'onglet Restaurer affichera l'état de la pré-lecture.

Figure 24: État de la pré-lecture



La page État affiche les éléments suivants :

- La section supérieure gauche comporte un graphique indiquant que les divers composants sont prêts à démarrer une restauration. Pour vérifier les données, survolez avec le curseur les composants. Les données associées s'affichent dans la section supérieure droite.
    - **Compartiment** : affiche l'état de la pré-lecture. Si les dernières données datent de plus de 45 minutes, elles s'affichent en rouge. Notez que les dernières données datant de plus de 45 minutes n'est pas un problème si la sauvegarde sur le périphérique actif prend plus de 45 minutes pour chaque point de contrôle.
    - **DNS** : Affiche les résolutions de nom de domaine complet (FQDN) Kafka et WSS par rapport aux adresses IP des grappes de secours. Pendant la restauration, si les noms de domaine complets ne sont pas mis à jour pour les adresses IP de grappe de secours, l'agent ne peut pas se connecter. Une fois que les noms de domaine complets ont commencé à être résolus vers la grappe de secours, l'état devient vert.
    - **Agents** : affiche le nombre d'agents logiciels qui ont basculé avec succès vers la grappe de secours. Cela n'est pertinent qu'après le déclenchement d'une restauration.
- La section supérieure droite affiche les renseignements pertinents pour le graphique choisi dans la section de gauche. Cliquez sur **Restore Now** (Restaurer maintenant) pour lancer le processus de restauration.
- La section inférieure gauche affiche les paramètres de stockage de prélecture qui sont utilisés.
- La section inférieure droite affiche un graphique des retards de pré-lecture.

Une pré-lecture des données met à jour plusieurs composants nécessaires pour assurer une restauration rapide. Si une pré-lecture de données ne peut pas se terminer, la raison de l'échec est affichée dans la page d'état.

Erreurs courantes qui peuvent entraîner des échecs de pré-lecture :

Erreur d'accès S3 : dans ce cas, les données du stockage n'ont pas pu être téléchargées avec succès. Cela peut se produire en raison de renseignements d'authentification non valides, d'une modification des politiques de stockage ou de problèmes réseau temporaires.

Versions de grappe incompatibles : les données peuvent être restaurées dans une grappe exécutant la même version (y compris la même version de correctif) de Cisco Secure Workload que la grappe principale. Cela peut probablement se produire lors des mises à niveau lorsqu'un seul de la grappe est mis à niveau. Ou, pendant le déploiement, lorsqu'une version différente est utilisée pour le déploiement. Le déploiement des grappes sur une version commune résoudra le problème.

Versions d'UGS incompatibles : notez les UGS autorisées pour les grappes de secours de la grappe principale. Seules des UGS spécifiques sont autorisées pour la restauration de l'UGS de grappe principale.

Phases de restauration de la grappe

Les données de la grappe sont restaurées en deux phases :

- **Phase obligatoire** : Les données nécessaires au redémarrage des services sont restaurées en premier. La durée d'une phase obligatoire dépend de la configuration, du nombre d'agents logiciels installés, de la quantité de données sauvegardées et des métadonnées de flux. Pendant la phase obligatoire, l'interface utilisateur n'est pas accessible. **Des clés d'invité TA fonctionnels sont nécessaires pour toute prise en charge pendant la phase obligatoire, le cas échéant.**
- **Phase de transmission** : les données de la grappe (y compris les données de flux) sont restaurées en arrière-plan et ne bloquent pas l'utilisation de la grappe. L'interface utilisateur de la grappe est accessible et une bannière s'affiche avec le pourcentage de restauration terminée. Pendant cette phase, la grappe est opérationnelle, les pipelines de données fonctionnent normalement et les recherches de flux sont également disponibles.

Une fois la phase obligatoire de la restauration terminée et l'interface utilisateur accessible, les modifications apportées à la grappe doivent être communiquées aux agents logiciels. Dans le serveur DNS utilisé par les agents, l'adresse IP associée au nom de domaine complet de la grappe doit être mise à jour et l'entrée DNS doit pointer vers la grappe restaurée. Une recherche DNS est déclenchée par les agents lorsque la connexion à la grappe principale est interrompue. En fonction de l'entrée DNS mise à jour, les agents se connectent à la grappe restaurée.

Objectif de temps de reprise (RTO) et objectif de point de reprise (RPO)

Cette section décrit l'objectif de temps de récupération (RTO) et l'objectif de point de récupération (RPO) pour la solution de sauvegarde et de restauration des données.

Une sauvegarde lancée sur la grappe principale nécessite un certain temps pour se terminer en fonction de la quantité de données sauvegardées et de la configuration de la sauvegarde. Les différents modes de sauvegarde définissent l'objectif de point de récupération (RPO) de la solution.

- Si elle est planifiée, la sauvegarde non continue est utilisée et est lancée une fois par jour. En cas de sinistre, la durée maximale de perte de données sera d'environ 24 heures, en plus du temps nécessaire pour copier les données dans le stockage de sauvegarde. Par conséquent, l'objectif de point de récupération (RPO) est d'au moins 24 heures.
- Si une sauvegarde en mode continu est utilisée, une nouvelle sauvegarde est lancée 15 minutes après la sauvegarde précédente. Chaque sauvegarde prend un certain temps à créer, puis à téléverser les données vers le stockage de sauvegarde. La première sauvegarde est une sauvegarde complète et les sauvegardes suivantes sont des sauvegardes différentielles , les sauvegardes différentielles ne prennent pas beaucoup

de temps. En cas de sinistre, la quantité de données perdues correspond à la somme du temps nécessaire pour créer la sauvegarde et du temps nécessaire pour téléverser la sauvegarde dans le système de stockage. Dans ce cas, en général, l'objectif de RPO sera d'environ quelques minutes à une heure.

Lors de la restauration d'une grappe, les données obligatoires sont d'abord extraites du stockage, puis la phase de restauration obligatoire est déclenchée. L'interface utilisateur n'est pas disponible pendant la phase de restauration obligatoire. Une fois la restauration obligatoire terminée, l'interface utilisateur est disponible pour utilisation. Le reste des données est restauré lors de la phase de restauration différée. Dans ce cas, le RTO correspond au temps nécessaire jusqu'à ce que l'interface utilisateur soit disponible pour utilisation une fois la phase obligatoire terminée. Les RTO dépendent du mode de déploiement en veille.

- Mode à froid : dans ce mode, la grappe doit d'abord être déployée, ce qui prend environ quelques heures. La grappe doit ensuite être configurée avec les informations d'authentification de stockage de sauvegarde. Comme c'est la première fois que la sauvegarde est téléversée dans la grappe de secours, il y aura beaucoup de données obligatoires qui doivent être récupérées et traitées. La durée de la lecture anticipée est d'environ plusieurs dizaines de minutes (selon la quantité de données sauvegardées). La phase de restauration obligatoire prend environ 30 minutes. L'ensemble forme un temps de RTO d'environ quelques heures, principalement dû au temps nécessaire pour démarrer et déployer la grappe.
- Mode de veille à chaud : dans ce mode, la grappe est déjà déployée, mais le stockage de sauvegarde n'est pas configuré. La grappe doit être configurée avec les informations d'authentification de stockage de sauvegarde. Comme c'est la première fois que la sauvegarde est téléversée dans la grappe de secours, il y aura beaucoup de données obligatoires qui doivent être récupérées et traitées. La durée de la lecture anticipée est d'environ plusieurs dizaines de minutes (selon la quantité de données sauvegardées). La phase de restauration obligatoire prend environ 30 minutes. L'ensemble forme un RTO d'environ une à deux heures, selon la quantité de données sauvegardées et le temps nécessaire pour extraire les données du stockage de sauvegarde.
- Mode de secours immédiat : dans ce mode, la grappe est déjà déployée, le stockage de sauvegarde est configuré et la prélecture récupère les données du stockage. La grappe peut maintenant être restaurée, ce qui déclenchera la phase de restauration obligatoire, qui prend environ 30 minutes. Cela forme le temps RTO d'environ 30 minutes. Notez qu'il s'écoule un certain délai entre le moment où la sauvegarde est téléversée des processus actifs vers le stockage et le moment où la sauvegarde est extraite par la sauvegarde. Ce délai dure environ quelques minutes. Si la dernière sauvegarde du système actif (avant qu'il ne subisse un sinistre) n'a pas été récupérée préalablement sur la sauvegarde, vous devez attendre quelques minutes pour qu'elle soit récupérée.

Mise à niveau avec la sauvegarde et la restauration des données

Lorsque la sauvegarde et la restauration des données sont activées sur la grappe, il est recommandé de désactiver la planification avant de commencer la mise à niveau. Reportez-vous à la section Désactiver la planification de sauvegarde. Cela garantit qu'il existe une sauvegarde réussie avant de commencer la mise à niveau et qu'aucune nouvelle sauvegarde n'est chargée. Une planification doit être désactivée lorsqu'un point de contrôle n'est pas en cours, afin d'éviter la création d'un point de contrôle défaillant.

Dépannage : sauvegarde et restauration des données

Les vérifications de la configuration S3 échouent

Si le test de stockage échoue, identifiez les scénarios de défaillance qui sont affichés dans le volet de droite et vérifiez que :

- L'URL de stockage conforme à S3 est correcte.
- Les clés d'accès et codes secrets du stockage sont corrects.
- Il existe un compartiment de stockage et des autorisations d'accès correctes (lecture/écriture) sont accordées.
- Le serveur mandataire est configuré si le stockage doit être accessible directement.
- L'option de chargement en plusieurs parties est désactivée si vous utilisez Cohesity.

Scénarios d'erreur des vérifications de la configuration S3

Le tableau énumère les scénarios d'erreur courants avec résolution et ne constitue pas une liste exhaustive.

Table 9: Messages d'erreur avec résolution lors de la vérification de la configuration S3

Message d'erreur	Scénario	Résolution
`Introuvable`	Nom de compartiment incorrect	Saisissez le nom correct du compartiment configuré pour le stockage
`Erreur de connexion SSL`	Erreur d'expiration ou de vérification du certificat SSL	Vérifiez le certificat SSL
	URL HTTPS non valide	• Saisissez à nouveau l'URL HTTPS correcte du stockage. • Résoudre les échecs lors de la vérification du certificat SSL.
`La connexion a expiré`	L'adresse IP du serveur S3 est inaccessible	Vérifier la connectivité du réseau entre la grappe et le serveur S3
`Connexion à l'URL impossible`	Région du compartiment incorrecte	Saisissez la bonne région du compartiment
	URL non valide	Saisissez à nouveau l'URL correcte du point de terminaison de stockage S3
`Interdit`	Clé secrète non valide	Saisissez la clé secrète correcte du stockage
	Clé d'accès non valide	Saisissez la clé d'accès correcte du stockage
`Impossible de vérifier la configuration S3`	Autres exceptions ou erreurs génériques	Essayez de configurer le stockage S3 après un certain temps

Codes d'erreur des points de contrôle

Le tableau répertorie les codes d'erreur courants des points de contrôle et ne constitue pas une liste exhaustive.

Table 10: Codes d'erreur des points de contrôle

Code d'erreur	Description
E101 : Échec du point de contrôle de la base de données	Impossible de prendre un instantané des journaux des opérations de Mongodb
E102 : Échec du point de contrôle des données de flux	Impossible de prendre un instantané de la base de données Druid
E103 : Échec du chargement de l'instantané de base de données	Impossible de télécharger l'instantané de la base de données Mongo
E201 : Échec de copie de base de données	Impossible de charger l'instantané Mongo dans HDFS
E202 : Échec de copie de configuration	Impossible de télécharger l'instantané de consultation ou coffre-fort dans HDFS
E203 : Échec du point de contrôle de la configuration	Impossible de vérifier les données de consultation ou coffre-fort
E204 : Incompatibilité des données de configuration au point de contrôle	Impossible de générer un point de contrôle de consultation ou de coffre-fort après le nombre maximal de tentatives
E301 : Échec du téléchargement des données de sauvegarde	Échec du point de contrôle HDFS
E302 : Échec de téléchargement du point de contrôle	Le pilote de copie n'a pas réussi à charger les données dans S3
E401 : Mise à niveau du système au point de contrôle	La grappe a été mise à niveau à ce point de contrôle; le point de contrôle ne peut pas être utilisé
E402 : Redémarrage du service au point de contrôle	BkpDriver a redémarré à l'état de création; le point de contrôle ne peut pas être utilisé
E403 : Échec au point de contrôle précédent	Échec du point de contrôle lors de l'exécution précédente
E404 : Un autre point de contrôle en cours	Un autre point de contrôle est en cours
E405 : Impossible de créer le point de contrôle	Erreur dans le sous-processus de point de contrôle
Échec : terminé	Un point de contrôle précédent a échoué; il s'agit probablement d'un chevauchement de plusieurs points de contrôle démarrant en même temps.

Erreurs lors du processus de restauration des données

- Phase de configuration du stockage : pour obtenir des suggestions de résolution des problèmes lors de la configuration du stockage S3, consultez la section *Scénarios d'erreur des vérifications de la configuration S3*.
- Vérifications préalables pour vérifier l'intégrité de la grappe secondaire : pour les services qui ne sont pas intègres ou ceux qui ont des avertissements, accédez à la page Service Status (État du service) pour obtenir de plus amples renseignements afin d'assurer l'intégrité des services.
- Vérifications préalables pour vérifier la connectivité au stockage :

Table 11: Erreurs lors des vérification préalables de la connectivité de stockage

Scénario d'erreur	Description
Impossible de télécharger les données à partir du stockage S3 configuré.	En raison de la connectivité du réseau, l'accès au stockage S3 a échoué. Le message d'erreur persiste jusqu'à ce qu'un nouveau point de contrôle soit extrait du stockage S3 après le rétablissement de la connectivité.
L'UGS de grappe secondaire (de secours) est incompatible avec la grappe principale.	Assurez-vous de restaurer les données d'une grappe 39 RU vers une autre grappe 39 RU uniquement. De même, les données de la grappe 8 RU ne peuvent être restaurées que dans une grappe 8 RU.
La version de la grappe secondaire (de secours) est différente de la grappe principale.	Assurez-vous que les grappes principale et secondaire exécutent la même version.
Échec de la restauration de la base de données MongoDB	Impossible de restaurer les métadonnées de MongoDB. Le problème sera résolu lors de la prochaine prélecture de point de contrôle.
Le document DBRInfo est dans un format inconnu.	Les métadonnées du point de contrôle dans le stockage S3 sont endommagées ou le document se trouve dans un stockage incorrect. Téléchargez le fichier *dbrinfo.json* à partir du stockage S3 et partagez-le avec le centre d'assistance technique Cisco TAC pour vérification.
Synchronisation impossible avec le service de copie.	Erreurs internes entre le gestionnaire de restauration des données et le service de copie S3. Communiquez avec le centre d'assistance technique (Cisco TAC) pour résoudre le problème.

- Vérifications préalables du nom de domaine complet (FQDN) : si un panneau d'avertissement s'affiche à côté des vérification préalables du nom de domaine complet (FQDN), cela signifie que l'entrée DNS pour les noms de domaine complets ne pointe pas vers la grappe secondaire.

  Résolution : après la restauration des données, modifiez l'entrée DNS pour activer la connectivité entre les agents logiciels et la grappe secondaire.

- Phase de restauration des données : dans la boîte de dialogue de confirmation de la restauration des données, si la case de l'orchestrateur externe n'est pas une coche verte, vérifiez la connectivité entre la grappe secondaire et les orchestrateurs externes.

Note Une fois les données restaurées et que la grappe secondaire a atteint l'état principal, la page de restauration des données est toujours accessible pour vérifier le temps qui a été nécessaire et le nombre d'agents qui se sont reconnectés. Pour une grappe où les données ne sont jamais restaurées, la page de restauration des données est vide.

Haute disponibilité dans Cisco Secure Workload

Cisco Secure Workload offre une haute disponibilité en cas de probabilité de défaillance des services, des nœuds et des machines virtuelles. La haute disponibilité fournit des méthodes de récupération en assurant un temps d'arrêt minimal et une intervention minimale de l'administrateur du site.

Dans Cisco Secure Workload, les services sont répartis sur les nœuds d'une grappe. Plusieurs instances de services sont exécutées simultanément sur les nœuds. Une instance principale et une ou plusieurs instances secondaires sont configurées pour une haute disponibilité sur plusieurs nœuds. Lorsque l'instance principale d'un service tombe en panne, une instance secondaire du service est considérée comme principale et devient active immédiatement.

Conception de grappe de Cisco Secure Workload

Les composants clés d'une grappe Cisco Secure Workload sont les suivants :

- Des serveurs sans système d'exploitation qui hébergent plusieurs machines virtuelles, qui hébergent à leur tour de nombreux services.
- Serveurs sur bâti Cisco UCS de série C avec les commutateurs de la gamme Cisco Nexus 9300 qui contribuent à un réseau intégré haute performance.
- Modèles d'appareils matériels en petit ou grand format pour prendre en charge un nombre précis de charges de travail :
  - Déploiement de petit format avec six serveurs et deux commutateurs Cisco Nexus 9300.
  - Déploiement de grand format avec 36 serveurs et trois commutateurs Cisco Nexus 9300.

Figure 25: Conception de la conception de grappe Cisco Secure Workload

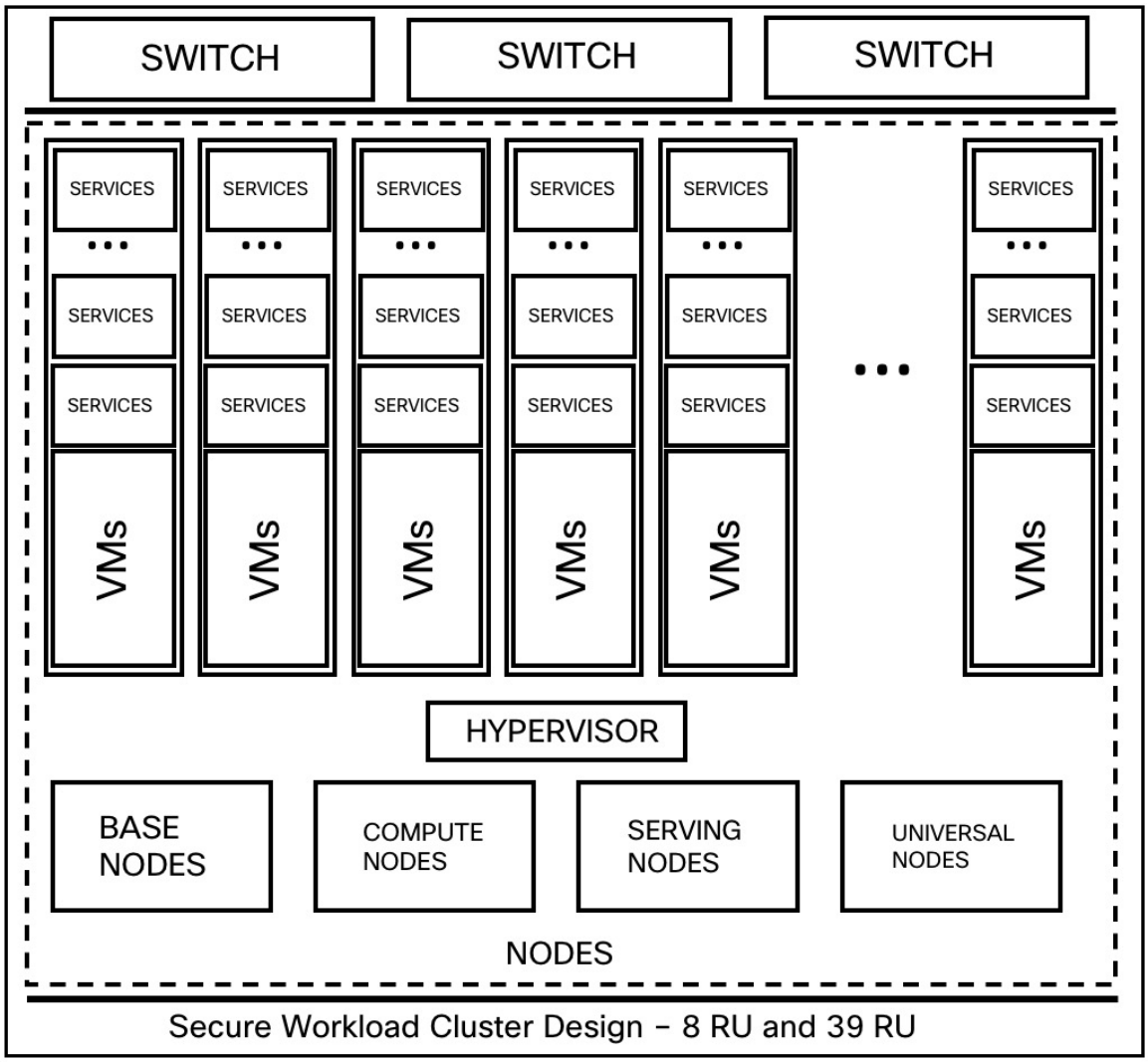


Table 12: Composants de la grappe Cisco Secure Workload

Attributs/Format	8 RU	39 RU
Nombre de nœuds	6	36
Nombre de nœuds de traitement informatiques	—	16
Nombre de nœuds de base	—	12
Nombre de nœuds de service	—	8
Nombre de nœuds universels	6	—
Nombre de machines virtuelles	50	106

Attributs/Format	8 RU	39 RU
Nombre de collecteurs	6	16
Nombre de commutateurs de réseau	2	3

Limites de la haute disponibilité dans Cisco Secure Workload

- Dans les deux formats (8RU et 39RU) de grappe, si un nœud défaillant héberge une machine virtuelle NameNode Hadoop, une intervention manuelle est nécessaire pour basculer vers une machine virtuelle NameNode secondaire.

Note Le basculement n'est pas automatique dans les versions 3.8.x et antérieures de Cisco Secure Workload.

- À partir de la version 3.9.x de Cisco Secure Workload, dans les facteurs de forme de grappe 8RU et 39RU, si un nœud qui héberge une VM Hadoop NameNode est défaillant, il n'est pas nécessaire d'intervenir manuellement pour basculer vers une VM secondaire.
- Avant d'effectuer une MISE À NIVEAU ou un REDÉMARRAGE, une intervention manuelle est nécessaire si la vérification préalable à la mise à niveau indique que Namenode-1 n'est pas actif ou dans un état normal. Si tel est le cas, vous devez effectuer un `POST namenode_failover` sur `launcherHost-1.node.consul` (ou sur tout autre `launcherHosts` en cours d'exécution) à partir de la page Explore.

Note Le basculement n'est pas automatique dans les versions 3.8.x et antérieures de Cisco Secure Workload.

- Pour un service à 2 ou 3 VM, comme les orchestrateurs, Redis, MongoDB, Elasticsearch, enforcementpolicystore, AppServer, ZooKeeper, TSDB, Grafana etc., une seule défaillance de machine virtuelle est prise en charge; une deuxième défaillance de la machine virtuelle rend le service inactif.

Impact and Recovery Details for Failure Scenarios

In Secure Workload, services are distributed across the nodes in a cluster. Multiple instances of services run simultaneously across the nodes. A primary instance and one or more secondary instances are configured for high availability across multiple nodes. When the primary instance of a service fails, a secondary instance of the service renders as primary and becomes active immediately.

- There is no impact to the cluster operation at any point in time.
- There is no single point of failure. If any of the nodes or VMs within the cluster fail, it does not result in failure of the entire cluster.
- There is minimal downtime of recovery from failure due to services, nodes, or VMs.

- There is no impact on the connections that are maintained by software agents to the Secure Workload cluster. The agents communicate with all the available collectors in the cluster. If a collector or VM fails, the software agents' connections to the other instances of the collectors ensure that the flow of data is not interrupted and there is no loss of functionality.
- The cluster services communicate with external orchestrators. When the primary instance of that service fails, the secondary instances take over to ensure the communication with external orchestrators is not lost.

Types of Failure Scenarios

High availability supports the following failure scenarios:

- Services Failure
- VM Failure
- Node Failure
- Network Switch Failure

Services Failure

When one or more services fail on any of the nodes, another instance of that particular service picks up and continues to run.

Figure 26: Normal Operation

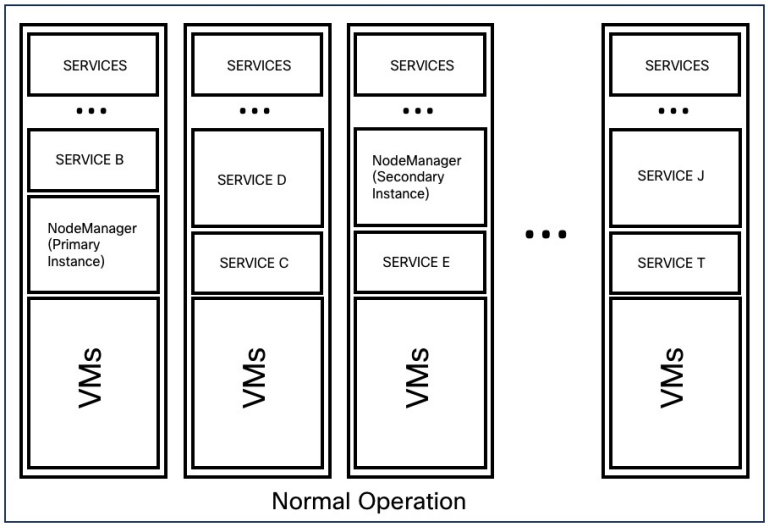
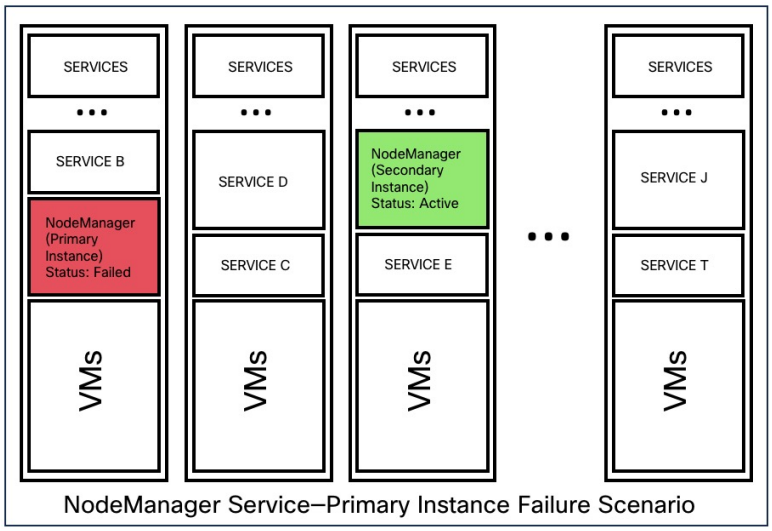


Figure 27: Failure Scenario of a Service



Impact	No visible impact.
Recovery	• Minimal downtime for the UI or dependent services to continue to run from the secondary instances. • Recovery is automatic.

VM Failure

When one of the VMs fails, the secondary VMs are available. The services on the secondary VMs pick up from where the services on the failed VM were running. Secure Workload restarts the failed VM to recover it. For example, as illustrated in the **Failure Scenario of a VM**, VM1 has failed and as a result the services running on it also has failed. The secondary VMs continue to be operational and the secondary instances picks up from where the services on the failed VM were running.

Figure 28: Normal Operation

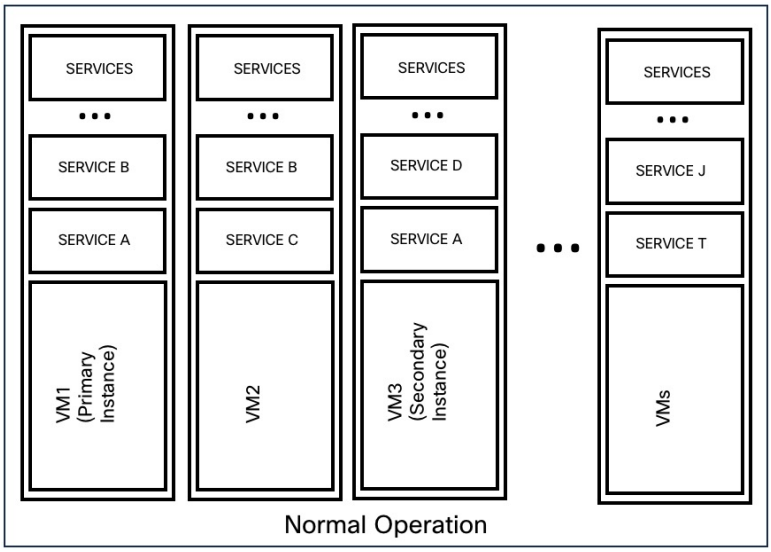
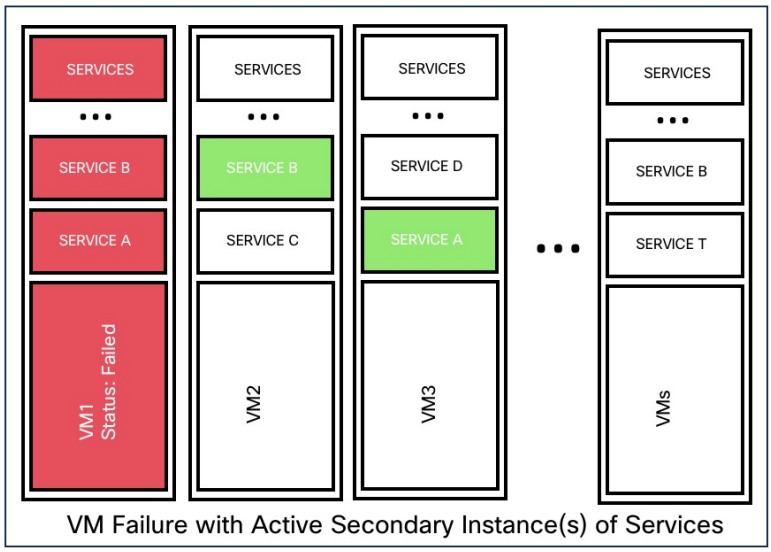


Figure 29: Failure Scenario of a VM



For services provided by symmetric VMs, such as collectordatamovers, datanode, nodemanager, and druidHistoricalBroker VMs, multiple VMs can fail but the applications will continue to function at reduced capacity.

Symmetric VM types:

Service Type	Total VMs	Number of VM Failures Supported
Datanode	6	4
DruidHistorical	4	2

Service Type	Total VMs	Number of VM Failures Supported
CollectorDataMover	6	5
NodeManager	6	4
UI/ AppServer	2	1

The nonsymmetric VM types tolerate only one VM failure before the services are rendered as unavailable.

Impact	No visible impact.
Recovery	• Minimal downtime for the UI or dependent services to continue to run from the secondary instances on other VMs. • Recovery is automatic. However, if a VM remains inactive for a longer duration, contact the TAC team to troubleshoot and find the RCA. You may need to replace the bare metal in a few instances.

Node Failure

Number of node failures tolerated:

Node Failures	8 RU	39 RU
Number of nodes that can fail for high availability	1	1*

* In 39 RU clusters, single node failure is always tolerated. A second node failure may be allowed as long as the two failed nodes do not host VMs for a 2 or 3-VM service, such as orchestrators, redis, mongodb, elasticsearch, enforcementpolicystore, appServer, zookeeper, TSDB, Grafana, and so on. In general, the second node failure results in a critical service becoming unavailable due to two VMs being affected. We recommend that you immediately restore the node upon a single node failure as the failure of a second node will most likely result in an outage.

Figure 30: Normal Operation

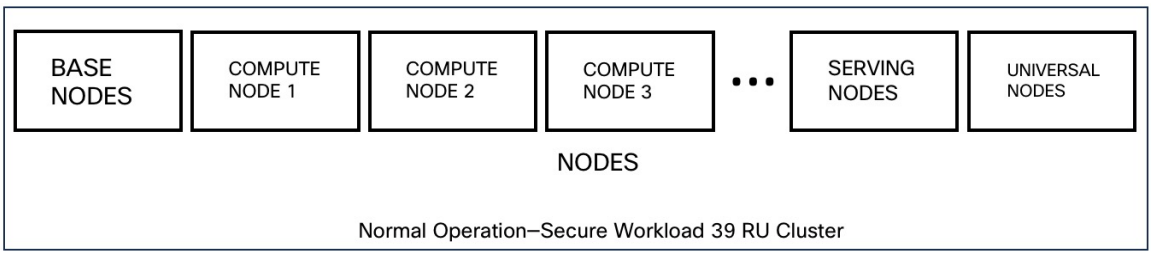
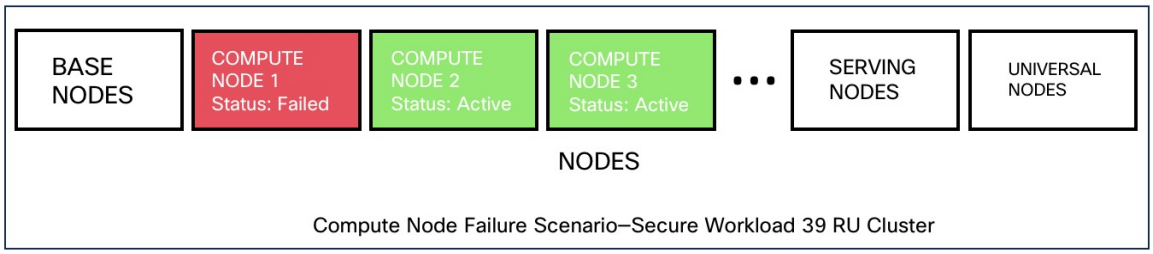


Figure 31: Failure Scenario of a Node



Impact	No impact in the functionality of the cluster. However, replace the failed node immediately using the RMA process. Failure of a second node will most likely result in an outage.
Recovery	• Minimal downtime. • If a node fails, we recommend that you contact Cisco TAC for assistance to remove the faulty node and replace it with another node.

Network Switch Failure

The switches in Secure Workload always remain active. In the 8 RU form factor deployment, there is no impact if a switch fails. In the 39 RU for factor deployment, the clusters experience half the input capacity if a switch fails. The switches do not have the recommended port density to support the VPC configuration for public networks.

Figure 32: Normal Operation

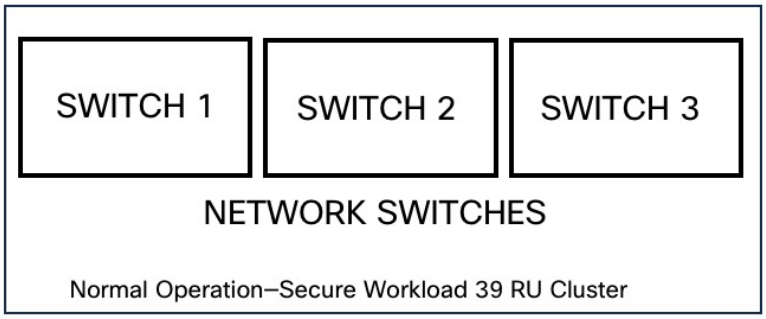
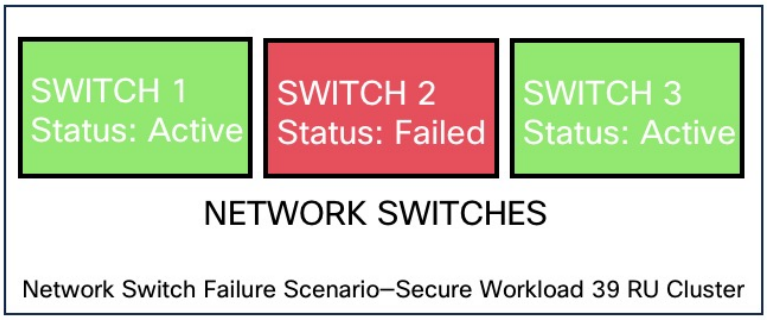


Figure 33: Failure Scenario of a Switch



Number of switch failures tolerated:

Form Factor	**8 RU**	**39 RU**
Number of switches that can fail for high availability	1 If two or more switches fail, it is likely to have an impact on the entire functionality of the cluster.	1* * A single switch failure results in half input capacity, two or more failures will likely impact the entire functionality of the cluster.

Impact	• A faulty switch or network card on a bare metal causes loss of network connectivity within the cluster. • No impact in the functionality of the cluster because of a single switch failure. However, two or more failures will likely impact the entire functionality of the cluster. • Connectivity issues to multiple VMs on the cluster, or intermittent and prolonged connectivity problems result in unpredictable behaviour within the cluster.
Recovery	• Recovery is automatic. • Contact Cisco TAC for assistance in troubleshooting faulty switches or network cards on bare metals.

Renseignements sur la machine virtuelle

La page **Virtual Machine** (Machines virtuelles), sous le menu **Troubleshoot** (Dépannage), affiche toutes les machines virtuelles qui font partie de la grappe Cisco Cisco Secure Workload. Elle affiche leur état de déploiement pendant le démarrage ou la mise à niveau (le cas échéant), ainsi que les adresses IP publiques.

Notez que toutes les machines virtuelles de la grappe ne font pas partie d'un réseau public, par conséquent, elles peuvent ne pas avoir d'adresse IP publique.

Mise à niveau d'une grappe Cisco Secure Workload

Cisco Secure Workload prend en charge deux types de mise à niveau : la mise à niveau complète et la mise à niveau avec correctifs. Les sections suivantes décrivent le processus de mise à niveau complète. Pendant la mise à niveau complète, toutes les machines virtuelles de la grappe sont arrêtées, de nouvelles machines virtuelles sont déployées et les services sont mis en service à nouveau. Toutes les données de la grappe sont conservées pendant cette mise à niveau, à l'exception du temps d'arrêt pendant la mise à niveau.

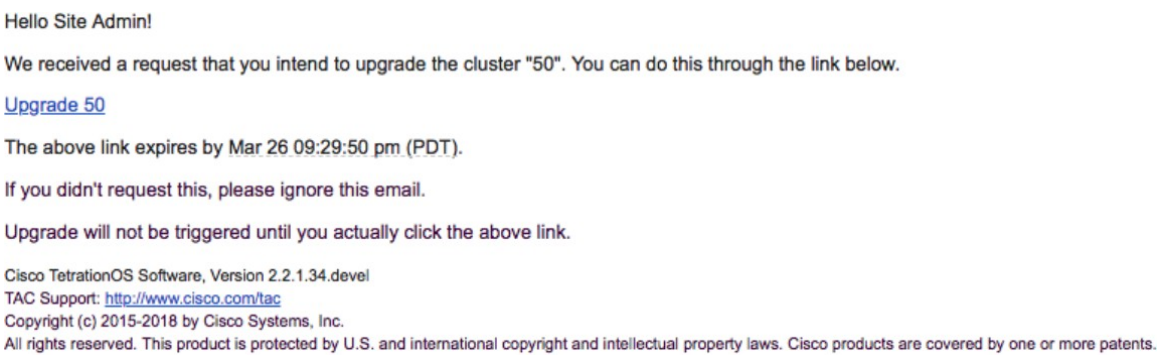
Options de mise à niveau de grappe

Types de mise à niveau prises en charge pour une grappe Cisco Secure Workload :

- **Mise à niveau complète** : pour lancer la mise à niveau complète, dans le volet de navigation, choisissez **Platform(Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)**. Dans l'onglet **Upgrade** (Mettre à niveau) , select **Upgrade** (Mettre à niveau). Pendant le processus de mise à niveau complet, les machines virtuelles sont éteintes, et sont mises à niveau et redéployées. Il se produit un temps d'arrêt de la grappe pendant lequel l'interface utilisateur de Cisco Secure Workload est inaccessible.
- **Mise à niveau des correctifs** : La mise à niveau des correctifs réduit le temps d'arrêt de la grappe. Les services auxquels un correctif doit être appliqué sont mis à jour et n'entraînent pas le redémarrage de la machine virtuelle. Le temps d'arrêt est généralement de l'ordre de quelques minutes. Pour lancer la mise à niveau des correctifs, sélectionnez **Patch Upgrade** (Mise à niveau de correctifs) et cliquez sur **Send Patch Upgrade Link** (Envoyer le lien de mise à niveau des correctifs).

Un courriel contenant un lien est envoyé à l'adresse courriel enregistrée pour lancer la mise à niveau.

Figure 34: Courriel contenant le lien de mise à niveau


Hello Site Admin!

We received a request that you intend to upgrade the cluster "50". You can do this through the link below.

Upgrade 50

The above link expires by Mar 26 09:29:50 pm (PDT).

If you didn't request this, please ignore this email.

Upgrade will not be triggered until you actually click the above link.

Cisco TetrationOS Software, Version 2.2.1.34.devel
TAC Support: http://www.cisco.com/tac
Copyright (c) 2015-2018 by Cisco Systems, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Cisco products are covered by one or more patents.

Avant d'envoyer le courriel, l'orchestrateur exécute plusieurs vérifications pour s'assurer que la grappe peut être mise à niveau. Les vérifications comprennent les actions suivantes :

- Vérifie qu'il n'y a aucun nœud mis hors service.
- Vérifie chaque élément nu pour s'assurer qu'il n'y a aucune défaillance matérielle, notamment des éléments suivants :
    - Défaillance du lecteur

- Défaillance prédictive du lecteur.
- Lecteur manquant
- Échecs de StorCLI
- Échecs des journaux MCE

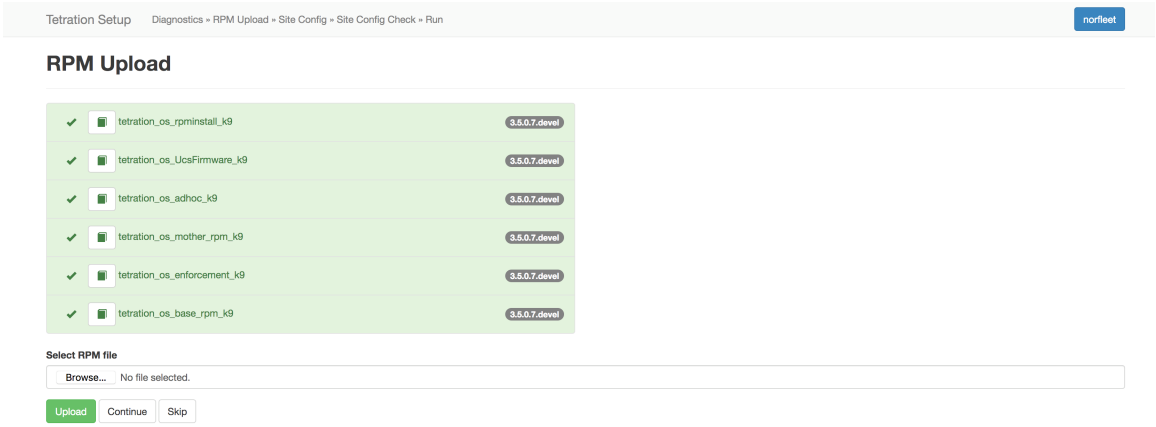
- Effectue des vérifications pour s'assurer que les machines à l'état sans système d'exploitation sont en service, qu(il n'y a pas moins de 36 serveurs pour le 39RU et six pour le 8RU.

Note En cas de défaillance, un lien de mise à niveau n'est pas envoyé à l'adresse courriel enregistrée et une erreur 500 s'affiche avec des informations telles qu'une défaillance matérielle ou un hôte manquant. Vérifiez les journaux de l'orchestrateur pour plus d'informations. Dans ce scénario, utilisez explore jusqu'à -100 sur /local/logs/tetration/orchestrator/orchestrator.log dans le fichier hôte orchestrator.service.consul. Le journal fournit des renseignements détaillés pour déterminer laquelle des trois vérifications est à l'origine de l'échec. Cela nécessite généralement de réparer le matériel et de remettre le nœud en service. Redémarrer le processus de mise à niveau.

RPM Upload

Click on the link in the email will connect to the setup UI in the cluster. Setup UI is a operations UI that will be used for deploy/upgrade of the cluster. The initial page will show the list of RPMs that are currently installed in the cluster. This is also the upload page to upload all the RPMs

Figure 35: RPM Upload



Upload the RPMs in the order that is shown on setup UI. The order is

1. tetration_os_rpminstall_k9
2. tetration_os_UcsFirmware_k9
3. tetration_os_adhoc_k9
4. tetration_os_mother_rpm_k9

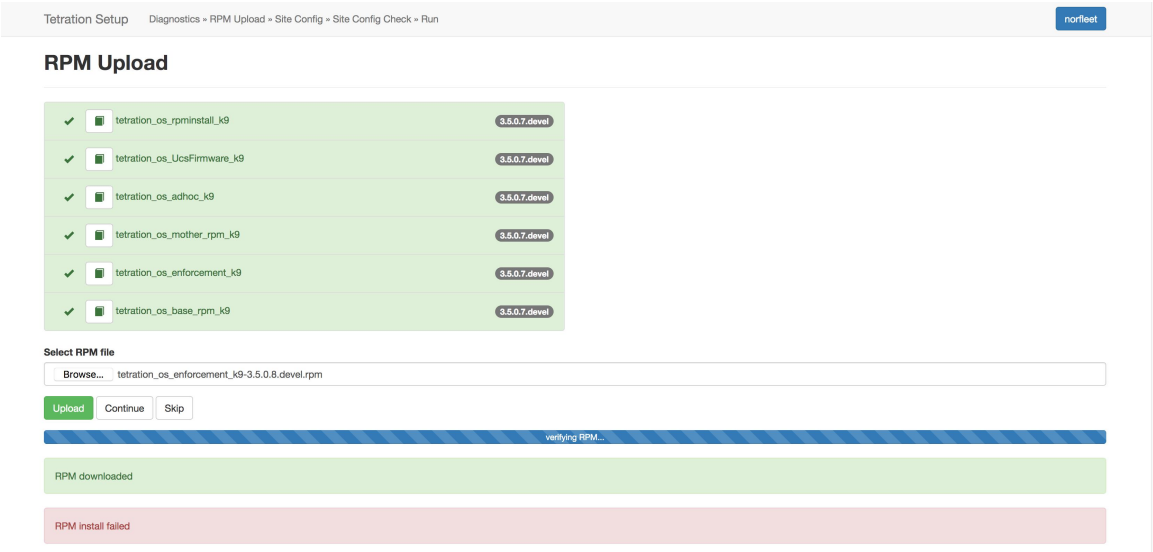
5. tetration_os_enforcement_k9
6. tetration_os_base_rpm_k9

Note For Cisco Secure Workload Virtual clusters deployed on vSphere, please be sure to also upgrade the tetration_os_ova_k9 RPM and do not upload the tetration_os_base_rpm_k9.

Uploading any other order will result in upload failure. Until all the RPMs are uploaded in the correct order Continue button will be disabled.

Logs for each upload can be seen by clicking on the Log symbol on the left of every RPM. Also uploads that failed will be marked RED in color.

Figure 36: RPM Upload log



Informations sur le site

L'étape suivante de la mise à niveau de la grappe consiste à mettre à jour les renseignements du site. Tous les champs de renseignements du site ne peuvent pas être mis à jour. Seuls les champs suivants peuvent être mis à jour :

- Clé publique SSH
- Courriel d'alerte Sentinel (pour Boosun)
- Réseau interne du contrôleur CIMC
- Passerelle de réseau interne du contrôleur CIMC
- Réseau externe

Note Ne modifiez pas le réseau externe existant. Vous pouvez ajouter des réseaux supplémentaires en les ajoutant à ceux existants. La modification ou la suppression du réseau existant rendra la grappe inexploitable.

- résolveurs DNS
- Domaines DNS
- Serveurs NTP
- SMTP Server
- Port SMTP
- Nom d'utilisateur SMTP (facultatif)
- Mot de passe SMTP (facultatif)
- Serveur Syslog (facultatif)
- Port Syslog (facultatif)
- Niveau de gravité Syslog (facultatif)

Note

- La gravité du serveur syslog varie de critique à informatif. La gravité doit être réglée à « avertissement » ou à un niveau supérieur (à titre indicatif) pour les alertes.
- À partir de la version 3.1, **le journal système externe via l'interface utilisateur de configuration n'est pas pris en charge**. Configurez l'appareil TAN pour exporter les données vers SYSLOG. Pour de plus amples renseignements, consultez la section La tunnelisation externe du syslog est déplacée vers le TAN.
- Cisco Secure Workload prend en charge la communication sécurisée SMTP vers les serveurs de messagerie qui prennent en charge la communication SSL ou TLS à l'aide de la commande STARTTLS. Le port standard des serveurs qui prennent en charge le trafic sécurisé est généralement le port 587/TCP, mais de nombreux serveurs acceptent également les communications sécurisées sur le port standard 25/TCP.

  Cisco Secure Workload ne prend pas en charge le protocole SMTPS pour la communication avec les serveurs de messagerie externes.

Les autres champs ne peuvent pas être mis à jour. S'il n'y a aucun changement, cliquez sur **Continue** (Continuer) pour déclencher les vérifications préalables à la mise à niveau, sinon mettez les champs à jour, puis cliquez sur **Continue**.

Vérifications préalables à la mise à niveau

Avant de mettre à niveau la grappe, quelques vérifications sont effectuées sur celle-ci afin de s'assurer que tout est en ordre. Les vérifications préalables à la mise à niveau suivantes sont effectuées :

- Vérifications dans la version du RPM : vérifie pour s'assurer que tous les RPM sont téléversés et que la version est correcte. La vérification ne porte pas sur l'exactitude de la commande, mais sur le fait que la

version a été téléversée. Notez que les vérifications de la commande sont effectuées lors du chargement lui-même.

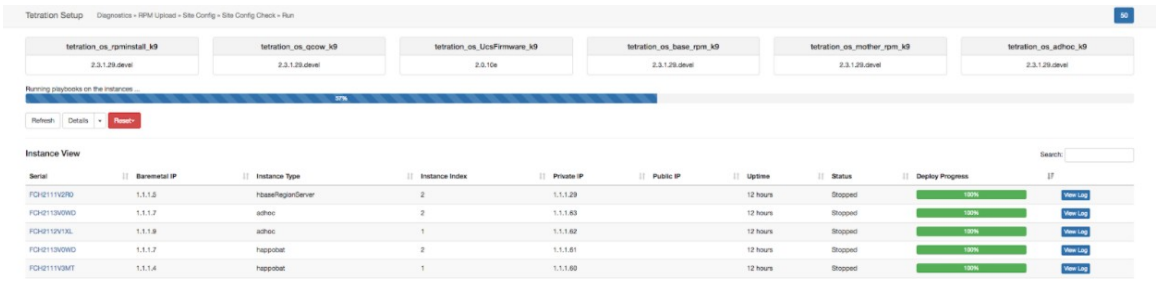
- Site Linter : effectue le linting des informations du site
- Configuration du commutateur : configure les commutateurs Leaves ou Spine
- Vérificateur de site : effectue les vérifications des serveurs DNS, NTP et SMTP. Envoie un courriel avec un jeton. Le courriel est envoyé au compte d'administrateur principal du site. Si l'un des services DNS, NTP ou SMTP n'est pas configuré, cette étape échoue.
- Validation du jeton : saisissez le jeton envoyé dans le courriel et continuez le processus de mise à niveau.

Mettre à niveau la grappe Cisco Secure Workload

Caution

- Nous vous recommandons de ne pas sélectionner l'option **Ignore stop Failures** (Ignorer les échecs d'arrêt). Il s'agit d'une option de récupération en cas d'échec de la mise à niveau lorsque certains services ne se ferment pas correctement. L'utilisation de cette option arrête les machines virtuelles qui peuvent créer des défaillances lorsque les services deviennent actifs.
- Utilisez cette option sous surveillance.

Figure 37: Mise à niveau de la grappe



Before you begin

Effectuez les vérifications préalables à la mise à niveau et saisissez le jeton reçu dans le *courriel de vérification du jeton*.

Procedure

Étape 1 Cliquez sur **Continue** (Continuer) pour commencer la mise à niveau.

Étape 2 (Facultatif) Cliquez sur le nom de la grappe pour afficher les renseignements sur le site.

Les RPM et les versions de Cisco Secure Workload sont affichés. La barre de mise à niveau affiche la progression de cette dernière. Le bleu indique les activités en cours, le vert les activités terminées et le rouge les activités qui ont échoué.

Quatre boutons sont disponibles :

- Refresh (Actualiser) : actualise la page.
- Details (Détails) : Cliquez sur **Details** (Détails) pour afficher les étapes qui ont été effectuées au cours de cette mise à niveau. Cliquez sur la flèche à côté du bouton pour afficher les journaux.
- Reset (Réinitialiser) : il s'agit d'une option pour réinitialiser l'état de l'orchestrateur. Cette option annule la mise à niveau et vous ramène au début. NE PAS L'UTILISER sauf si la mise à niveau a échoué et que quelques minutes se sont écoulées après l'échec de la mise à niveau pour que tous les processus soient terminés avant de redémarrer cette dernière.
- Restart (Redémarrer) : lorsqu'une mise à niveau échoue, cliquez sur **Restart** (Redémarrer) pour redémarrer la grappe et lancer une nouvelle mise à niveau. Cela peut permettre de résoudre les opérations de nettoyage en attente ou les problèmes qui bloquent les processus de mise à niveau.

Dans la vue de l'instance, chaque état de déploiement de machine virtuelle est suivi. Les colonnes comprennent :

- Série : série sans système d'exploitation qui héberge cette machine virtuelle
- IP sans système d'exploitation : l'adresse IP interne attribuée au routeur sans système d'exploitation
- Instance Type : le type de la machine virtuelle
- Index d'instance : index de la machine virtuelle : il existe plusieurs machines virtuelles du même type pour une haute disponibilité.
- Adresse IP privée : l'adresse IP interne attribuée à cette machine virtuelle
- Adresse IP publique : l'adresse IP routable attribuée à cette machine virtuelle. Toutes les machines virtuelles n'en ont pas.
- Disponibilité : temps de disponibilité de la machine virtuelle
- État : peut être Stopped, Deployed, Failed, Not Started ou In Progress (Arrêté, Déployé, Échec, Non démarré ou En cours).
- Avancement du déploiement : pourcentage de déploiement
- View Log (Afficher le journal) : bouton pour afficher l'état de déploiement de la machine virtuelle

Journaux de mise à niveau de grappe

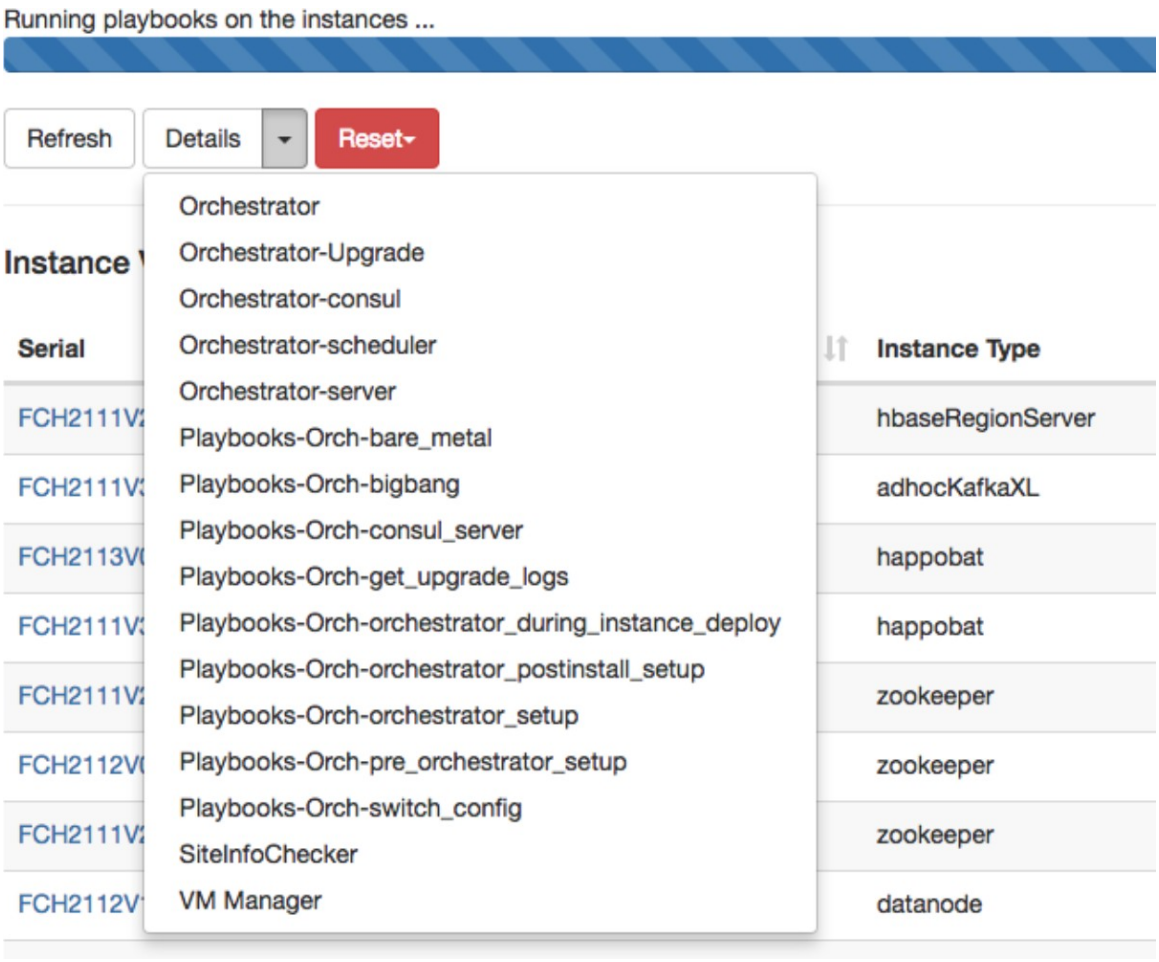
Il existe deux types de journaux :

Procedure

Étape 1 Journaux de déploiement de **machines virtuelles** : cliquez sur **View Log** (Afficher le journal) pour afficher les journaux de déploiement des machines virtuelles.

Étape 2 **Journaux d'orchestration** : Cliquez sur la flèche à côté du bouton **Details** (détails) pour afficher les journaux d'orchestration.

Figure 38: Journaux d'orchestration



Chacun des liens pointe vers les journaux.

- Orchestrateur - Journal de l'orchestrateur - c'est le premier endroit pour suivre la progression. Toute défaillance pointe vers un journal à consulter.
- Mise à niveau d'Orchestrator – non présente dans la version 2.3
- Orchestrator-consul – Journaux de conseil qui s'exécutent sur l'orchestrateur principal.
- Orchestrateur-Planificateur – Journaux du planificateur de machine virtuelle – quelle machine virtuelle a été placée sur quelle machine sans système d'exploitation et le journal de planification.
- Orchestrator-server – Journaux du serveur HTTP de l'orchestrateur.
- Playbooks-* : tous les journaux de guides qui s'exécutent sur l'orchestrateur.

Exécuter des vérifications avant la mise à niveau

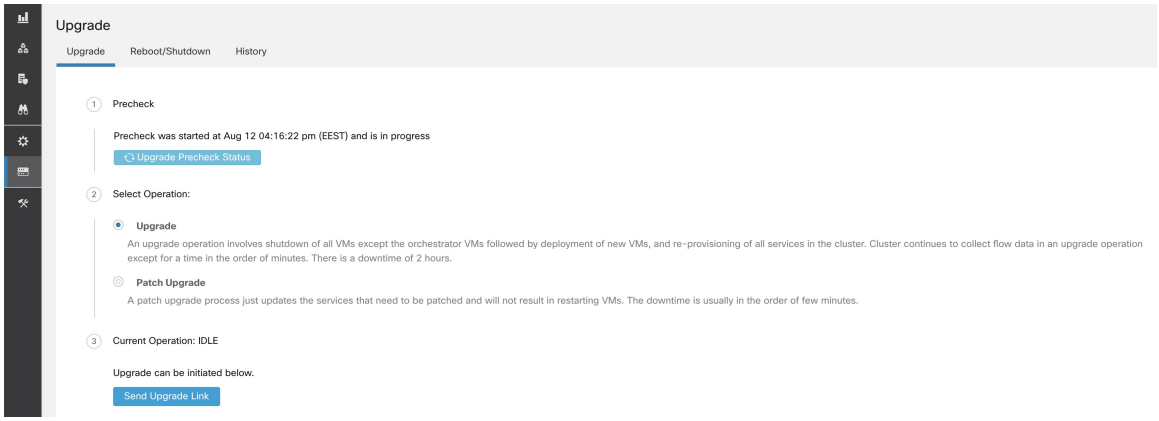
Il peut arriver que des défaillances matérielles se produisent ou que la grappe ne soit pas prête à être mise à niveau après la programmation et le lancement de cette dernière. Ces erreurs doivent être corrigées avant de procéder aux mises à niveau. Au lieu d'attendre une fenêtre de mise à niveau, vous pouvez lancer des vérifications préalables à la mise à niveau, qui peuvent être exécutées autant de fois que vous le souhaitez et à tout moment, sauf lors d'une mise à niveau, d'une mise à jour de correctifs ou d'un redémarrage.

Pour exécuter des vérifications avant la mise à niveau :

1. Dans l'onglet **Upgrade** (Mise à niveau), cliquez sur **Start Upgrade Precheck**(démarrer la vérification préalable à la mise à niveau).

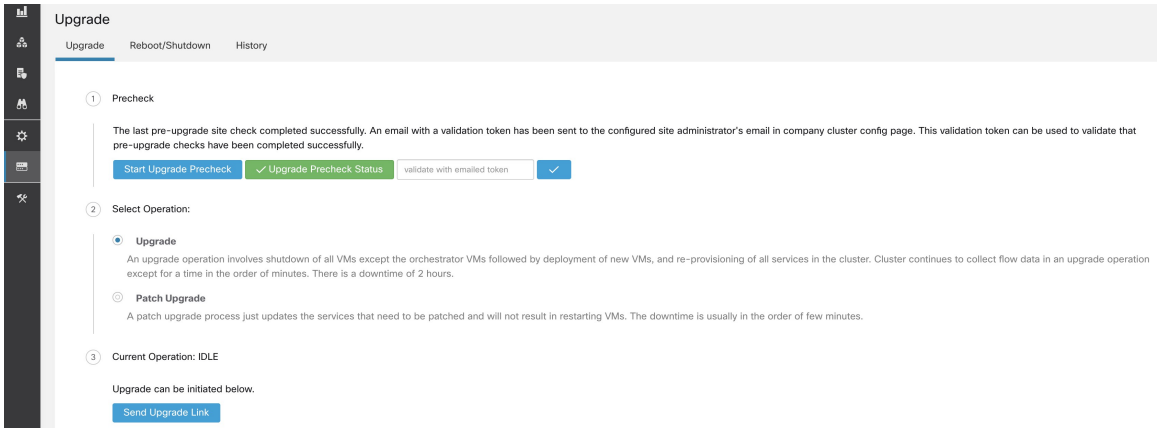
   Cela lance les vérifications préalables à la mise à niveau et passe l'état à En cours d'exécution.

   Figure 39: Exécution des vérifications préalables à la mise à niveau



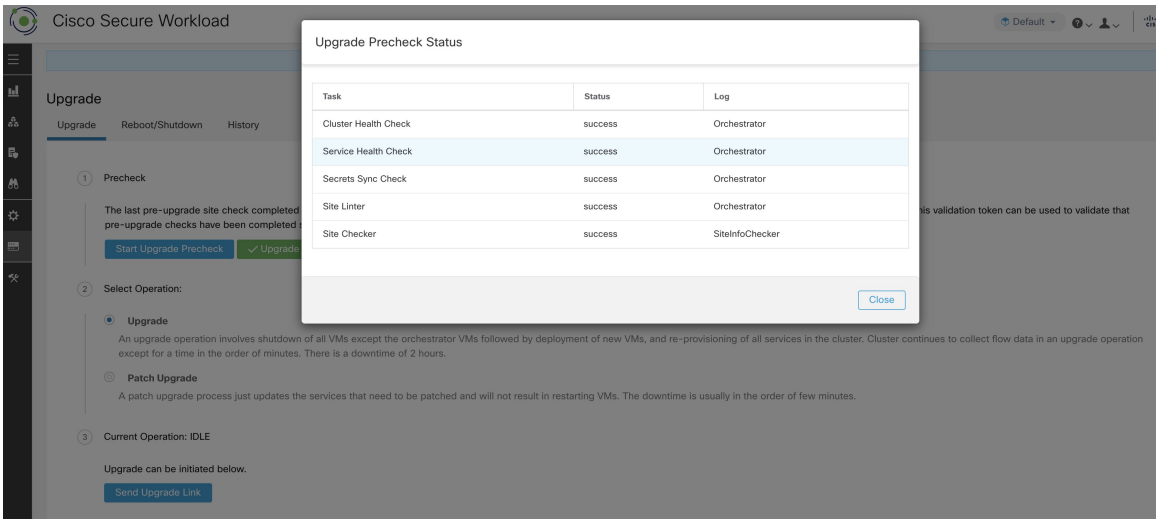
2. Une fois toutes les vérifications exécutées par les orchestrateurs réussies, un courriel avec un jeton est envoyé à l'ID de courriel enregistré. Saisissez le jeton pour terminer les vérifications préalables à la mise à niveau.

   Figure 40: Saisir un jeton pour les vérifications préalables à la mise à niveau



Vous pouvez vérifier l'état des vérifications. En cas d'échec des vérifications préalables à la mise à niveau, vous pouvez visualiser les vérifications qui ont échoué et le passage à l'état d'échec de la vérification concernée.

Figure 41: État des vérifications préalables à la mise à niveau



Sauvegarde et restauration des données (DBR)

Si **DBR** est activé sur la grappe, consultez également Mise à niveau avec la sauvegarde et la restauration des données

Instantanés de grappe Cisco Secure Workload

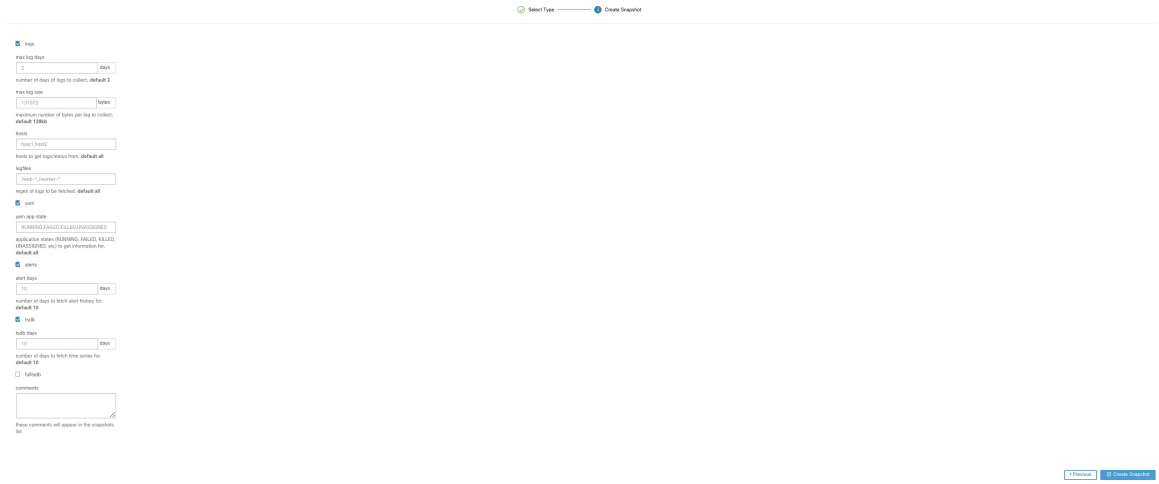
Accès à l'interface utilisateur de création d'instantanés

Les utilisateurs disposant du **rôle de service d'assistance à la clientèle** peuvent accéder à l'outil de capture d'instantanés en sélectionnant **Troubleshooting (Dépannage)** > **Snapshots(Instantanés)** dans la barre de navigation sur le côté gauche de la fenêtre.

Pour créer un instantané classique ou des offres groupées de support technique Cisco Integrated Management Controller (CIMC). Cliquer sur le bouton Create Snapshot (Créer un instantané) dans la page de la liste du fichier Instantané charge une page permettant de choisir un instantané classique ou CIMC (offre groupée de soutien technique). L'option permettant de choisir un instantané CIMC est désactivée sur les Cisco Secure Workload Logiciel uniquement (ESXi) et les logiciels-services Cisco Secure Workload.

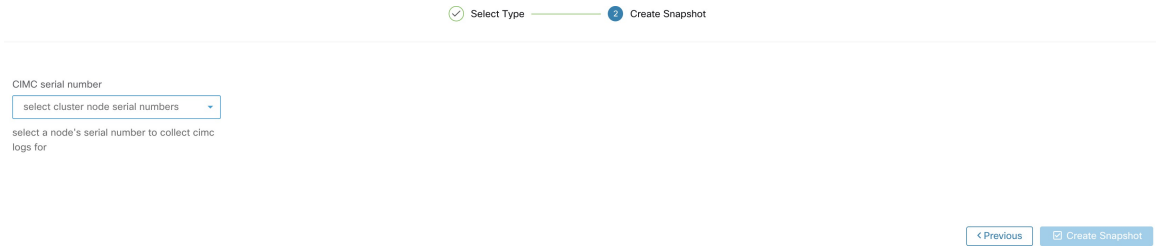
Cliquer sur le bouton d'instantané classique pour charger l'interface utilisateur du programme d'exécution de l'outil Snapshot (Instantané) :

Figure 42: Module d'exécution de l'outil Snapshot (Instantané)



Cliquer sur le bouton CIMC Snapshot (Instantané CIMC) pour charger l'interface utilisateur du programme d'exécution de l'outil de soutien technique de CIMC :

Figure 43: Programme d'exécution de l'outil de l'assistance technique CIMC



Créer un instantané

Sélectionnez **Create Snapshot** (Créer un instantané) avec les options par défaut, l'outil Snapshot recueille :

- Journaux
- L'état de l'application et des journaux Hadoop ou YARN
- L'historique des alertes
- De nombreuses statistiques de la TSDB

Il est possible de remplacer les valeurs par défaut et de préciser certaines options.

- Options du journal
  - max log days : nombre de jours de journaux à collecter, par défaut 2.
  - max log size : nombre maximal d'octets par journal à collecter, 128 Ko par défaut
  - hosts : hôtes pour obtenir les journaux/l'état, par défaut tous.
  - logfiles : expression régulière des journaux à récupérer, tous par défaut.

- options yarn
  - yarn app state ; États de l’application (RUNNING, FAILED, KILLED, UNASSIGNED, etc). pour obtenir des informations, par défaut tous.
- options d’alertes
  - alert days : le nombre de jours de données d’alerte à collecter.
- Options de tsdb
  - tsdb days : le nombre de jours de données tsdb à collecter. Son augmentation peut créer de très gros instantanés.
- Options Fulltsdb
  - fulltsdb : un objet JSON qui peut être utilisé pour spécifier startTime, endTime, FullDumpPath, localDumpFile et NameFilterInclureRegex pour limiter les mesures à collecter.
- comments : commentaires qui peuvent être ajoutés pour décrire la raison et l’entité qui recueille l’instantané.

Après avoir sélectionné Create Snapshot (Créer un instantané), une barre de progression pour l’instantané s’affiche en haut de la page de liste des fichiers d’instantané. Lorsque l’instantané est terminé, il peut être téléchargé à l’aide du bouton Download (Télécharger) sur la page de la liste des fichiers d’instantané. Un seul instantané peut être réalisé à la fois.

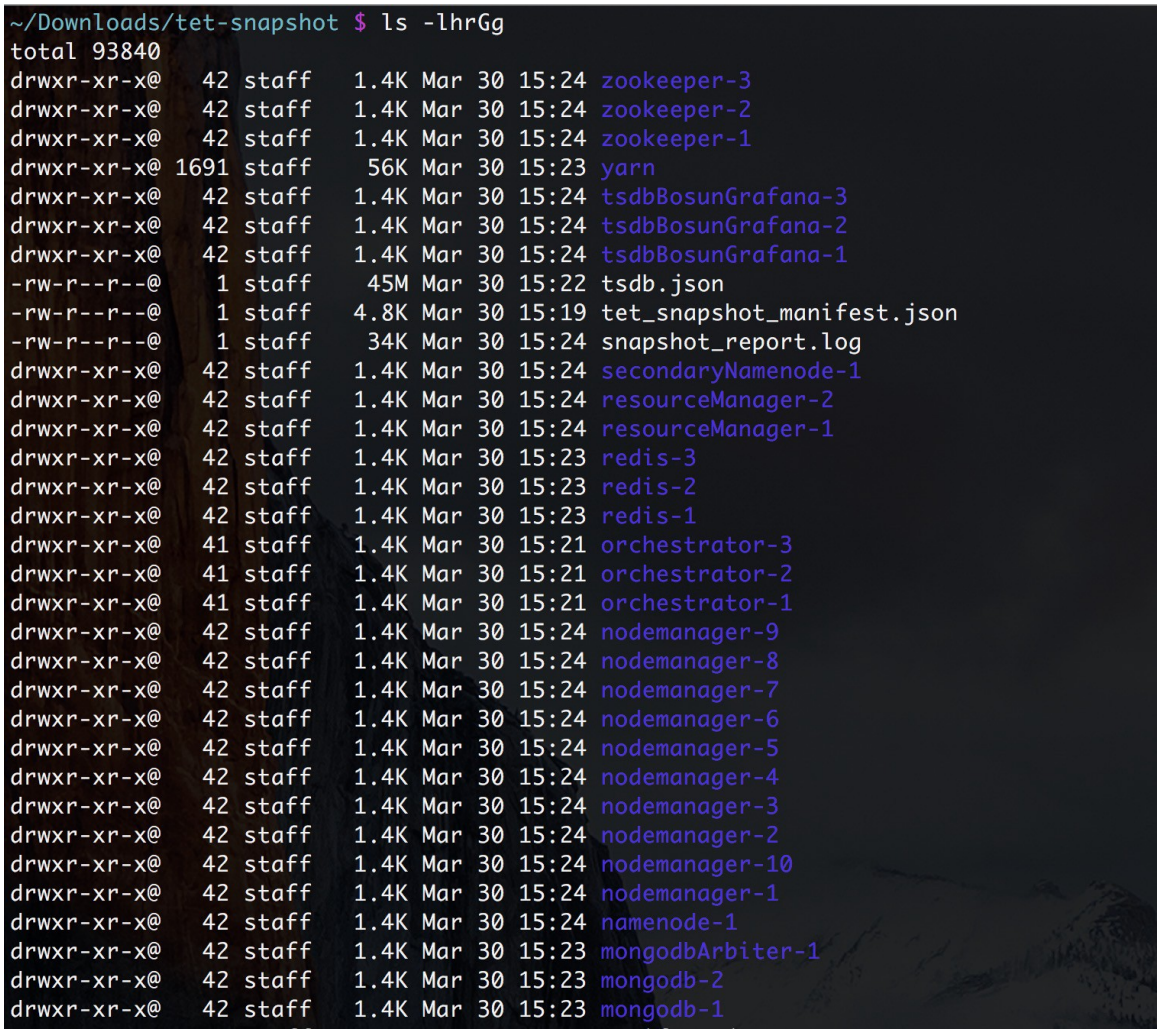
Création d'un ensemble de fichiers de soutien technique du CIMC

Sur la page CIMC Snapshot (Instantané CIMC) (ensemble de soutien technique), sélectionnez le numéro de série du nœud pour lequel l’ensemble de soutien technique CIMC doit être créé et cliquez sur le bouton **Create Snapshot** (Créer un instantané). Une barre de progression pour la collecte de l'ensemble de soutien technique du contrôleur CIMC s’affiche dans la page de liste des fichiers d’instantané et la section des commentaires indique que la collecte de l’ensemble de soutien technique du contrôleur CIMC a été déclenchée. Lorsque la collecte de l’ensemble de soutien technique du contrôleur CIMC est terminée, le fichier peut être téléchargé à partir de la page de liste des fichiers Snapshot Instantanés).

Utilisation d'un instantané

Le traitement d’un instantané crée un répertoire ./clustername_sNAPshot qui contient les journaux pour chaque machine. Les journaux sont enregistrés en tant que fichiers texte qui contiennent les données de plusieurs répertoires des machines. L’instantané enregistre également toutes les données Hadoop/TSDB enregistrées au format JSON.

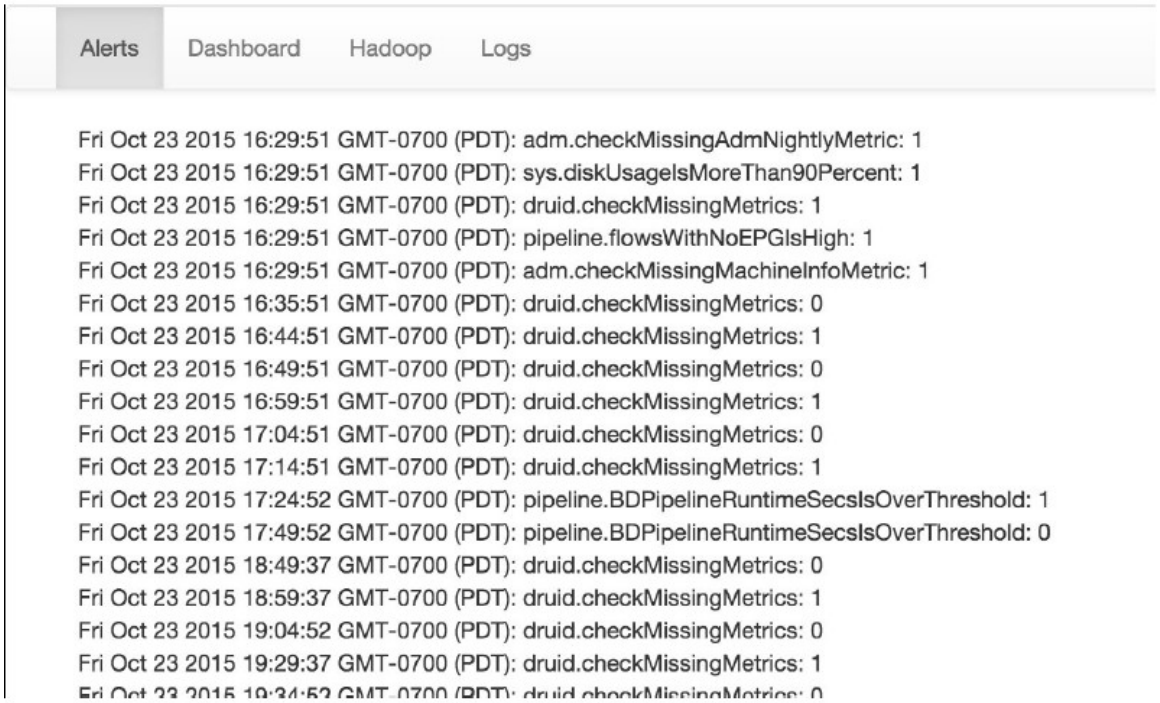
Figure 44: Utilisation d'un instantané



Lorsque vous ouvrez le fichier index.html dans un navigateur, vous trouverez des onglets concernant :

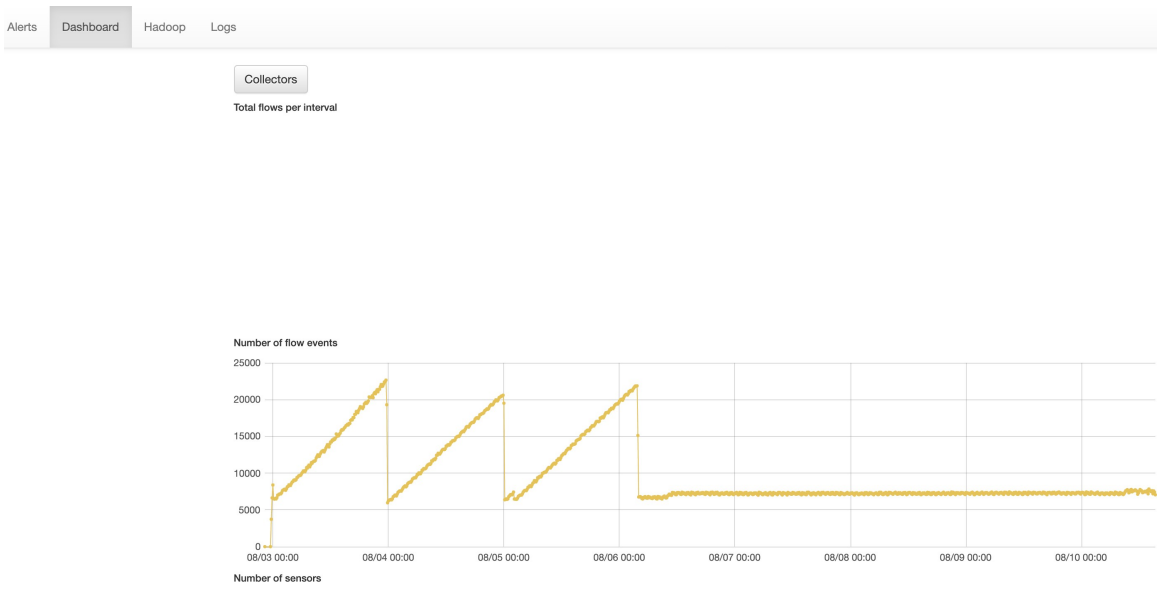
- Liste courte des changements d'état d'alerte.

Figure 45: Liste courte des changements d'état d'alerte



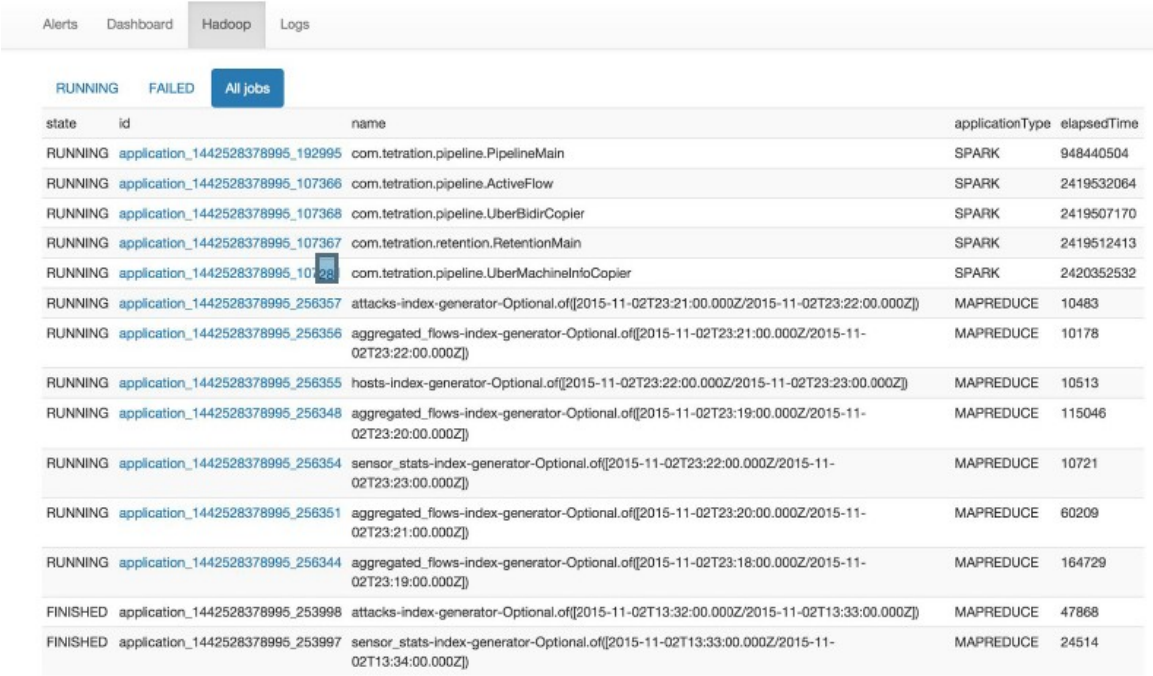
- Reproduction des tableaux de bord Graffana.

Figure 46: Reproduction des tableaux de bord Graffana



- Reproduction du serveur frontal Hadoop Resource Manager qui contient les tâches et leur état. La sélection d'une tâche affiche les journaux de la tâche.

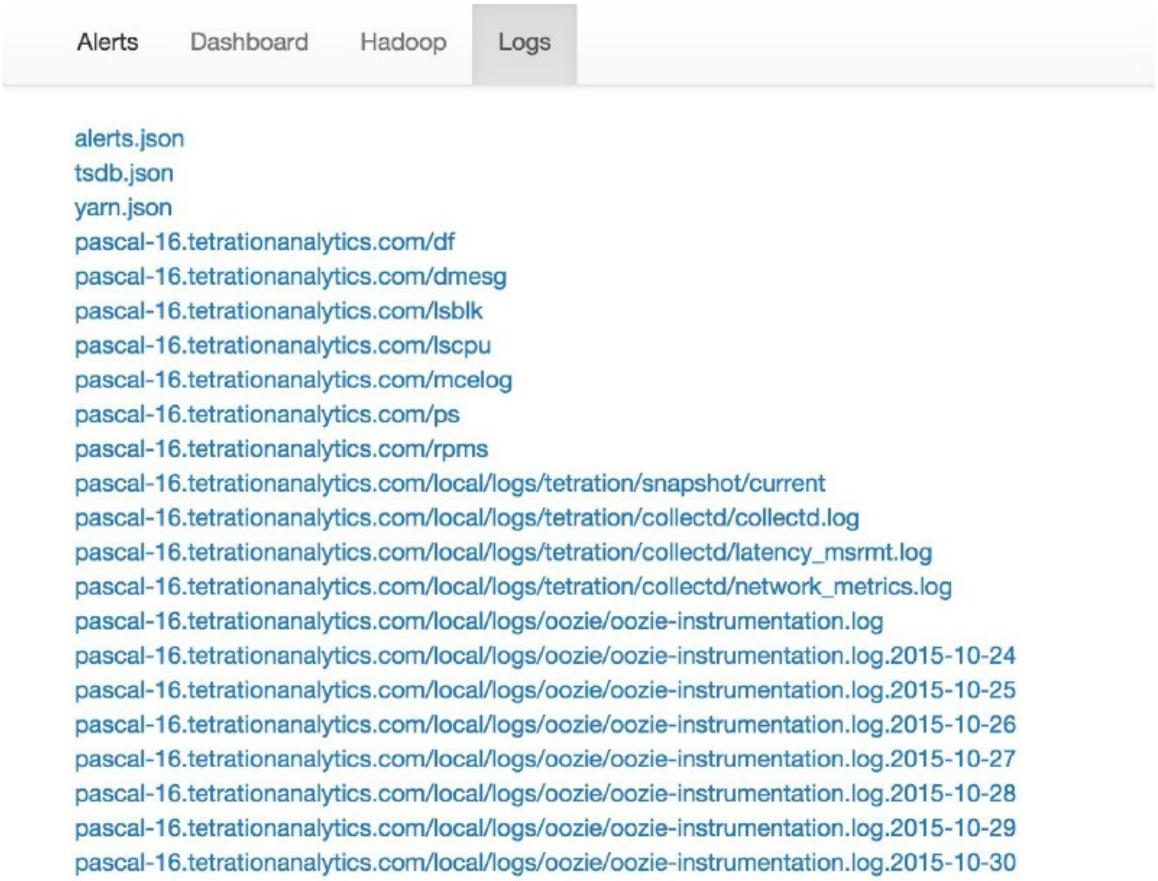
Figure 47: Reproduction du gestionnaire de ressources Hadoop



state	id	name	applicationType	elapsedTime
RUNNING	application_1442528378995_192995	com.tetration.pipeline.PipelineMain	SPARK	948440504
RUNNING	application_1442528378995_107366	com.tetration.pipeline.ActiveFlow	SPARK	2419532064
RUNNING	application_1442528378995_107368	com.tetration.pipeline.UberBidirCopier	SPARK	2419507170
RUNNING	application_1442528378995_107367	com.tetration.retention.RetentionMain	SPARK	2419512413
RUNNING	application_1442528378995_107281	com.tetration.pipeline.UberMachineInfoCopier	SPARK	2420352532
RUNNING	application_1442528378995_256357	attacks-index-generator-Optional.of([2015-11-02T23:21:00.000Z/2015-11-02T23:22:00.000Z])	MAPREDUCE	10483
RUNNING	application_1442528378995_256356	aggregated_flows-index-generator-Optional.of([2015-11-02T23:21:00.000Z/2015-11-02T23:22:00.000Z])	MAPREDUCE	10178
RUNNING	application_1442528378995_256355	hosts-index-generator-Optional.of([2015-11-02T23:22:00.000Z/2015-11-02T23:23:00.000Z])	MAPREDUCE	10513
RUNNING	application_1442528378995_256348	aggregated_flows-index-generator-Optional.of([2015-11-02T23:19:00.000Z/2015-11-02T23:20:00.000Z])	MAPREDUCE	115046
RUNNING	application_1442528378995_256354	sensor_stats-index-generator-Optional.of([2015-11-02T23:22:00.000Z/2015-11-02T23:23:00.000Z])	MAPREDUCE	10721
RUNNING	application_1442528378995_256351	aggregated_flows-index-generator-Optional.of([2015-11-02T23:20:00.000Z/2015-11-02T23:21:00.000Z])	MAPREDUCE	60209
RUNNING	application_1442528378995_256344	aggregated_flows-index-generator-Optional.of([2015-11-02T23:18:00.000Z/2015-11-02T23:19:00.000Z])	MAPREDUCE	164729
FINISHED	application_1442528378995_253998	attacks-index-generator-Optional.of([2015-11-02T13:32:00.000Z/2015-11-02T13:33:00.000Z])	MAPREDUCE	47868
FINISHED	application_1442528378995_253997	sensor_stats-index-generator-Optional.of([2015-11-02T13:33:00.000Z/2015-11-02T13:34:00.000Z])	MAPREDUCE	24514

- Liste de tous les journaux collectés.

Figure 48: Liste des journaux collectés

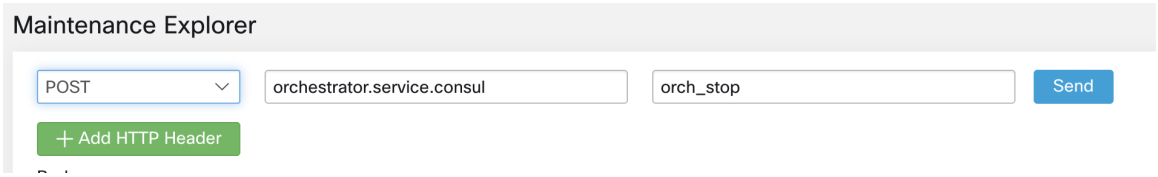


Utilisation du service d'instantané pour le débogage et l'entretien

Le service d’instantané peut être utilisé pour exécuter des commandes de service, mais il nécessite des privilèges de service d'assistance à la clientèle.

À l’aide de l’outil Explore (Explorer) (**Troubleshoot (Dépannage)** > **de l’explorateur de maintenance**), vous pouvez accéder à toute URI au sein de la grappe :

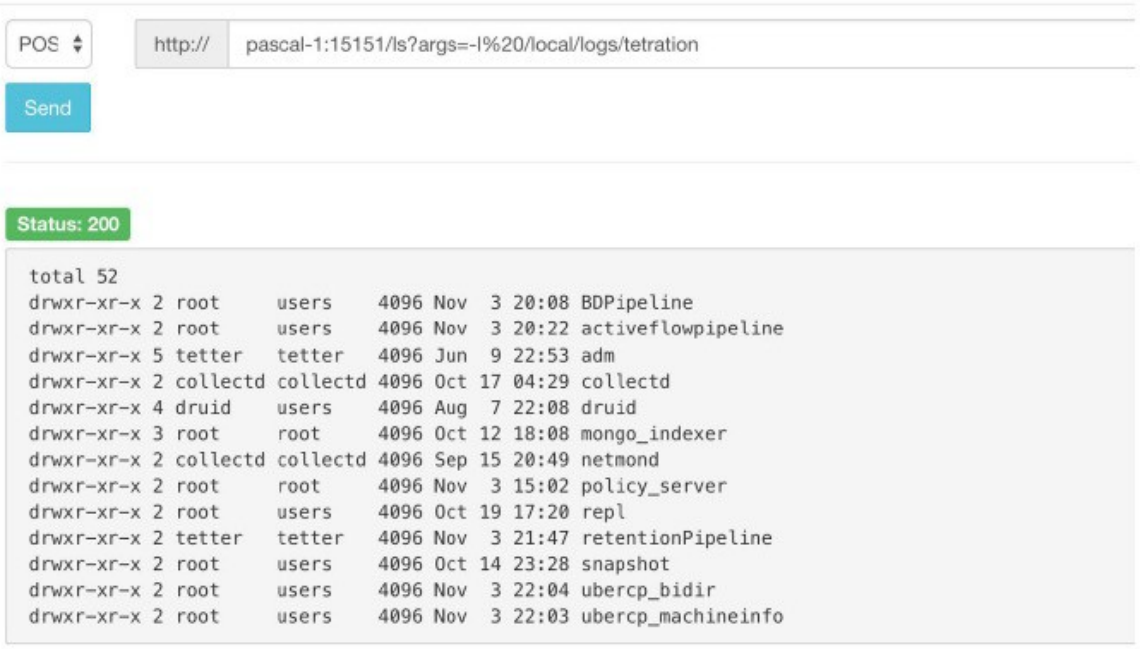
Figure 49: Service Snapshot (Instantané) pour le débogage et la maintenance



L’outil Explore (Explorer) ne s’affiche que pour les utilisateurs disposant de privilèges de service d'assistance à la clientèle.

Le service d’instantané s’exécute sur le port 15151 de chaque nœud. Il écoute uniquement sur le réseau interne (non accessible à l’extérieur) et possède des points terminaux POST pour diverses commandes.

Figure 50: Utilisation du service d'instantané pour le débogage et l'entretien



L'URI que vous devez atteindre est **POST** http://<nom d'hôte> : 15151/<cmd> ?args=<args>, où les arguments sont séparés par des espaces et codés en URI. Il n'exécute **pas** votre commande avec un shell. Cela empêcherait d'exécuter n'importe quelle opération.

Les points terminaux d'un instantané sont définis pour :

- **snapshot 0.2.5**

  –ls

  –**svstatus, svrestart - runs sv status, sv restart** Exemple :1.1.11.15:15151/svrestart?args=snapshot

  –hadoopls runs hadoop fs -ls <args>

  –hadoopdu - runs hadoop fs -du <args>

  Exemple pour **ps** : 1.1.11.31:15151/ps?args=eafux

  –du

  –ambari - runs ambari_service.py

  –monit

  –MegaCli64 (/usr/bin/MegaCli64)

  –service

  Hadoopfsck – exécute Hadoop -fsck

- **snapshot 0.2.6**

  –makecurrent - runs make -C /local/deploy-ansible current

  –netstat

- **snapshot 0.2.7 (exécuté en tant que UID « personne »)**

−cat

−head

queue

grep

−ip -6 neighbor

Adresse IP

−ip neighbor

Il existe un autre point terminal, POST /runsigned, qui exécutera les scripts Shell signés par Cisco Secure Workload. Il exécute gpg -d sur les données faisant l'objet d'un POST. Si cela peut être vérifié par rapport à une signature, le texte chiffré est exécuté dans un shell. Cela signifie l'importation d'une clé publique sur chaque serveur dans le cadre de la configuration d'Ansible et la nécessité de sécuriser la clé privée.

Guide de l'exécution

Les utilisateurs disposant de privilèges d'assistance client peuvent utiliser le répertoire en sélectionnant **Troubleshoot (Dépannage)** > **Maintenance Explorer (Explorateur d'entretien)** dans la barre de navigation dans la partie gauche de la fenêtre. Sélectionnez **POST** dans la liste déroulante. (Sinon, vous recevrez des erreurs Page introuvable lors de l'exécution des commandes).

Utilisation du point terminal REST d'instantané pour redémarrer les services :

- **druid: 1.1.11.17:15151/service?args=supervisord%20restart**
  - −Les hôtes druid ont tous des adresses IP 0.17 à .24; .17, .18 sont les coordonnateurs, .19 est l'indexeur et .20-.24 sont les intermédiaires
- **lanceurs de pipelines Hadoop :**
  - −1.1.11.25:15151/svrestart?args=activeflowpipeline
  - −1.1.11.25:15151/svrestart?args=adm
  - −1.1.11.25:15151/svrestart?args=batchmover_bidir
  - −1.1.11.25:15151/svrestart?args=batchmover_machineinfo
  - −1.1.11.25:15151/svrestart?args=BDPipeline
  - −1.1.11.25:15151/svrestart?args=mongo_indexer
  - −1.1.11.25:15151/svrestart?args=retentionPipeline
- **moteur de politique**
  - −1.1.11.25:15151/svrestart?args=policy_server
- **wss**
  - −1.1.11.47:15151/svrestart?args=wss

Présentation des points terminaux Explore ou Instantané

Pour exécuter un terminal, vous devez vous rendre à la page **Troubleshoot** > **Maintenance Explorer** (Dépannage > Explorateur de maintenance) à partir de la barre de navigation sur le côté gauche de la fenêtre.

Vous pouvez également afficher chaque présentation de chaque point terminal dans la page d'exploration en exécutant une commande **POST** sur n'importe quel hôte, telle que **<end- point>?usage=vrai**.

Par exemple : **makecurrent?usage=vrai**

Commandes get

Point d'accès	Description
bm_details	Affiche les informations sur les composants sans système d'exploitation
points terminaux	Répertorie tous les points terminaux sur l'hôte
members	Affiche la liste actuelle des membres consul, ainsi que leur statut
port2cimc	• Répertorie les adresses IP auxquelles le port est connecté • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
état	Affiche l'état du service d'instantané sur l'hôte
vm_info	• Affiche les informations sur la machine virtuelle de l'emplacement • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécutez le point terminal sous la forme **vm_info?args=<vmname>**

Commandes post

Table 13: Commandes post

Point d'accès	Description
bm_shutdown_or_reboot	• Arrêtez ou redémarrez progressivement un hôte sans système d'exploitation en commençant par arrêter toutes les machines virtuelles sur cet hôte, puis en exécutant une commande d'arrêt ou redémarrage de l'hôte sans système d'exploitation. Vous pouvez également obtenir l'état d'arrêt ou de redémarrage à l'aide de ce point terminal. • Pour obtenir l'état d'arrêt ou de redémarrage d'un nœud, utilisez : `bm_shutdown_or_reboot? query=serial=FCH2308V0FH` • Pour démarrer un arrêt progressif sans système d'exploitation, utilisez : `bm_shutdown_or_reboot? method=POST` et définissez le corps comme un objet JSON qui décrit le numéro de série de l'hôte. Par exemple : `{"serial": "FCH2308V0FH"}` • Pour effectuer un redémarrage progressif des machines sans système d'exploitation, utilisez : `bm_shutdown_or_reboot? method=POST` et définissez le corps comme un objet JSON qui décrit le numéro de série de l'hôte et comprend une clé de redémarrage définie sur « vrai ». Par exemple : `{"serial" : "FCH2308V0FH", "reboot" : vrai}`
cat	Commande d'encapsulation pour la commande *cat* Unix
cimc_password_random	• Rend aléatoire le mot de passe CIMC. • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
cleancmdlogs	Efface les journaux de `/local/logs/tetration/snapshot/cmdlogs/snapshot_cleancmdlogs_log`
clear_sel	• Efface les journaux des événements du système • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**

Point d'accès	Description
cluster_fw_upgrade	• Il s'agit d'une fonctionnalité **bêta** pour cette version. • Exécute une mise à niveau du micrologiciel UCS dans l'ensemble de la grappe. • Une fois cette opération terminée, chaque système sans système d'exploitation doit être redémarré pour activer le BIOS et les micrologiciels des autres composants. • Exécuter sous la forme : **cluster_fw_upgrade** • Ce point terminal lance et surveille la mise à niveau du micrologiciel et met à jour le fichier journal lorsqu'une étape de la mise à niveau a été commencée ou terminée. • Pour obtenir l'état de la mise à niveau, utilisez le point de terminaison **cluster_fw_upgrade_status**.
cluster_fw_upgrade_status	• Il s'agit d'une fonctionnalité **bêta** pour cette version. • Obtenez l'état de la mise à niveau complète du micrologiciel de l'UCS de la grappe. • Exécuter sous la forme **cluster_fw_upgrade_status**
cluster_powerdown	• Met la grappe hors tension. • *À utiliser avec prudence, car la grappe est désactivée*. • Exécutez le point terminal sous la forme `cluster_powerdown?args=-start`.
collector_status	• Affiche l'état du collecteur. • Il doit être exécuté sur les hôtes du collecteur uniquement.
consul_kv_export	• Affiche les paires k-v de cons au format JSON • Doit être exécuté uniquement sur les hôtes de l'orchestrateur.

Point d'accès	Description
consul_kv_recurse	• Affiche les paires k-v de consul sous forme de tableau • Doit être exécuté uniquement sur les hôtes de l'orchestrateur.
df	Commande d'encapsulation pour la commande *df* Unix
dig	Commande d'encapsulation pour la commande *dig* Unix
dmesg	Commande d'encapsulation pour la commande *dmesg* Unix
dmidecode	Commande d'encapsulation pour la commande Unix *dmidecode*
druid_coordinator_v1	Affiche les statistiques du druide.
du	Commande d'encapsulation pour la commande *du* Unix
dusorted	Commande d'encapsulation pour la commande *dusorted* Unix
Externalize_change_tunnel	• Modifie l'adresse IP du collecteur qui sera utilisée pour tunneliser l'interface utilisateur du contrôleur CIMC • Exécuter en tat que : **externalize_change_tunnel?method=POST** • Passer **{"collector_ip" : "<IP>"}** dans le corps • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
externalize_mgmt	• Affiche l'état de l'externalisation de l'interface utilisateur du contrôleur CIMC pour chaque serveur • Affiche l'adresse et le temps restant pour l'externalisation • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**

Point d'accès	Description
externalize_mgmt_read_only_password	• Modifie le mot de passe en lecture seule (ta_guest) pour le commutateur et l'interface utilisateur du contrôleur CIMC • Ne change que lorsqu'ils sont extériorisés. • Exécuter sous la forme : **externalize_mgmt_read_only_password?method=POST** • Passer **{"password" : "<password>"}** dans le corps • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
fsck	• Commande d'encapsulation pour la commande *fsck* Unix • Doit être exécuté uniquement sur **l'hôte sans système d'exploitation**
get_cimc_techsupport	• Saisissez l'adresse IP interne de la machine sans système d'exploitation. • Récupère l'offre groupée de soutien technique du contrôleur CIMC. • Une fois la commande achevée, le résultat peut être téléchargé à partir de la page des instantanés de l'interface utilisateur. • Elle peut être exécutée à partir de n'importe quel hôte de la grappe et nécessite l'adresse IP interne sans système d'exploitation comme argument. • Exemple : **get_cimc_techsupport?args=1.1.0.9**
syslog_endpoints	• Contrôle les configurations syslog pour un ou plusieurs serveurs UCS. • Exécutez la commande accompagnée de *-h* pour obtenir une liste complète des paramètres.
grep	Commande d'encapsulation pour la commande Unix *grep*
hadoopbalancer	• Distribue les données HDFS uniformément sur tous les nœuds • Doit être exécuté sur **des hôtes dotés de HDFS**. Par exemple, hôte de lancement

Point d'accès	Description
hadoopdu	• Imprime l'utilisation de répertoire de HDFS • Elle doit être exécutée sur **des hôtes dotés de HDFS**. Par exemple, hôte de lancement
hadoopfsck	• Exécute Hadoop fsck et signale l'état du système de fichiers HDFS fourni • Elle utilise également « -delete » (supprimer) comme argument pour effacer les blocs corrompus ou manquants. • Avant de supprimer, assurez-vous que tous les DataNodes sont actifs, sinon vous pourriez perdre des données • Doit être exécuté sur les hôtes de lancement uniquement. • Pour rapporter l'état qui est exécuté comme : `hadoopfsck?args=/raw` • Pour supprimer les fichiers corrompus, exécutez-la sous la forme : `hadoopfsck?args=/raw -delete`
hadoopls	• Répertorie le système de fichiers Hadoop • Doit être exécuté sur **des hôtes qui comportent HDFS**, par exemple l'hôte de lancement.
hbasehbck	• Vérifie les problèmes de cohérence et d'intégrité des tableaux et la réparation d'une HBase endommagée • Doit être exécuté **uniquement sur les hôtes HBase** • Pour identifier une incohérence, exécutez-la sous la forme : `hbasehbck?args=-details` • Pour réparer une HBase endommagée, exécutez-la sous la forme : `hbasehbck?args=-repair` • Le résultat figure dans /local/logs/tetration/snapshot/crondlogs/snapshot_hbasehbck_log.txt • *Réparez avec prudence*

Point d'accès	Description
hdfs_safe_state_recover	• Supprime HDFS de l'état sans échec • Requis si HDFS est en READ_ONLY_STATE (ÉTAT EN LECTURE) en raison de la capacité complète et que de l'espace a été libéré • Doit être exécuté sur les **hôtes de lancement uniquement** • Exécuter sous la forme : **hadoopfs-rm'{{ hdfs_safe_state_marker_location }}/HDFS_READ_ONLY'**
initctl	Commande d'encapsulation pour la commande *initctl* Unix
head	Commande d'encapsulation pour la commande *head* Unix
internal_haproxy_status	• Imprime l'état et les statistiques internes haproxy • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
ip	Commande d'encapsulation pour la commande *ip* Unix
ipmifru	• Imprime des informations sur les unités remplaçables sur site (FRU) • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
ipmilan	• Imprime la configuration du réseau local. • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
ipmisel	• Imprime les entrées du journal des événements du système (SEL) • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
ipmisensorlist	• Imprime les informations du capteur IPMI • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
jstack	Imprime les traces de pile des threads (unités d'exécution) Java pour un processus Java ou un fichier central donné.

Point d'accès	Description
ls	Commande d'encapsulation pour la commande *ls* Unix
lshw	Commande d'encapsulation pour la commande *lshw* Unix
lsof	Commande d'encapsulation pour la commande *lsof* Unix
lvdisplay	Commande d'encapsulation pour la commande *lvdisplay* Unix
lvs	Commande d'encapsulation pour la commande *lvs* Unix
lvscan	Commande d'encapsulation pour la commande *lvscan* Unix
makecurrent	• Réinitialise ou accélère le pipeline qui traite le marqueur en fonction des horodatages actuels. • Doit être exécuté sur les **nœuds de l'orchestrateur uniquement** • Exécutez le point terminal en tant que **makecurrent?args=–start**
mongo_rs_status	• Affiche l'état de la duplication mongo • Doit être exécuté sur les hôtes **mongodb ou enforcementpolicystore**
mongo_stats	• Affiche les statistiques mongo • Doit être exécuté sur les hôtes **mongodb ou enforcementpolicystore**
mongodump	• Vide les collectes de la base de données • Doit être exécuté sur les hôtes **mongodb ou enforcementpolicystore** • Exécuter sous la forme : mongodump?args=<collection>[–db DB]
monit	Commande d'encapsulation pour la commande de *monit* Unix
namenode_jmx	Affiche les métriques jmx du nœud de nom principal

Point d'accès	Description
namenode_checkpoint	La vérification a lieu toutes les heures sur le nœud de nom en veille. Si `Namenode-1` ou `Secondarynamenode-1`est en panne pour maintenance pendant une longue période, l'état de service `NN_checkpoint` affiche **UNHEALTHY** (NON INTÈGRE). Une vérification manuelle est nécessaire pour effacer cette condition. Exécutez le POST `Namenode_checkpoint` sur le `launcherHost-1` (ou tout autre `launcherHost` en cours d'exécution). **Note** Si un point de reprise n'est pas effectué régulièrement, les journaux de modification maintenus par le service **journalnode** exécuté dans les instances de Zookeeper ne sont pas purgés et le disque risque d'être saturé.
namenode_failover	Avant d'exécuter **UPGRADE** (METTRE À NIVEAU) ou **REBOOT** (REDÉMARRER), assurez-vous d'exécuter la vérification préalable à la mise à niveau. Si le service `Namenode` n'est pas en cours d'exécution, vous pouvez rencontrer une erreur de vérification de l'intégrité du service avec le message suivant : « `Failed: (Namenode service on NN-1/check) namenode.service.consul and namenode-1.node.consul resolve differently.` (Échec : (Service Namenode sur NN-1/check) namenode.service.consul et namenode-1.node.consul se résolvent différemment). »
namenodeha_get_details	Affiche l'état actuel **ACTIVE** (ACTIF) ou **STANDBY** (VEILLE) pour chaque instance de `namenode` (nom de nœud). Si le service d'instance est en panne ou si le service `namenode` n'est pas en cours d'exécution sur l'instance, l'état affiche **DOWN** (EN PANNE).
ndisc6	Commande d'encapsulation pour la commande *ndisc6* Unix
netstat	Commande d'encapsulation pour la commande *netstat* Unix
ntpq	Commande d'encapsulation pour la commande *ntpq* Unix

Point d'accès	Description
orch_reset	• Réinitialise l'état de l'orchestrateur à IDLE (INACTIF) • Exécuter après un échec de mise en service ou de désactivation • Doit être exécuté sur l'**hôte orchestrator.service.consul uniquement** • **N'utilisez pas cette commande sans consulter le service d'assistance à la clientèle**
orch_stop	• Arrête l'orchestrateur principal et déclenche un basculement • Doit être exécuté sur l'**hôte orchestrator.service.consul uniquement** • **UTILISER AVEC PRÉCAUTION**
ping	Commande d'encapsulation pour la commande *ping* Unix
ping6	Commande d'encapsulation pour la commande *ping6* Unix
ps	Commande d'encapsulation pour la commande *ps* Unix
pv	Commande d'encapsulation pour la commande *pv* Unix
pvs	Commande d'encapsulation pour la commande *pvs* Unix
pvdisplay	Commande d'encapsulation pour la commande *pvdisplay* Unix
rdisc6	Commande d'encapsulation pour la commande *rdisc6* Unix
rebootnode	• Redémarre le nœud • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
recover_rpmdb	• Récupère un RPMDB endommagé sur un nœud • Peut être exécuté sur des machines sans système d'exploitation ou des machines virtuelles

Point d'accès	Description
recoverhbase	• Récupère le service HBase et TSDB • Doit être exécuté sur **les hôtes de l'orchestrateur uniquement** • Doit être exécuté lorsque HDFS est à l'état intègre
recovervm	• Essayer de récupérer la machine virtuelle via la commande stop/fsck/start • Doit être exécuté sur **les hôtes de l'orchestrateur uniquement** • Exécutez le point terminal ainsi **recovervm?args=<vmname>**
restartservices	• Arrête et démarre tous les services non liés à l'interface utilisateur • Doit être exécuté sur l'**hôte orchestrator.service.consul uniquement** • **UTILISER AVEC PRÉCAUTION** • Exécutez le point terminal sous la forme **restartservices?args=–start**
runsigned	• Exécute le script signé fourni par Cisco • Suivez les étapes fournies dans les instructions relatives au script
service	Commande d'encapsulation pour la commande de *service* Unix
smartctl	• Exécutez l'exécutable smartctl • Ne doit être exécuté que sur un nœud sans système d'exploitation
storcli	Commande d'encapsulation pour la commande *storcli* Unix
sudocat	Emballage pour la commande *cat* qui fonctionne uniquement sous /var/log ou /local/logs
sudogrep	Commande d'encapsulation pour la commande *grep* qui fonctionne uniquement sous /var/log ou /local/logs

Point d'accès	Description
sudohead	Commande d'encapsulation pour la commande « head » qui fonctionne uniquement sous /var/log ou /local/logs
sudols	Commande d'encapsulation pour la commande « ls » qui fonctionne uniquement sous /var/log ou /local/logs
sudotail	Commande d'encapsulation pour la commande « tail » qui fonctionne uniquement sous /var/log ou /local/logs
sudozgrep	Commande d'encapsulation pour la commande « zgrep » qui fonctionne uniquement sous /var/log ou /local/logs
sudozcat	Commande d'encapsulation pour la commande « zcat » qui fonctionne uniquement sous /var/log ou /local/logs
svrestart	Redémarre le service saisi. Exécutez la commande sous la forme `svrestart?args=<servicename>`
svstatus	Imprime l'état du service saisi, exécutez-le sous la forme `svstatus?args=<servicename>`
switchinfo	Obtenir des renseignements sur les commutateurs de la grappe.
switch_namenode	• Basculement manuel du nœud désigné par le nom du nœud principal ou secondaire • Doit être exécuté sur l'hôte **orchestrator.service.consul** uniquement • Exécuter lors de la remise en service ou de la désactivation des hôtes de nœud de nom • Exécutez le point terminal sous la forme **switch_namenode?args=--start**
switch_secondarynamenode	• Basculement manuel du nœud désigné par le nom secondaire du nœud secondaire au nœud principal • Doit être exécuté sur l'hôte **orchestrator.service.consul** uniquement • Exécuter lors de la remise en service ou de la désactivation des hôtes de nœud de nom • Exécuter le point terminal sous la forme **switch_secondarynamenode?args=--start**

Point d'accès	Description
switch_yarn	• Basculement manuel du gestionnaire de ressources à partir du serveur principal ou secondaire, ou inversement • Doit être exécuté sur l'**hôte orchestrator.service.consul uniquement** • Exécuter lors de la désactivation ou de la désactivation des hôtes du gestionnaire de ressources • Exécuter le point terminal sous la forme **switch_yarn?args=–start**
tail	Commande d'encapsulation pour la commande *tail* Unix
toggle_chassis_locator	• Activez ou désactivez un localisateur de châssis sur une base physique sans système d'exploitation spécifiée par le numéro de série du nœud. • Exécuté à partir de n'importe quel nœud sous la forme : **toggle_chassis_locator?method=POST** • Définissez dans le corps du texte un objet JSON qui décrit le numéro de série de l'hôte (un seul numéro de série à la fois est pris en charge), par exemple : **{"serials": ["FCH2308V0FH"]}**
tnp_agent_logs	• Créer un instantané de tous les fichiers journaux fournis par les agents de l'équilibreur de charge enregistrés en tant qu'orchestrateurs externes • Doit être exécuté sur les hôtes du serveur de lancement
tnp_datastream	• Créer un instantané avec les données de flux de politique utilisées par les agents d'application de la politique de l'équilibreur de charge enregistrés en tant qu'orchestrateurs externes • Doit être exécuté sur les hôtes de l'orchestrateur • Pour télécharger les données de flux d'état des politiques, exécutez le point terminal sous la forme **tnp_datastream?args=–ds_type datasink**
ui_haproxy_status	Imprime les statistiques et l'état haproxy pour l'haproxy externe

Point d'accès	Description
uptime	Commande d'encapsulation pour la commande *uptime* Unix
userapps_kill	• Arrête toutes les applications utilisateur en cours d'exécution • Doit être exécuté **uniquement sur les hôtes du lanceur**
vgdisplay	Commande d'encapsulation pour la commande *vgdisplay* Unix
vgs	Commande d'encapsulation pour la commande *vgs* Unix
vmfs	• Répertorie le système de fichiers sur une machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vmfs?args=<vmname>**
vminfo	• Imprime les informations de la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vminfo?args=<vmname>**
vmlist	• Listes de toutes les machines virtuelles sur un système sans système d'exploitation • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point de terminaison sous la forme **vmlist?args=<vmname>**
vmreboot	• Redémarre la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vmreboot?args=<vmname>**

Point d'accès	Description
vmshutdown	• Arrêter progressivement la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sus la forme **vmshutdown?args=<vmname>**
vmstart	• Démarre la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vmstart?args=<vmname>**
vmstop	• Forcer l'arrêt de la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vmstop?args=<vmname>**
yarnkill	• Arrête une application Yarn en cours d'exécution • Doit être exécuté **uniquement sur les hôtes du lanceur** • Exécuter le point terminal sous la forme **yarnkill?args=<application id>** • Pour arrêter toutes les applications, exécutez-le sous la forme **yarnkill?args=ALL**
yarnlogs	• Vide les 500 derniers Mo de journaux d'application yarn • Doit être exécuté **uniquement sur les hôtes du lanceur** • Exécuter le point terminal sous la forme **yarnlogs?args=<application id> <job user>**
zcat	Commande d'encapsulation pour la commande *zcat* Unix
zgrep	Commande d'encapsulation pour la commande *zgrep* Unix

Entretien du serveur

L'entretien du serveur implique le remplacement de tout composant défectueux, comme le disque dur, la mémoire ou le remplacement du serveur lui-même.

Note Si plusieurs serveurs de la grappe ont besoin d'être maintenus, procédez à leur entretien l'un après l'autre. La désactivation de plusieurs serveurs en même temps peut entraîner une perte de données.

Pour effectuer toutes les étapes de l'entretien d'un serveur, dans le volet de navigation, choisissez **Troubleshoot (Dépannage)** > **Cluster Status(État de la grappe)** . Tous les utilisateurs y accèdent, mais les actions peuvent être effectuées par les utilisateurs du **service d'assistance à la clientèle** uniquement. Il affiche l'état de tous les serveurs physiques du support Cisco Cisco Secure Workload.

Figure 51: Entretien du serveur

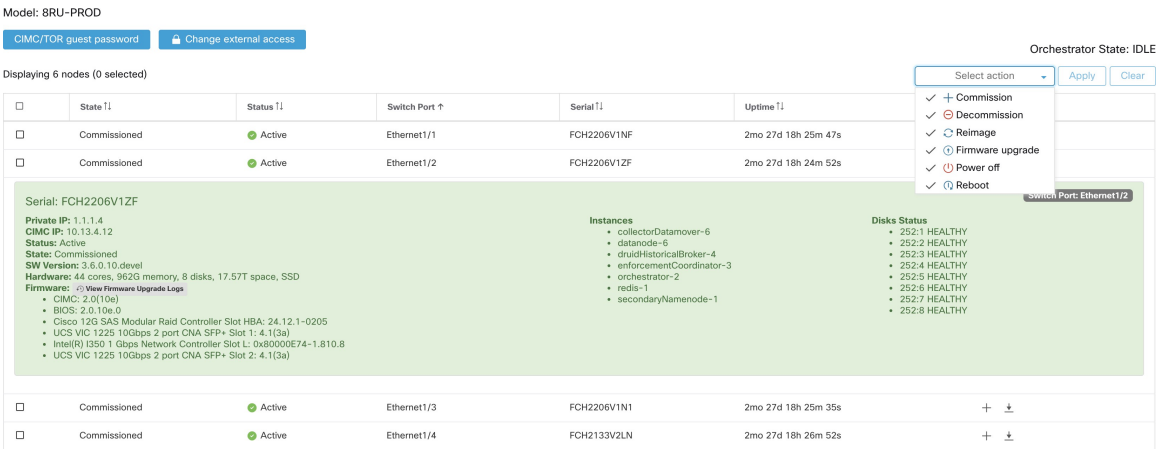
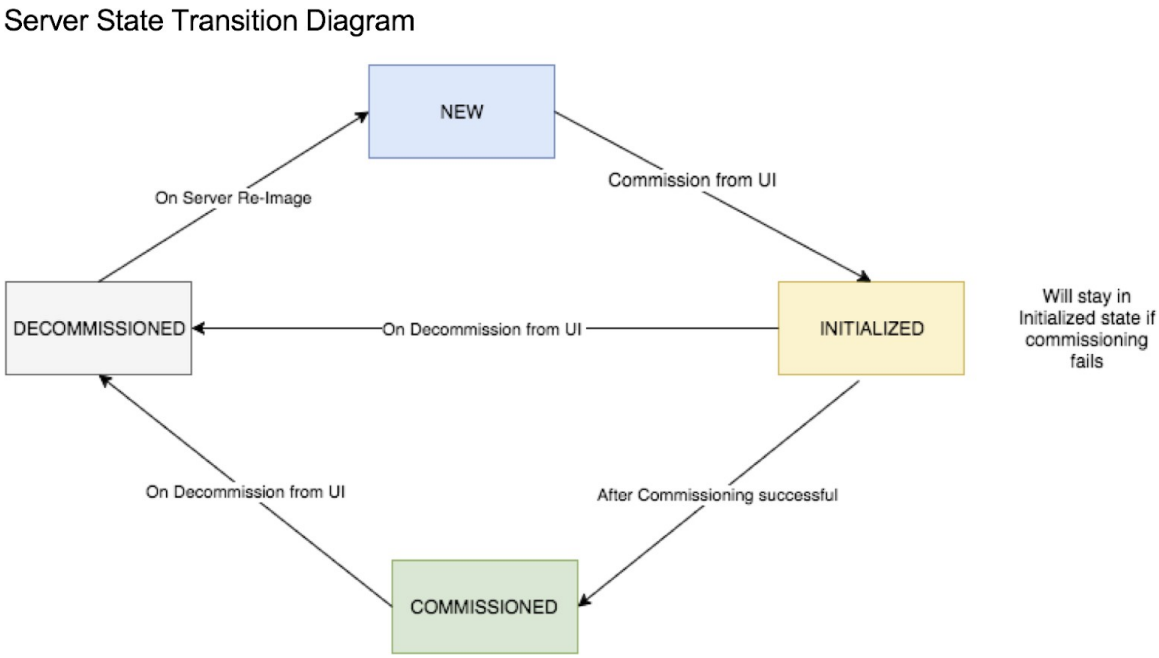


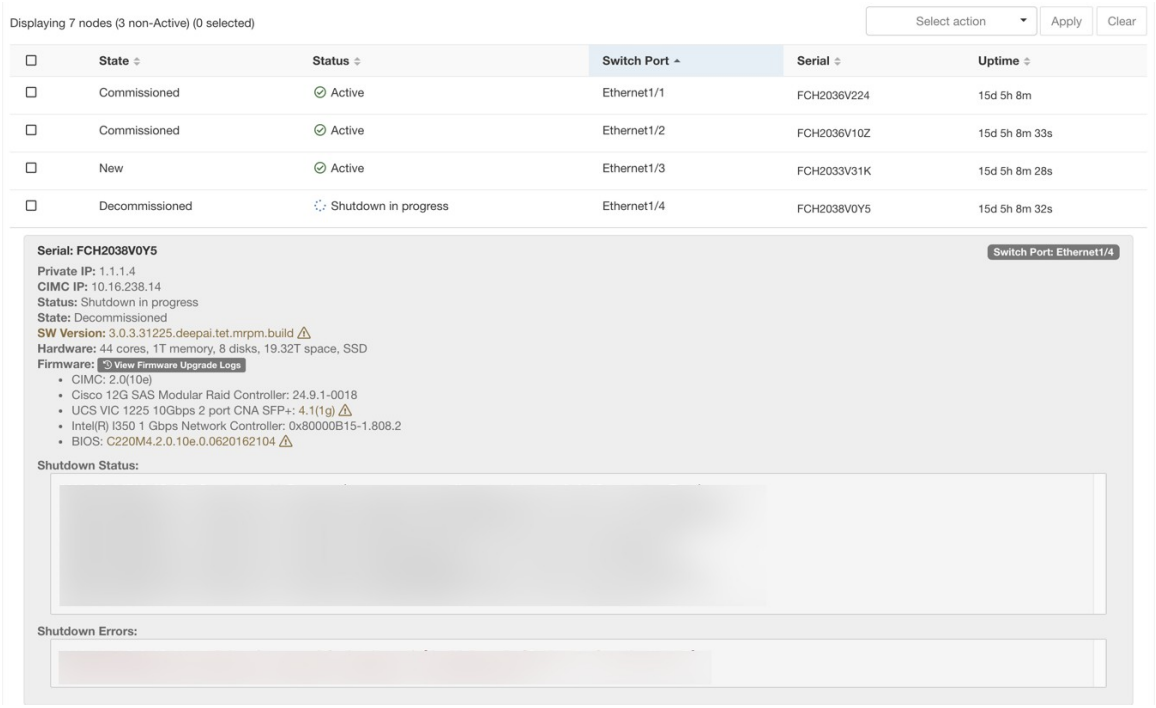
Figure 52: Diagramme de transition d'état du serveur



Étapes nécessaires pour remplacer un serveur ou un composant

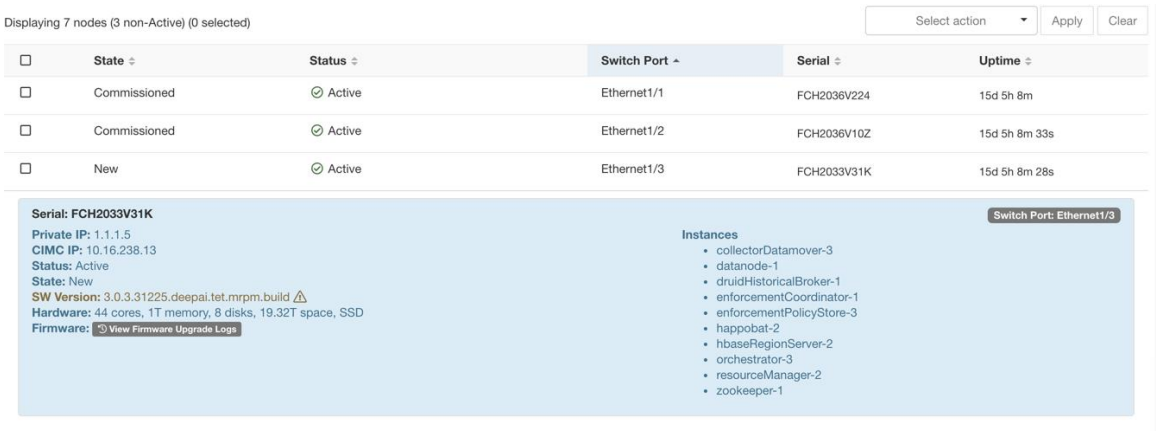
- **Déterminer le serveur qui nécessite une maintenance** : cela peut être fait en utilisant le numéro de *série* du serveur ou le *port de commutation* auquel le serveur est connecté, dans la page *Cluster Status* (État de la grappe). Notez l'adresse IP CIMC du serveur à remplacer. Elle est affichée dans la zone server (serveur) de la page *Cluster Status* (État de la grappe).
- **Vérifier les actions pour les machines virtuelles spéciales** : dans les zones serveur, recherchez les machines virtuelles ou les instances présentes sur le serveur et vérifiez si des actions spéciales doivent être effectuées pour ces machines virtuelles. La section suivante répertorie les actions pour les machines virtuelles pendant l'entretien du serveur.
- **Désactiver le serveur** : lorsque des actions préalables à la mise hors service sont effectuées, utiliser la page **Cluster Status** (État de la grappe) pour désactiver le serveur. Même si le serveur est en panne et semble *inactif* sur la page, vous pouvez toujours effectuer toutes les étapes d'entretien du serveur. Les étapes de désactivation peuvent être effectuées même si le serveur est hors tension.

Figure 53: Désactiver le serveur.



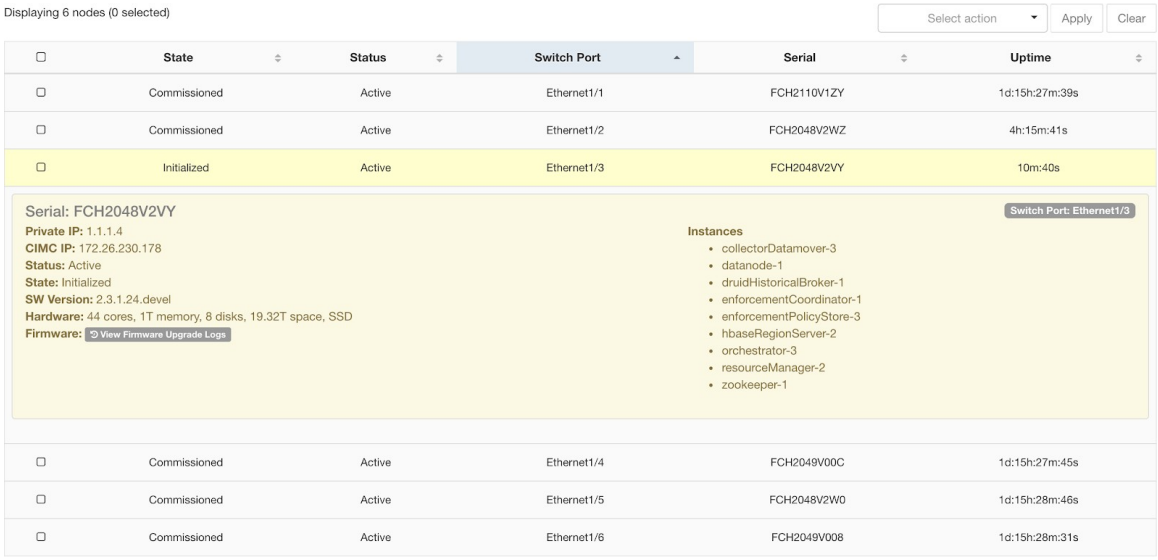
1. **Effectuez l'entretien du serveur** : une fois que le nœud est marqué *Decommissioned* (mis hors-service) dans la page **Cluster Status**, (État de la grappe) effectuez toutes les actions spéciales postérieures à la désactivation des machines virtuelles. Tout remplacement de composant ou de serveur peut être effectué dès maintenant. Si le serveur entier est remplacé, modifiez l'adresse IP du contrôleur CIMC du nouveau serveur pour qu'elle corresponde à celle du serveur remplacé. L'adresse IP du contrôleur CIMC de chaque serveur est indiquée dans la page **Cluster Status** (État de la grappe).
2. **Recréer l'image après le remplacement de composant** : Réinitialisez le serveur après le remplacement de composant à l'aide de la page **Cluster Status** (État de la grappe). La recréation de l'image prend environ 30 minutes et nécessite un accès CIMC aux serveurs. Le serveur est marqué *NEW* (NOUVEAU) une fois la recréation d'image terminée.
3. **Remplacement entier du serveur** : si le serveur en totalité est remplacé, il apparaîtra à l'état *NEW* (NOUVEAU) dans la page **Cluster Status** (État de la grappe). La version du logiciel du serveur est visible sur la même page. Si la version du logiciel est différente dans la version de la grappe, recréez l'image du serveur.

Figure 54: Remplacement du serveur



4. **Mettre en service le serveur** : une fois que le serveur est marqué *NEW* (NOUVEAU), nous pouvons lancer la mise en service du nœud à partir de la page **Cluster Status** (État de la grappe). Cette étape met en service les machines virtuelles sur le serveur. La mise en service d'un serveur prend environ 45 minutes. Le serveur sera marqué « *Commissioned* » (mis en service) une fois la mise en service terminée.

Figure 55: Mettre le serveur en service

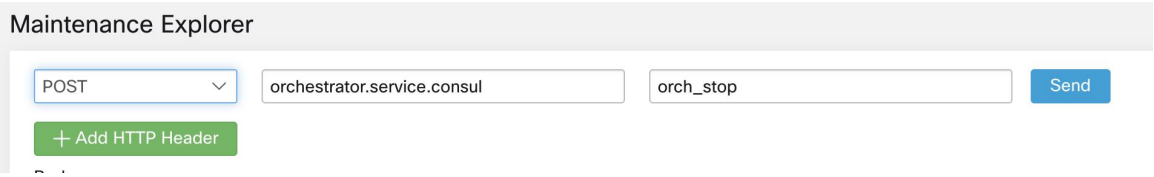


Actions sur les machines virtuelles pendant l'entretien du serveur

Certaines machines virtuelles nécessitent des actions spécifiques pendant la procédure d'entretien du serveur. Ces actions peuvent être préalables, se situer après la mise hors-service, ou après la mise en service.

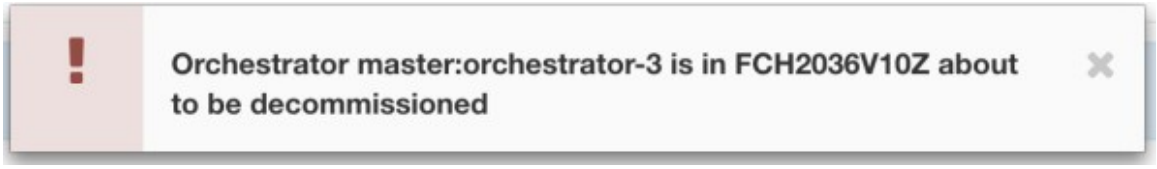
- **Orchestrateur principal** : il s'agit d'une action préalable à la mise hors-service. Si le serveur faisant l'objet d'entretien est doté d'un Orchestrateur principal, exécutez la commande POST *orch_ stop* sur orchestrator.service.consul à partir de la page d'exploration avant de procéder à la mise hors-service. Cela commute l'orchestrateur principal.

Figure 56: Explorateur de maintenance



Si vous essayez de désactiver un serveur doté d'un orchestrateur principal, l'erreur suivante s'affiche.

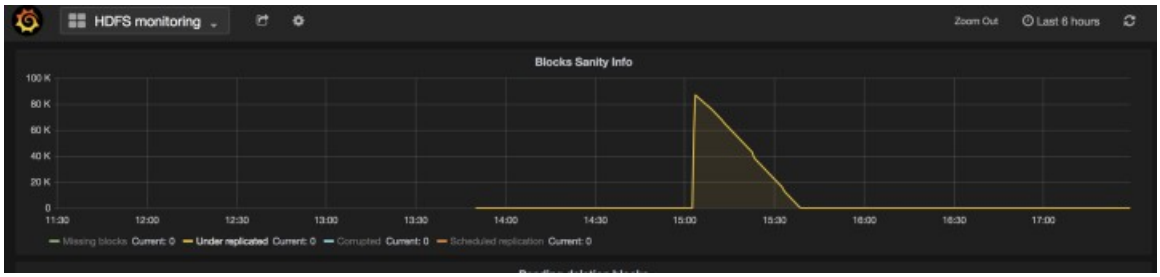
Figure 57: Désactiver un serveur avec une erreur d'orchestrateur principal



Pour déterminer l'orchestrateur principal, exécutez la commande explore `primaryorchestrator` sur n'importe quel hôte.

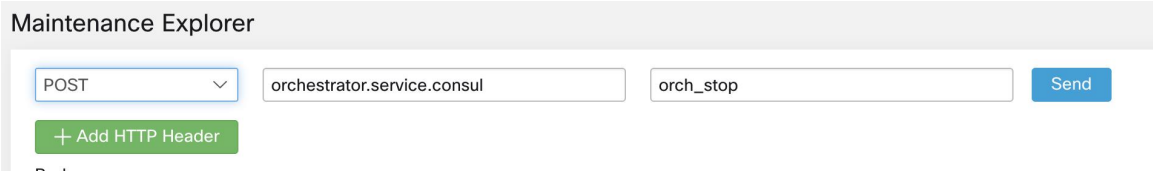
- **Namenode** : Si le serveur en cours d'entretien contient une machine virtuelle (namenode), exécutez la commande POST *switch_namenode* sur orchestrator.service.consul à partir de la page explore après la désactivation, puis la commande POST *switch_namenode* sur orchestrator.service.consul après la mise en service. Il s'agit d'actions postérieures à la désactivation et à la mise en service.
- **Secondary namenode** : Si le serveur en cours d'entretien comporte une VM secondaire, alors exécutez la commande POST *switch_secondarynamenode* sur orchestrator.service.consul à partir de la page explore après la désactivation, puis la commande POST *switch_ Secondarynamenode* sur orchestrator.service.consul après la mise en service. Il s'agit d'actions postérieures à la désactivation et à la mise en service.
- **Resource Manager primary** : si le serveur en cours d'entretien est doté du gestionnaire de ressources principal, exécutez la commande POST *switch_yARN* sur orchestrator.service.consul à partir de la page d'exploration. Il s'agit d'actions postérieures à la désactivation et à la mise en service.
- **Datanode** : la grappe ne tolère qu'une seule défaillance Datanode à la fois. Si plusieurs serveurs contenant des machines virtuelles Datanode ont besoin d'être entretenus, effectuez l'entretien du serveur un à la fois. Après chaque entretien de serveur, attendez que le tableau sous Surveillance | hawkeye | hdfs-monitoring | Block Sanity Info, Missing blocks et Under replicated couts (Informations sur la sécurité des blocs, blocs manquants et nombre de réplications insuffisant) soit à 0.

Figure 58: Maintenance du serveur : nœud de données



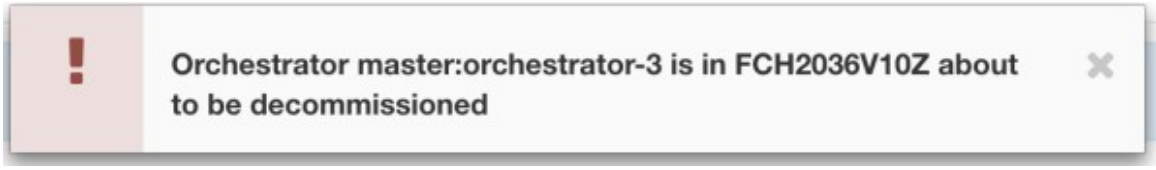
- **Orchestrateur principal** : il s'agit d'une action préalable à la mise hors-service. Si le serveur faisant l'objet d'entretien est doté d'un Orchestrateur principal, exécutez la commande POST *orch_ stop* sur orchestrator.service.consul à partir de la page d'exploration avant de procéder à la mise hors-service. Cela commute l'orchestrateur principal.

Figure 59: Explorateur de maintenance



Si vous essayez de désactiver un serveur doté d'un orchestrateur principal, l'erreur suivante s'affiche.

Figure 60: Désactiver un serveur avec une erreur d'orchestrateur principal



Pour déterminer l'orchestrateur principal, exécutez la commande explore `primaryorchestrator` sur n'importe quel hôte.

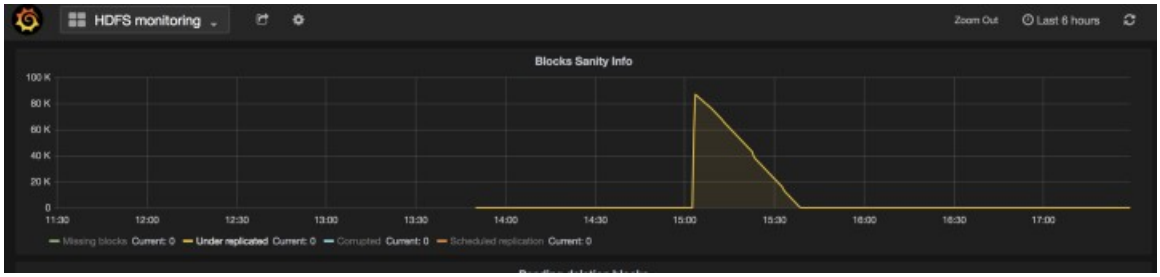
- **Namenode** : Si le serveur en cours d'entretien comporte une machine virtuelle Namenode, vérifiez que l'instance secondaryNamenode-1 est en cours d'exécution et que le service Namenode est actif. Exécutez la commande Explore POST `namenodeha_get_details` sur launcherHost-1 ou tout autre hôte launcherHosts en cours d'exécution, pour vérifier l'état. L'état SecondaryNamenode-1 doit être **Actif** ou **En attente**. Ne pas procéder à la désactivation si SecondaryNamenode-1 n'est pas à l'état **Actif** ou **En attente**.

- **Secondarynamenode** : si le serveur en cours d'entretien comporte une machine virtuelle secondarynamenode, vérifiez que l'instance namenode-1 est en cours d'exécution et que le service namenode est actif. Exécutez la commande Explore POST `namenodeha_get_details` sur launcherHost-1 ou tout autre hôte launcherHosts en cours d'exécution, pour vérifier l'état. L'état de namenode-1 doit être soit **Actif**, soit **En veille**. Ne procédez pas à la désactivation si `namenode-1` n'est pas à l'état **Actif** ou **En veille**.

- **Resource Manager primary** : si le serveur en cours d'entretien est doté du gestionnaire de ressources principal, exécutez la commande POST *switch_yARN* sur orchestrator.service.consul à partir de la page d'exploration. Il s'agit d'actions postérieures à la désactivation et à la mise en service.

- **Datanode** : la grappe ne tolère qu'une seule défaillance Datanode à la fois. Si plusieurs serveurs contenant des machines virtuelles Datanode ont besoin d'être entretenus, effectuez l'entretien du serveur un à la fois. Après chaque entretien de serveur, attendez que le tableau sous Surveillance | hawkeye | hdfs-monitoring | Block Sanity Info, Missing blocks et Under replicated couts (Informations sur la sécurité des blocs, blocs manquants et nombre de réplications insuffisant) soit à 0.

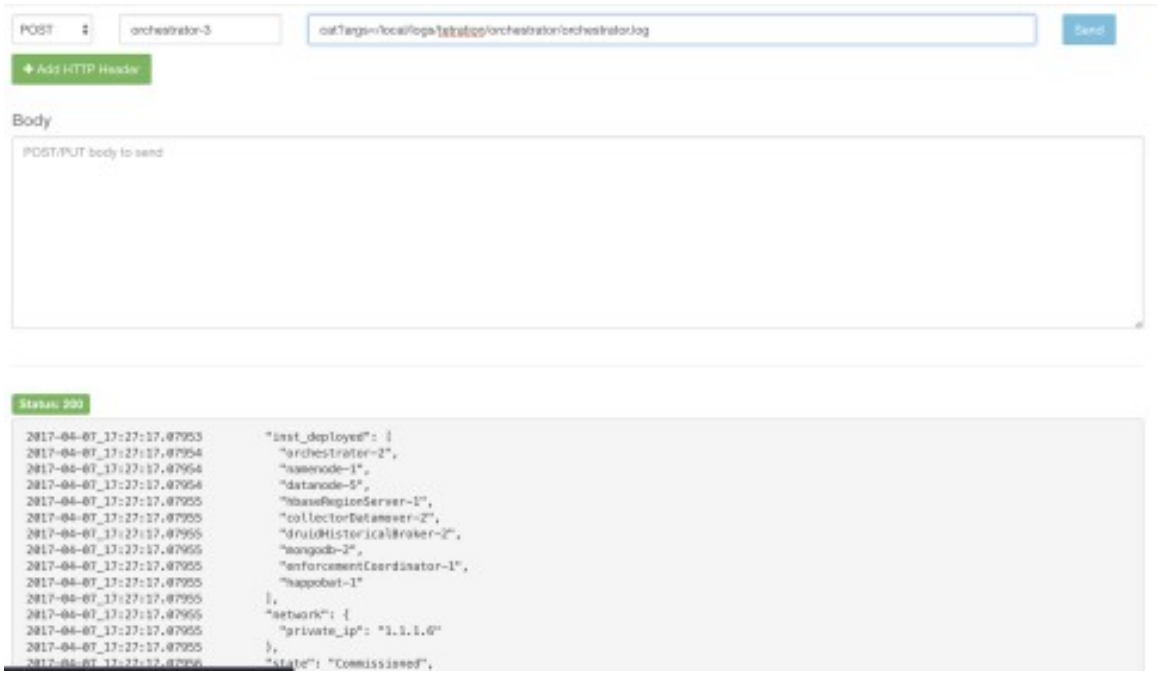
Figure 61: Maintenance du serveur : nœud de données



Dépannage de l'entretien du serveur

- **Journaux** : tous les journaux d'entretien du serveur font partie du journal de l'orchestrateur. L'emplacement est `/local/logs/tetration/orchestrator/orchestrator.log` sur orchestrator.service.consul.

Figure 62: Journal d'entretien du serveur



- **Mise hors service**
  - Cette étape supprime les machines virtuelles ou les instances sur le serveur.
  - Il supprime ensuite l'entrée de ces instances dans les tables de consul principales (backend).
  - Cette étape prend environ 5 minutes.
  - Le serveur sera marqué comme *Désactivé* une fois l'étape terminée.

Note Désactivé ne signifie pas que le serveur est éteint. La désactivation supprime uniquement le contenu Cisco Secure Workload sur le serveur.

- Si le serveur est éteint, il sera indiqué comme **Inactif**. Nous pouvons toujours exécuter la désactivation sur ce serveur à partir de la page d'état de la grappe. Mais l'étape de suppression des machines virtuelles ne s'exécutera pas, car le serveur est hors tension. Assurez-vous que ce serveur ne rejoint pas la grappe à l'état hors service. Il doit être recréé et rajouté à la grappe.

- **Recréation d'image**
  - Cette étape installe le système d'exploitation de base Cisco Secure Workload ou le système d'exploitation de l'hyperviseur sur le serveur.
  - Elle formate également les disques durs et installe quelques bibliothèques Cisco Secure Workload sur le serveur.
  - La fonction Reimage (recréation d'image) exécute un script appelé **mjolnir** pour lancer la création d'image du serveur. L'exécution de mjolnir prend environ 5 minutes, après quoi la création d'image commence. La création d'image prend environ 30 minutes. Les journaux pendant la création d'image peuvent uniquement être consultés sur la console du serveur en cours de recréation. L'utilisateur peut utiliser la clé ta_dev pour vérifier des informations supplémentaires sur la recréation, comme les journaux /var/log/nginx lors du démarrage pxe, /var/log/messages pour vérifier l'adresse IP DHCP et les configurations de démarrage pxe.
  - La recréation d'image nécessite une connectivité de contrôleur CIMC de l'orchestrateur. Le moyen le plus simple de vérifier la connectivité du contrôleur CIMC est d'utiliser la page explore et la commande POST ping?args=<cimc ip> à partir de orchestrator.service.consul. **N'oubliez** pas de modifier l'adresse IP du contrôleur CIMC dans le cas où le serveur est remplacé et de définir le mot de passe du contrôleur CIMC au mot de passe par défaut
  - De plus, le réseau CIMC aurait dû être défini dans les renseignements du site lors du déploiement de la grappe afin que les commutateurs soient configurés avec les bons routages. Dans le cas où la connectivité du contrôleur CIMC de grappe n'est pas définie correctement, vous verrez le résultat suivant dans les journaux de l'orchestrateur.

- **Mise en service**
  - Les programmes de mise en service des machines virtuelles sur le serveur et les guides d'exécutions dans les machines virtuelles pour installer le logiciel Cisco Secure Workload.
  - La mise en service dure environ 45 minutes.
  - Le flux de travail est similaire à un déploiement ou à une mise à niveau.
  - Les journaux indiquent les défaillances survenues lors de la mise en service.
  - Le serveur sur la page d'état de la grappe ne sera initialisé lors de la mise en service et marqué comme Mis en service qu'après que vous ayez terminé les étapes.

Exclure les systèmes sans système d'exploitation : bmexclude

Si une défaillance matérielle est détectée au redémarrage d'une grappe après une panne de courant, la grappe reste bloquée dans un état où nous ne pouvons ni exécuter le flux de travail de redémarrage pour obtenir des services stables, ni exécuter le flux de travail de mise en service, car l'arrêt des services entraîne un échec de la mise en service. Cette fonction devrait être utile dans de tels scénarios en permettant à l'utilisateur de redémarrer (mise à niveau) avec un matériel défectueux, après quoi le processus RMA habituel pour le système sans système d'exploitation défectueux peut être exécuté.

L'utilisateur doit utiliser un POST pour examiner le point terminal avec le numéro de série du système sans système d'exploitation à exclure :

1. Action : POST
2. Hôte : orchestrator.service.consul
3. Point terminal : exclude_bms?method=POST
4. Corps du texte : {"baremetal": ["BMSERIAL"]}

L'orchestrateur effectue quelques vérifications pour déterminer si l'exclusion est faisable. Auquel cas, il configure quelques clés consul et renvoie un message de réussite indiquant quelles machines sans système d'exploitation et quelles machines virtuelles seront exclues du prochain flux de travail de redémarrage ou de mise à niveau. Si les systèmes sans système d'exploitation comprennent certaines machines virtuelles, elles ne peuvent pas être exclues, comme décrit dans la section sur les limites ci-dessous. Le point terminal explore répond par un message indiquant pourquoi l'exclusion n'est pas possible. Après le POST réussi sur le point terminal explore, l'utilisateur peut lancer le redémarrage ou la mise à niveau au moyen de l'interface graphique principale et procéder au redémarrage habituel. À la fin de la mise à niveau, nous supprimons la liste bm d'exclusion. S'il est nécessaire d'exécuter la mise à niveau ou de redémarrer à nouveau avec les machines sans SE exclues, les utilisateurs doivent de nouveau effectuer un POST sur le point de terminaison bmexclude explore.

Restrictions

Les machines virtuelles suivantes ne peuvent pas être exclues :

- namenode
- secondaryNamenode
- mongodb
- mongodbArbiter

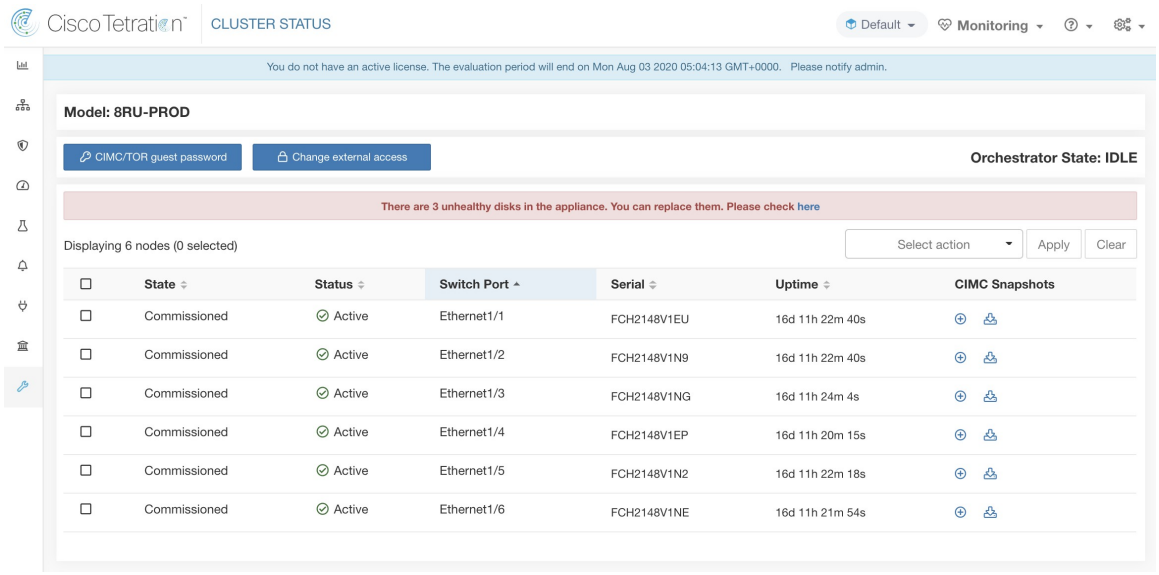
Entretien des disques

L'entretien des disques comprend le remplacement de tout disque dur défectueux sur un ou plusieurs serveurs. L'orchestrateur surveille l'intégrité des disques signalée par bmmgr sur chaque serveur de la grappe. S'il y a des disques défectueux, une bannière indique l'erreur dans la page **Cluster Status** (État de la grappe). Dans le volet de navigation, choisissez **Troubleshoot(Dépannage)** > **Cluster Status (État de la grappe)**.

La bannière affiche le nombre de disques qui sont dans un état **UNHEALTHY (NON INTÈGRE).** Cliquez *ici* sur la bannière, vous mènera à l'assistant de remplacement de disque. Vous ne pouvez qu'accéder à la page

de remplacement des disques, mais, à l'aide de l'assistant, le **service d'assistance à la clientèle** peut effectuer toutes les étapes nécessaires à l'entretien des disques.

Figure 63: Bannière de disque défectueux

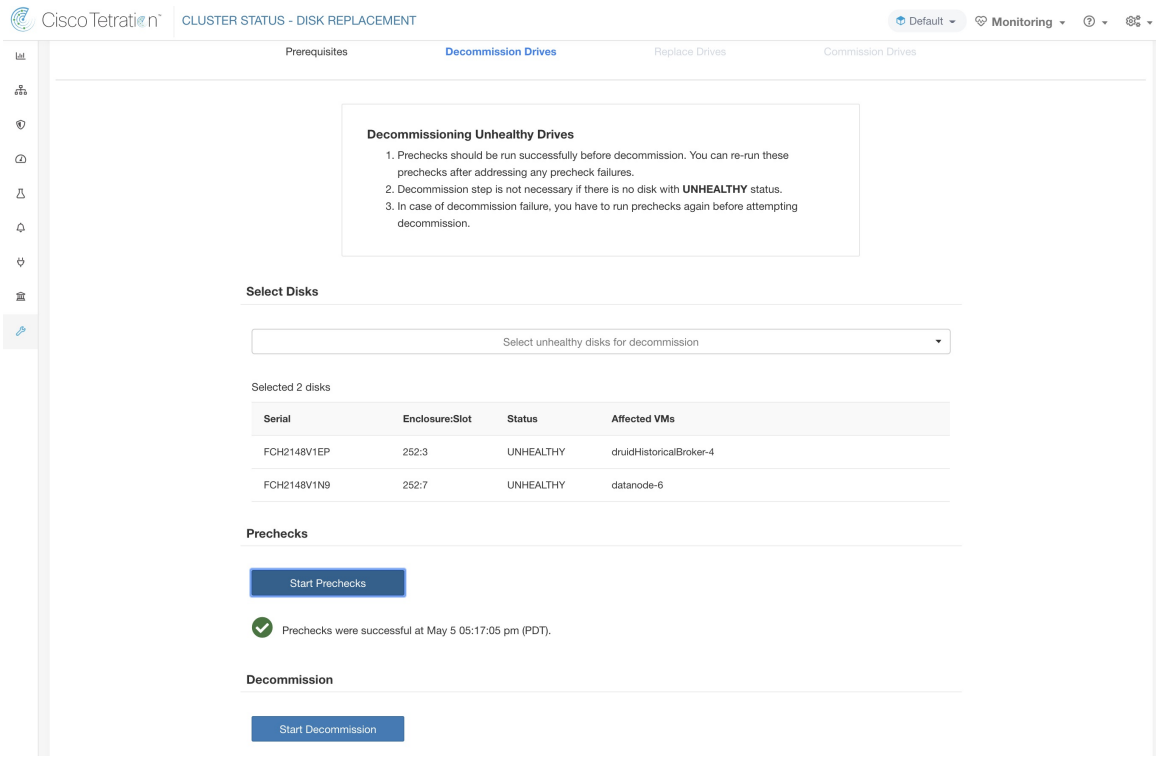


Vérifications préalables des exigences

Avant d'effectuer la désactivation ou la mise en service des disques, diverses vérifications sont effectuées au niveau du serveur de gestion. Toutes les vérifications doivent être réussies avant que vous puissiez procéder à la désactivation ou à la mise en service des disques.

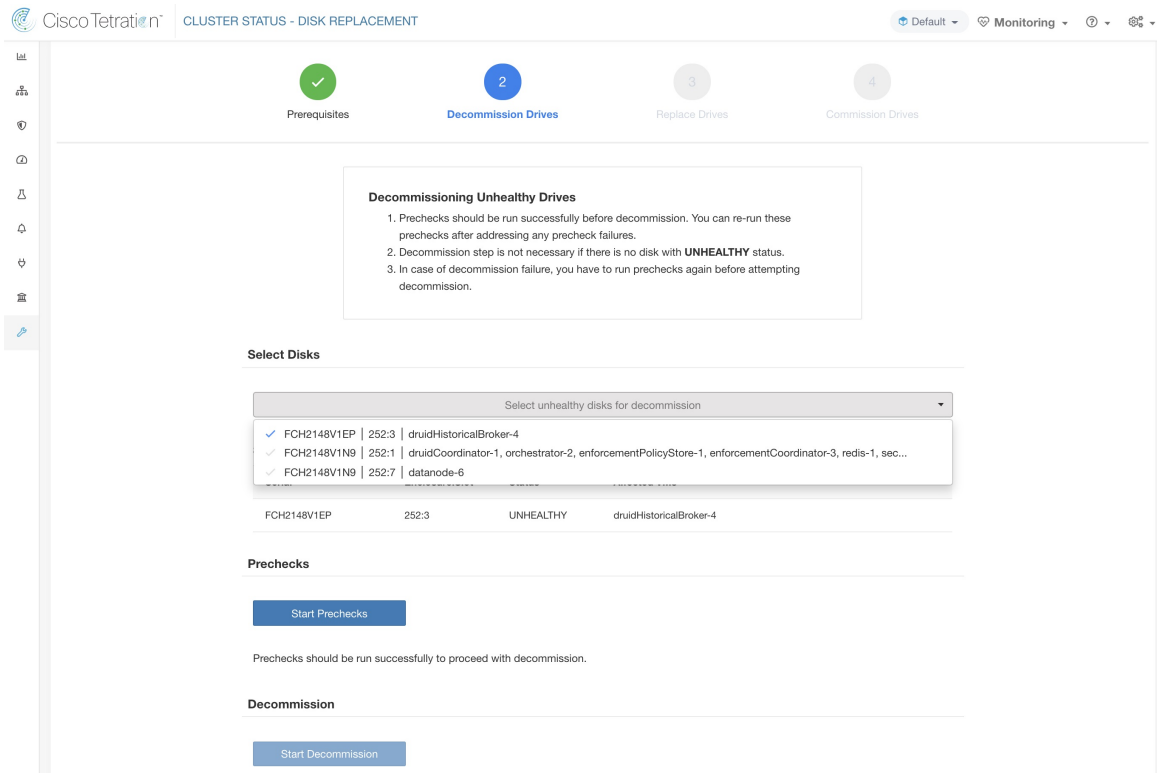
LLes vérifications infructueuses sont signalées dans **l'assistant de remplacement de disque** avec les détails de l'échec et les mesures correctives à prendre avant de passer à l'étape suivante ; par exemple, un seul nœud de données peut être mis hors service à la fois. Le Namenode et le secondaryNamenode ne peuvent pas être désactivés ensemble ; il faut également vérifier l'intégrité du Namenode avant de mettre le disque en service.

Figure 64: Vérifications préalables du remplacement de disques



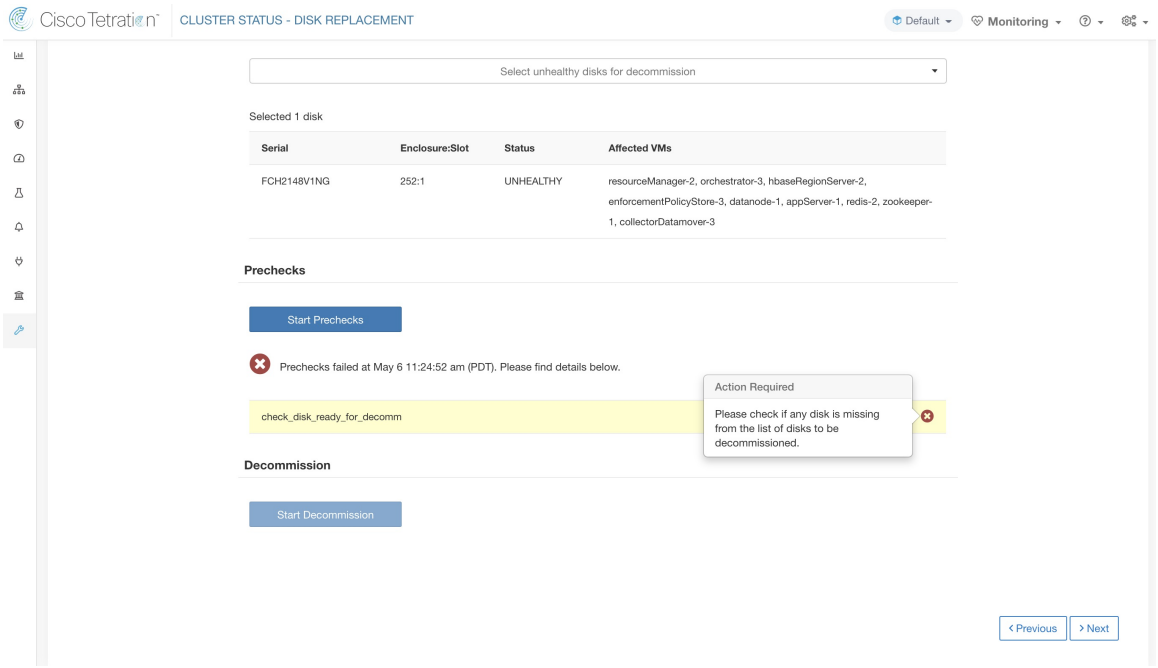
Vous pouvez sélectionner n'importe quel ensemble de disques défaillants à mettre hors service ensemble et lancer les contrôles préalables à la désactivation. La modification de l’ensemble des disques défaillants nécessite une réexécution des vérifications préalables. Effectuez à nouveau les vérification préalables avant de commencer la mise hors service ou la mise en service des disques. Vérifiez qu’il n’y a pas de nouvel échec de vérification préalable entre la dernière exécution de la vérification préalable et le début de la tâche de désactivation.

Figure 65: Disques non intègres pour la désactivation



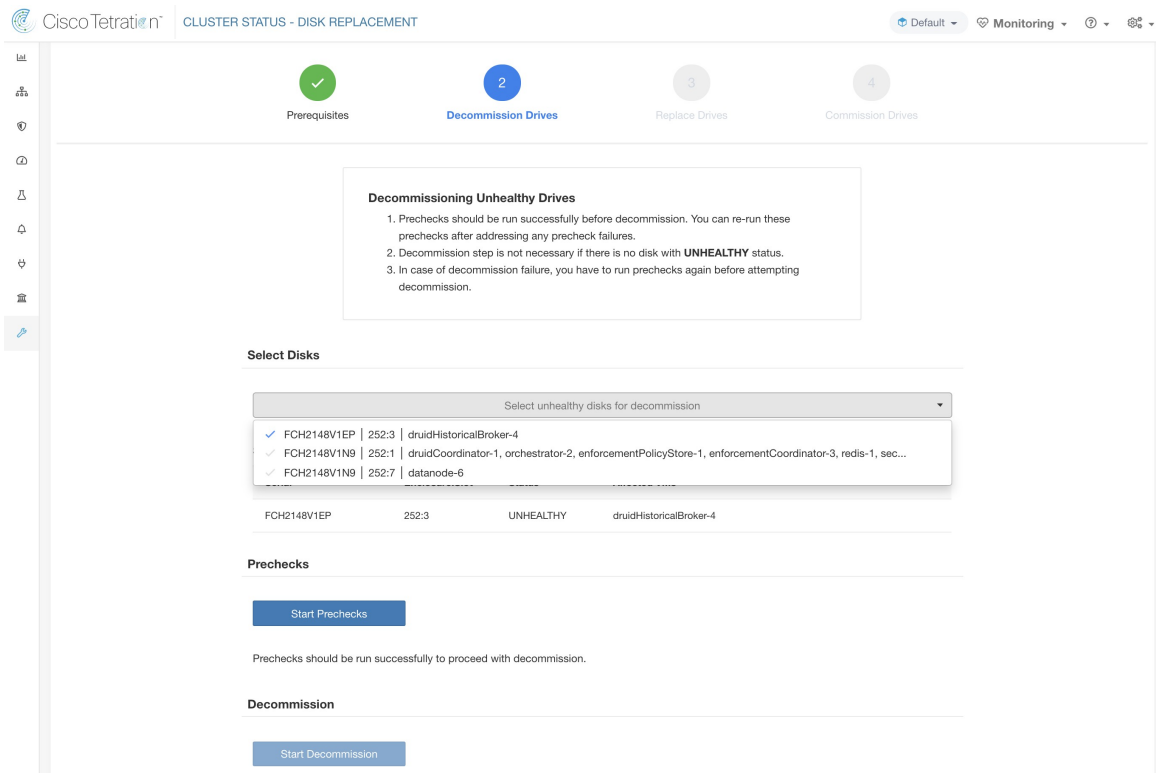
Si une vérification préalable échoue, un message détaillé s'affiche. Cliquez sur le message d'échec; une proposition d'action s'affichera dans une fenêtre contextuelle lorsque le pointeur survolera le bouton en forme de croix.

Figure 66: Action suggérée en cas d'échec de la vérification préalable



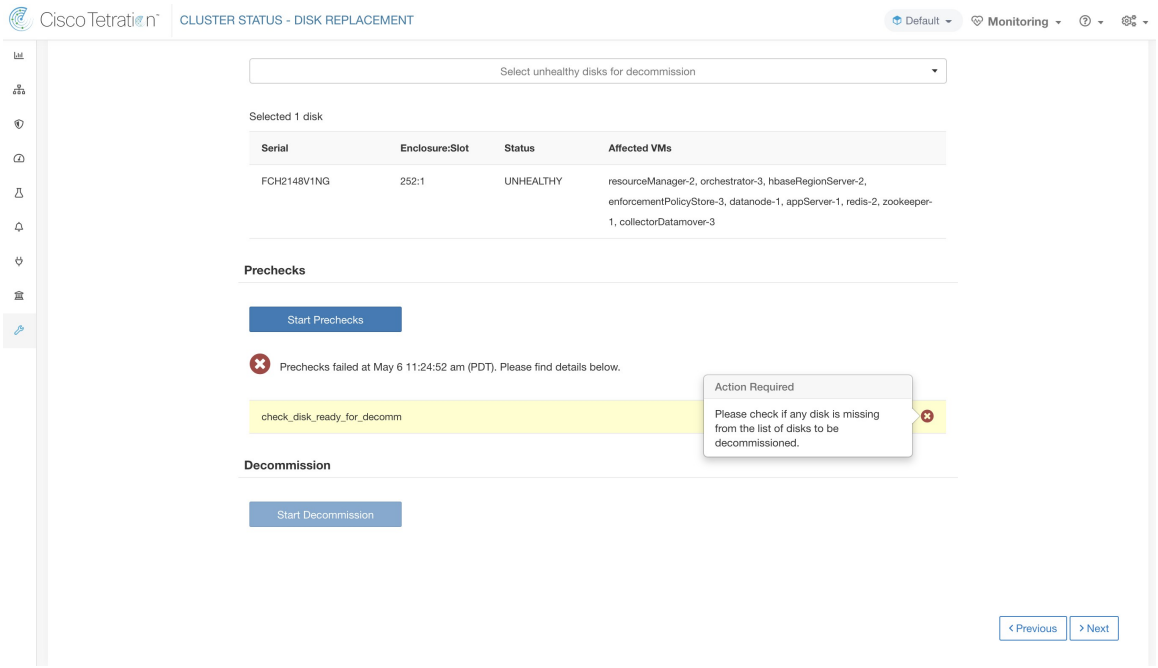
Vous pouvez sélectionner n'importe quel ensemble de disques défaillants à mettre hors service simultanément et lancer la vérification préalable de la mise hors service. La modification de l'ensemble de disques défaillants nécessitera une réexécution de la vérification préalable. Les mêmes vérification préalables sont effectuées à nouveau avant le début de la tâche (mise hors service ou en service) pour s'assurer qu'il n'y a pas de nouvelle défaillance entre la dernière vérification préalable et le début de la tâche de mise hors service.

Figure 67: Sélectionnez les disques NON INTÈGRES à mettre hors service



Après l'échec d'une vérification préalable, un message détaillé s'affiche en cliquant sur le message d'échec, de même qu'une proposition d'action s'affiche dans une fenêtre contextuelle lorsque le pointeur survole le bouton en forme de croix rouge.

Figure 68: Action suggérée dans l'écran contextuel en cas d'échec de la vérification préalable



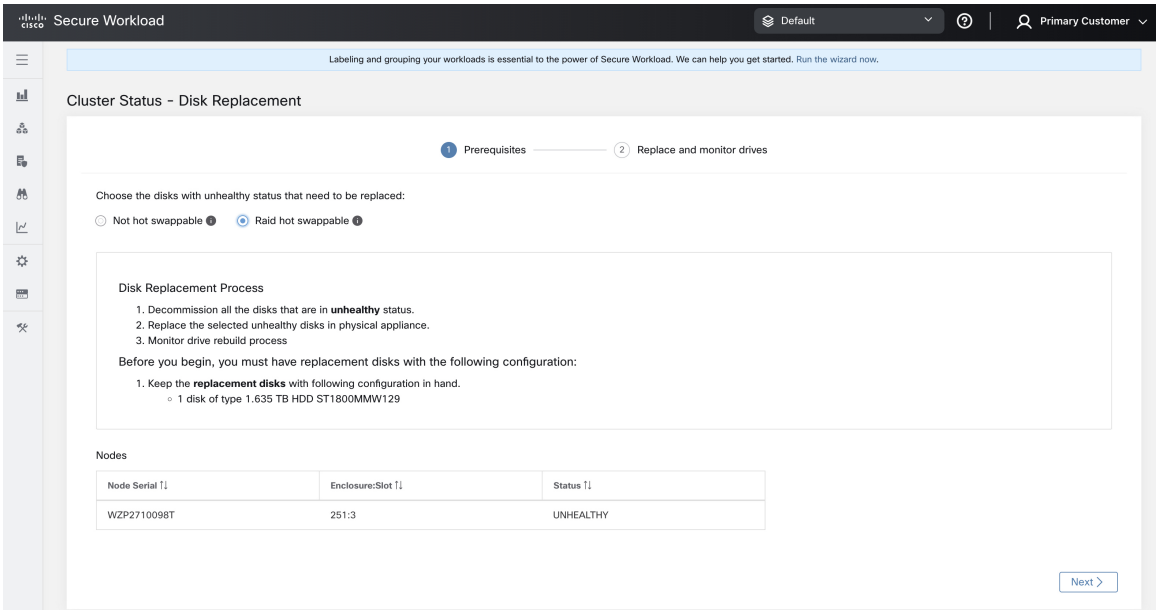
Assistant de remplacement de disques RAID échangeables à chaud

Avant de commencer

Avant de démarrer le processus de remplacement des disques non intègres, assurez-vous que les nouveaux disques sont disponibles.

L' **assistant de remplacement des disques** affiche les détails des disques défaillants, y compris la taille, le type, la marque et le modèle de chaque disque à remplacer. En outre, vous pouvez également afficher l'ID du logement et la liste de toutes les machines virtuelles qui utilisent chacun de ces disques.

Figure 69: Assistant de remplacement de disque



Physiquement, les lecteurs et le matériel sont échangeables à chaud. Cependant, seules les grappes 39RU-G3 (M6) possèdent la configuration matérielle requise pour permettre l'échange d'un lecteur. Une fois le lecteur remplacé, vous pouvez en échanger un sans mettre hors service les machines virtuelles qui utilisent le lecteur avant de pouvoir mettre en service les machines virtuelles sur les grappes.

Si un lecteur s'affiche sous « Non échangeable à chaud », vous devez suivre le processus de « remplacement d'un seul lecteur » pour remplacer ce dernier. Sinon, si un lecteur s'affiche sous « Raid échangeable à chaud », vous pouvez remplacer le lecteur sans désactiver aucune machine virtuelle, car le nœud utilise RAID5 basé sur le matériel.

Note Dans une grappe 39RU M6, les lecteurs compatibles avec RAID sont disponibles sur les nœuds de disque dur. Vous pouvez remplacer les disques RAID échangeables à chaud sans éteindre le système ni perturber son fonctionnement.

Dans une grappe 39RU M6, pour les disques non RAID, vous ne pouvez pas remplacer les disques pendant que le système est en marche. Vous devez éteindre le système avant de remplacer les disques.

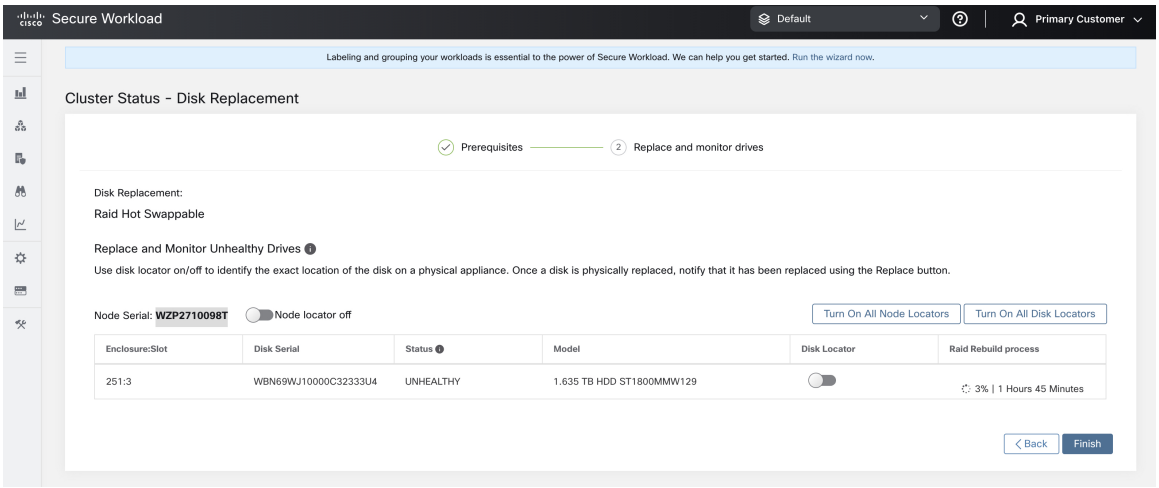
Transition d'état du disque

Dans n'importe quelle grappe pour disques RAID échangeables à chaud, les disques durs ont trois états : **HEALTHY** (INTÈGRE) , **UNHEALTHY** (NON INTÈGRE), et **NEW** (NOUVEAU). Un lecteur **UNHEALTHY** (NON INTÈGRE) passe à un état **HEALTHY** (INTÈGRE), vous pouvez le remplacer une fois que le contrôleur de stockage a terminé le processus de reconstruction de la matrice RAID.

Remplacer des disques RAID échangeables à chaud

Après la désactivation des disques, retirez-les et remplacez-les par de nouveaux. Pour faciliter ce processus, nous avons ajouté un accès repéré par un voyant DEL du localisateur de disque et du serveur sur la page de remplacement. Veillez à éteindre les voyants DEL du serveur et du localisateur de disques.

Figure 70: Reconfigurer les disques nouvellement ajoutés



Les disques peuvent être remplacés physiquement dans n'importe quel ordre, mais ils doivent être reconfigurés dans les numéros d'emplacement du plus petit au plus grand pour un serveur donné. Cet ordre est appliqué sur l'interface utilisateur et le serveur principal (backend). Sur l'interface utilisateur, vous aurez un bouton de remplacement actif pour le disque avec le numéro de logement le plus bas et l'état UNUSED.

Lorsque tous les disques sont remplacés, procédez à la mise en service. Comme pour la désactivation, nous devons exécuter un ensemble de vérification préalables avant de pouvoir poursuivre la mise en service. La progression de la mise en service est surveillée sur la page de mise en service du disque. Une fois la mise en service réussie, l'état de tous les disques passe à HEALTHY (INTÈGRE).

Figure 71: Avancement de la mise en service

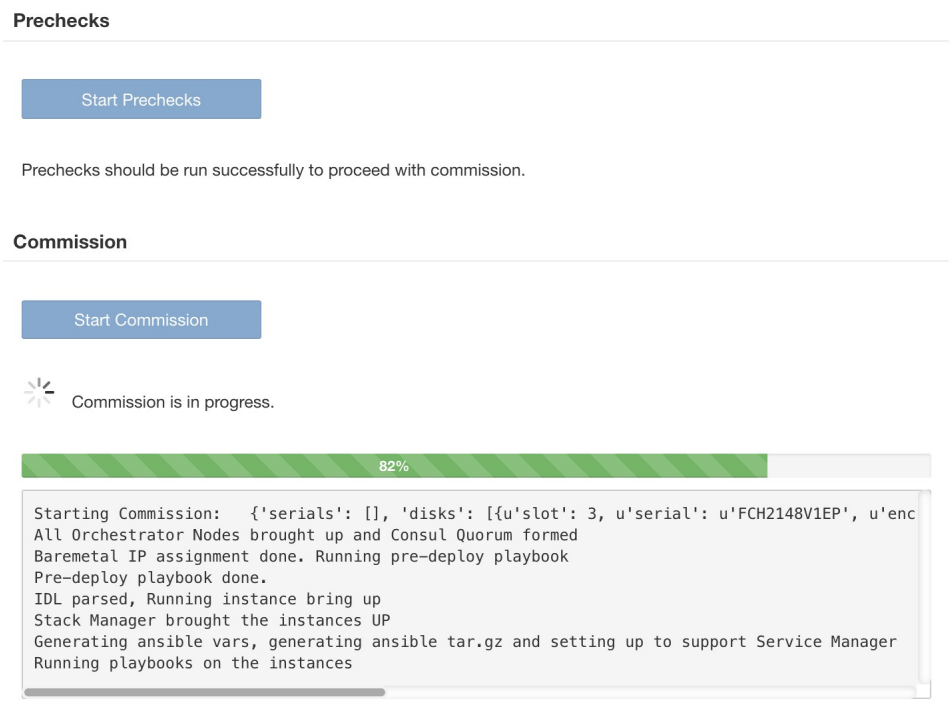
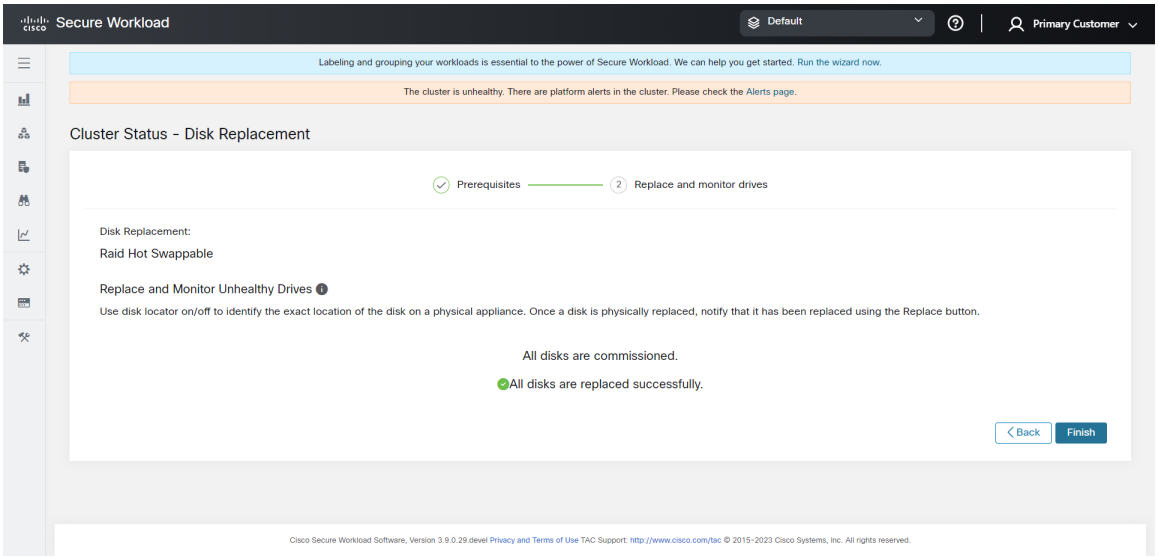


Figure 72: Remplacement du disque



Comportements connus

1. Pour les lecteurs non échangeables à chaud des serveurs, le système d'exploitation de l'hôte est stocké sur le premier lecteur du serveur. Si le premier lecteur (logement 1) du serveur tombe en panne, dans la

plupart des cas, le nœud entier devient inactif et doit être mis hors service, le lecteur doit être remplacé, l'image du serveur est recréée et remise en service dans le système. Contactez l'assistance technique de Cisco pour obtenir de l'aide.

2. Les serveurs RAID échangeables à chaud utilisent un matériel RAID5, qui stocke un bloc de parité pour chaque bloc de données, ce qui permet au système de continuer à fonctionner sans problème tant qu'un seul lecteur est défaillant sur ce serveur. Si plus d'un lecteur tombe en panne sur un serveur doté de lecteurs RAID échangeables à chaud, dans la plupart des cas, le serveur devient inactif et doit être mis hors service, les lecteurs doivent être remplacés, puis le serveur peut être recréé et remis en service dans le système. Contactez l'assistance technique de Cisco pour obtenir de l'aide.
3. Si plusieurs lecteurs non échangeables à chaud tombent en panne sur le même serveur, cliquez sur les boutons **Replace** (remplacer) dans l'interface utilisateur pour passer du numéro de logement le plus bas au numéro de logement le plus élevé sur chaque serveur.
4. Après avoir cliqué sur le bouton **Replace** (Remplacer) pour un lecteur non échangeable à chaud, il faut de 3 à 10 minutes au lecteur pour passer de REPLACED (REMPLACÉ) à NEW (NOUVEAU) dans l'interface utilisateur.
5. Après le remplacement physique d'un lecteur RAID échangeable à chaud, il faut de 3 à 10 minutes avant que l'état du processus de reconstruction s'affiche dans l'interface utilisateur.
6. Une grappe 39RU-G3 déployée à l'aide de Cisco Secure Workload version 3.8 ne sera pas configurée avec des disques RAID échangeables à chaud. La grappe devra être redéployée à l'aide de Cisco Secure Workload version 3.9, ou chaque TA-BNODE-G3 et TA-CNODE-G3 devra être mis hors service, recréé et remis en service un à la fois après la mise à niveau de la grappe vers la version Cisco Secure Workload 3.9. Si la méthode de désactivation, de recréation ou de mise en service de conversion de TA-BNODE-G3 et de TA-CNODE-G3 en disques RAID échangeables à chaud est utilisée, vérifiez que l'état du service de grappe est vert pour tous les services avant de commencer la désactivation.

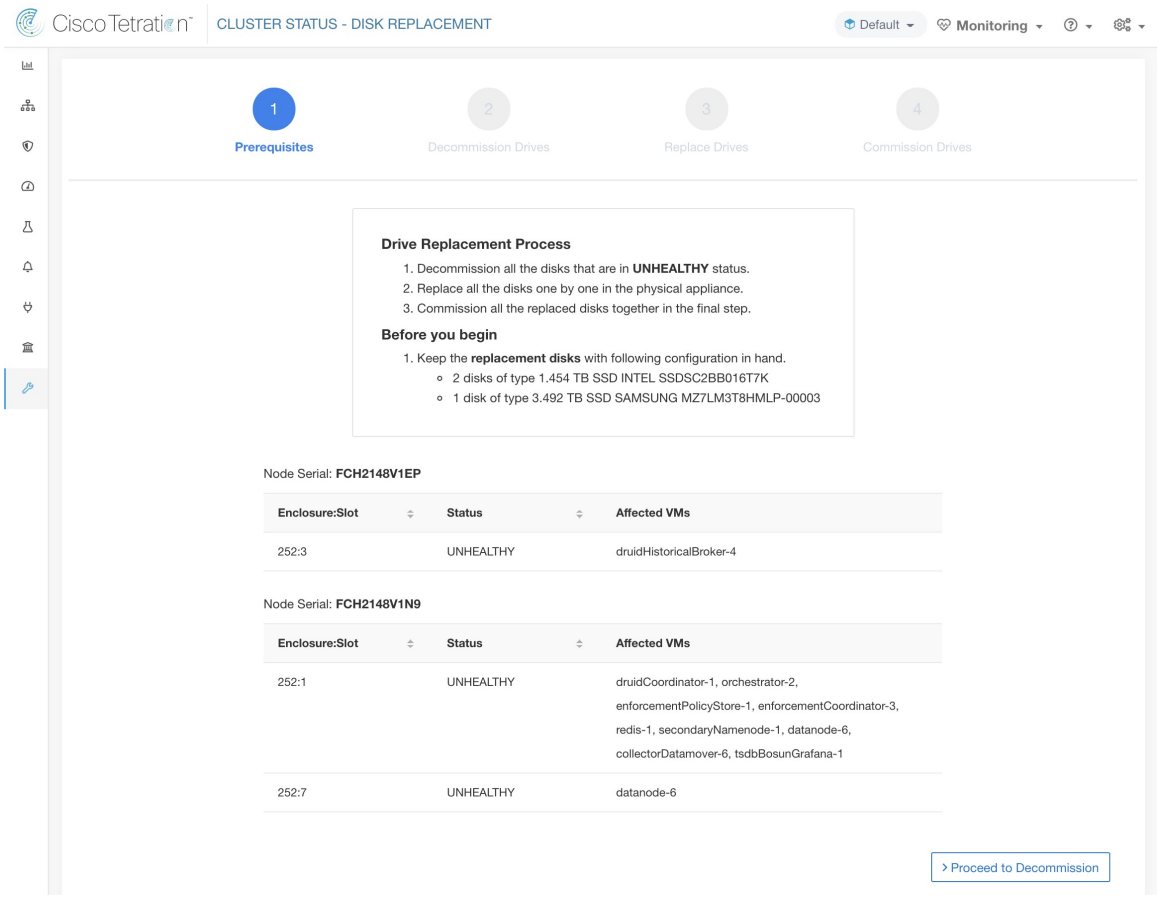
Assistant de remplacement de disque, non échangeable à chaud

Avant de commencer

Avant de commencer le processus de remplacement des disques non intègres, assurez-vous que les nouveaux disques sont disponibles.

L' **assistant de remplacement de disques** affiche les détails des disques défaillants, y compris la taille, le type, la marque et le modèle de chaque disque à remplacer. En outre, vous pouvez également afficher l'ID de logement et les listes de toutes les machines virtuelles qui utilisent chacun de ces disques.

Figure 73: Assistant de remplacement de disque



Note Physiquement, les lecteurs et le matériel sont échangeables à chaud.

Transitions d'état de disque

Dans une grappe, pour un système non-RAID, il y a six états pour les disques durs ;**HEALTHY** (INTÈGRE), **UNHEALTHY** (NON INTÈGRE), **UNUSED** (INUTILISÉ, **REPLACED** (REMPLACÉ), **NEW** (NOUVEAU), et **INITIALIZED** (INITIALISÉ). Après le déploiement ou la mise à niveau de la grappe, l'état de chaque disque de la grappe est **HEALTHY**. L'état d'un ou de plusieurs disques peut devenir **UNHEALTHY** en fonction de la détection de diverses erreurs.

Note Les disques non échangeables à chaud sont disponibles uniquement pour les grappes M4 et M5.

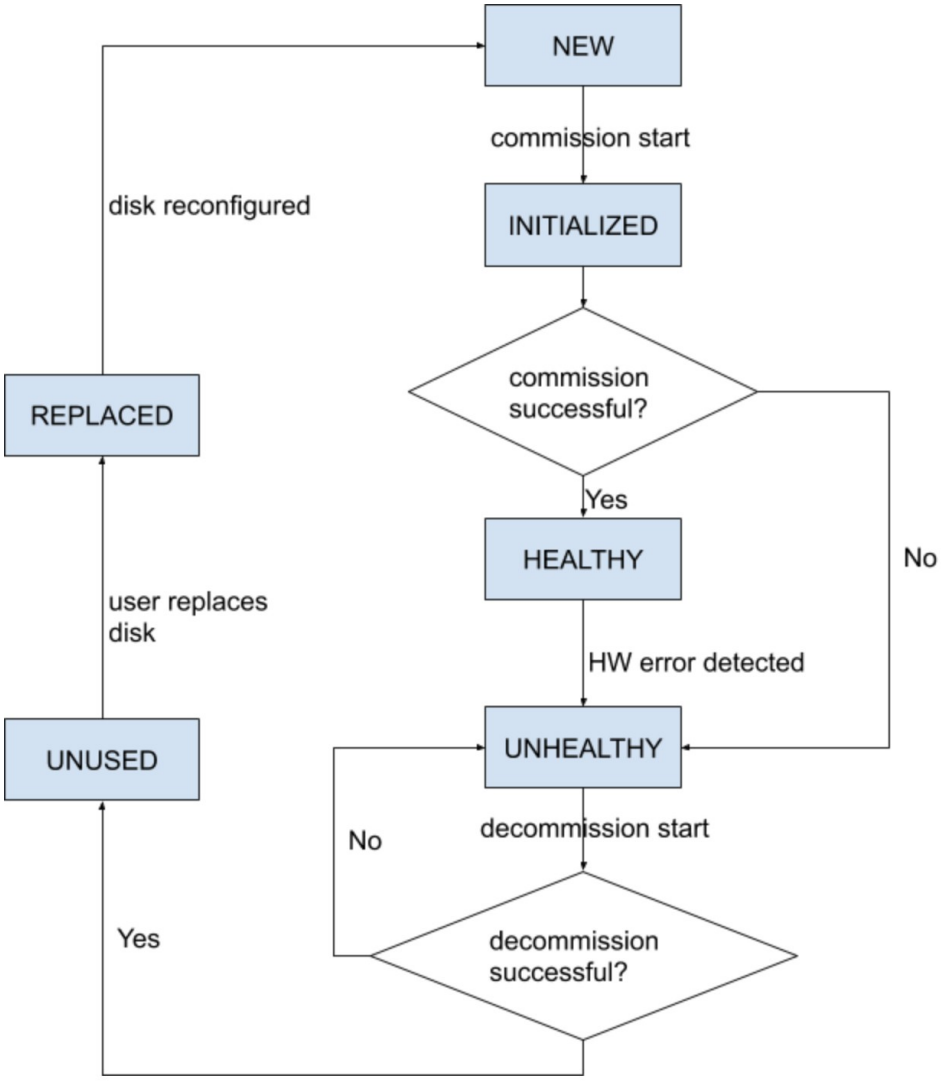
Aucune action n'est entreprise, sauf si l'état d'un disque passe à **UNHEALTHY**. Avant de commencer la mise en service des disques, déployez toutes les machines virtuelles qui ont été supprimées dans le cadre du processus de désactivation.

Une fois que vous avez mis en service les disques sans erreur, l'état des disques passe à **HEALTHY**. Dans le cas où la mise en service du disque échoue, l'état affiche **UNHEALTHY**. Pour les disques qui sont à l'état **UNHEALTHY**, démarrez le processus de désactivation du disque. Si le processus de désactivation réussit, l'état du disque passe à **UNUSED**, et si les disques tombent en panne lors de la désactivation, répétez le processus jusqu'à ce que l'état des disques devienne **UNUSED**.

Retirez les disques **UNHEALTHY** de la grappe et remplacez-les par de nouveaux disques, l'état devient **REPLACED).** Reconfigurer les disques de remplacement et analyser le matériel à la recherche d'anomalies. Si aucune anomalie n'est détectée, l'état des disques devient **NEW**, sinon vous devrez peut-être résoudre le problème; La modification d'état peut prendre jusqu'à trois minutes.

Pour comprendre comment les modifications d'état du disque sont gérées, consultez l'ordinogramme ci-dessous :

Figure 74: Transitions d'état de disque



Désactiver le disque

Une fois les vérifications préalables effectuées, vous pouvez procéder à la désactivation du disque. La progression de la désactivation sera affichée lors de l'assistant de remplacement du disque. Lorsque la progression de la désactivation atteint 100 %, l'état de tous les disques mis hors service devient UNUSED (INUTILISÉ).

Figure 75: Surveiller la progression de la désactivation des disques

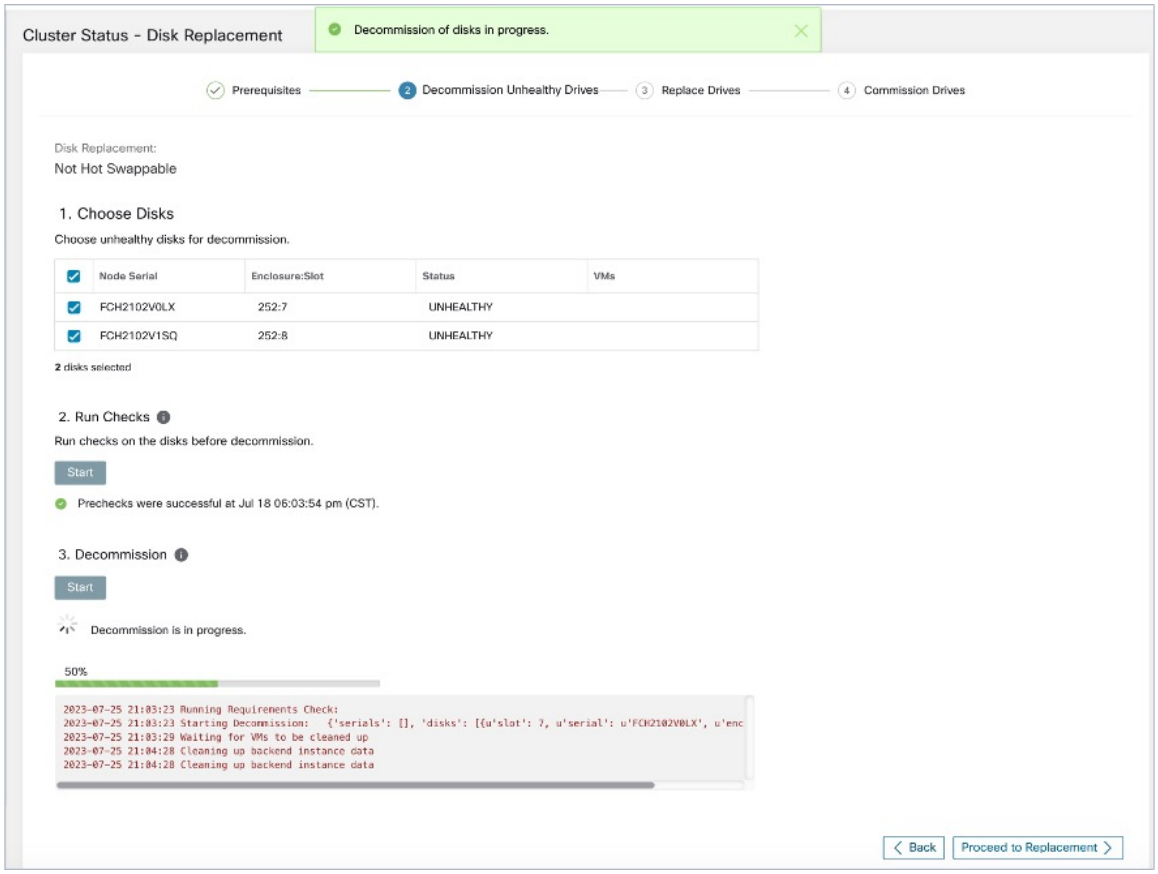
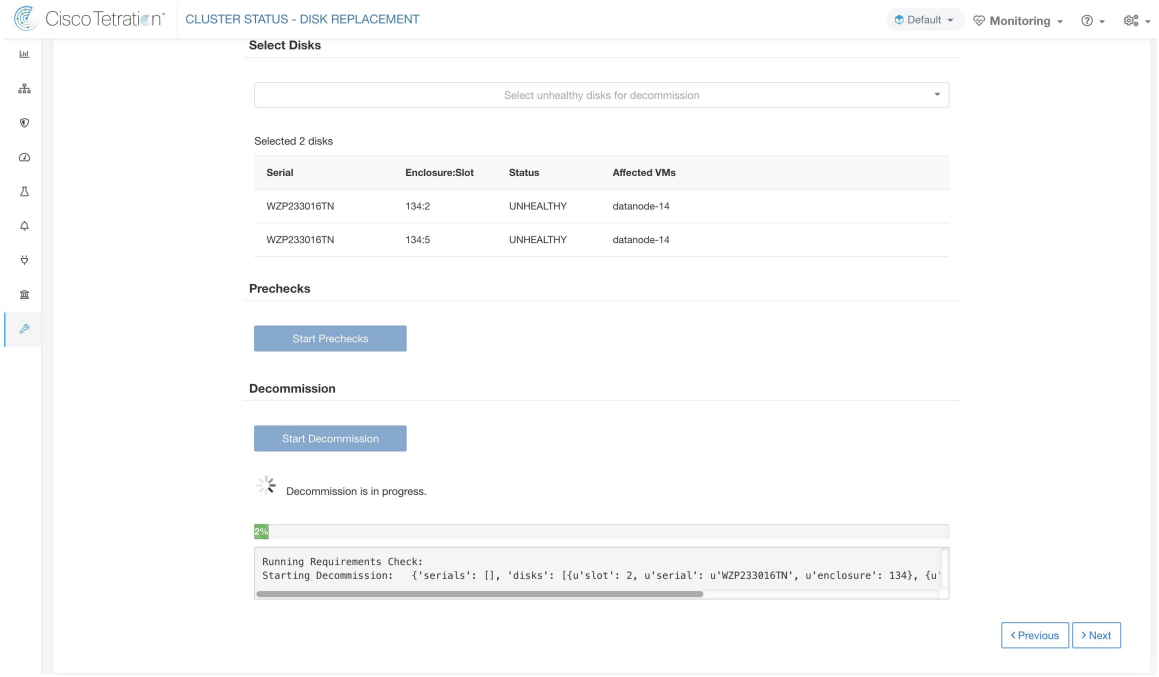


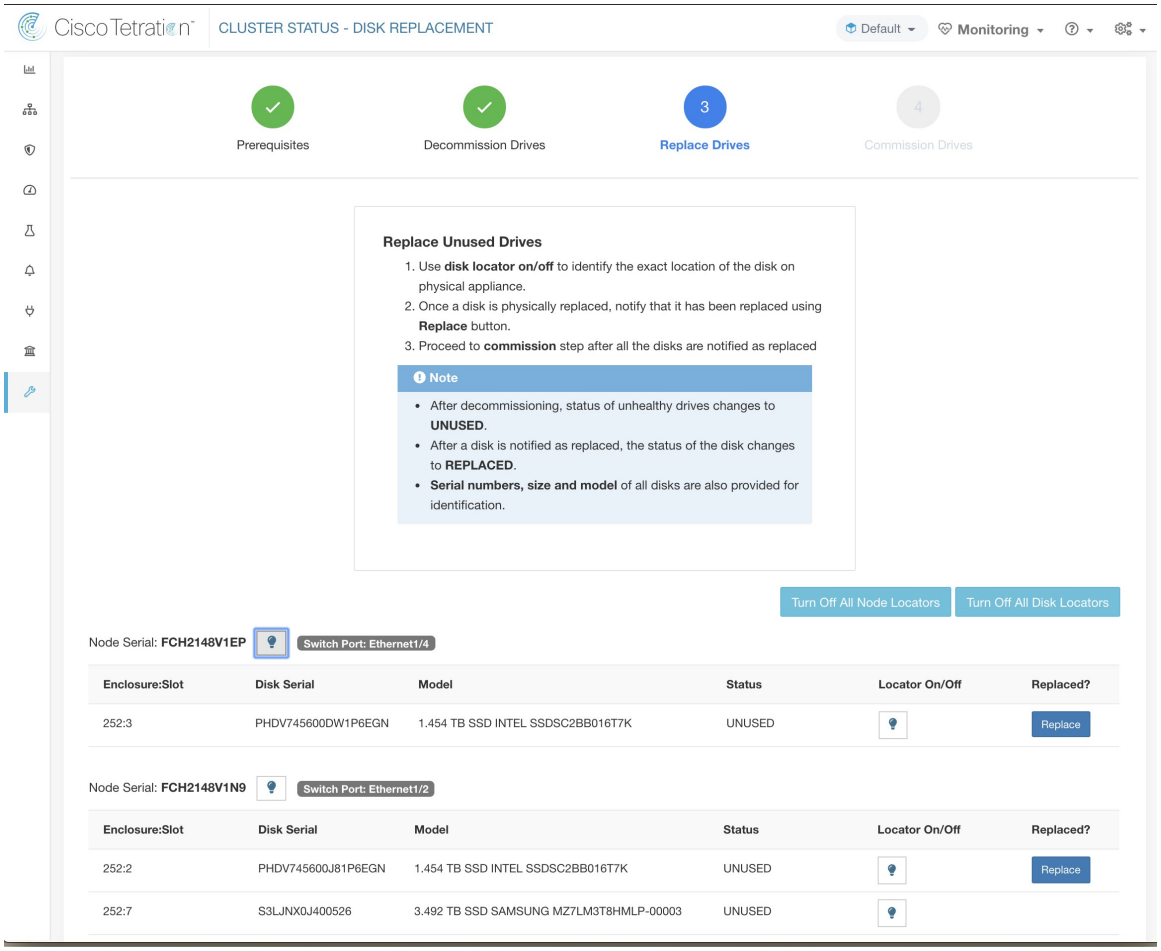
Figure 76: Surveiller la progression de la désactivation des disques



Remplacer le disque

Après la désactivation des disques, retirez-les et remplacez-les par de nouveaux. Pour faciliter ce processus, nous avons ajouté un accès repéré par un voyant DEL du localisateur de disque et du serveur sur la page de remplacement. Veillez à éteindre les voyants DEL du serveur et du localisateur de disques.

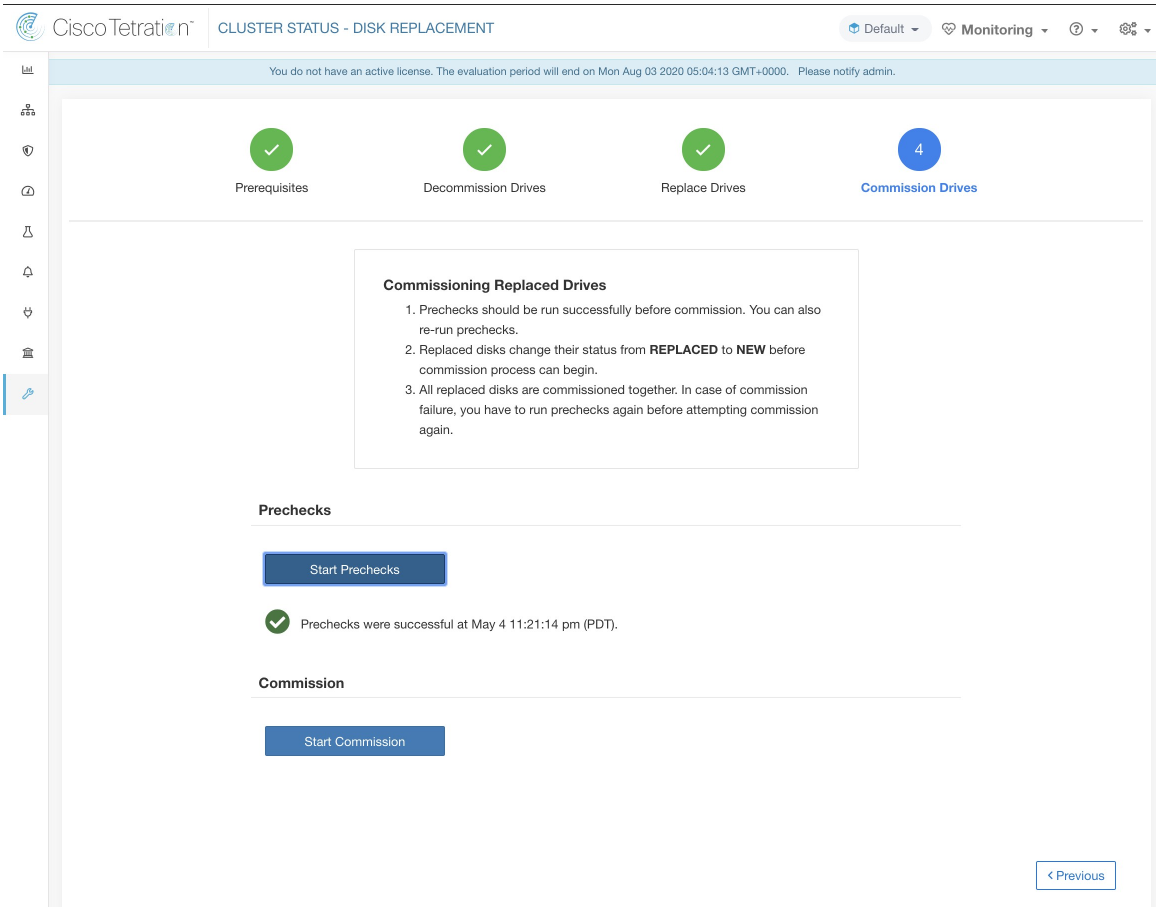
Figure 77: Reconfigurer les disques nouvellement ajoutés (non échangeables à chaud)



Les disques peuvent être remplacés physiquement dans n'importe quel ordre, mais ils doivent être reconfigurés dans les numéros d'emplacement du plus petit au plus grand pour un serveur donné. Cet ordre est appliqué sur l'interface utilisateur et le serveur principal (backend). Sur l'interface utilisateur, vous aurez un bouton de remplacement actif pour le disque avec le numéro de logement le plus bas et l'état UNUSED.

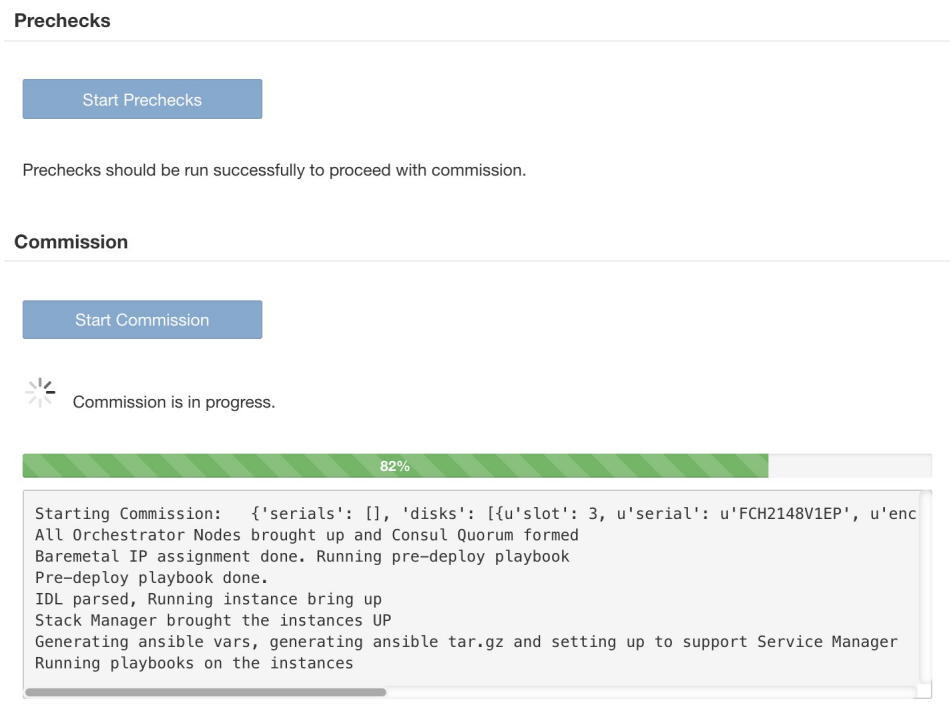
Mettre à disposition le disque

Lorsque tous les disques sont remplacés, procédez à la mise en service. Comme pour la désactivation, nous devons exécuter un ensemble de vérification préalables avant de pouvoir poursuivre la mise en service.



La progression de la mise en service est surveillée sur la page de mise en service du disque. Une fois la mise en service réussie, l'état de tous les disques passe à HEALTHY (INTÈGRE).

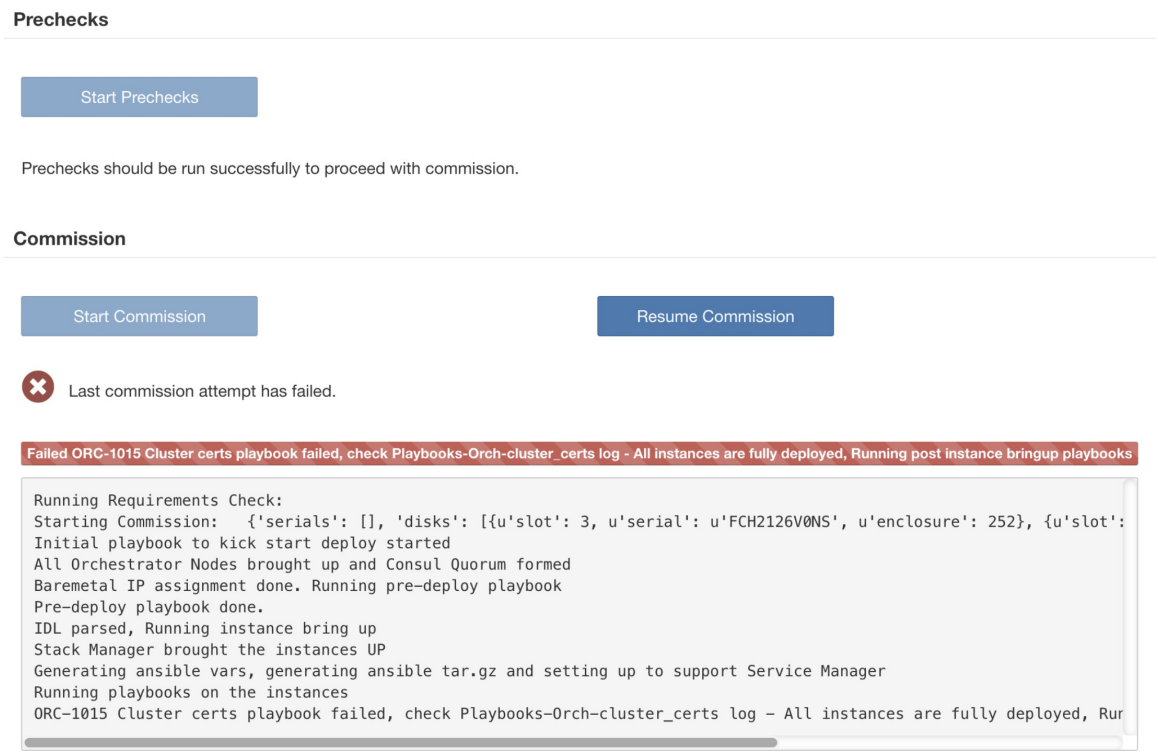
Figure 78: Avancement de la mise en service



Reprise sur échec pendant la mise en service du disque

Après avoir déployé les machines virtuelles et en cas de défaillance, vous pouvez les restaurer à l'aide du bouton**Resume Commission** (Reprendre la mise en service). Pour poursuivre la mise en service du disque, cliquez sur le bouton **Resume Commission** (Reprendre a mise e service) pour redémarrer les guides post-déploiement.

Figure 79: Reprendre la mise en service



En cas de défaillance avant le déploiement des machines virtuelles, les disques mis en service précédemment verront leur état passer à UNHEALTHY (NON INTÈGRE). Cela nous obligera à redémarrer le processus de remplacement à partir de la désactivation des disques UNHEALTHY (NON INTÈGRE).

Défaillance de disque pendant la mise en service

En cas de défaillance d'un disque autre que ceux qui sont remplacés alors que la mise en service du disque est en cours, l'assistant de remplacement de disque affichera une notification de cette défaillance à la fin du processus de mise en service en cours, qu'il ait réussi ou échoué.

En cas d'échec avec reprise, les utilisateurs ont deux possibilités quant aux prochaines étapes à effectuer.

1. Ils peuvent essayer de reprendre et de terminer la mise en service en cours et effectuer ultérieurement le processus de remplacement du disque en ce qui concerne les nouvelles défaillances.
2. Ils peuvent également commencer à mettre hors service le nouveau disque défectueux et procéder à la mise en service de tous les disques simultanément.

Cette deuxième possibilité est la seule disponible en cas de défaillance ne pouvant pas être reprise. Si l'échec post-déploiement est causé en raison des nouveaux disques défaillants, la deuxième possibilité sera à nouveau la seule voie à suivre, bien qu'un bouton de reprise soit disponible.

Problèmes connus et dépannage

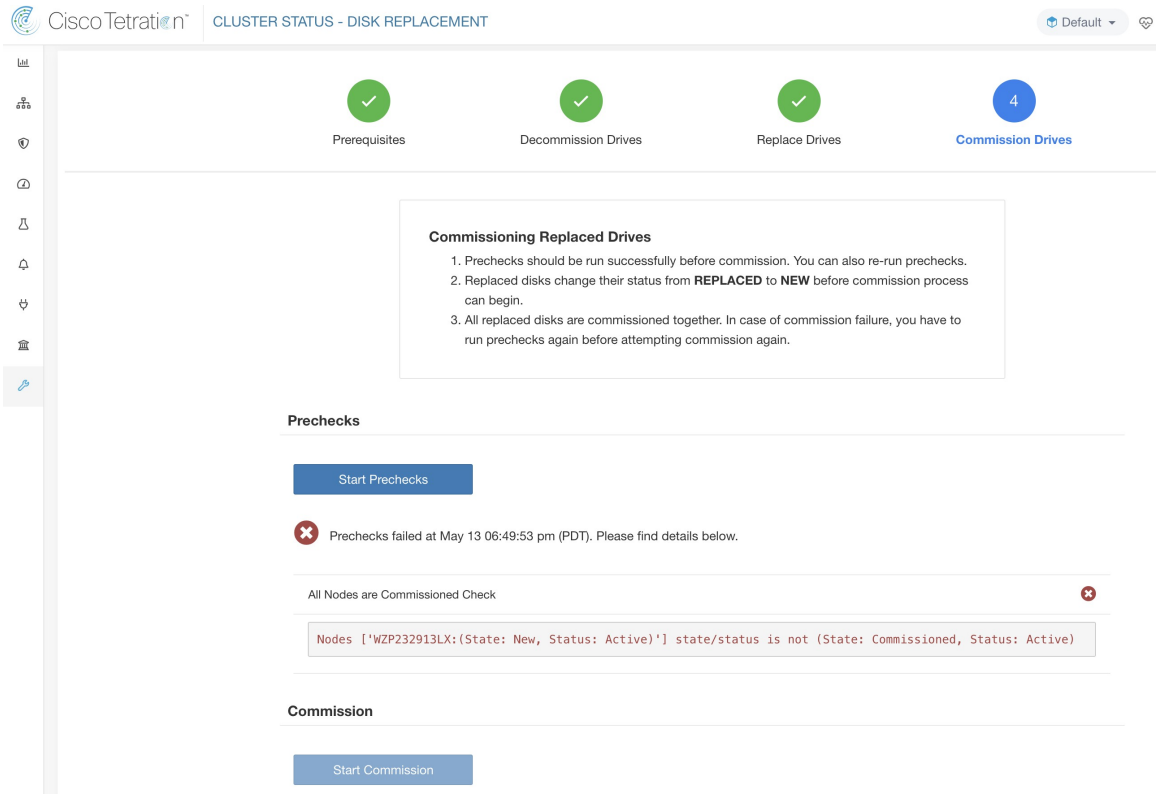
- Le disque contenant les volumes racine du serveur ne peut pas être remplacé à l'aide de cette procédure. De telles défaillances de disques doivent être corrigées à l'aide du processus de maintenance du serveur.

- La mise en service du disque ne peut avoir lieu que lorsque tous les serveurs sont actifs et en état de mise en service. Consultez la section *Special Handling* (manutention spéciale) qui décrit comment procéder dans les cas où une combinaison de remplacement du disque et du serveur est nécessaire.
- Les disques SSD sont trop chers et ont un taux de défaillance très faible. Nous ne voulons donc pas perdre une capacité précieuse pour le stockage de données redondantes.
- Sur les grappes M6 déployées à l'origine avec le logiciel 3.8, lorsqu'un serveur est mis en service avec le logiciel 3.9, la configuration RAID sera appliquée aux disques durs. Ainsi, une grappe contiendra certains nœuds avec la configuration de disques RAID et d'autres non RAID dans la version 3.8. Il est probable que votre matériel Cisco Secure Workload 39RU ait été livré à l'origine avec la version 3.9 déjà installée, mais certains des premiers M6 ont été livrés avec la version 3.8 déployée.
- Vous pouvez convertir une grappe au format RAID si la désactivation et la mise en service du serveur sont effectuées progressivement sur tous les serveurs après mise à niveau vers la version 3.9 du logiciel.
- Les grappes M6 8RU sont uniquement des nœuds SSD et RAID n'est pas configuré sur les disques SSD. Par conséquent, les 8RU ne disposent pas de RAID.
- La configuration de disques sur des générations antérieures (M4/M5) nous empêche de prendre en charge RAID sur ces générations de matériel Cisco Secure Workload.

Remplacements des disques et des serveurs

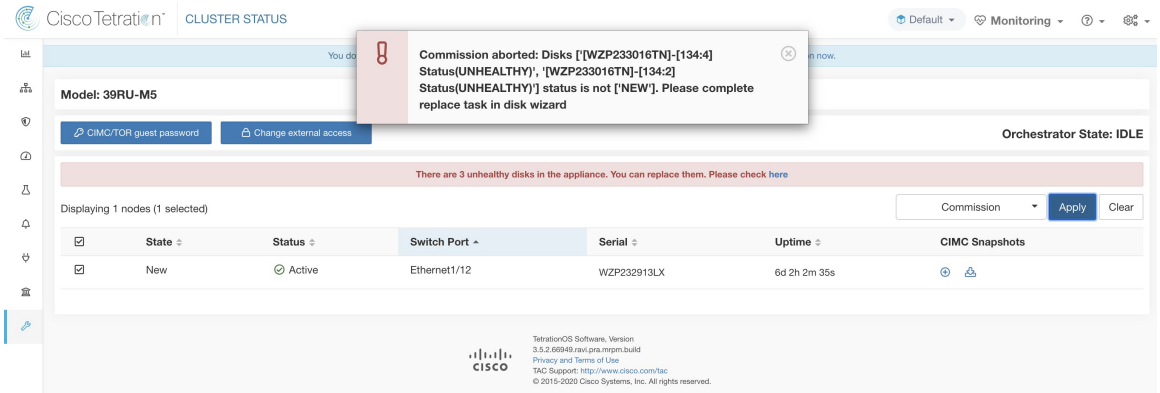
Dans le cas des scénarios de défaillance dans lesquels un disque et un serveur doivent être mis en service simultanément, l'utilisateur est censé mettre hors service et remplacer tous les disques qui peuvent être mis hors service. La mise en service de ces disques serait empêchée par la vérification préalable qui assure que

1. Tous les disques non intègres sont à l'état NEW (NOUVEAU)
2. Tous les serveurs sont dans l'état *commissioned* (mis en service) avec l'état *active* (actif)



Une fois que tous les disques UNHEALTHY (NON INTÈGRE) sont à l'état NEW (NOUVEAU), le serveur défaillant doit être mis hors service/recréé dans l'image/remis en service à l'aide de la procédure d'entretien du serveur.

Désormais, la mise en service du serveur sera bloquée si un disque n'est pas dans l'état HEALTHY (INTÈGRE) ou NEW (NOUVEAU). Une mise en service réussie du serveur aura également pour effet de rendre l'état de tous les disques HEALTHY (INTÈGRE)



Opérations d'entretien de la grappe

Cette section décrit les opérations d'entretien qui affectent l'ensemble de la grappe.

Arrêter la grappe Cisco Secure Workload

L'arrêt de la grappe arrête tous les processus Cisco Secure Workload en cours et met hors tension tous les nœuds. Effectuez les étapes suivantes pour arrêter la grappe.

Lancer l'arrêt de la grappe

Procedure

Étape 1 Dans le volet de navigation, choisissez **Platform (Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)** .

Étape 2 Cliquez sur l'onglet **Reboot/Shutdown** (Redémarrage/arrêt).

Étape 3 Sélectionnez **Shutdown** (Arrêt) et cliquez sur **Send Shutdown Link** (Envoyer un lien d'arrêt). Le lien d'arrêt est envoyé à l'adresse courriel .

Figure 80: Adresse courriel relative à l'arrêt

Hello Site Admin!

We received a request that you intend to shutdown the cluster "98". You can do this through the link below.

Shutdown 98 (For best results, please use Google Chrome)

The above link expires by Jul 22 08:34:30 pm (PDT).

If you didn't request this, please ignore this email.

Shutdown will not be triggered until you actually click the above link.

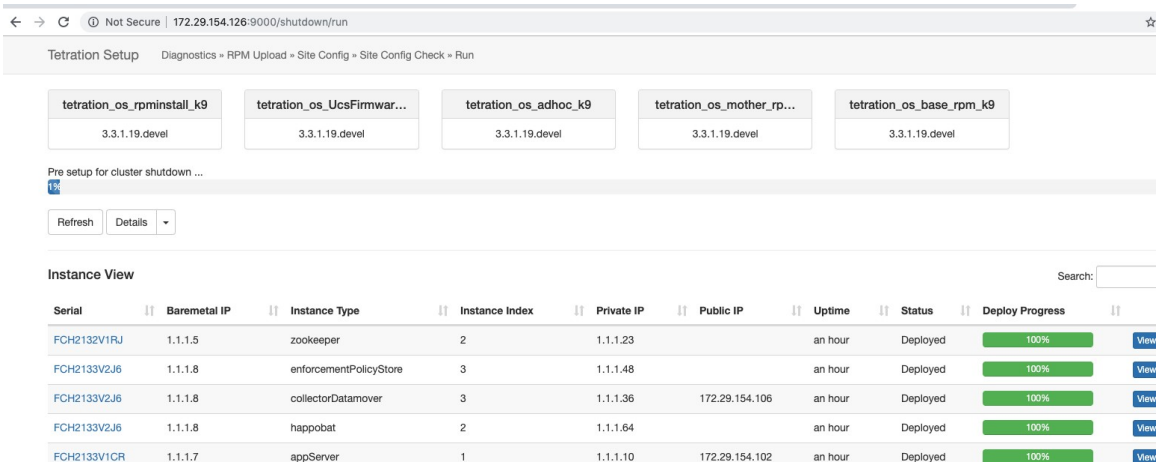
Étape 4 Dans la page **Cluster Shutdown** (arrêt de la grappe), cliquez sur **Shutdown** (Arrêt).

Important Vous ne pouvez pas annuler l'arrêt après avoir cliqué sur le bouton **Shutdown** (Arrêt).

Progression de l'arrêt de la grappe

Après avoir lancé l'arrêt de la grappe, la progression de l'arrêt et l'état sont affichés.

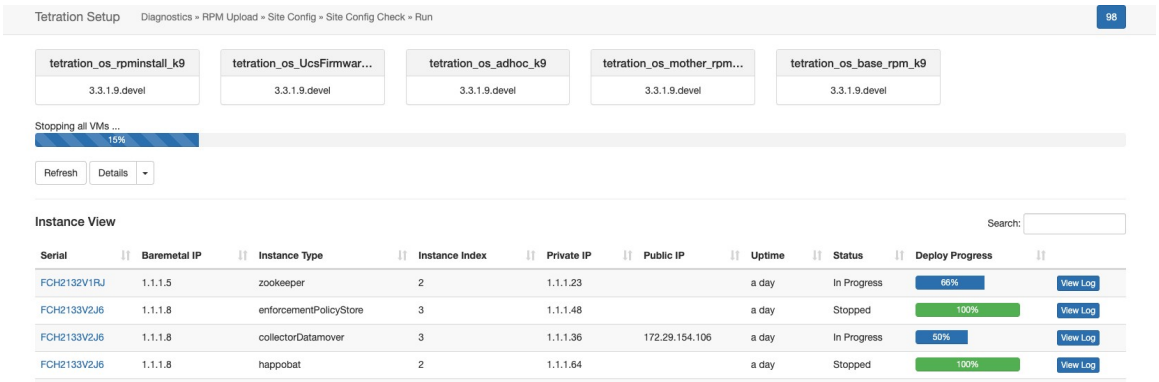
Figure 81: Progression de l'arrêt de la grappe



Si une erreur se produit lors des vérifications préalables à l'arrêt initiales, la barre de progression devient rouge. Vous devez alors cliquer sur le bouton de reprise pour redémarrer l'arrêt après avoir corrigé les erreurs.

Une fois les vérification préalables terminées, les machines virtuelles sont arrêtées. Au fur et à mesure que les machines virtuelles s'arrêtent, la progression s'affiche. La page est similaire à l'arrêt de la machine virtuelle en cas de mises à niveau. Pour en savoir plus, reportez-vous à la section relative aux mises à niveau de chaque champ. L'arrêt de toutes les machines virtuelles peut prendre jusqu'à 30 minutes.

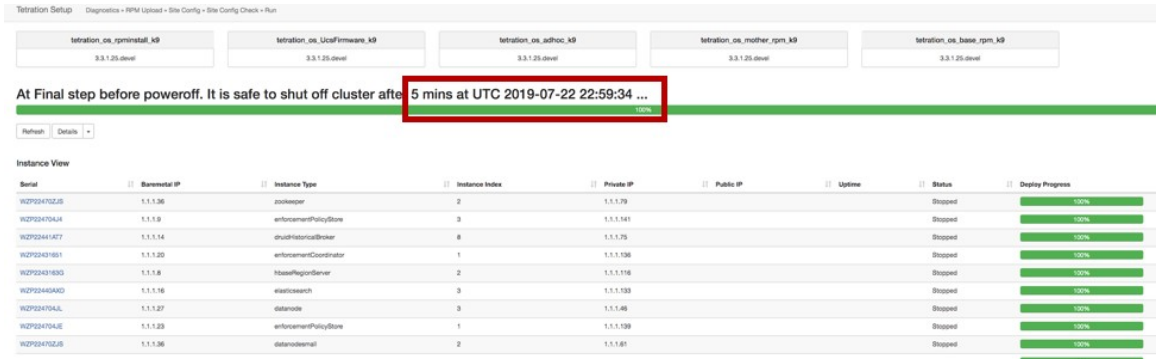
Figure 82: Arrêter les VM



Lorsque la grappe est prête à être arrêtée, la barre de progression passe à 100 % et indique le délai après lequel il est possible d'éteindre la grappe en toute sécurité. Consultez la mise en évidence dans la capture d'écran suivante.

Note Ne mettez pas la grappe hors tension avant d'avoir attendu que l'heure s'affiche dans la barre de progression.

Figure 83: Arrêt à 100 %



Redémarrer la grappe Cisco Secure Workload

Pour récupérer la grappe après l'arrêt, mettez sous tension les éléments sans système d'exploitation. Lorsque tous les éléments sans système d'exploitation sont opérationnels, l'interface utilisateur devient accessible. Après vous être connecté à la grappe, redémarrez-la pour la rendre opérationnelle.

Note Vous *devez* redémarrer la grappe après un arrêt pour la rendre opérationnelle.

Initier le redémarrage de la grappe

Procedure

Étape 1 Dans le volet de navigation, choisissez **Platform (Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)** .

Étape 2 Cliquez sur l'onglet **Reboot/Shutdown** (Redémarrage/arrêt).

Étape 3 Sélectionnez **Reboot** (Redémarrer) et cliquez sur **Send Reboot Link**(Envoyer le lien de redémarrage).

Cliquez sur le lien que vous recevez sur votre identifiant de courriel pour redémarrer la grappe. Dans la page de configuration de l'interface utilisateur, lancez le redémarrage de la grappe. Pendant le redémarrage, une opération de mise à niveau restreinte est effectuée.

Afficher l'historique des tâches d'entretien de la grappe

Pour afficher les tâches d'entretien de la grappe précédemment exécutées :

1. Accédez à **Platform(Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)**, puis cliquez sur l'onglet **History** (Historique).

   La colonne des opérations de grappe répertorie les tâches telles que le déploiement, la mise à niveau, le redémarrage ou l'arrêt.

2. Pour télécharger les journaux des tâches de grappe, cliquez sur **Download Logs** (Télécharger les journaux).

Reset the Secure Workload Cluster

Caution

- The cluster reset process is irreversible. All the data stores within the cluster are cleared.
- During the reset, information about the previous state of the cluster is not saved.
- All the services running on the cluster are stopped.

Note Do not use the **Cluster Reset** option to troubleshoot cluster-related issues. Use the option only when required.

We recommend that you contact Cisco Technical Assistance Center for assistance in resetting the cluster.

The **Reset** option is used to stop all the services and clear all the data stores within the Secure Workload cluster. The reset process takes up to six hours to complete. After the cluster is reset, the services are initialized from the beginning and brought back online.

Note

- The **Cluster Reset** option is applicable to Secure Workload on-premises clusters.
- Both the primary and the secondary clusters can be reset.
- *The **Cluster Reset** option can also be used to switch the cluster mode from active to standby (to configure the primary cluster as the secondary cluster.)*
- Only site admins can reset clusters.

Procedure

Étape 1 From the navigation pane, choose **Platform** > **Upgrade/Reboot/Shutdown**.

Étape 2 Click **Reset** and perform the following actions:

a) Import and verify the SSH key.
b) After the SSH key is verified, select **I acknowledge that the above SSH key is valid**.
c) Select **Reset**.
d) Click **Send Reset Link**.

An email with the IPv4 link and access token is sent to the registered email ID to reset the cluster. The link remains active for six hours. Clicking the link redirects you to the **Cisco Secure Workload Setup** page.

Étape 3 On the **Cisco Secure Workload Setup** page, perform the following actions:

a) Click **Reset**, and to confirm, click **Yes**.

The services are stopped and the data stores within the cluster are deleted. The progress of the activity is displayed and it takes around 10 minutes to complete.

Caution During the cluster reset process, the Secure Workload GUI and Secure Workload Setup page are not available for 20 to 30 minutes.

After the process is completed, the **Site Config** page is displayed. The required RPMs that have to deploy the cluster are automatically uploaded and the corresponding site configurations configured.

Note You are automatically redirected to the **Site Config** page. The following steps will not work if you try to access the page before the redirection. If redirection takes time to get completed when RPMs and backup data are being uploaded, contact Cisco Technical Assistance Center.

b) To change the cluster mode to **Standby**, click the **Standby Config** toggle button.
c) Enter the primary cluster site name and FQDNs.
d) Click **Continue**.

Note On the **Deploy** page, if you click **Reset Deployment** during the cluster reset operation, then the external IP address is cleared and all the site information must be configured. The **Secure Workload Setup** page can be accessed only on 2.2.2.2.

After 4 to 5 hours, the Secure Workload cluster is deployed and the services are brought back online.

Note If the primary cluster is reset, you must reconfigure all the required software agents, secure connector, connectors, external orchestrators, and other configurations.

Known Issues During Secure Workload Cluster Reset

Note The Secure Workload UI is not available during Cluster Reset. Any failure after the UI becomes inaccessible cannot be resumed. To troubleshoot and deploy the cluster, contact Cisco Technical Assistance Center .

Known Issues

- During the cluster reset operation, the Secure Workload UI and Secure Workload Setup page are not accessible for 20–30 minutes.
- The cluster is reset to the base Secure Workload release version and not to the patch release. Manually upgrade the cluster to the patch release. For more information on upgrading to the patch releases, see Cisco Secure Workload Upgrade Guide.
- You must use the IPv4 link that is provided in the email to reset the cluster; IPv6 link is not supported.
- Only the necessary site configurations are editable during cluster reset, other options cannot be edited.

Administrateur de surveilleur de données : surveilleurs de données

Dérivations de données

Note Cisco Secure Workload prend en charge l'écriture sur Kafka Broker 0.9.x, 10.1.x, 1.0.x et 1.1.x pour les dérivations de données.

Pour envoyer des alertes à partir de la grappe Cisco Secure Workload, vous devez utiliser un surveilleur de données configuré. Les utilisateurs administrateurs surveilleurs de données peuvent configurer et activer des surveilleurs de données nouveaux ou existants. Vous pouvez afficher les dérivations de données de votre **détenteur**.

Figure 84: Dérivations de données disponibles

Pour gérer les surveilleurs de données, dans le volet de navigation, choisissez **Manage (Gestion)** > **Data Tap Admin (Administration des surveilleurs de données)**.

Configuration KafKa recommandée

Lors de la configuration de la grappe Kafka, nous vous recommandons d'utiliser les ports de 9092, 9093 ou 9094, car Cisco Secure Workload ouvre ces ports pour le trafic sortant pour Kafka.

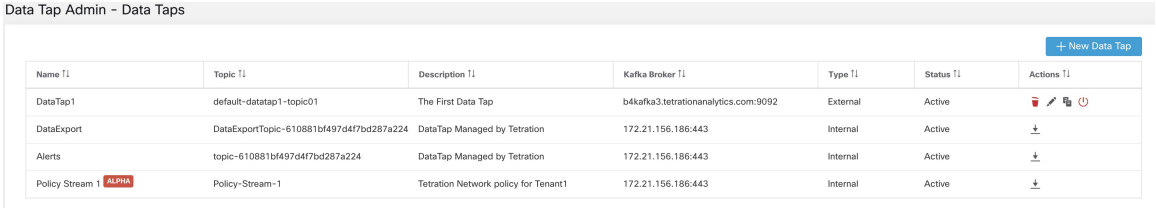
Voici les paramètres recommandés pour les intermédiaires de Kafka :

```
  broker.id=<incremental number based on the size of the cluster>
  auto.create.topics.enable=true
  delete.topic.enable=true
  listeners=PLAINTEXT://:9092
  port=9092
  default.replication.factor=2
  host.name=<your_host_name>
  advertised.host.name=<your_adversited_hostname>
  num.network.threads=12
  num.io.threads=12
  socket.send.buffer.bytes=102400
  socket.receive.buffer.bytes=102400
  socket.request.max.bytes=104857600
  log.dirs=<directory where logs can be written, ensure that there is sufficient space to
hold the kafka journal logs>
  num.partitions=72
  num.recovery.threads.per.data.dir=1
  log.retention.hours=24
  log.segment.bytes=1073741824
  log.retention.check.interval.ms=300000
  log.cleaner.enable=false
  zookeeper.connect=<address of zookeeper ensemble>
  zookeeper.connection.timeout.ms=18000
```

Section d'administration du surveilleurs de données

Les **administrateurs de surveilleurs de données** peuvent afficher les surveilleurs de données disponibles et les configurer en accédant à **Manage(Gestion)** > **Data Tap Admin(Administration des surveilleurs de données)** > **Data Taps (Surveilleurs de données)**. Les dérivations de données sont configurées par **détenteur**.

Figure 85: Toutes les dérivations de données disponibles

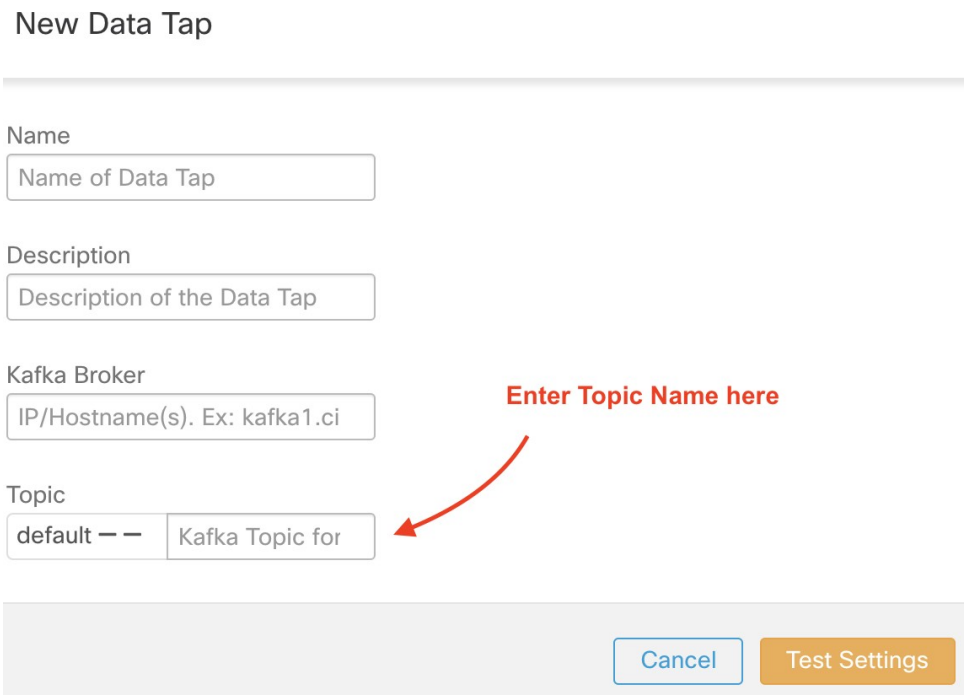


Ajout d'un nouveau surveilleur de données

Les administrateurs de dérivateurs de données peuvent cliquer sur le bouton 

pour ajouter un nouveau dérivateur de données.

Figure 86: Ajout d'un nouveau surveilleur de données

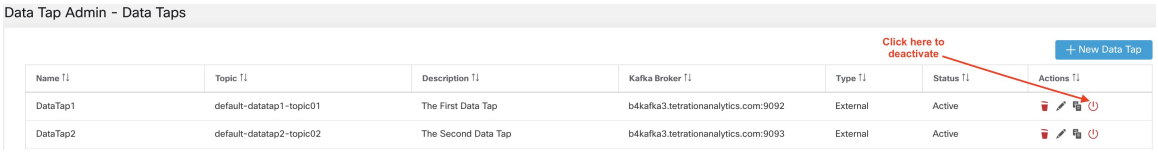


Note La modification des valeurs de surveillance de données nécessite la validation des paramètres.

Désactivation d'un surveilleur de données

Pour empêcher temporairement les messages sortants de Cisco Secure Workload, un administrateur de surveilleurs de données peut en désactiver un. Les messages destinés à ce surveilleur de données ne seront pas envoyés. Le surveilleur de données peut être réactivé à tout moment.

Figure 87: Désactivation d'un surveilleur de données



Suppression d'un surveilleur de données

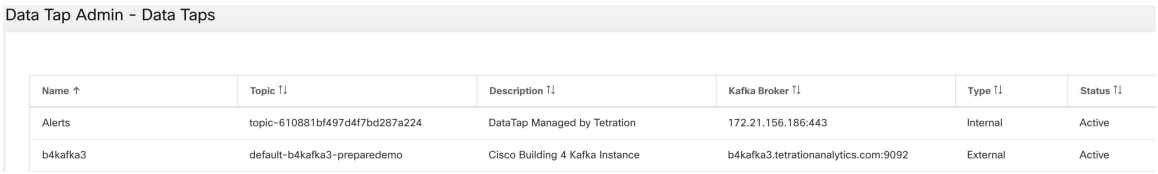
La suppression d'un surveilleur de données supprime toutes les instances des applications Cisco Secure Workload qui dépendent de cette application. Par exemple, si un utilisateur a spécifié que des alertes de conformité doivent être envoyées à surveilleur de données (DataTap) A (dans l'application alerts Cisco Secure Workload), et qu'un administrateur supprime le surveilleur de données A, l'application Alerts ne répertoriera plus le surveilleur de données A comme sortie d'alerte.

Dérivations de données gérées

Les dérivations de données gérées (MDT) sont des dérivations de données hébergées dans la grappe Cisco Secure Workload. Il est sécurisé en termes d'authentification, de chiffrement et d'autorisation. Pour envoyer et recevoir des messages des MDT, les clients doivent être authentifiés, les données envoyées de manière filaire sont chiffrées, et seuls les utilisateurs autorisés peuvent lire ou écrire des messages depuis ou à destination de Cisco Secure Workload MDT. Cisco Secure Workload fournit des certificats clients à télécharger à partir de l'interface graphique. Cisco Secure Workload utilise Apache Kafka 1.1.0 comme agent de messages, et nous recommandons que les clients utilisent des clients sécurisés compatibles avec la même version.

Les MDT sont automatiquement créés après la création de la portée racine. Un MDT Alertes est créé pour chaque portée racine. Pour récupérer des alertes de la grappe Cisco Secure Workload, vous devez utiliser l'outil MDT Alerts. Seuls les utilisateurs administrateurs de surveilleurs de données peuvent télécharger les certificats. Vous pouvez afficher les programmes MDT de votre **portée racine**.

Figure 88: Liste des dérivations de données configurées



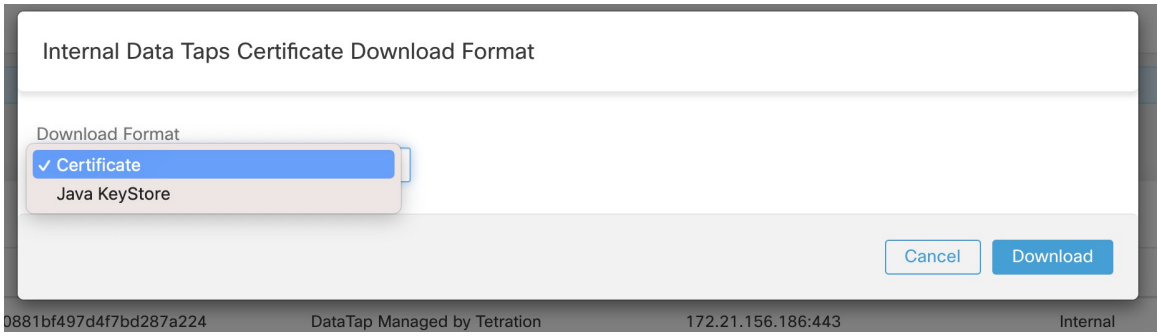
Toutes les alertes Cisco Secure Workload sont envoyées à MDT par défaut, mais peuvent être remplacées par d'autres dérivations de données.

Vous avez le choix entre deux options pour télécharger les certificats :

- Java KeyStore : le format JKS fonctionne bien avec le client Java.
- Certificat : les certificats standard sont plus faciles à utiliser avec les clients Go.

Figure 89: Télécharger des certificats

Figure 90: Types de certificats



Magasin de clés Java

Après avoir téléchargé *alerts.jks.tar.gz*, vous devriez voir les fichiers suivants qui contiennent des informations pour se connecter au MDT Cisco Secure Workload pour recevoir des messages :

- kafkaBrokerIps.txt : ce fichier contient la chaîne d'adresse IP que le client Kafka utilise pour se connecter au MDT Cisco Secure Workload.
- topic.txt : ce fichier contient la rubrique à partir de laquelle ce client peut lire les messages. Les sujets sont au format topic<root_scope_id>. Utilisez ce root_scope_id lors de la configuration d'autres propriétés du client Java.
- keystore.jks : magasin de clés que le client Kafka doit utiliser dans les paramètres de connexion indiqués ci-dessous.
- truststore.jks : le fichier de confiance que le client Kafka doit utiliser dans les paramètres de connexion indiqués ci-dessous.
- passphrase.txt : ce fichier contient le mot de passe à utiliser pour les numéros 3 et 4.

Les paramètres Kafka suivants doivent être utilisés lors de la configuration du fichier Consumer.properties (client Java) qui utilise le fichier de clés et le fichier de certificats :

```
security.protocol=SSL
ssl.truststore.location=<location_of_truststore_downloaded>
ssl.truststore.password=<passphrase_mentioned_in_passphrase.txt>
ssl.keystore.location=<location_of_truststore_downloaded>
ssl.keystore.password=<passphrase_mentioned_in_passphrase.txt>
ssl.key.password=<passphrase_mentioned_in_passphrase.txt>
```

Lors de la configuration du consommateur Kafka dans le code Java, utilisez les propriétés suivantes :

```
Properties props = new Properties();
props.put("bootstrap.servers", brokerList);
```

```
    props.put("group.id", ConsumerGroup-<root_scope_id>);  // root_scope_id is same as
mentioned above
    props.put("key.deserializer",
"org.apache.kafka.common.serialization.StringDeserializer");
    props.put("value.deserializer",
"org.apache.kafka.common.serialization.StringDeserializer");
    props.put("enable.auto.commit", "true");
    props.put("auto.commit.interval.ms", "1000");
    props.put("session.timeout.ms", "30000");
    props.put("security.protocol", "SSL");
    props.put("ssl.truststore.location", "<filepath_to_truststore.jks>");
    props.put("ssl.truststore.password", passphrase);
    props.put("ssl.keystore.location", <filepath_to_keystore.jks>);
    props.put("ssl.keystore.password", passphrase);
    props.put("ssl.key.password", passphrase);
    props.put("zookeeper.session.timeout.ms", "500");
    props.put("zookeeper.sync.time.ms", "250");
    props.put("auto.offset.reset", "earliest");
```

Certificat

Si vous souhaitez utiliser des certificats, utilisez les clients Go en utilisant la bibliothèque Sarama Kafka pour vous connecter au MDT Cisco Secure Workload. Après avoir téléchargé *alerts.cert.tar.gz*, vous devriez voir les fichiers suivants :

- kafkaBrokerIps.txt : ce fichier contient la chaîne d'adresse IP que le client Kafka utilise pour se connecter au MDT Cisco Secure Workload
- topic : ce fichier contient la rubrique à partir de laquelle ce client peut lire les messages. Les sujets sont au format topic<root_scope_id>. Utilisez cet identifiant root_scope_id lors de la configuration d'autres propriétés du client Java.
- KafkaConsumerCA.cert : ce fichier contient le certificat client Kafka.
- KafkaConsumerPrivateKey.key : ce fichier contient la clé privée du consommateur Kafka.
- KafkaCA.cert : ce fichier doit être utilisé dans la liste des certificats d'autorité de certification racine dans le client Go.

Pour voir un exemple d'un client Go se connectant au MDT Cisco Secure Workload, consultez Exemple de client Go recevant les alertes de MDT.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.