Red Hat Enterprise Linux 9

Gestion des systèmes à l'aide de la console web RHEL 9

Gestion du serveur à l'aide d'une interface graphique basée sur le web

Last Updated: 2024-02-27

Red Hat Enterprise Linux 9 Gestion des systèmes à l'aide de la console web RHEL 9

Gestion du serveur à l'aide d'une interface graphique basée sur le web

Notice légale

Copyright © 2023 Red Hat, Inc.

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

Résumé

La console web RHEL est une interface graphique basée sur le web, qui repose sur le projet Cockpit en amont. En l'utilisant, vous pouvez effectuer des tâches d'administration du système, telles que l'inspection et le contrôle des services systemd, la gestion du stockage, la configuration des réseaux, l'analyse des problèmes de réseau et l'inspection des journaux.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le message de notre directeur technique Chris Wright.

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

Soumettre des commentaires sur des passages spécifiques

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

Soumettre des commentaires via Bugzilla (compte requis)

1. Connectez-vous au site Web de Bugzilla.
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.

CHAPITRE 1. COMMENCER À UTILISER LA CONSOLE WEB RHEL

Installer la console web dans Red Hat Enterprise Linux 9 et apprendre à ajouter des hôtes distants et à les surveiller dans la console web de RHEL 9.

Conditions préalables

- Installation de Red Hat Enterprise Linux 9.
- Activation de la mise en réseau.
- Système enregistré avec l'abonnement approprié.

1.1. QU'EST-CE QUE LA CONSOLE WEB RHEL ?

La console web RHEL est une interface web Red Hat Enterprise Linux conçue pour gérer et surveiller votre système local, ainsi que les serveurs Linux situés dans votre environnement réseau.

La console web RHEL vous permet d'effectuer un large éventail de tâches d'administration, notamment :

- Gestion des services
- Gestion des comptes d'utilisateurs
- Gestion et surveillance des services du système
- Configuration des interfaces réseau et du pare-feu
- Examen des journaux du système
- Gestion des machines virtuelles
- Création de rapports de diagnostic
- Configuration de la vidange du noyau
- Configuration de SELinux
- Mise à jour du logiciel
- Gestion des abonnements au système

La console web RHEL utilise les mêmes API système que celles d'un terminal, et les actions effectuées dans un terminal sont immédiatement répercutées dans la console web RHEL.

Vous pouvez surveiller les journaux des systèmes dans l'environnement réseau, ainsi que leurs performances, affichées sous forme de graphiques. En outre, vous pouvez modifier les paramètres directement dans la console web ou via le terminal.

1.2. INSTALLATION ET ACTIVATION DE LA CONSOLE WEB

Pour accéder à la console web RHEL 9, il faut d'abord activer le service **cockpit.socket**.

Red Hat Enterprise Linux 9 inclut la console web RHEL 9 installée par défaut dans de nombreuses variantes d'installation. Si ce n'est pas le cas sur votre système, installez le paquetage **cockpit** avant d'activer le service **cockpit.socket**.

Procédure

1. Si la console web n'est pas installée par défaut sur votre variante d'installation, installez manuellement le paquet **cockpit**:

```
# dnf install cockpit
```

2. Activez et démarrez le service **cockpit.socket**, qui exécute un serveur web :

```
# systemctl enable --now cockpit.socket
```

3. Si la console web n'a pas été installée par défaut sur votre variante d'installation et que vous utilisez un profil de pare-feu personnalisé, ajoutez le service **cockpit** à **firewalld** pour ouvrir le port 9090 dans le pare-feu :

```
# firewall-cmd --add-service=cockpit --permanent
# firewall-cmd --reload
```

Verification steps

- Pour vérifier l'installation et la configuration précédentes, ouvrez la console web.

1.3. SE CONNECTER À LA CONSOLE WEB

Suivez les étapes de cette procédure pour la première connexion à la console web RHEL à l'aide d'un nom d'utilisateur et d'un mot de passe système.

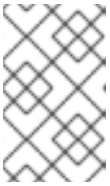
Conditions préalables

- Utilisez l'un des navigateurs suivants pour ouvrir la console web :
  - Mozilla Firefox 52 et versions ultérieures
  - Google Chrome 57 et versions ultérieures
  - Microsoft Edge 16 et versions ultérieures
- Informations d'identification du compte d'utilisateur du système
  La console web RHEL utilise une pile PAM spécifique située à l'adresse **/etc/pam.d/cockpit**. Utilisez PAM pour vous connecter avec le nom d'utilisateur et le mot de passe de n'importe quel compte local sur le système.

Procédure

1. Dans votre navigateur web, entrez l'adresse suivante pour accéder à la console web :

```
https://localhost:9090
```



NOTE

Cela permet de se connecter à la console web sur votre machine locale. Si vous souhaitez vous connecter à la console web d'un système distant, voir Section 1.6, « Connexion à la console web à partir d'une machine distante »

Si vous utilisez un certificat auto-signé, le navigateur affiche un avertissement. Vérifiez le certificat et acceptez l'exception de sécurité pour poursuivre la connexion.

La console charge un certificat à partir du répertoire **/etc/cockpit/ws-certs.d** et utilise le dernier fichier avec une extension **.cert** dans l'ordre alphabétique. Pour éviter de devoir accorder des exceptions de sécurité, installez un certificat signé par une autorité de certification (CA).

2. Dans l'écran de connexion, saisissez votre nom d'utilisateur et votre mot de passe.
3. Cliquez sur **Log In**.

Une fois l'authentification réussie, l'interface de la console web RHEL s'ouvre.

NOTE

Pour passer de l'accès limité à l'accès administratif, cliquez sur **Administrative access** ou **Limited access** dans le panneau supérieur de la page de la console web. Vous devez fournir votre mot de passe d'utilisateur pour obtenir l'accès administratif.

1.4. MODIFIER LE STYLE PAR DÉFAUT DE LA CONSOLE WEB

Par défaut, la console web adopte les paramètres de style de votre navigateur. Vous pouvez remplacer le paramètre de style par défaut à partir de l'interface de la console web RHEL 9.

Conditions préalables

- La console web est installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Dans le coin supérieur droit, cliquez sur le bouton **Session**.
3. Dans la section **Style**, choisissez le paramètre préféré. Le paramètre **Default** utilise le même paramètre de style que votre navigateur.

Verification steps

1. Le réglage du style a été modifié en fonction du style défini.

1.5. DÉSACTIVATION DE L'AUTHENTIFICATION DE BASE DANS LA CONSOLE WEB

Vous pouvez modifier le comportement d'un schéma d'authentification en modifiant le fichier **cockpit.conf**. Utilisez l'action **none** pour désactiver un schéma d'authentification et n'autoriser que l'authentification via GSSAPI et les formulaires.

Conditions préalables

- La console web est installée et accessible. Pour plus de détails, voir Installation de la console web.
- Vous devez avoir les privilèges sudo.

Procédure

1. Ouvrez ou créez le fichier **cockpit.conf** dans le répertoire **/etc/cockpit/** dans un éditeur de texte de votre choix.

```
$ sudo vi cockpit.conf
```

2. Ajouter le texte suivant :

```
[basic]
action = none
```

3. Enregistrer le fichier.
4. Redémarrez la console web pour que les modifications soient prises en compte.

```
# systemctl try-restart cockpit
```

1.6. CONNEXION À LA CONSOLE WEB À PARTIR D'UNE MACHINE DISTANTE

Il est possible de se connecter à l'interface de votre console web à partir de n'importe quel système d'exploitation client, ainsi qu'à partir de téléphones mobiles ou de tablettes.

Conditions préalables

- Appareil équipé d'un navigateur Internet compatible, tel que :
  - Mozilla Firefox 52 et versions ultérieures
  - Google Chrome 57 et versions ultérieures
  - Microsoft Edge 16 et versions ultérieures
- Le serveur RHEL 9 auquel vous souhaitez accéder dispose d'une console web installée et accessible.

Procédure

1. Ouvrez votre navigateur web.
2. Saisissez l'adresse du serveur distant dans l'un des formats suivants :

a. Avec le nom d'hôte du serveur : **https://server.hostname.example.com:port_number**.
Par exemple :

```
https://example.com:9090
```

b. Avec l'adresse IP du serveur : **https://server.IP_address:port_number**
Par exemple :

```
https://192.0.2.2:9090
```

3. Une fois l'interface de connexion ouverte, connectez-vous avec vos informations d'identification de la machine RHEL.

1.7. CONNEXION À LA CONSOLE WEB À PARTIR D'UNE MACHINE DISTANTE EN TANT QU'UTILISATEUR ROOT

Sur les nouvelles installations de RHEL 9.2 ou ultérieures, la console web RHEL désactive par défaut les connexions au compte root pour des raisons de sécurité. Vous pouvez autoriser le login **root** dans le fichier **/etc/cockpit/disallowed-users**.

Conditions préalables

- La console web RHEL 9 est installée et activée. Pour plus de détails, voir Installation de la console web.

Procédure

1. Ouvrez le fichier disallowed-users dans le répertoire **/etc/cockpit/** dans un éditeur de texte de votre choix.

```
# cat /etc/cockpit/disallowed-users
# List of users which are not allowed to login to Cockpit root
```

1. Modifiez ce fichier et supprimez la ligne relative à l'utilisateur **root**.

Vérification

- Connectez-vous à la console web en tant qu'utilisateur **root**. Pour plus de détails, voir Connexion à la console web .

1.8. CONNEXION À LA CONSOLE WEB À L'AIDE D'UN MOT DE PASSE À USAGE UNIQUE

Si votre système fait partie d'un domaine de gestion des identités (IdM) avec une configuration de mot de passe à usage unique (OTP) activée, vous pouvez utiliser un OTP pour vous connecter à la console web RHEL.

IMPORTANT

Il n'est possible de se connecter à l'aide d'un mot de passe à usage unique que si votre système fait partie d'un domaine de gestion des identités (IdM) dont la configuration OTP est activée.

Conditions préalables

- La console web RHEL a été installée.
- Un serveur de gestion des identités dont la configuration OTP est activée.
- Dispositif matériel ou logiciel configuré générant des jetons OTP.

Procédure

1. Ouvrez la console web RHEL dans votre navigateur :
   - Localement : **https://localhost:PORT_NUMBER**
   - À distance avec le nom d'hôte du serveur : **https://example.com:PORT_NUMBER**
   - A distance avec l'adresse IP du serveur : **https://EXAMPLE.SERVER.IP.ADDR:PORT_NUMBER**
     Si vous utilisez un certificat auto-signé, le navigateur émet un avertissement. Vérifiez le certificat et acceptez l'exception de sécurité pour procéder à la connexion.

     La console charge un certificat à partir du répertoire **/etc/cockpit/ws-certs.d** et utilise le dernier fichier avec une extension **.cert** dans l'ordre alphabétique. Pour éviter de devoir accorder des exceptions de sécurité, installez un certificat signé par une autorité de certification (CA).
2. La fenêtre de connexion s'ouvre. Dans la fenêtre de connexion, saisissez votre nom d'utilisateur et votre mot de passe.
3. Générer un mot de passe à usage unique sur votre appareil.
4. Saisissez le mot de passe à usage unique dans un nouveau champ qui apparaît dans l'interface de la console web après avoir confirmé votre mot de passe.
5. Cliquez sur **Log in**.
6. Une connexion réussie permet d'accéder à la page **Overview** de l'interface de la console web.

1.9. REDÉMARRAGE DU SYSTÈME À L'AIDE DE LA CONSOLE WEB

Vous pouvez utiliser la console web pour redémarrer un système RHEL auquel la console web est attachée.

Conditions préalables

- La console web est installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Dans la page **Overview**, cliquez sur le bouton **Reboot**.

3. Si des utilisateurs sont connectés au système, indiquez la raison du redémarrage dans la boîte de dialogue **Reboot**.
4. Facultatif : dans la liste déroulante **Delay**, sélectionnez un intervalle de temps pour le délai de redémarrage.
5. Cliquez sur **Reboot**.

1.10. ARRÊT DU SYSTÈME À L'AIDE DE LA CONSOLE WEB

Vous pouvez utiliser la console web pour arrêter un système RHEL auquel la console web est attachée.

Conditions préalables

- La console web est installée et accessible.

Procédure

1. Connectez-vous à la console web RHEL.
2. Cliquez sur **Overview**.
3. Dans la liste déroulante **Restart**, sélectionnez **Shut Down**.
4. Si des utilisateurs sont connectés au système, indiquez la raison de l'arrêt dans la boîte de dialogue **Shut Down**.
5. Facultatif : dans la liste déroulante **Delay**, sélectionnez un intervalle de temps.
6. Cliquez sur **Shut Down**.

1.11. CONFIGURATION DES PARAMÈTRES HORAIRES À L'AIDE DE LA CONSOLE WEB

Vous pouvez définir un fuseau horaire et synchroniser l'heure du système avec un serveur NTP (Network Time Protocol).

Conditions préalables

- La console web est installée et accessible.

Procédure

1. Connectez-vous à la console web RHEL.
2. Cliquez sur l'heure actuelle du système sur **Overview**.
3. Cliquez sur **System time**.
4. Dans la boîte de dialogue **Change System Time**, modifiez le fuseau horaire si nécessaire.
5. Dans le menu déroulant **Set Time**, sélectionnez l'une des options suivantes :

   Manuellement

   Utilisez cette option si vous devez régler l'heure manuellement, sans serveur NTP.

Utilisation automatique du serveur NTP

Il s'agit d'une option par défaut, qui synchronise automatiquement l'heure avec les serveurs NTP prédéfinis.

Utilisation automatique de serveurs NTP spécifiques

N'utilisez cette option que si vous devez synchroniser le système avec un serveur NTP spécifique. Spécifiez le nom DNS ou l'adresse IP du serveur.

6. Cliquez sur **Change**.

- Vérifiez l'heure système affichée dans l'onglet **System**.

1.12. DÉSACTIVATION DE SMT POUR ÉVITER LES PROBLÈMES DE SÉCURITÉ DE L'UNITÉ CENTRALE EN UTILISANT LA CONSOLE WEB

Désactiver le multithreading simultané (SMT) en cas d'attaques utilisant abusivement le SMT du CPU. La désactivation du SMT peut atténuer les failles de sécurité, telles que L1TF ou MDS.

IMPORTANT

La désactivation de SMT peut réduire les performances du système.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Dans l'onglet **Overview**, trouvez le champ **System information** et cliquez sur **View hardware details**.
3. Sur la ligne **CPU Security**, cliquez sur **Mitigations**.
   Si ce lien n'est pas présent, cela signifie que votre système ne prend pas en charge le SMT et qu'il n'est donc pas vulnérable.
4. Dans le tableau **CPU Security Toggles**, activez l'option **Disable simultaneous multithreading (nosmt)**.
5. Cliquez sur le bouton **Enregistrer et redémarrer**.

Après le redémarrage du système, l'unité centrale n'utilise plus le SMT.

Ressources supplémentaires

- L1TF - L1 Terminal Fault Attack - CVE-2018-3620 & CVE-2018-3646
- MDS - Microarchitectural Data Sampling - CVE-2018-12130, CVE-2018-12126, CVE-2018-12127, et CVE-2019-11091

1.13. AJOUTER UNE BANNIÈRE À LA PAGE DE CONNEXION

Les entreprises ou les agences ont parfois besoin d'afficher un avertissement indiquant que l'utilisation de l'ordinateur se fait à des fins légales, que l'utilisateur est soumis à une surveillance et que toute personne s'introduisant dans l'ordinateur sera poursuivie en justice. L'avertissement doit être visible avant la connexion. Comme pour SSH, la console web peut optionnellement afficher le contenu d'un fichier de bannière sur l'écran de connexion. Pour activer les bannières dans vos sessions de console web, vous devez modifier le fichier **/etc/cockpit/cockpit.conf**. Notez que ce fichier n'est pas obligatoire et que vous devrez peut-être le créer manuellement.

Conditions préalables

- La console web est installée et accessible.
- Vous devez avoir les privilèges sudo.

Procédure

1. Créez le fichier **/etc/issue.cockpit** dans l'éditeur de texte de votre choix si vous ne l'avez pas encore. Ajoutez au fichier le contenu que vous souhaitez afficher comme bannière.
   N'incluez pas de macros dans le fichier car il n'y a pas de reformatage entre le contenu du fichier et le contenu affiché. Utilisez les sauts de ligne prévus. Il est possible d'utiliser l'art ASCII.
2. Enregistrer le fichier.
3. Ouvrez ou créez le fichier **cockpit.conf** dans le répertoire **/etc/cockpit/** dans un éditeur de texte de votre choix.

```
$ sudo vi cockpit.conf
```

4. Ajoutez le texte suivant au fichier :

```
[Session]
Banner=/etc/issue.cockpit
```

5. Enregistrer le fichier.
6. Redémarrez la console web pour que les modifications soient prises en compte.

```
# systemctl try-restart cockpit
```

Verification steps

- Ouvrez à nouveau l'écran de connexion de la console web pour vérifier que la bannière est désormais visible.

Exemple 1.1. Ajout d'un exemple de bannière à la page de connexion

1. Créez un fichier **/etc/issue.cockpit** avec le texte souhaité à l'aide d'un éditeur de texte :

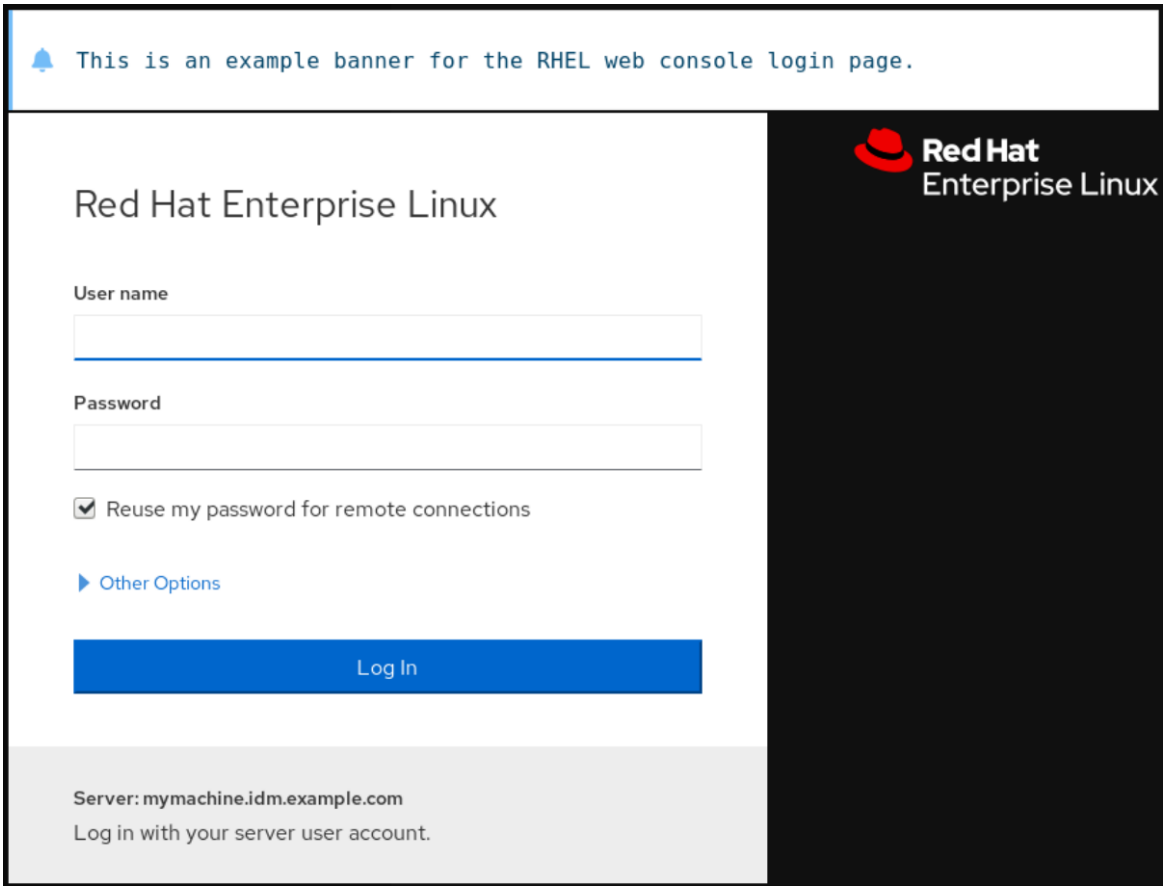
```
Voici un exemple de bannière pour la page de connexion de la console web RHEL.
```

2. Ouvrez ou créez le fichier **/etc/cockpit/cockpit.conf** et ajoutez le texte suivant :

```
[Session]
Banner=/etc/issue.cockpit
```

3. Redémarrez la console web.

4. Ouvrez à nouveau l'écran de connexion de la console web.



1.14. CONFIGURATION DU VERROUILLAGE AUTOMATIQUE DE L'INACTIVITÉ DANS LA CONSOLE WEB

Par défaut, aucun délai d'inactivité n'est défini dans l'interface de la console web. Si vous souhaitez activer un délai d'inactivité sur votre système, vous pouvez le faire en modifiant le fichier de configuration **/etc/cockpit/cockpit.conf**. Notez que ce fichier n'est pas obligatoire et que vous devrez peut-être le créer manuellement.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.
- Vous devez avoir les privilèges sudo.

Procédure

1. Ouvrez ou créez le fichier **cockpit.conf** dans le répertoire **/etc/cockpit/** dans un éditeur de texte de votre choix.

```
$ sudo vi cockpit.conf
```

2. Ajoutez le texte suivant au fichier :

```
[Session]
IdleTimeout=X
```

Remplacez **X** par un nombre pour une période de temps de votre choix en minutes.

3. Enregistrer le fichier.
4. Redémarrez la console web pour que les modifications soient prises en compte.

```
# systemctl try-restart cockpit
```

Verification steps

- Vérifiez si la session vous déconnecte après une période déterminée.

CHAPITRE 2. CONFIGURER LE NOM D'HÔTE DANS LA CONSOLE WEB

Apprenez à utiliser la console web de Red Hat Enterprise Linux pour configurer différentes formes de nom d'hôte sur le système auquel la console web est attachée.

2.1. NOM D'HÔTE

Le nom d'hôte identifie le système. Par défaut, le nom d'hôte est défini sur **localhost**, mais vous pouvez le modifier.

Un nom d'hôte se compose de deux parties :

Nom d'hôte

Il s'agit d'un nom unique qui identifie un système.

Domaine

Ajoutez le domaine comme suffixe derrière le nom d'hôte lorsque vous utilisez un système dans un réseau et lorsque vous utilisez des noms au lieu de simples adresses IP.

Un nom d'hôte auquel est associé un nom de domaine est appelé nom de domaine pleinement qualifié (FQDN). Par exemple : **mymachine.example.com**.

Les noms d'hôtes sont stockés dans le fichier **/etc/hostname**.

2.2. JOLI NOM D'HÔTE DANS LA CONSOLE WEB

Vous pouvez configurer un joli nom d'hôte dans la console web RHEL. Le joli nom d'hôte est un nom d'hôte avec des majuscules, des espaces, etc.

Le joli nom d'hôte s'affiche dans la console web, mais il ne doit pas nécessairement correspondre au nom d'hôte.

> **Exemple 2.1. Formats des noms d'hôtes dans la console web**
>
> **Joli nom d'hôte**
>
> **My Machine**
>
> **Nom d'hôte**
>
> **mymachine**
>
> **Nom d'hôte réel - nom de domaine complet (FQDN)**
>
> **mymachine.idm.company.com**

2.3. DÉFINITION DU NOM D'HÔTE À L'AIDE DE LA CONSOLE WEB

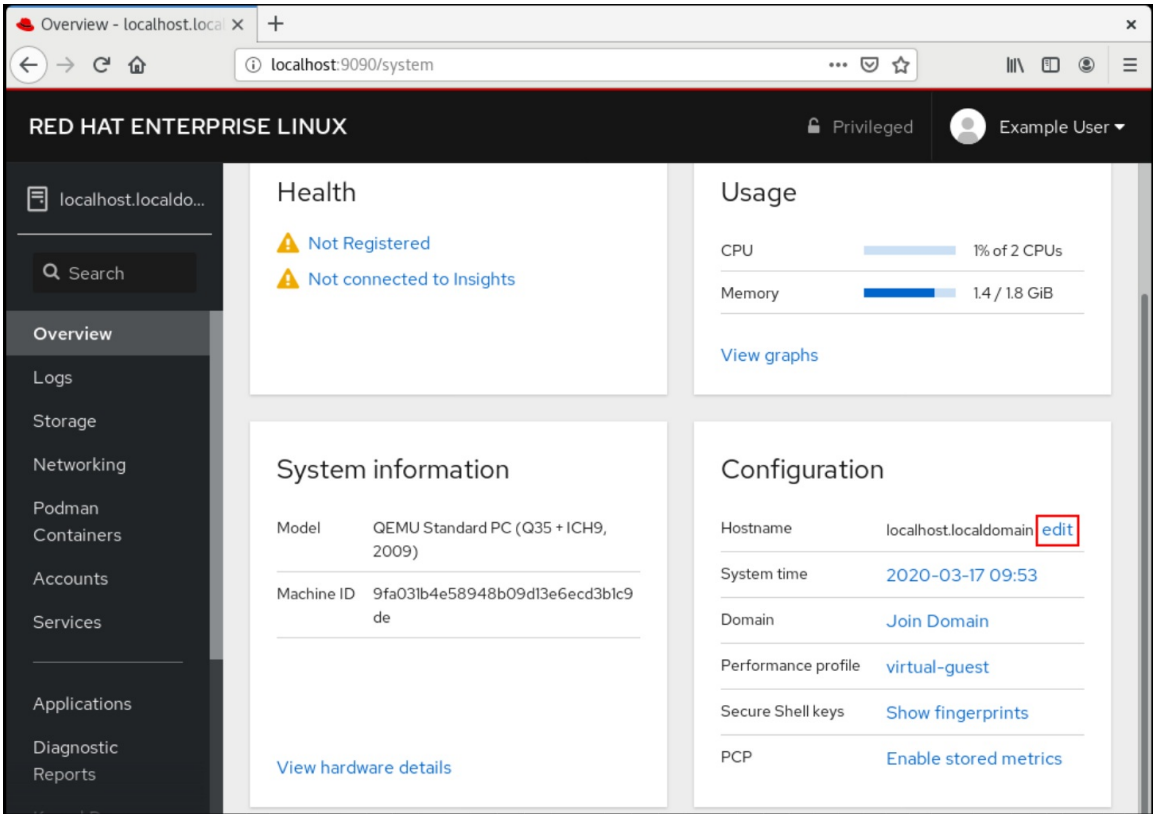
Cette procédure permet de définir le nom d'hôte réel ou le joli nom d'hôte dans la console web.

Conditions préalables

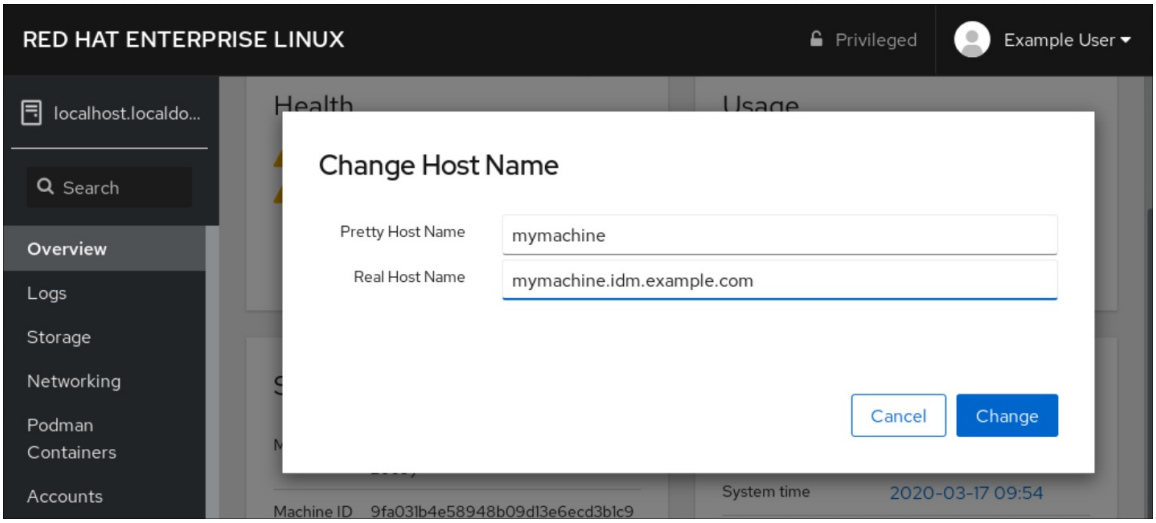
- La console web est installée et accessible.

Procédure

1. Connectez-vous à la console web.
2. Cliquez sur **Vue d'ensemble**.
3. Cliquez sur **modifier** à côté du nom d'hôte actuel.



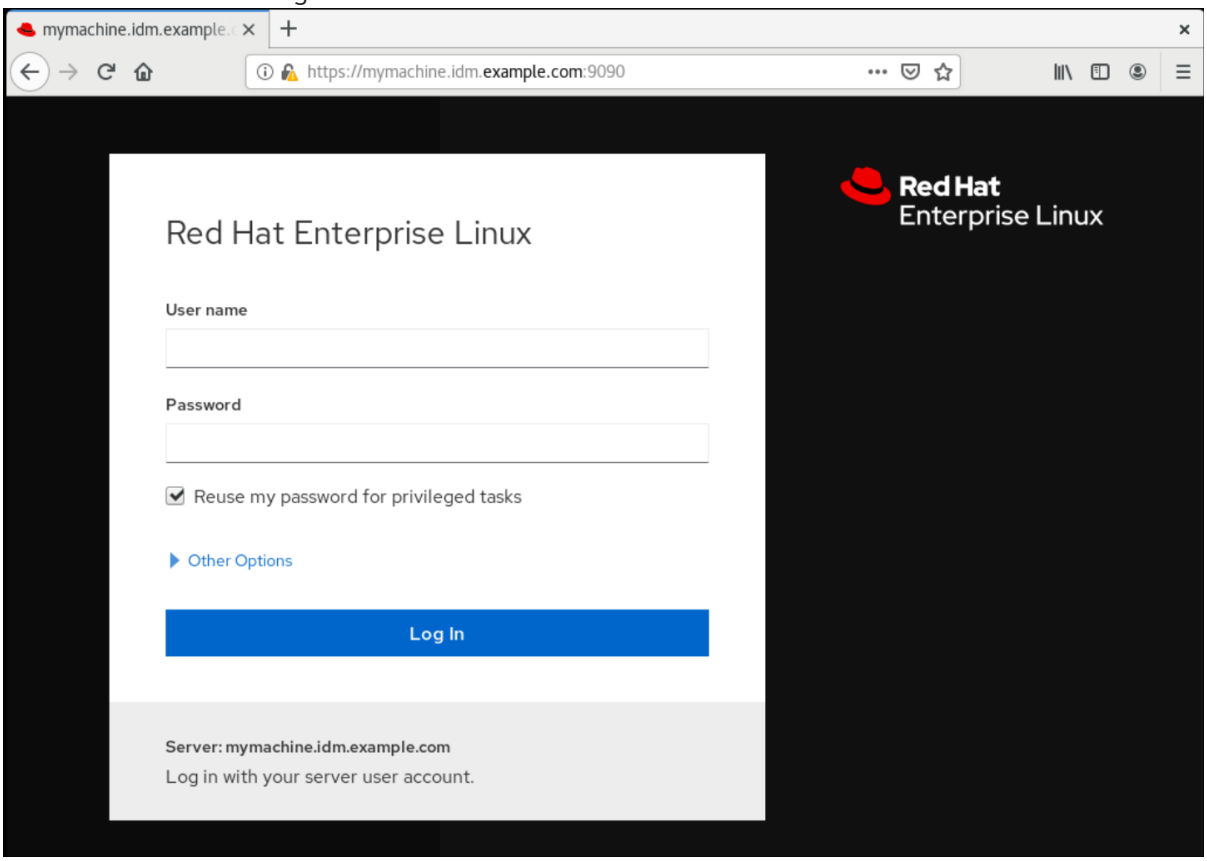
4. Dans la boîte de dialogue **Change Host Name**, saisissez le nom d'hôte dans le champ **Pretty Host Name**.
5. Le champ **Real Host Name** associe un nom de domaine au joli nom.
   Vous pouvez modifier manuellement le nom d'hôte réel s'il ne correspond pas au joli nom d'hôte.
6. Cliquez sur **Modifier**.



Verification steps

1. Déconnectez-vous de la console web.

2. Rouvrez la console web en saisissant une adresse avec le nouveau nom d'hôte dans la barre d'adresse de votre navigateur.



CHAPITRE 3. COMPLÉMENTS À LA CONSOLE WEB DE RED HAT

Installez des modules complémentaires dans la console web RHEL et découvrez les applications complémentaires disponibles.

3.1. INSTALLATION DES MODULES COMPLÉMENTAIRES

Le paquetage **cockpit** fait partie de Red Hat Enterprise Linux par défaut. Pour pouvoir utiliser les applications complémentaires, vous devez les installer séparément.

Conditions préalables

- Installation et activation du paquet **cockpit**.

Procédure

- Installer un module complémentaire.

```
# dnf install <add-on>
```

3.2. MODULES COMPLÉMENTAIRES POUR LA CONSOLE WEB RHEL

Le tableau suivant répertorie les applications complémentaires disponibles pour la console web RHEL.

Nom de la fonctionnalité	Nom du paquet	Utilisation
Compositeur	cockpit-compositeur	Création d'images personnalisées du système d'exploitation
Machines	cockpit-machines	Gérer les machines virtuelles libvirt
PackageKit	kit cockpit-package	Mises à jour de logiciels et installation d'applications (généralement installées par défaut)
PCP	cockpit-pcp	Données de performance persistantes et plus fines (installées à la demande à partir de l'interface utilisateur)
Podman	cockpit-podman	Gestion des conteneurs et gestion des images de conteneurs
Enregistrement de la session	enregistrement des sessions dans le cockpit	Enregistrement et gestion des sessions utilisateur

CHAPITRE 4. OPTIMISER LES PERFORMANCES DU SYSTÈME À L'AIDE DE LA CONSOLE WEB

Découvrez comment définir un profil de performance dans la console web RHEL afin d'optimiser les performances du système pour une tâche donnée.

4.1. OPTIONS DE RÉGLAGE DES PERFORMANCES DANS LA CONSOLE WEB

Red Hat Enterprise Linux 9 fournit plusieurs profils de performance qui optimisent le système pour les tâches suivantes :

- Systèmes utilisant le bureau
- Performance en termes de débit
- Performance en matière de latence
- Performance du réseau
- Faible consommation d'énergie
- Machines virtuelles

Le service **TuneD** optimise les options du système en fonction du profil sélectionné.

Dans la console web, vous pouvez définir le profil de performance utilisé par votre système.

Ressources supplémentaires

- Démarrer avec TuneD

4.2. DÉFINITION D'UN PROFIL DE PERFORMANCE DANS LA CONSOLE WEB

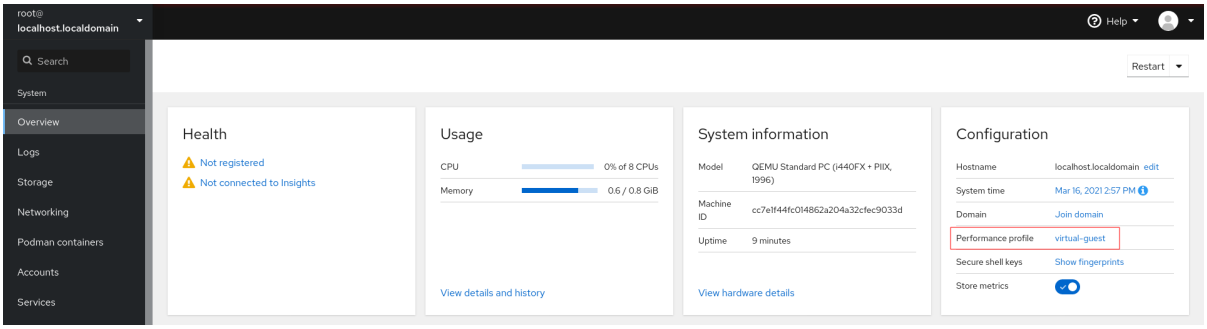
Cette procédure utilise la console web pour optimiser les performances du système pour une tâche sélectionnée.

Conditions préalables

- Assurez-vous que la console web est installée et accessible. Pour plus de détails, voir Installation de la console web.

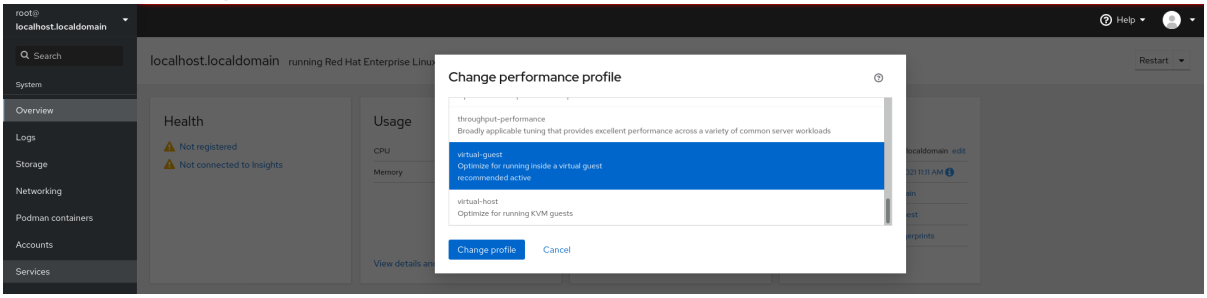
Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur **Overview**.
3. Dans le champ **Performance Profile**, cliquez sur le profil de performance actuel.



4. Dans la boîte de dialogue **Change Performance Profile**, modifiez le profil si nécessaire.

5. Cliquez sur **Change Profile**.



Verification steps

- L'onglet **Overview** affiche désormais le profil de performance sélectionné.

4.3. CONTRÔLE DES PERFORMANCES SUR LE SYSTÈME LOCAL À L'AIDE DE LA CONSOLE WEB

La console web de Red Hat Enterprise Linux utilise la méthode USE (Utilization Saturation and Errors) pour le dépannage. La nouvelle page de mesures de performance présente une vue historique de vos données organisée chronologiquement avec les données les plus récentes en haut de la page.

Vous pouvez y consulter les événements, les erreurs et la représentation graphique de l'utilisation et de la saturation des ressources.

Conditions préalables

- La console web est installée et accessible. Pour plus de détails, voir Installation de la console web.

- Le paquet **cockpit-pcp**, qui permet de collecter les mesures de performance, est installé :

  a. Pour installer le paquet à partir de l'interface de la console web :

     i. Connectez-vous à la console web avec des privilèges administratifs. Pour plus d'informations, voir Connexion à la console web .

     ii. Dans la page **Overview**, cliquez sur **View details and history**.

     iii. Cliquez sur le bouton **Installer cockpit-pcp**.

     iv. Dans la fenêtre de dialogue **Install software**, cliquez sur **Install**.

  b. Pour installer le paquet à partir de l'interface de ligne de commande, utilisez :

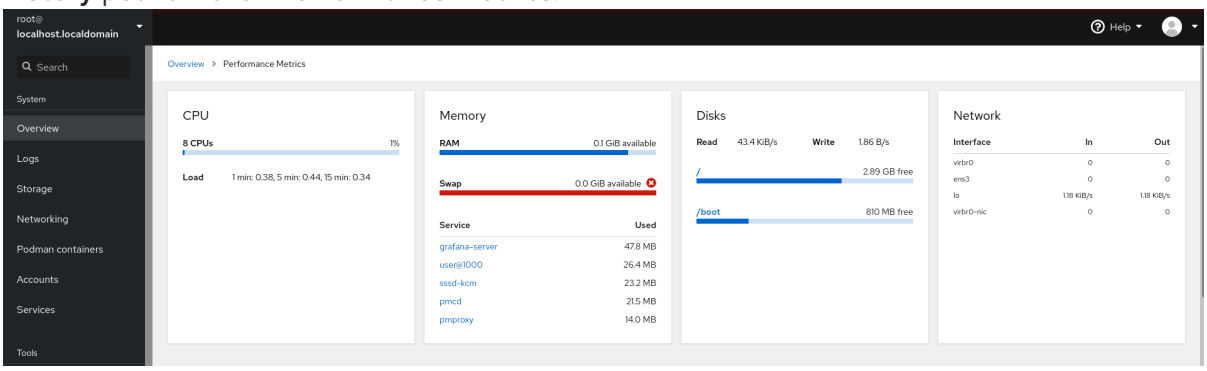
```
# dnf install cockpit-pcp
```

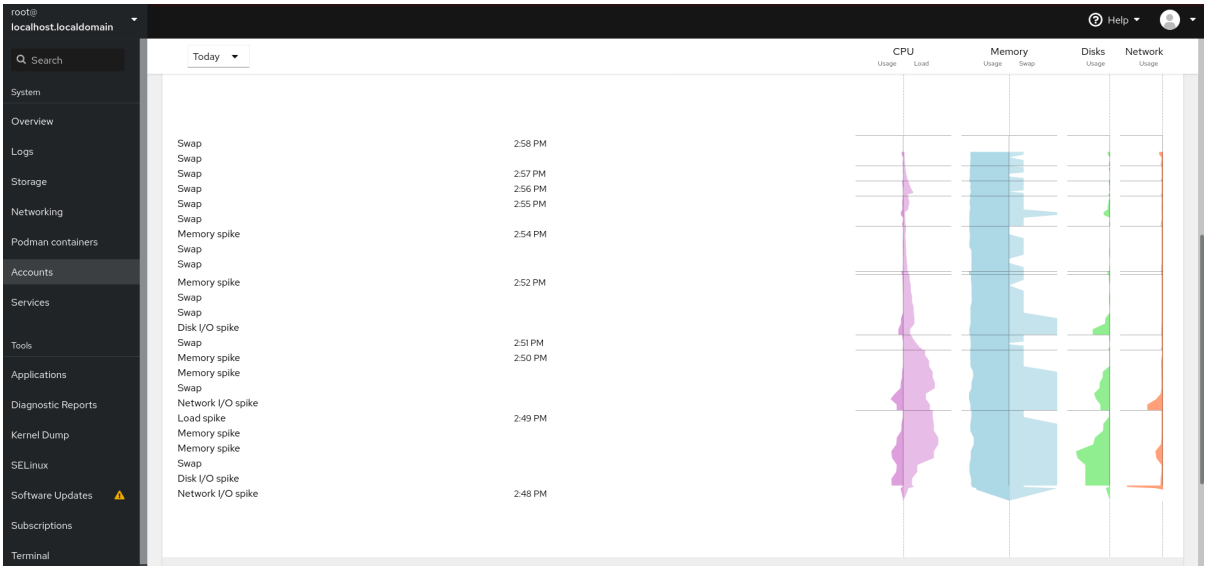
- Le service PCP est activé :

```
# systemctl enable --now pmlogger.service pmproxy.service
```

Procédure

1. Connectez-vous à la console web RHEL 9. Dans la page **Overview**, cliquez sur **View details and history** pour afficher **Performance Metrics**.





4.4. SURVEILLANCE DES PERFORMANCES SUR PLUSIEURS SYSTÈMES À L'AIDE DE LA CONSOLE WEB ET DE GRAFANA

Grafana vous permet de collecter des données à partir de plusieurs systèmes à la fois et d'examiner une représentation graphique de leurs métriques PCP collectées. Vous pouvez configurer la surveillance et l'exportation des mesures de performance pour plusieurs systèmes dans l'interface de la console web.

Cette procédure vous montre comment activer l'exportation des mesures de performance avec PCP à partir de l'interface de la console Web de RHEL 9.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir le lien: Installation de la console web.
- Installez le paquetage **cockpit-pcp**.

1. Depuis l'interface de la console web :
   a. Connectez-vous à la console web avec des privilèges administratifs. Pour plus d'informations, voir Connexion à la console web .
   b. Dans la page **Overview**, cliquez sur **View details and history**.
   c. Cliquez sur le bouton **Installer cockpit-pcp**.
   d. Dans la fenêtre de dialogue **Install software**, cliquez sur **Install**.
   e. Déconnectez-vous et reconnectez-vous pour voir l'historique des mesures.
2. Pour installer le paquet à partir de l'interface de ligne de commande, utilisez :

```
# dnf install cockpit-pcp
```

- Activer le service PCP :

```
# systemctl enable --now pmlogger.service pmproxy.service
```

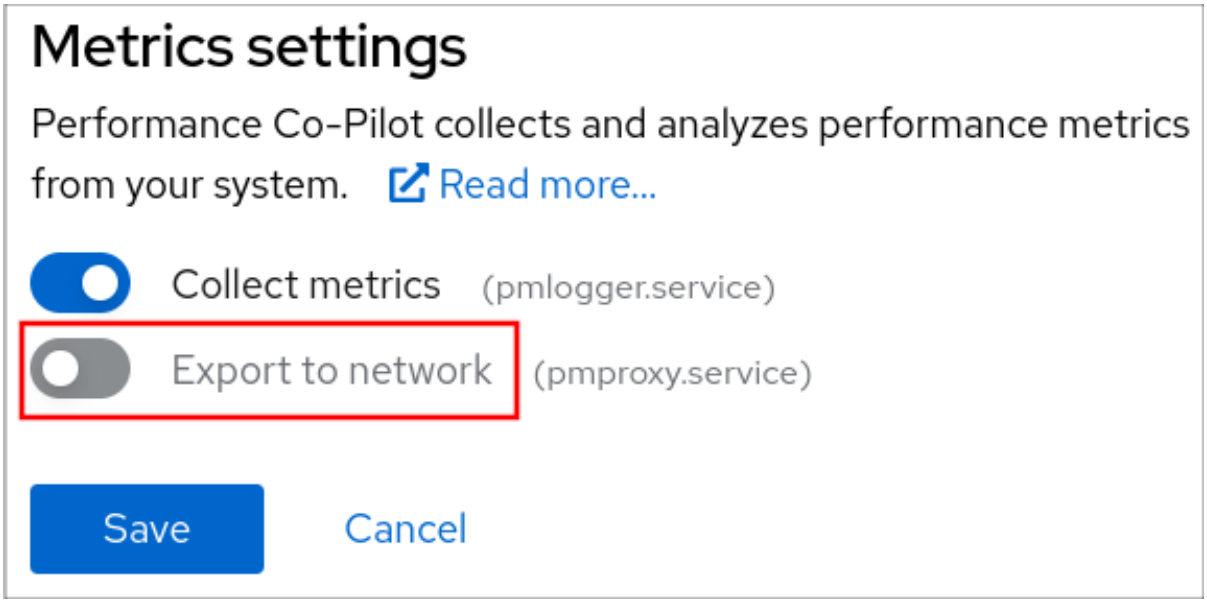
- Configurez le tableau de bord Grafana. Pour plus d'informations, voir Configurer un serveur Grafana.
- Installez le paquetage **redis**.

```
# dnf install redis
```

Vous pouvez également installer le paquet à partir de l'interface de la console web plus tard dans la procédure.

Procédure

1. Dans la page **Overview**, cliquez sur **View details and history** dans le tableau **Usage**.
2. Cliquez sur le bouton **Paramètres de mesure**.
3. Placez le curseur **Export to network** en position active.



Si le service **redis** n'est pas installé, vous serez invité à l'installer.

4. Pour ouvrir le service **pmproxy**, sélectionnez une zone dans une liste déroulante et cliquez sur le bouton **Add pmproxy**.

5. Cliquez sur **Save**.

Vérification

1. Cliquez sur **Networking**.

2. Dans le tableau **Firewall**, cliquez sur **n active zones** ou sur le bouton **Modifier les règles et les zones**.

3. Recherchez **pmproxy** dans la zone que vous avez sélectionnée.

IMPORTANT

Répétez cette procédure sur tous les systèmes que vous souhaitez surveiller.

CHAPITRE 5. CONSULTATION DES JOURNAUX DANS LA CONSOLE WEB

Apprenez à accéder aux journaux, à les examiner et à les filtrer dans la console web RHEL.

5.1. CONSULTATION DES JOURNAUX DANS LA CONSOLE WEB

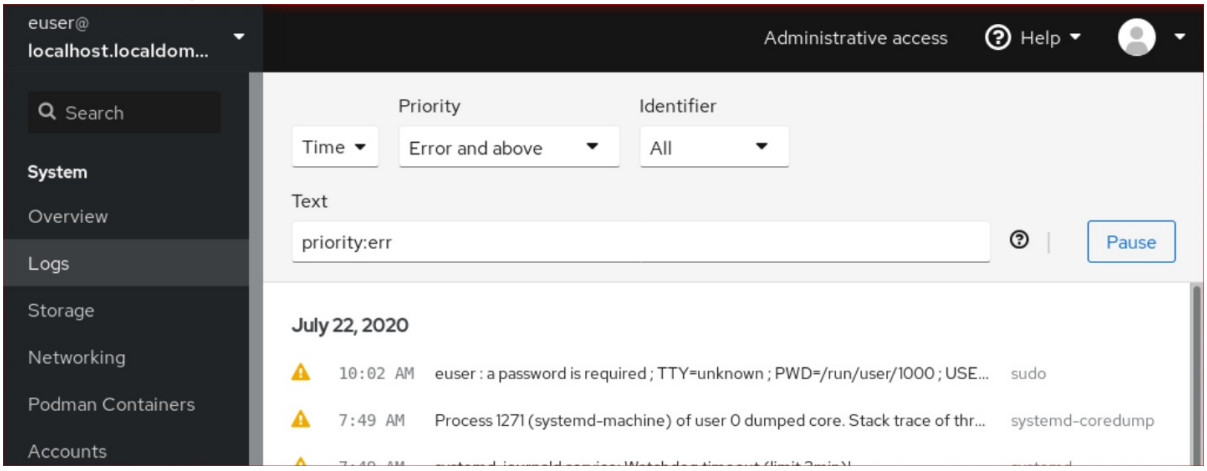
La section Logs de la console web RHEL 9 est une interface utilisateur pour l'utilitaire **journalctl**. Cette section décrit comment accéder aux journaux du système dans l'interface de la console web.

Conditions préalables

- La console web RHEL 9 a été installée.
  Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL.
   Pour plus de détails, voir Connexion à la console web.
2. Cliquez sur **Logs**.



3. Ouvrez les détails de l'enregistrement en cliquant sur l'enregistrement sélectionné dans la liste.

NOTE

Vous pouvez utiliser le bouton **Pause** pour interrompre l'affichage de nouvelles entrées de journal. Lorsque vous reprenez les nouvelles entrées de journal, la console web charge toutes les entrées de journal qui ont été signalées après l'utilisation du bouton **Pause**.

Vous pouvez filtrer les journaux par heure, priorité ou identifiant. Pour plus d'informations, voir Filtrer les journaux dans la console web

5.2. FILTRER LES JOURNAUX DANS LA CONSOLE WEB

Cette section montre comment filtrer les entrées de journal dans la console web.

Conditions préalables

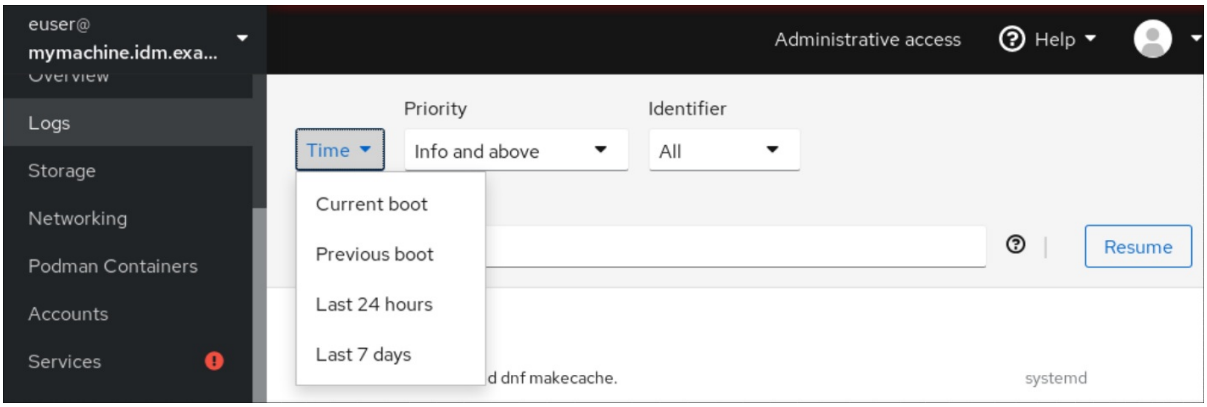
- L'interface de la console web doit être installée et accessible.
  Pour plus de détails, voir Installation de la console web.

Procédure

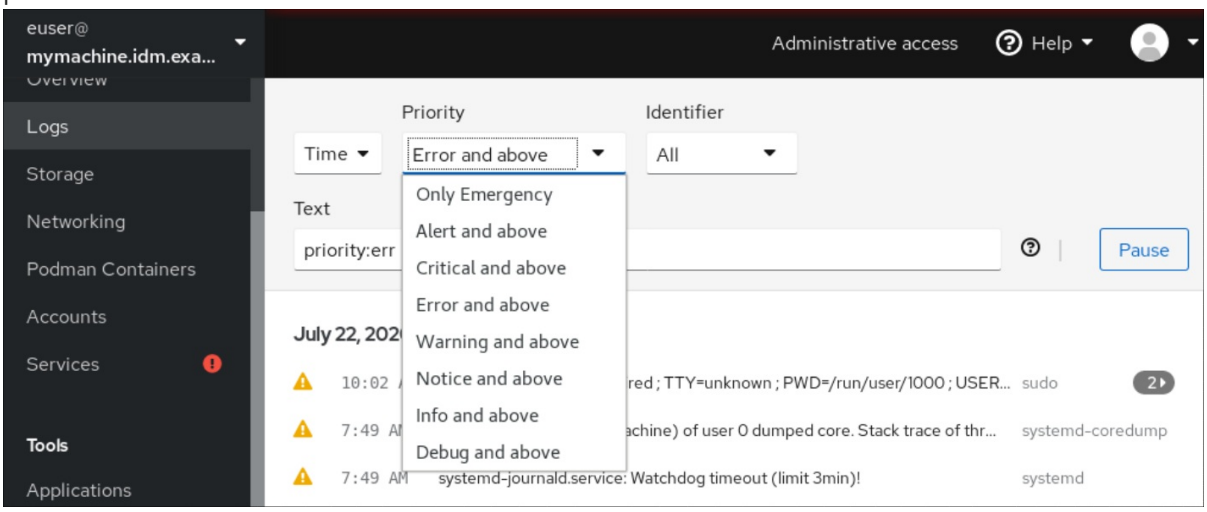
1. Connectez-vous à la console web RHEL 9.
   Pour plus de détails, voir Connexion à la console web.

2. Cliquez sur **Logs**.

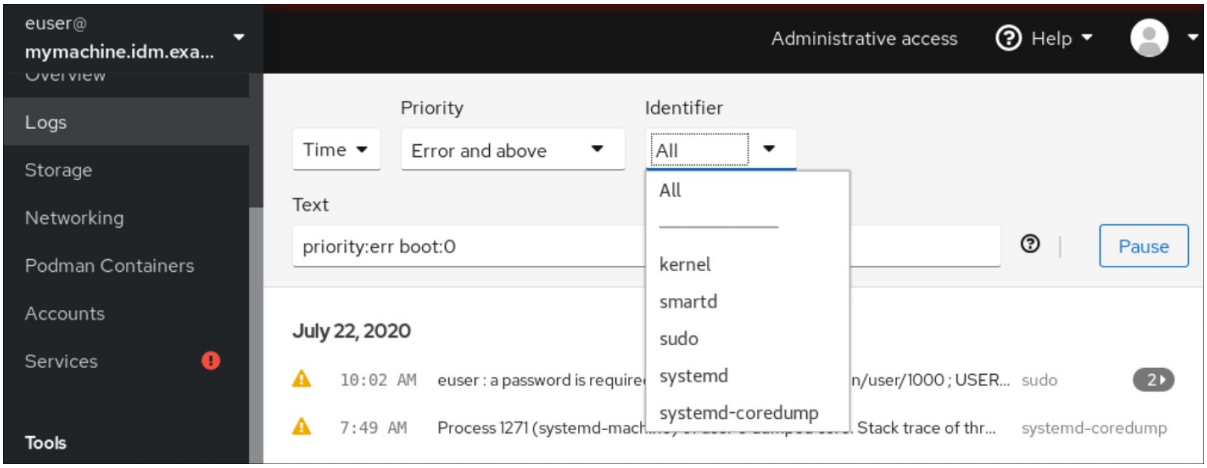
3. Par défaut, la console web affiche les dernières entrées du journal. Pour filtrer selon un intervalle de temps spécifique, cliquez sur le menu déroulant **Time** et choisissez l'option qui vous convient.



4. **Error and above** la liste des journaux de gravité est affichée par défaut. Pour filtrer selon une priorité différente, cliquez sur le menu déroulant **Error and above** et choisissez une priorité préférée.



5. Par défaut, la console web affiche les journaux de tous les identifiants. Pour filtrer les journaux d'un identifiant particulier, cliquez sur le menu déroulant **All** et sélectionnez un identifiant.



6. Pour ouvrir une entrée de journal, cliquez sur un journal sélectionné.

5.3. OPTIONS DE RECHERCHE TEXTUELLE POUR FILTRER LES JOURNAUX DANS LA CONSOLE WEB

La fonctionnalité de recherche de texte offre une grande variété d'options pour filtrer les enregistrements. Si vous décidez de filtrer les journaux en utilisant la recherche de texte, vous pouvez utiliser les options prédéfinies qui sont définies dans les trois menus déroulants, ou vous pouvez taper toute la recherche vous-même.

Menus déroulants

Trois menus déroulants vous permettent de spécifier les principaux paramètres de votre recherche :

- **Time**: Ce menu déroulant contient des recherches prédéfinies pour différentes périodes de votre recherche.
- **Priority**: Ce menu déroulant propose des options pour différents niveaux de priorité. Il correspond à l'option **journalctl --priority**. La valeur de priorité par défaut est **Error and above**. Elle est définie chaque fois que vous ne spécifiez pas d'autre priorité.
- **Identifier**: Dans ce menu déroulant, vous pouvez sélectionner un identifiant que vous souhaitez filtrer. Correspond à l'option **journalctl --identifier**.

Quantificateurs

Il existe six quantificateurs que vous pouvez utiliser pour spécifier votre recherche. Ils sont décrits dans le tableau Options de filtrage des journaux.

Champs du journal

Si vous souhaitez rechercher un champ d'enregistrement spécifique, il est possible de spécifier le champ ainsi que son contenu.

Recherche de texte libre dans les messages du journal

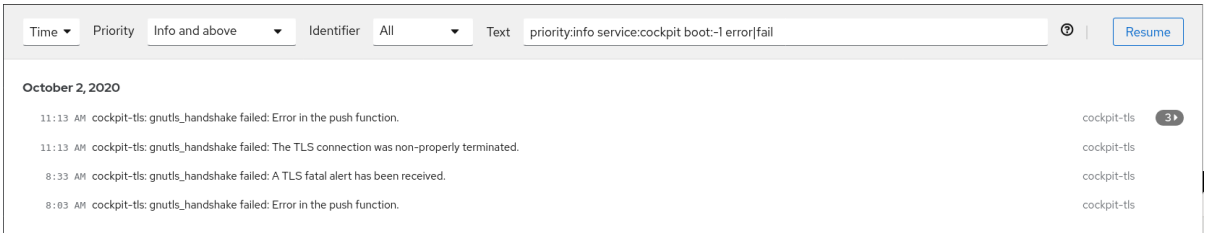
Vous pouvez filtrer n'importe quelle chaîne de texte de votre choix dans les messages du journal. La chaîne peut également se présenter sous la forme d'une expression régulière.

Filtrage avancé des journaux I

Filtrer tous les messages de journal identifiés par 'systemd' qui se sont produits depuis le 22 octobre 2020 à minuit et dont le champ 'JOB_TYPE' est soit 'start', soit 'restart'.

1. Tapez **identifier:systemd since:2020-10-22 JOB_TYPE=start,restart** dans le champ de recherche.

2. Vérifier les résultats.

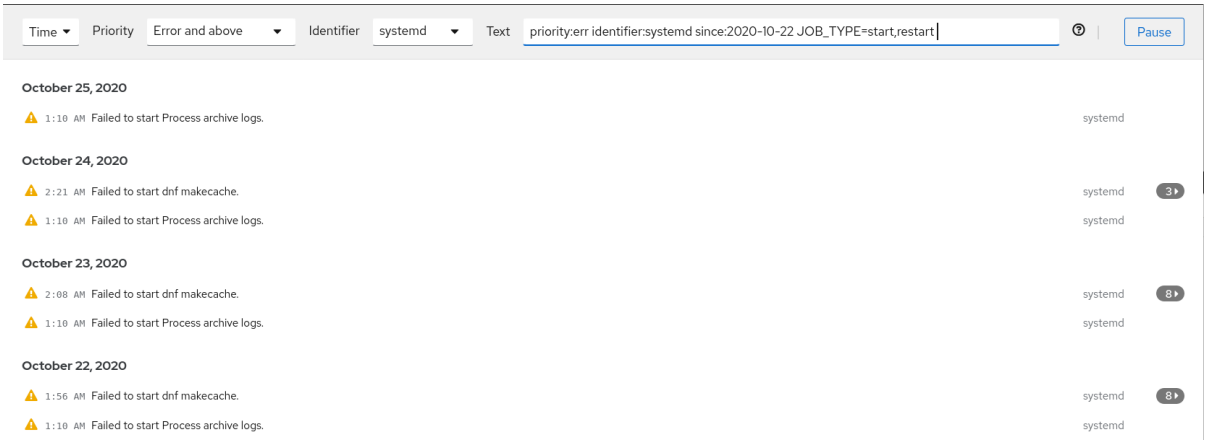


Filtrage avancé des journaux II

Filtrer tous les messages provenant de l'unité systemd 'cockpit.service' qui se sont produits lors de l'avant-dernier démarrage et dont le corps du message contient soit "error", soit "fail".

1. Tapez **service:cockpit boot:-1 error|fail** dans le champ de recherche.

2. Vérifier les résultats.



5.4. UTILISATION D'UNE ZONE DE RECHERCHE TEXTUELLE POUR FILTRER LES JOURNAUX DANS LA CONSOLE WEB

La zone de recherche textuelle vous permet de filtrer les enregistrements en fonction de différents paramètres. La recherche combine l'utilisation des menus déroulants de filtrage, des quantificateurs, des champs d'enregistrement et de la recherche de chaîne de caractères libre.

Conditions préalables

- L'interface de la console web doit être installée et accessible.
  Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL.
   Pour plus de détails, voir Connexion à la console web.

2. Cliquez sur **Logs**.

3. Utilisez les menus déroulants pour spécifier les trois principaux quantificateurs - intervalle de temps, priorité et identificateur(s) - que vous souhaitez filtrer.

Le quantificateur **Priority** doit toujours avoir une valeur. Si vous ne le spécifiez pas, il filtre automatiquement la priorité **Error and above**. Notez que les options que vous avez définies se reflètent dans la zone de recherche textuelle.

4. Spécifiez le champ du journal que vous souhaitez filtrer.
   Il est possible d'ajouter plusieurs champs d'enregistrement.

5. Vous pouvez utiliser une chaîne de caractères libre pour rechercher n'importe quoi d'autre. Le champ de recherche accepte également les expressions régulières.

5.5. OPTIONS DE FILTRAGE DES JOURNAUX

Il existe plusieurs options **journalctl**, que vous pouvez utiliser pour filtrer les journaux dans la console web, et qui peuvent être utiles. Certaines d'entre elles sont déjà couvertes par les menus déroulants de l'interface de la console web.

Tableau 5.1. Tableau

Nom de l'option	Utilisation	Notes
priority	Filtre la sortie en fonction de la priorité des messages. Prend un seul niveau d'enregistrement numérique ou textuel. Les niveaux de journalisation sont les niveaux de journalisation syslog habituels. Si un seul niveau de journalisation est spécifié, tous les messages de ce niveau ou d'un niveau inférieur (donc plus important) sont affichés.	Couvert dans le menu déroulant **Priority**.
identifier	Affiche les messages pour l'identifiant syslog spécifié SYSLOG_IDENTIFIER. Peut être spécifié plusieurs fois.	Couvert dans le menu déroulant **Identifier**.
follow	Affiche uniquement les entrées les plus récentes du journal et imprime en continu les nouvelles entrées au fur et à mesure qu'elles sont ajoutées au journal.	Non couvert par une liste déroulante.
service	Affiche les messages pour l'unité **systemd** spécifiée. Peut être spécifié plusieurs fois.	N'est pas couvert par une liste déroulante. Correspond au paramètre **journalctl --unit**.

Nom de l'option	Utilisation	Notes
boot	Afficher les messages d'un démarrage spécifique. Un nombre entier positif cherchera les bottes à partir du début du journal, et un nombre entier égal ou inférieur à zéro cherchera les bottes à partir de la fin du journal. Par conséquent, 1 signifie la première botte trouvée dans le journal par ordre chronologique, 2 la deuxième et ainsi de suite ; tandis que -0 est la dernière botte, -1 l'avant-dernière botte, et ainsi de suite.	Couvert uniquement par **Current boot** ou **Previous boot** dans le menu déroulant **Time**. Les autres options doivent être écrites manuellement.
since	Commencer à afficher les entrées à la date spécifiée ou plus récentes, ou à la date spécifiée ou plus anciennes, respectivement. Les dates spécifiées doivent être au format "2012-10-30 18:17:16". Si la partie relative à l'heure est omise, le format "00:00:00" est pris en compte. Si seule la composante "secondes" est omise, le format "2012-10-30 18:17:16" est pris en compte. Si la partie date est omise, le jour en cours est pris en compte. Les chaînes de caractères "hier", "aujourd'hui" et "demain" peuvent également être comprises, car elles font référence à 00:00:00 du jour précédant le jour en cours, du jour en cours ou du jour suivant le jour en cours, respectivement. \L'expression "maintenant" fait référence à l'heure actuelle. Enfin, des heures relatives peuvent être spécifiées, préfixées par "-" ou "-", se référant respectivement à des heures antérieures ou postérieures à l'heure actuelle.	Non couvert par une liste déroulante.

CHAPITRE 6. GESTION DES COMPTES D'UTILISATEURS DANS LA CONSOLE WEB

La console web RHEL offre une interface permettant d'ajouter, de modifier et de supprimer des comptes d'utilisateurs système.

Après avoir lu cette section, vous saurez

- D'où proviennent les comptes existants.
- Comment ajouter de nouveaux comptes.
- Comment définir l'expiration du mot de passe.
- Comment et quand mettre fin aux sessions des utilisateurs.

Conditions préalables

- Être connecté à la console web RHEL avec un compte auquel des autorisations d'administrateur ont été attribuées. Pour plus d'informations, voir Connexion à la console web

6.1. COMPTES D'UTILISATEURS DU SYSTÈME GÉRÉS DANS LA CONSOLE WEB

Avec les comptes d'utilisateurs affichés dans la console web RHEL, vous pouvez :

- Authentifier les utilisateurs lors de l'accès au système.
- Définir les droits d'accès au système.

La console web RHEL affiche tous les comptes d'utilisateurs situés dans le système. Par conséquent, vous pouvez voir au moins un compte d'utilisateur juste après la première connexion à la console web.

Après vous être connecté à la console web RHEL, vous pouvez effectuer les opérations suivantes :

- Créer de nouveaux comptes utilisateurs.
- Modifier leurs paramètres.
- Verrouiller les comptes.
- Mettre fin aux sessions des utilisateurs.

6.2. AJOUTER DE NOUVEAUX COMPTES À L'AIDE DE LA CONSOLE WEB

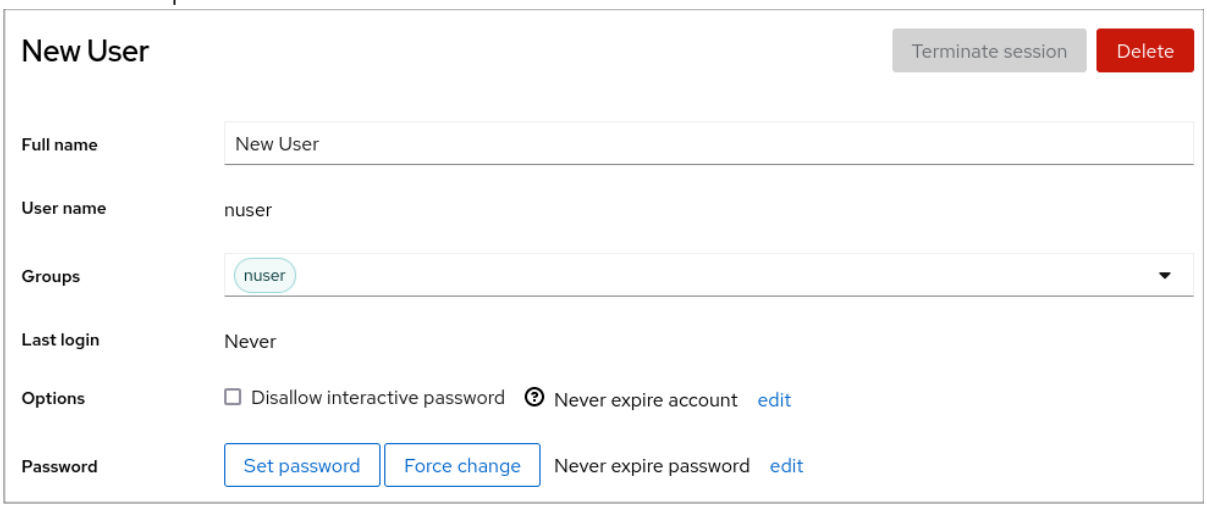
Les étapes suivantes permettent d'ajouter des comptes d'utilisateurs au système et de définir des droits d'administration pour les comptes via la console web RHEL.

Conditions préalables

- La console web RHEL doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL.
2. Cliquez sur **Comptes**.
3. Cliquez sur **Créer un nouveau compte**.
4. Dans le champ **Full Name**, saisissez le nom complet de l'utilisateur.
   La console web RHEL suggère automatiquement un nom d'utilisateur à partir du nom complet et le remplit dans le champ **User Name**. Si vous ne souhaitez pas utiliser la convention de dénomination originale qui consiste à utiliser la première lettre du prénom et le nom de famille complet, mettez à jour la suggestion.
5. Dans les champs **Password/Confirm**, saisissez le mot de passe et retapez-le pour vérifier qu'il est correct.
   La barre de couleur située sous les champs indique le niveau de sécurité du mot de passe saisi, ce qui ne permet pas de créer un utilisateur avec un mot de passe faible.
6. Cliquez sur **Créer** pour enregistrer les paramètres et fermer la boîte de dialogue.
7. Sélectionnez le compte nouvellement créé.
8. Dans le menu déroulant **Groups**, sélectionnez les groupes que vous souhaitez ajouter au nouveau compte.



Vous pouvez maintenant voir le nouveau compte dans les paramètres de **Accounts** et vous pouvez utiliser ses informations d'identification pour vous connecter au système.

6.3. RENFORCER L'EXPIRATION DES MOTS DE PASSE DANS LA CONSOLE WEB

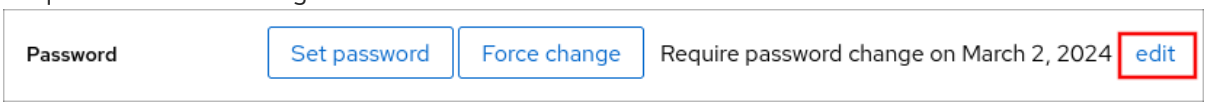
Par défaut, les mots de passe des comptes d'utilisateurs n'expirent jamais. Vous pouvez configurer les mots de passe du système de manière à ce qu'ils expirent après un nombre défini de jours. Lorsque le mot de passe expire, la prochaine tentative de connexion demandera un changement de mot de passe.

Procédure

1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Comptes**.

3. Sélectionnez le compte utilisateur pour lequel vous souhaitez appliquer l'expiration du mot de passe.

4. Cliquez sur **edit** sur la ligne **Password**.



5. Dans la boîte de dialogue **Password expiration**, sélectionnez **Require password change every ... days** et entrez un nombre entier positif représentant le nombre de jours après lesquels le mot de passe expire.

6. Cliquez sur **Modifier**.
La console web affiche immédiatement la date de la future demande de changement de mot de passe sur la ligne **Password**.

6.4. TERMINER LES SESSIONS D'UTILISATEURS DANS LA CONSOLE WEB

Un utilisateur crée des sessions utilisateur lorsqu'il se connecte au système. Mettre fin aux sessions utilisateur signifie déconnecter l'utilisateur du système. Cela peut s'avérer utile si vous devez effectuer des tâches administratives liées à des changements de configuration, par exemple des mises à niveau du système.

Dans chaque compte d'utilisateur de la console RHEL 9web, vous pouvez mettre fin à toutes les sessions du compte, à l'exception de la session de la console web que vous utilisez actuellement. Cela vous évite de perdre l'accès à votre système.

Procédure

1. Connectez-vous à la console web RHEL 9.

2. Cliquez sur **Comptes**.

3. Cliquez sur le compte utilisateur pour lequel vous souhaitez mettre fin à la session.

4. Cliquez sur **Terminer la session**.
Si le bouton **Terminer la session** est inactif, cela signifie que l'utilisateur n'est pas connecté au système.

   La console web RHEL met fin aux sessions.

CHAPITRE 7. GESTION DES SERVICES DANS LA CONSOLE WEB

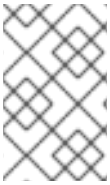
Apprenez à gérer les services système dans l'interface de la console web RHEL. Vous pouvez activer ou désactiver des services, les redémarrer ou les recharger, ou gérer leur démarrage automatique.

7.1. ACTIVATION OU DÉSACTIVATION DES SERVICES SYSTÈME DANS LA CONSOLE WEB

Cette procédure permet d'activer ou de désactiver les services du système à l'aide de l'interface de la console web.

Conditions préalables

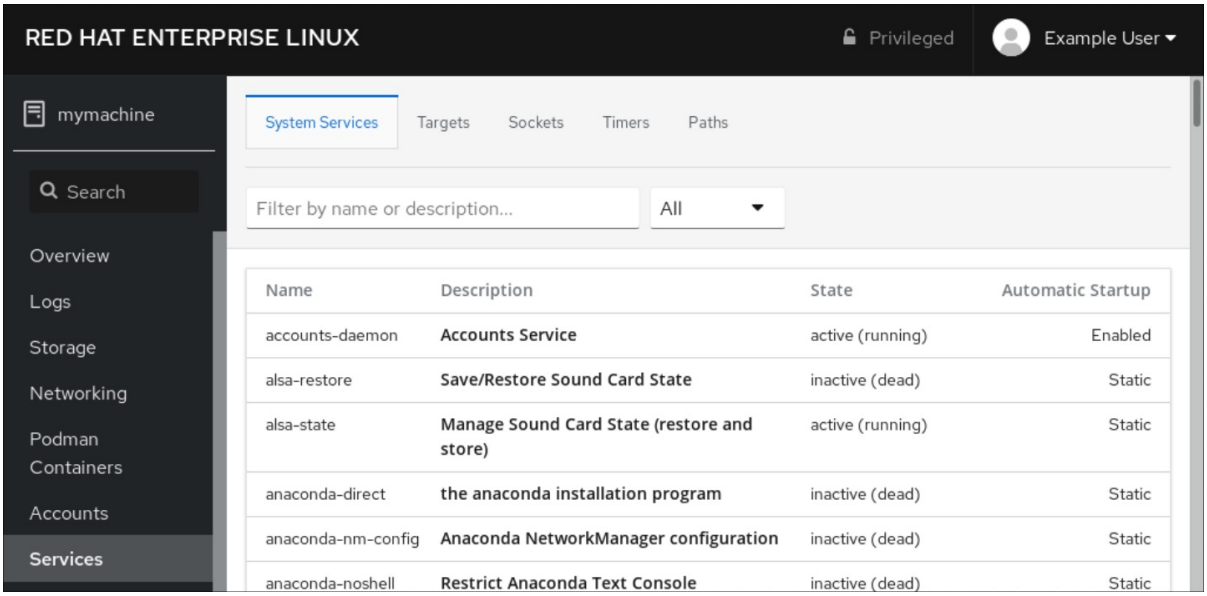
- La console web RHEL 9 a été installée.
  Pour plus de détails, voir Installation de la console web.



PROCÉDURE

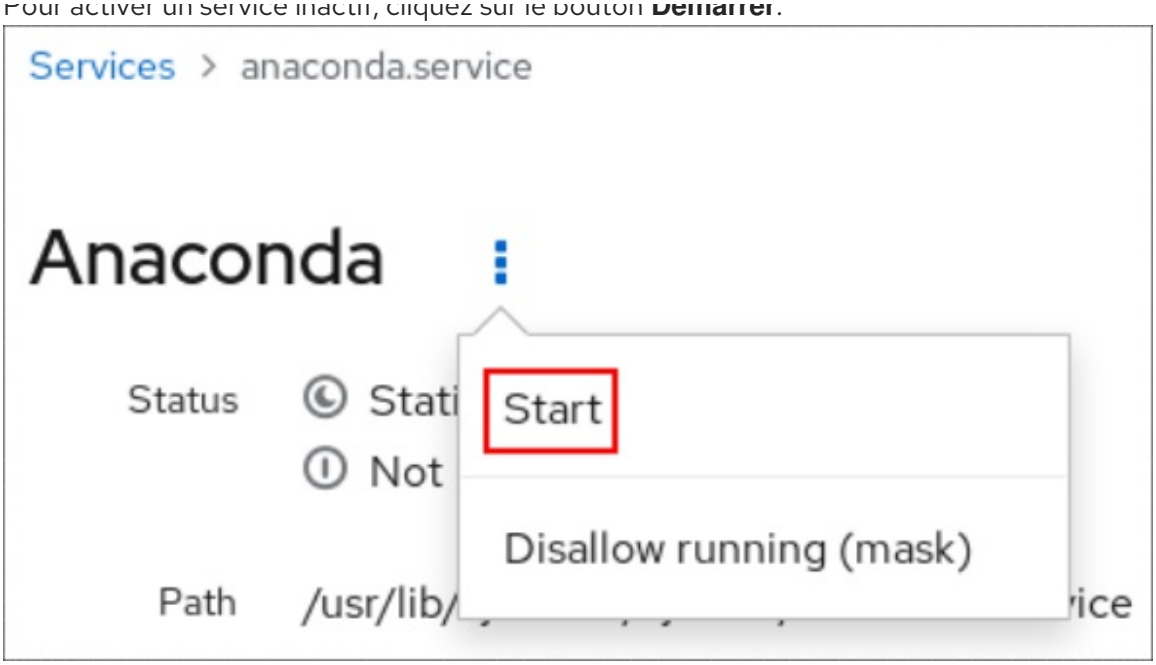
Vous pouvez filtrer les services par nom ou par description, ainsi que par Activé, Désactivé ou Démarrage automatique statique. L'interface affiche l'état actuel du service et ses journaux récents.

1. Connectez-vous à la console web RHEL avec des privilèges d'administrateur.
   Pour plus de détails, voir Connexion à la console web.
2. Cliquez sur **Services** dans le menu de la console web à gauche.
3. L'onglet par défaut pour **Services** est **System Services**. Si vous souhaitez gérer des cibles, des sockets, des temporisateurs ou des chemins, passez à l'onglet correspondant dans le menu supérieur.

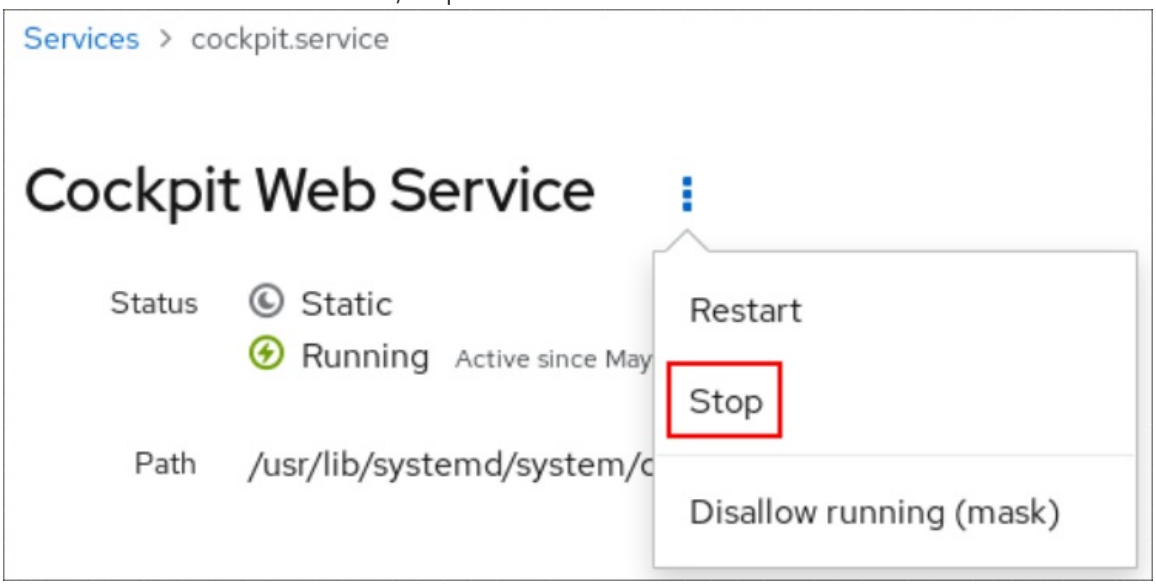


4. Pour ouvrir les paramètres d'un service, cliquez sur un service sélectionné dans la liste. Vous pouvez savoir quels services sont actifs ou inactifs en consultant la colonne **State**.
5. Activer ou désactiver un service :
   - Pour activer un service inactif, cliquez sur le bouton **Démarrer**

- Pour activer un service inactif, cliquez sur le bouton **Démarrer**.



- Pour désactiver un service actif, cliquez sur le bouton **Arrêter**.

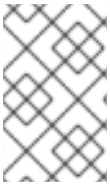


7.2. REDÉMARRAGE DES SERVICES SYSTÈME DANS LA CONSOLE WEB

Cette procédure permet de redémarrer les services du système à l'aide de l'interface de la console web.

Conditions préalables

- La console web RHEL 9 a été installée.
  Pour plus de détails, voir Installation de la console web.



PROCÉDURE

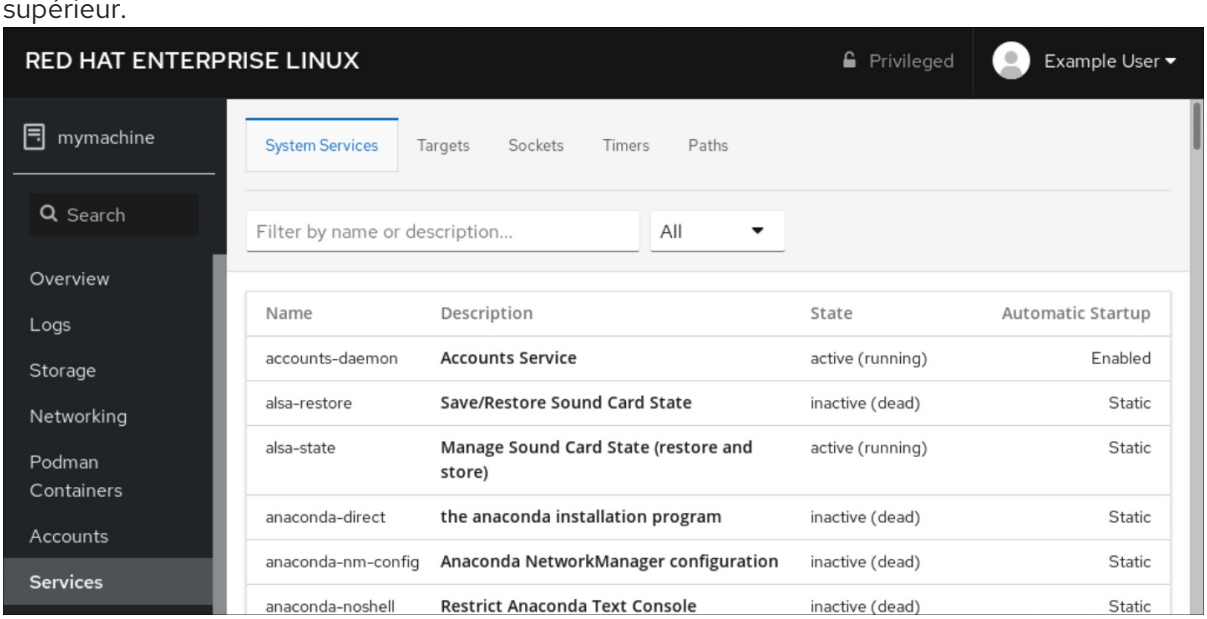
Vous pouvez filtrer les services par nom ou par description, ainsi que par Activé, Désactivé ou Démarrage automatique statique. L'interface affiche l'état actuel du service et ses journaux récents.

1. Connectez-vous à la console web RHEL avec des privilèges d'administrateur.

Pour plus de détails, voir Connexion à la console web .

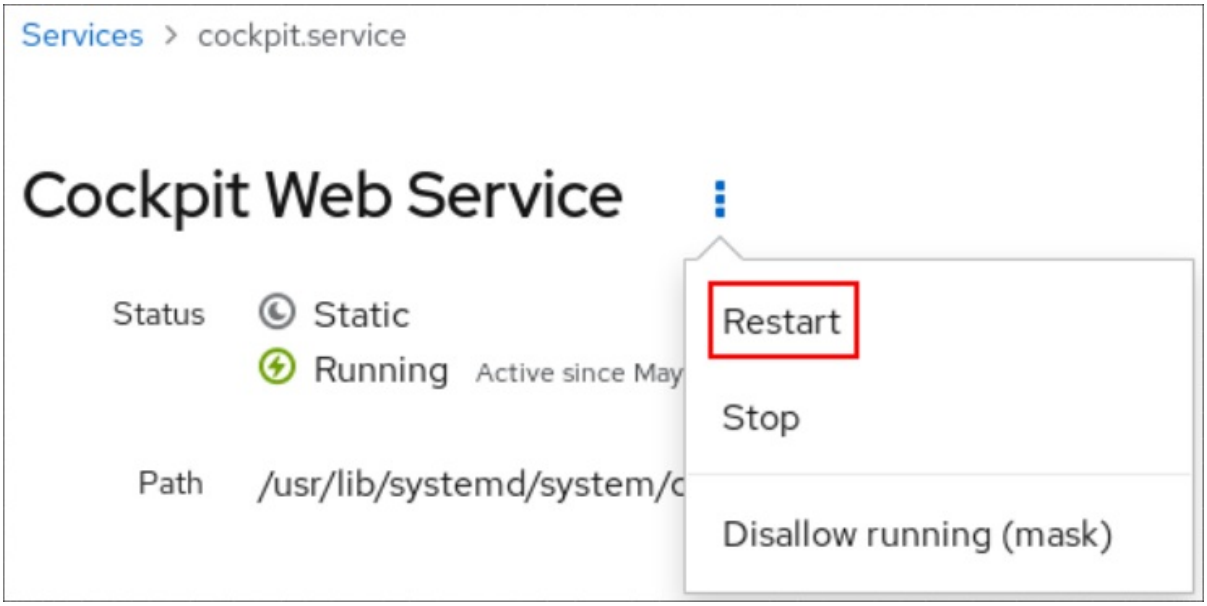
2. Cliquez sur **Services** dans le menu de la console web à gauche.

3. L'onglet par défaut pour **Services** est **System Services**. Si vous souhaitez gérer des cibles, des sockets, des temporisateurs ou des chemins, passez à l'onglet correspondant dans le menu supérieur.



4. Pour ouvrir les paramètres d'un service, cliquez sur un service sélectionné dans la liste.

5. Pour redémarrer un service, cliquez sur le bouton **Redémarrer**.



CHAPITRE 8. CONFIGURATION DES LIAISONS RÉSEAU À L'AIDE DE LA CONSOLE WEB

Découvrez le fonctionnement de la liaison réseau et configurez les liaisons réseau dans la console web RHEL 9.

NOTE

La console web RHEL 9 est construite sur le service NetworkManager.

Pour plus d'informations, voir la section Premiers pas avec NetworkManager pour la gestion des réseaux.

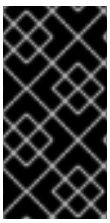
Conditions préalables

- La console web RHEL 9 est installée et activée. Pour plus de détails, voir Installation de la console web.

8.1. COMPRENDRE LA LIAISON RÉSEAU

La liaison réseau est une méthode permettant de combiner ou d'agréger des interfaces réseau afin de fournir une interface logique avec un débit plus élevé ou une redondance.

Les modes **active-backup**, **balance-tlb** et **balance-alb** ne nécessitent aucune configuration spécifique du commutateur réseau. Cependant, d'autres modes de liaison nécessitent de configurer le commutateur pour agréger les liens. Par exemple, les commutateurs Cisco nécessitent **EtherChannel** pour les modes 0, 2 et 3, mais pour le mode 4, le protocole LACP (Link Aggregation Control Protocol) et **EtherChannel** sont nécessaires. Pour plus de détails, consultez la documentation de votre commutateur.



IMPORTANT

Certaines fonctions de liaison réseau, telles que le mécanisme de basculement, ne prennent pas en charge les connexions directes par câble sans commutateur réseau. Pour plus de détails, voir la section Le bonding est-il pris en charge avec une connexion directe utilisant des câbles croisés ? Solution KCS.

8.2. MODES D'OBLIGATIONS

Dans RHEL 9, il existe plusieurs options de mode. Chaque option de mode est caractérisée par un équilibrage de charge et une tolérance aux pannes spécifiques. Le comportement des interfaces liées dépend du mode. Les modes de liaison offrent une tolérance aux pannes, un équilibrage de la charge ou les deux.

Modes d'équilibrage de la charge

- **Round Robin**: Transmission séquentielle de paquets depuis la première interface disponible jusqu'à la dernière.

Modes de tolérance aux pannes

- **Active Backup**: Ce n'est que lorsque l'interface primaire tombe en panne que l'une des interfaces de secours la remplace. Seule l'adresse MAC utilisée par l'interface active est visible.

- **Broadcast**: Toutes les transmissions sont envoyées sur toutes les interfaces.

NOTE

La diffusion augmente considérablement le trafic réseau sur toutes les interfaces liées.

Modes de tolérance aux pannes et d'équilibrage de la charge

- **XOR**: Les adresses MAC de destination sont réparties de manière égale entre les interfaces avec un hachage modulo. Chaque interface dessert alors le même groupe d'adresses MAC.
- **802.3ad**: Définit une politique d'agrégation de liens dynamique IEEE 802.3ad. Crée des groupes d'agrégation qui partagent les mêmes paramètres de vitesse et de duplex. Transmet et reçoit sur toutes les interfaces de l'agrégateur actif.

NOTE

Ce mode nécessite un commutateur conforme à la norme 802.3ad.

- **Adaptive transmit load balancing**: Le trafic sortant est distribué en fonction de la charge actuelle sur chaque interface. Le trafic entrant est reçu par l'interface actuelle. Si l'interface de réception tombe en panne, une autre interface prend en charge l'adresse MAC de l'interface en panne.
- **Adaptive load balancing**: Comprend l'équilibrage de la charge de transmission et de réception pour le trafic IPv4.
  L'équilibrage de la charge de réception est réalisé par la négociation du protocole de résolution d'adresses (ARP), il est donc nécessaire de régler **Link Monitoring** sur **ARP** dans la configuration de la liaison.

8.3. CONFIGURATION D'UNE LIAISON RÉSEAU À L'AIDE DE LA CONSOLE WEB RHEL

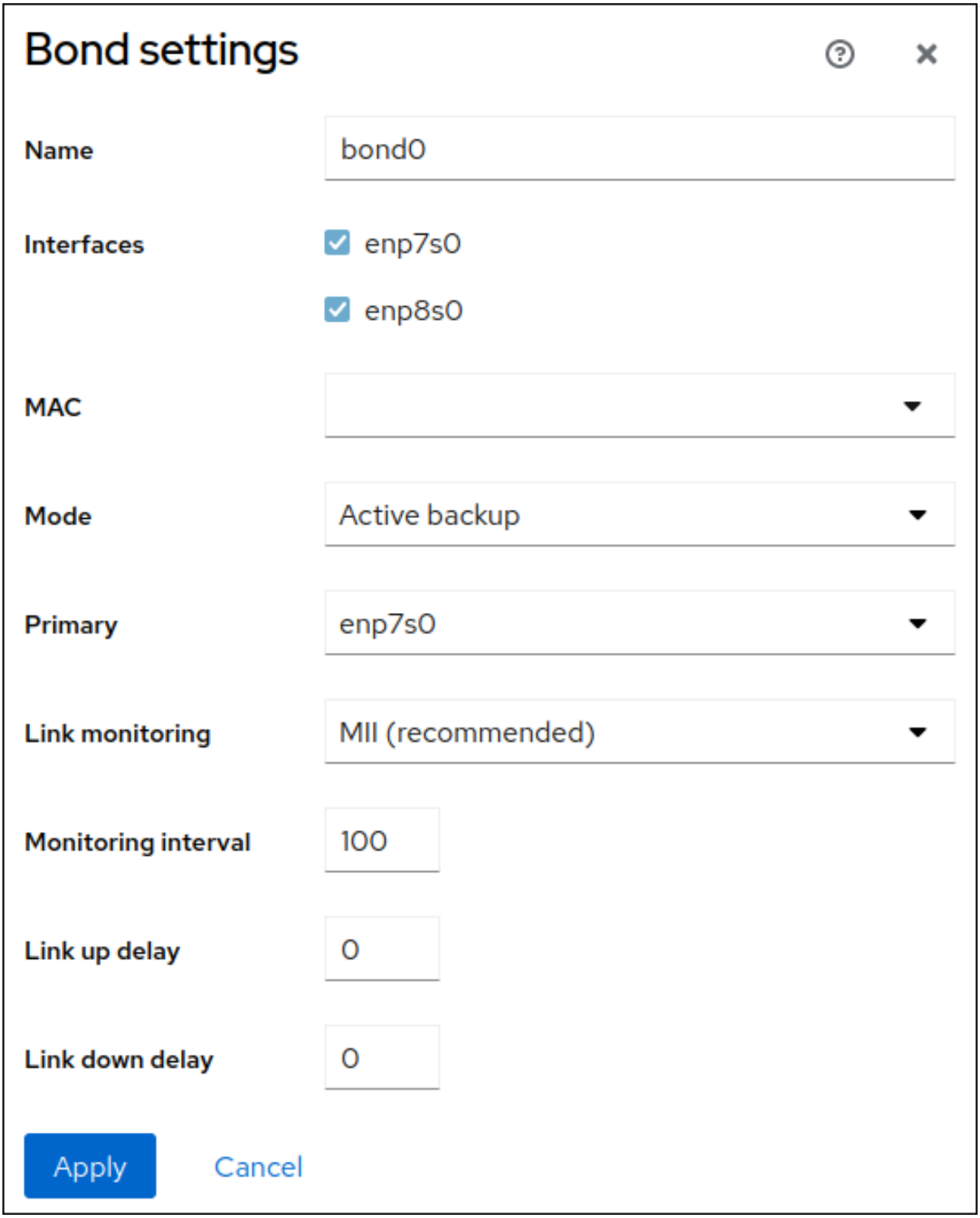
Utilisez la console web RHEL pour configurer une liaison réseau si vous préférez gérer les paramètres réseau à l'aide d'une interface basée sur un navigateur web.

Conditions préalables

- Vous êtes connecté à la console web RHEL.
- Deux ou plusieurs périphériques réseau physiques ou virtuels sont installés sur le serveur.
- Pour utiliser des périphériques Ethernet comme membres du lien, les périphériques Ethernet physiques ou virtuels doivent être installés sur le serveur.
- Pour utiliser des périphériques d'équipe, de pont ou de VLAN en tant que membres du lien, créez-les à l'avance comme décrit dans la section :
  - Configuration d'une équipe réseau à l'aide de la console web RHEL
  - Configuration d'un pont réseau à l'aide de la console web RHEL
  - Configuration du marquage VLAN à l'aide de la console web RHEL

Procédure

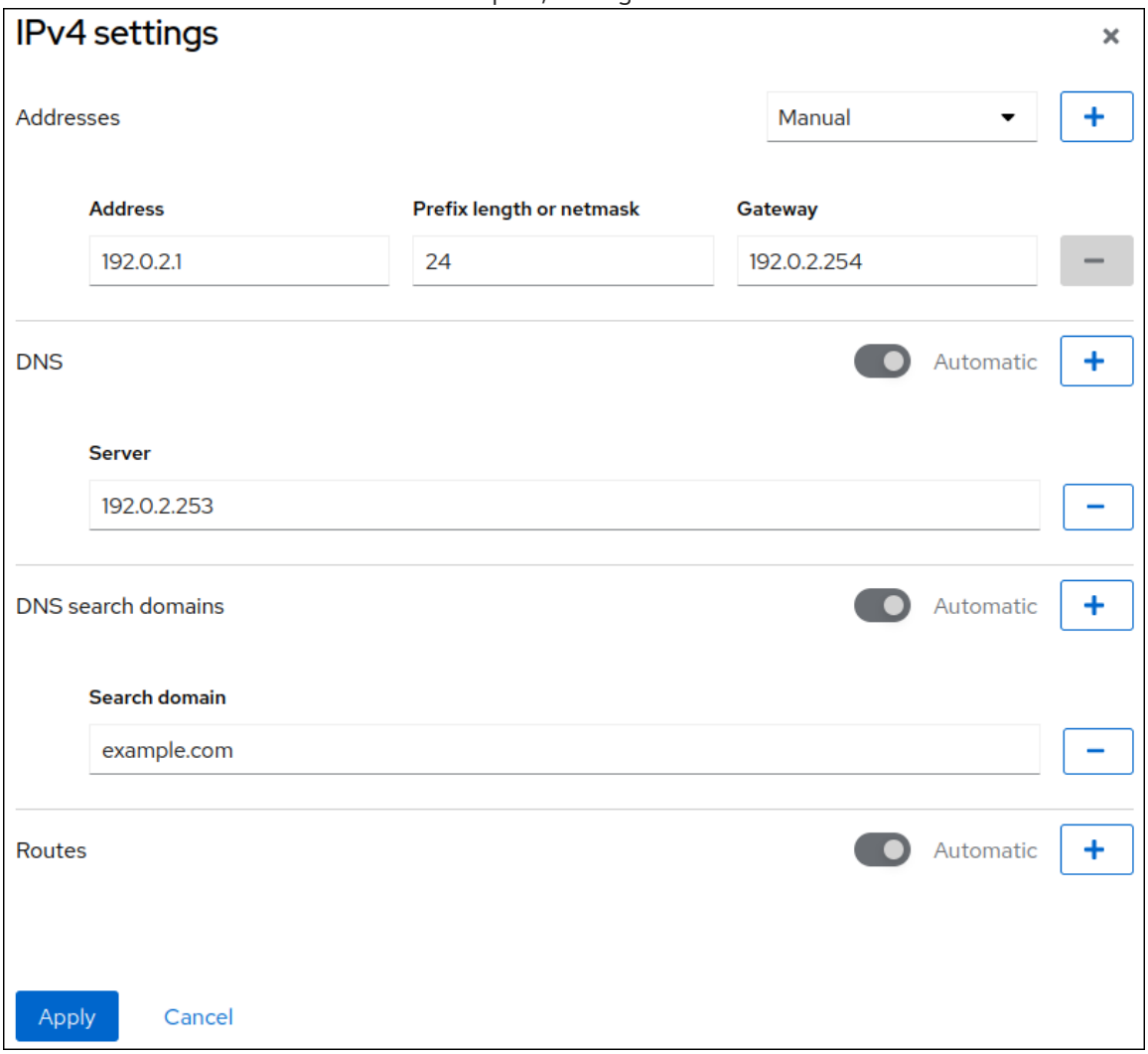
1. Sélectionnez l'onglet **Networking** dans le menu de navigation situé à gauche de l'écran.
2. Cliquez sur **Add bond** dans la section **Interfaces**.
3. Saisissez le nom du dispositif de liaison que vous souhaitez créer.
4. Sélectionnez les interfaces qui doivent être membres de la liaison.
5. Sélectionnez le mode de l'obligation.
   Si vous sélectionnez **Active backup**, la console web affiche le champ supplémentaire **Primary** dans lequel vous pouvez sélectionner l'appareil actif préféré.
6. Définissez le mode de surveillance des liens. Par exemple, lorsque vous utilisez le mode **Adaptive load balancing**, réglez-le sur **ARP**.
7. En option : Ajustez les paramètres de l'intervalle de surveillance, du délai d'établissement de la liaison et du délai de rétablissement de la liaison. En général, vous ne modifiez les paramètres par défaut qu'à des fins de dépannage.



8. Cliquez sur **Appliquer**.
9. Par défaut, la liaison utilise une adresse IP dynamique. Si vous souhaitez définir une adresse IP statique :
    a. Cliquez sur le nom de l'obligation dans la section **Interfaces**.
    b. Cliquez sur **Edit** en regard du protocole que vous souhaitez configurer.
    c. Sélectionnez **Manual** à côté de **Addresses**, et entrez l'adresse IP, le préfixe et la passerelle par défaut.
    d. Dans la section **DNS**, cliquez sur le bouton et entrez l'adresse IP du serveur DNS. Répétez cette étape pour définir plusieurs serveurs DNS.

e. Dans la section **DNS search domains**, cliquez sur le bouton et entrez le domaine de recherche.

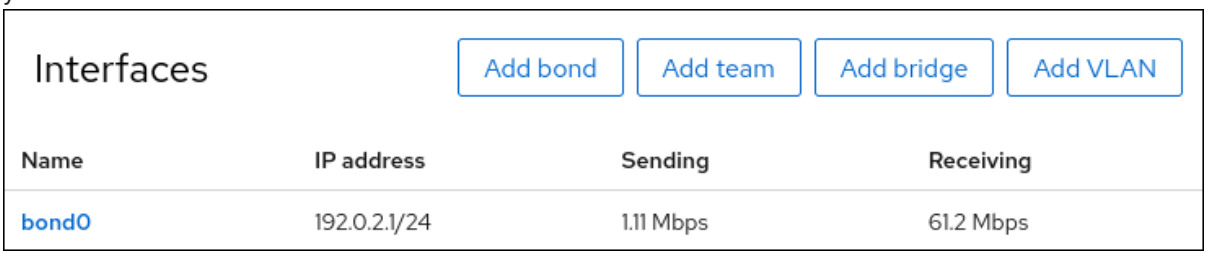
f. Si l'interface nécessite des routes statiques, configurez-les dans la section **Routes**.



g. Cliquez sur **Appliquer**

Vérification

1. Sélectionnez l'onglet **Networking** dans la navigation sur le côté gauche de l'écran, et vérifiez s'il y a du trafic entrant et sortant sur l'interface :



2. Retirez temporairement le câble réseau de l'hôte.
   Notez qu'il n'existe aucune méthode permettant de tester correctement les événements de défaillance de liaison à l'aide d'utilitaires logiciels. Les outils qui désactivent les connexions, comme la console web, ne montrent que la capacité du pilote de liaison à gérer les changements de configuration des membres et non les événements réels de défaillance de la liaison.

3. Affiche l'état de la liaison :

```
# cat /proc/net/bonding/bond0
```

8.4. AJOUT D'INTERFACES À LA LIAISON À L'AIDE DE LA CONSOLE WEB

Les liens réseau peuvent inclure plusieurs interfaces et vous pouvez ajouter ou supprimer l'une d'entre elles à tout moment.

Apprenez à ajouter une interface réseau à une liaison existante.

Conditions préalables

- Avoir un lien avec plusieurs interfaces configurées comme décrit dans Configuration d'un lien réseau à l'aide de la console web

Procédure

1. Connectez-vous à la console web.
   Pour plus de détails, voir Connexion à la console web .
2. Ouvrir **Networking**.
3. Dans le tableau **Interfaces**, cliquez sur la liaison que vous souhaitez configurer.
4. Dans l'écran des paramètres de liaison, faites défiler vers le bas jusqu'au tableau des membres (interfaces).
5. Cliquez sur l'icône déroulante **Ajouter un membre**.
6. Sélectionnez l'interface dans le menu déroulant et cliquez dessus.

Verification steps

- Vérifiez que l'interface sélectionnée apparaît dans le tableau **Interface members** de l'écran bond settings.

8.5. SUPPRESSION OU DÉSACTIVATION D'UNE INTERFACE DE LA LIAISON À L'AIDE DE LA CONSOLE WEB

Les liaisons réseau peuvent inclure plusieurs interfaces. Si vous devez modifier un appareil, vous pouvez supprimer ou désactiver certaines interfaces de la liaison, ce qui fonctionnera avec le reste des interfaces actives.

Pour cesser d'utiliser une interface incluse dans une obligation, vous pouvez.. :

- Retirer l'interface de la liaison.
- Désactiver temporairement l'interface. L'interface fait toujours partie de la liaison, mais celle-ci ne l'utilisera pas tant que vous ne l'aurez pas réactivée.

Conditions préalables

- Avoir un lien avec plusieurs interfaces configurées comme décrit dans Configuration d'un lien réseau à l'aide de la console web

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Ouvrir **Networking**.
3. Cliquez sur la liaison que vous souhaitez configurer.
4. Dans l'écran des paramètres de liaison, faites défiler vers le bas jusqu'au tableau des ports (interfaces).
5. Sélectionnez l'interface et supprimez-la ou désactivez-la :
   - Pour supprimer l'interface, cliquez sur le bouton **-**.
   - Pour désactiver ou activer l'interface, basculez l'interrupteur situé à côté de l'interface sélectionnée.

En fonction de votre choix, la console web supprime ou désactive l'interface du lien et vous pouvez la voir à nouveau dans la section **Networking** en tant qu'interface autonome.

8.6. SUPPRESSION OU DÉSACTIVATION D'UNE LIAISON À L'AIDE DE LA CONSOLE WEB

Supprimez ou désactivez une liaison réseau à l'aide de la console web. Si vous désactivez la liaison, les interfaces restent dans la liaison, mais celle-ci n'est pas utilisée pour le trafic réseau.

Conditions préalables

- Il y a un lien existant dans la console web.

Procédure

1. Connectez-vous à la console web.
   Pour plus de détails, voir Connexion à la console web .
2. Ouvrir **Networking**.
3. Cliquez sur l'obligation que vous souhaitez supprimer.
4. Dans l'écran des paramètres du lien, vous pouvez désactiver ou activer le lien en basculant un commutateur ou cliquer sur le bouton **Supprimer** pour supprimer le lien de façon permanente.

Verification steps

- Retournez sur **Networking** et vérifiez que toutes les interfaces de la liaison sont maintenant des interfaces autonomes.

CHAPITRE 9. CONFIGURATION DES ÉQUIPES RÉSEAU À L'AIDE DE LA CONSOLE WEB

Apprenez comment fonctionne le network bonding, quelles sont les différences entre les équipes de réseau et les liens de réseau, et quelles sont les possibilités de configuration dans la console web.

En outre, vous trouverez des lignes directrices pour :

- Ajout d'une nouvelle équipe de réseau
- Ajout de nouvelles interfaces à une équipe de réseau existante
- Suppression des interfaces d'une équipe de réseau existante
- Suppression d'une équipe de réseau

IMPORTANT

Si vous prévoyez de mettre à niveau votre serveur vers une version ultérieure de RHEL, envisagez d'utiliser le pilote de liaison du noyau comme alternative. Pour plus de détails, voir Configuration de la liaison réseau .

Conditions préalables

- La console web RHEL est installée et activée.
  Pour plus de détails, voir Installation de la console web.

9.1. COMPRENDRE LE TRAVAIL EN ÉQUIPE EN RÉSEAU

L'équipe réseau est une fonction qui combine ou agrège des interfaces réseau pour fournir une interface logique avec un débit plus élevé ou une redondance.

Le teaming réseau utilise un pilote de noyau pour mettre en œuvre le traitement rapide des flux de paquets, ainsi que des bibliothèques et des services de l'espace utilisateur pour d'autres tâches. Ainsi, le teaming de réseau est une solution facilement extensible et évolutive pour les besoins d'équilibrage de charge et de redondance.

IMPORTANT

Certaines fonctions de teaming réseau, telles que le mécanisme de basculement, ne prennent pas en charge les connexions directes par câble sans commutateur réseau. Pour plus de détails, voir Le bonding est-il pris en charge avec une connexion directe utilisant des câbles croisés ?

9.2. COMPARAISON DES FONCTIONS DE TEAMING ET DE BONDING DU RÉSEAU

Découvrez les fonctionnalités prises en charge par les équipes de réseau et les liens de réseau :

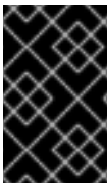
Fonctionnalité	Lien avec le réseau	L'équipe du réseau
Politique d'émission de radiodiffusion	Oui	Oui

Fonctionnalité	Lien avec le réseau	L'équipe du réseau
Politique d'émission à la ronde	Oui	Oui
Politique Tx de sauvegarde active	Oui	Oui
Support LACP (802.3ad)	Oui (actif uniquement)	Oui
Politique de transmission basée sur le hachage	Oui	Oui
L'utilisateur peut définir la fonction de hachage	Non	Oui
Prise en charge de l'équilibrage de la charge Tx (TLB)	Oui	Oui
Sélection du port de hachage LACP	Oui	Oui
Équilibrage de la charge pour la prise en charge du protocole LACP	Non	Oui
Ethtool link monitoring	Oui	Oui
Surveillance de la liaison ARP	Oui	Oui
Surveillance des liens NS/NA (IPv6)	Non	Oui
Délais de montée/descente des ports	Oui	Oui
Priorités portuaires et intérêt (amélioration de l'option "primaire")	Non	Oui
Configuration séparée de la surveillance des liens par port	Non	Oui
Configuration de la surveillance de liaisons multiples	Limitée	Oui
Chemin Tx/Rx sans verrouillage	Non (rwlock)	Oui (RCU)
Support VLAN	Oui	Oui
Contrôle de l'exécution dans l'espace utilisateur	Limitée	Oui
Logique dans l'espace utilisateur	Non	Oui
Extensibilité	Dur	Facile

Fonctionnalité	Lien avec le réseau	L'équipe du réseau
Conception modulaire	Non	Oui
Frais généraux de performance	Faible	Très faible
Interface D-Bus	Non	Oui
Empilement de plusieurs appareils	Oui	Oui
Configuration zéro à l'aide de LLDP	Non	(en cours de planification)
Support du NetworkManager	Oui	Oui

9.3. CONFIGURATION D'UNE ÉQUIPE RÉSEAU À L'AIDE DE LA CONSOLE WEB RHEL

Utilisez la console web RHEL pour configurer une équipe réseau si vous préférez gérer les paramètres réseau à l'aide d'une interface basée sur un navigateur web.



IMPORTANT

L'association de réseaux est obsolète dans Red Hat Enterprise Linux 9. Considérez l'utilisation du pilote de liaison réseau comme une alternative. Pour plus de détails, voir Configuration de la liaison réseau .

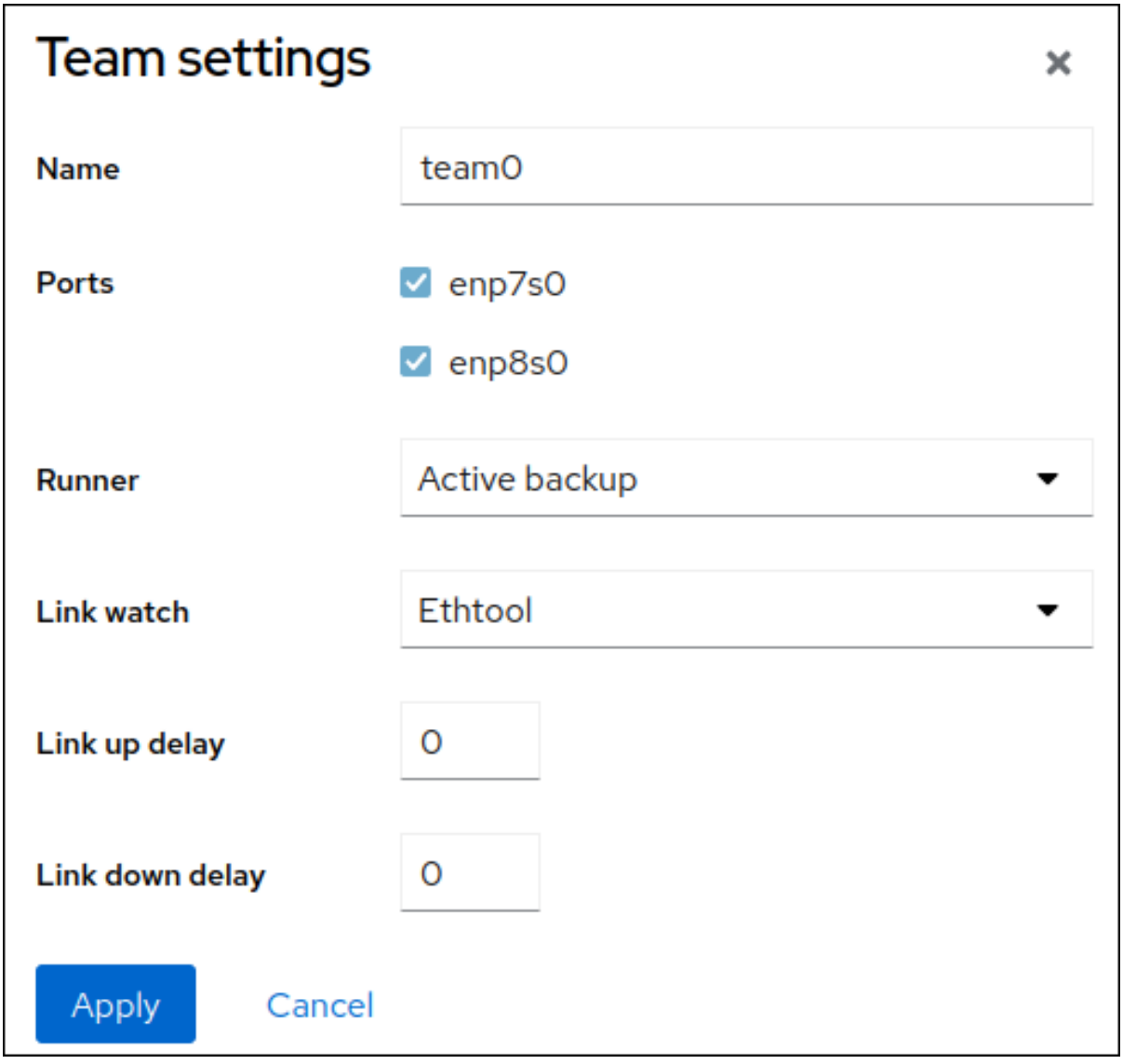
Conditions préalables

- Les paquets **teamd** et **NetworkManager-team** sont installés.
- Deux ou plusieurs périphériques réseau physiques ou virtuels sont installés sur le serveur.
- Pour utiliser des périphériques Ethernet comme ports de l'équipe, les périphériques Ethernet physiques ou virtuels doivent être installés sur le serveur et connectés à un commutateur.
- Pour utiliser des périphériques bond, bridge ou VLAN comme ports de l'équipe, créez-les à l'avance comme décrit dans la section :
- Configuration d'une liaison réseau à l'aide de la console web RHEL
- Configuration d'un pont réseau à l'aide de la console web RHEL
- Configuration du marquage VLAN à l'aide de la console web RHEL

Procédure

1. Sélectionnez l'onglet **Networking** dans le menu de navigation situé à gauche de l'écran.
2. Cliquez sur **Ajouter une équipe** dans la section **Interfaces**.

3. Saisissez le nom de l'appareil d'équipe que vous souhaitez créer.
4. Sélectionnez les interfaces qui doivent être des ports de l'équipe.
5. Sélectionnez le coureur de l'équipe.
   Si vous sélectionnez **Load balancing** ou **802.3ad LACP**, la console web affiche le champ supplémentaire **Balancer**.
6. Définir l'observateur de liens :
   - Si vous sélectionnez **Ethtool**, définissez en outre un délai d'établissement de la liaison et un délai de rétablissement de la liaison.
   - Si vous avez défini **ARP ping** ou **NSNA ping**, définissez également un intervalle de ping et une cible de ping.



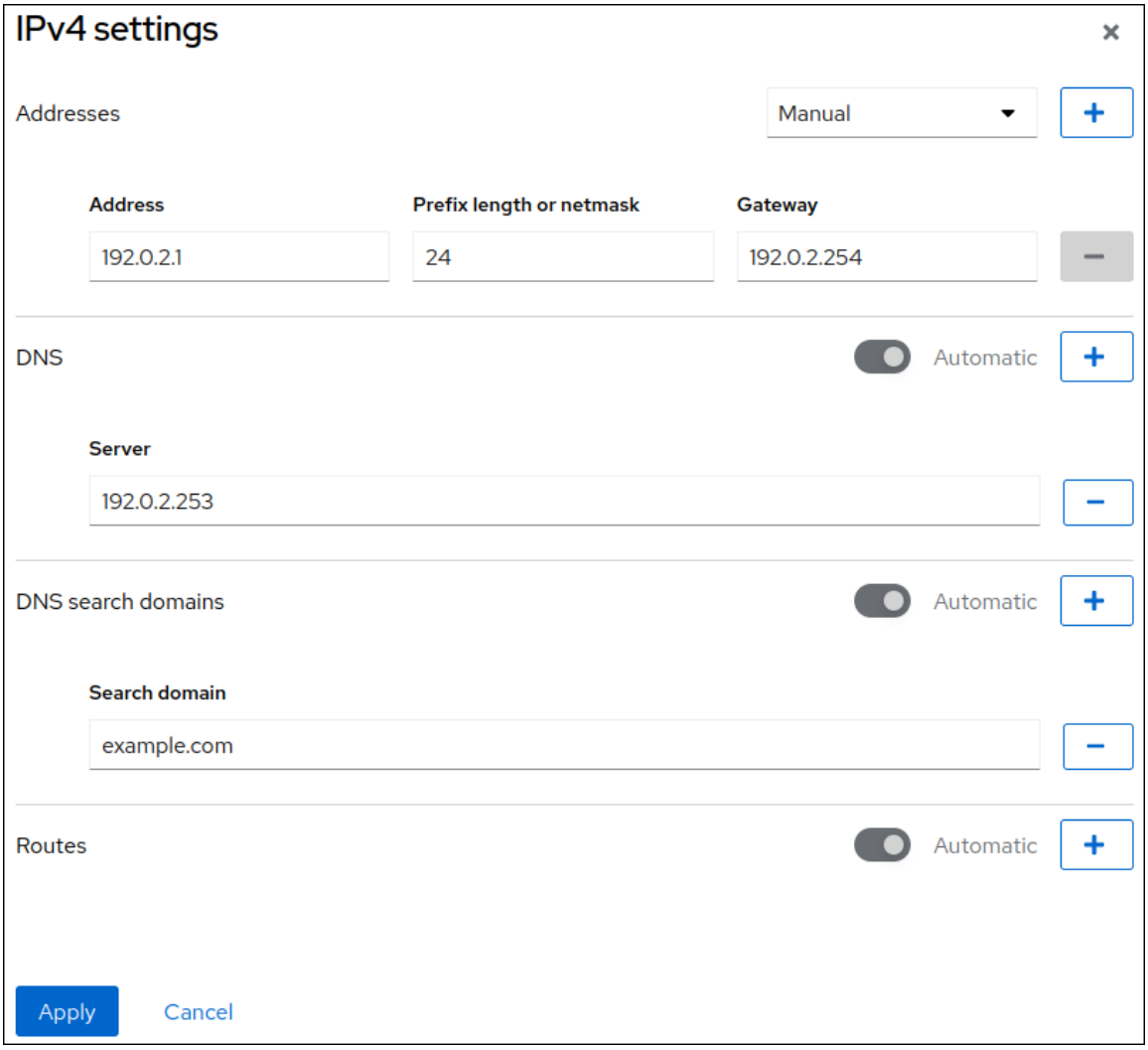
7. Cliquez sur **Appliquer**.
8. Par défaut, l'équipe utilise une adresse IP dynamique. Si vous souhaitez définir une adresse IP statique :
   a. Cliquez sur le nom de l'équipe dans la section **Interfaces**.
   b. Cliquez sur **Edit** en regard du protocole que vous souhaitez configurer.

c. Sélectionnez **Manual** à côté de **Addresses**, et entrez l'adresse IP, le préfixe et la passerelle par défaut.

d. Dans la section **DNS**, cliquez sur le bouton et entrez l'adresse IP du serveur DNS. Répétez cette étape pour définir plusieurs serveurs DNS.

e. Dans la section **DNS search domains**, cliquez sur le bouton et entrez le domaine de recherche.

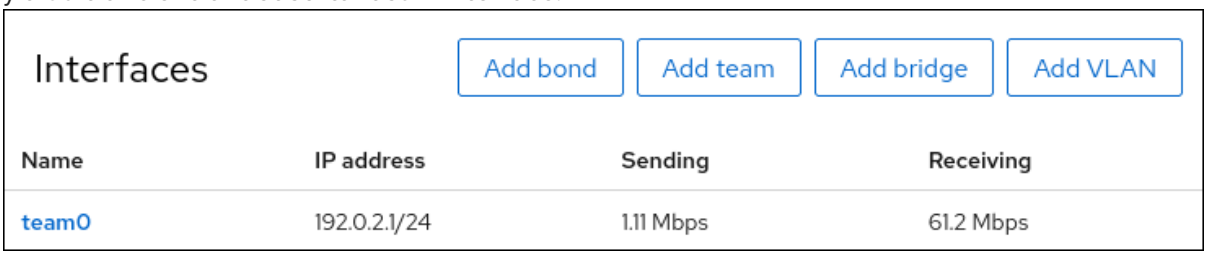
f. Si l'interface nécessite des routes statiques, configurez-les dans la section **Routes**.



g. Cliquez sur **Appliquer**

Vérification

1. Sélectionnez l'onglet **Networking** dans la navigation sur le côté gauche de l'écran, et vérifiez s'il y a du trafic entrant et sortant sur l'interface.



2. Afficher le statut de l'équipe :

```
# teamdctl team0 state
setup:
  runner: activebackup
ports:
  enp7s0
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
  enp8s0
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
runner:
  active port: enp7s0
```

Dans cet exemple, les deux ports sont activés.

Ressources supplémentaires

- Les coureurs de l'équipe du réseau

9.4. AJOUT DE NOUVELLES INTERFACES À L'ÉQUIPE À L'AIDE DE LA CONSOLE WEB

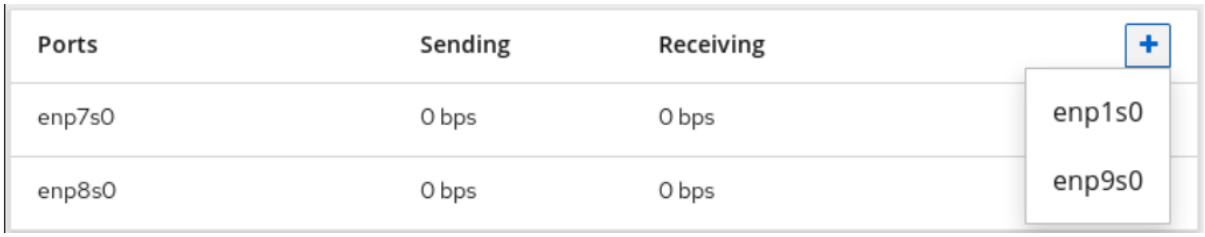
Les équipes réseau peuvent inclure plusieurs interfaces et il est possible d'en ajouter ou d'en supprimer à tout moment. La section suivante décrit comment ajouter une nouvelle interface réseau à une équipe existante.

Conditions préalables

- Une équipe réseau avec est configurée.

Procédure

1. Connectez-vous à la console web.
   Pour plus de détails, voir Connexion à la console web .
2. Passez à l'onglet **Networking**.
3. Dans le tableau **Interfaces**, cliquez sur l'équipe que vous souhaitez configurer.
4. Dans la fenêtre des paramètres de l'équipe, descendez jusqu'au tableau **Ports**.
5. Cliquez sur le bouton .
6. Sélectionnez l'interface que vous souhaitez ajouter dans la liste déroulante.



La console web RHEL ajoute l'interface à l'équipe.

9.5. SUPPRESSION OU DÉSACTIVATION D'UNE INTERFACE DE L'ÉQUIPE À L'AIDE DE LA CONSOLE WEB

Les équipes de réseau peuvent comprendre plusieurs interfaces. Si vous devez modifier un appareil, vous pouvez supprimer ou désactiver certaines interfaces de l'équipe réseau, qui fonctionneront avec le reste des interfaces actives.

Il existe deux options pour cesser d'utiliser une interface incluse dans une équipe :

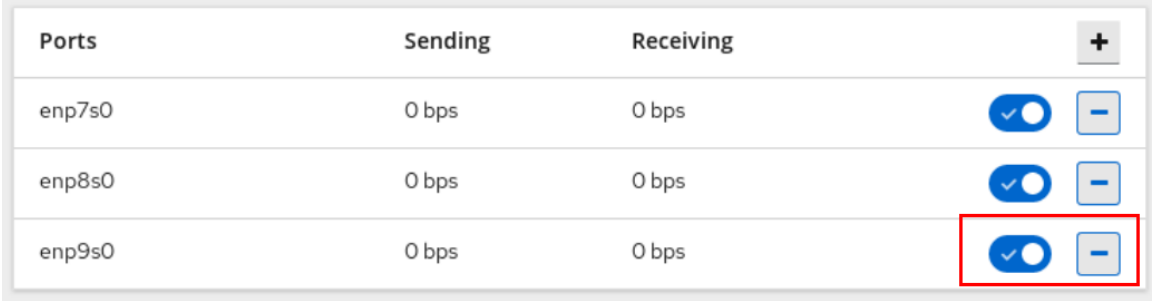
- Supprimer l'interface de l'équipe
- Désactiver temporairement l'interface. L'interface fait toujours partie de l'équipe, mais celle-ci ne l'utilisera pas tant que vous ne l'aurez pas réactivée.

Conditions préalables

- Une équipe réseau avec plusieurs interfaces existe sur l'hôte.

Procédure

1. Connectez-vous à la console web RHEL.
   Pour plus de détails, voir Connexion à la console web .
2. Passez à l'onglet **Networking**.
3. Cliquez sur l'équipe que vous souhaitez configurer.
4. Dans la fenêtre des paramètres de l'équipe, descendez jusqu'au tableau des ports (interfaces).
5. Sélectionnez une interface et supprimez-la ou désactivez-la.
   a. Placez le bouton **ON**/**OFF** sur Off pour désactiver l'interface.
   b. Cliquez sur le bouton **-** pour supprimer l'interface.



En fonction de votre choix, la console web supprime ou désactive l'interface. Si vous supprimez l'interface, elle sera disponible sur **Networking** en tant qu'interface autonome.

9.6. SUPPRESSION OU DÉSACTIVATION D'UNE ÉQUIPE À L'AIDE DE LA CONSOLE WEB

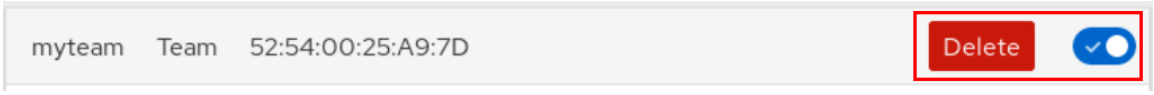
Supprimez ou désactivez une équipe réseau à l'aide de la console web. Si vous désactivez uniquement l'équipe, les interfaces de l'équipe y resteront, mais l'équipe ne sera pas utilisée pour le trafic réseau.

Conditions préalables

- Une équipe réseau est configurée sur l'hôte.

Procédure

1. Connectez-vous à la console web.
   Pour plus de détails, voir Connexion à la console web .
2. Passez à l'onglet **Networking**.
3. Cliquez sur l'équipe que vous souhaitez supprimer ou désactiver.
4. Supprimer ou désactiver l'équipe sélectionnée.
   a. Vous pouvez supprimer l'équipe en cliquant sur le bouton **Supprimer**.
   b. Vous pouvez désactiver l'équipe en plaçant l'interrupteur **ON/OFF** en position de désactivation.



Verification steps

- Si vous avez supprimé l'équipe, allez sur **Networking**, et vérifiez que toutes les interfaces de votre équipe sont maintenant listées comme des interfaces autonomes.

CHAPITRE 10. CONFIGURATION DES PONTS RÉSEAU DANS LA CONSOLE WEB

Les ponts de réseau sont utilisés pour connecter plusieurs interfaces à un sous-réseau avec la même plage d'adresses IP.

Conditions préalables

- La console web RHEL 9 est installée et activée.
  Pour plus de détails, voir Installation de la console web .

10.1. CONFIGURATION D'UN PONT RÉSEAU À L'AIDE DE LA CONSOLE WEB RHEL

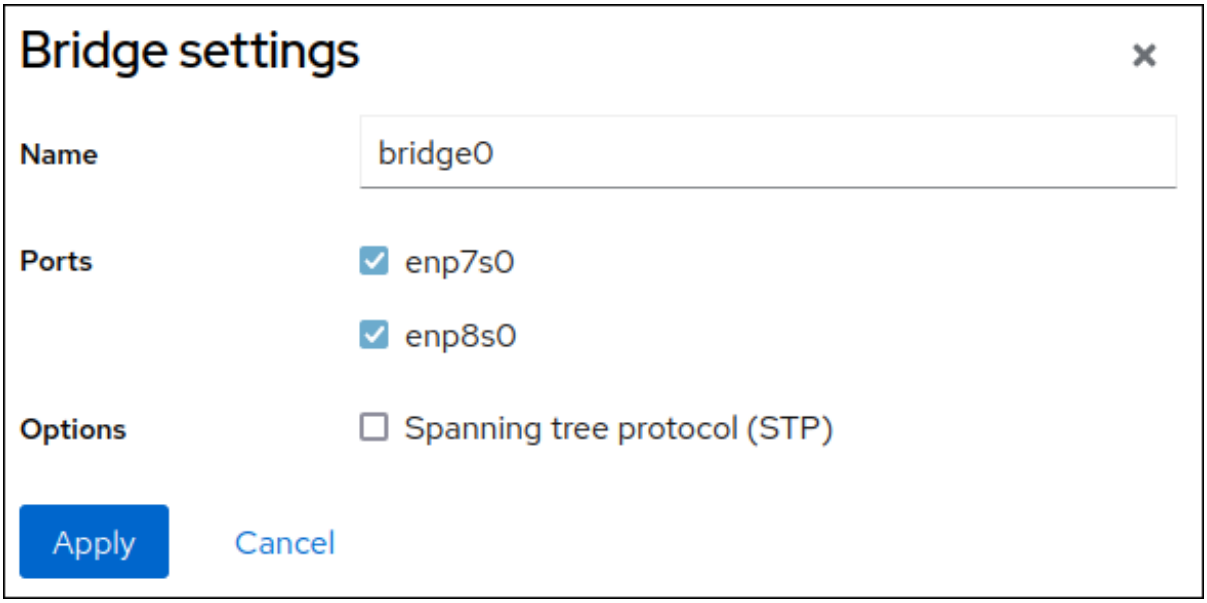
Utilisez la console web RHEL pour configurer un pont réseau si vous préférez gérer les paramètres réseau à l'aide d'une interface basée sur un navigateur web.

Conditions préalables

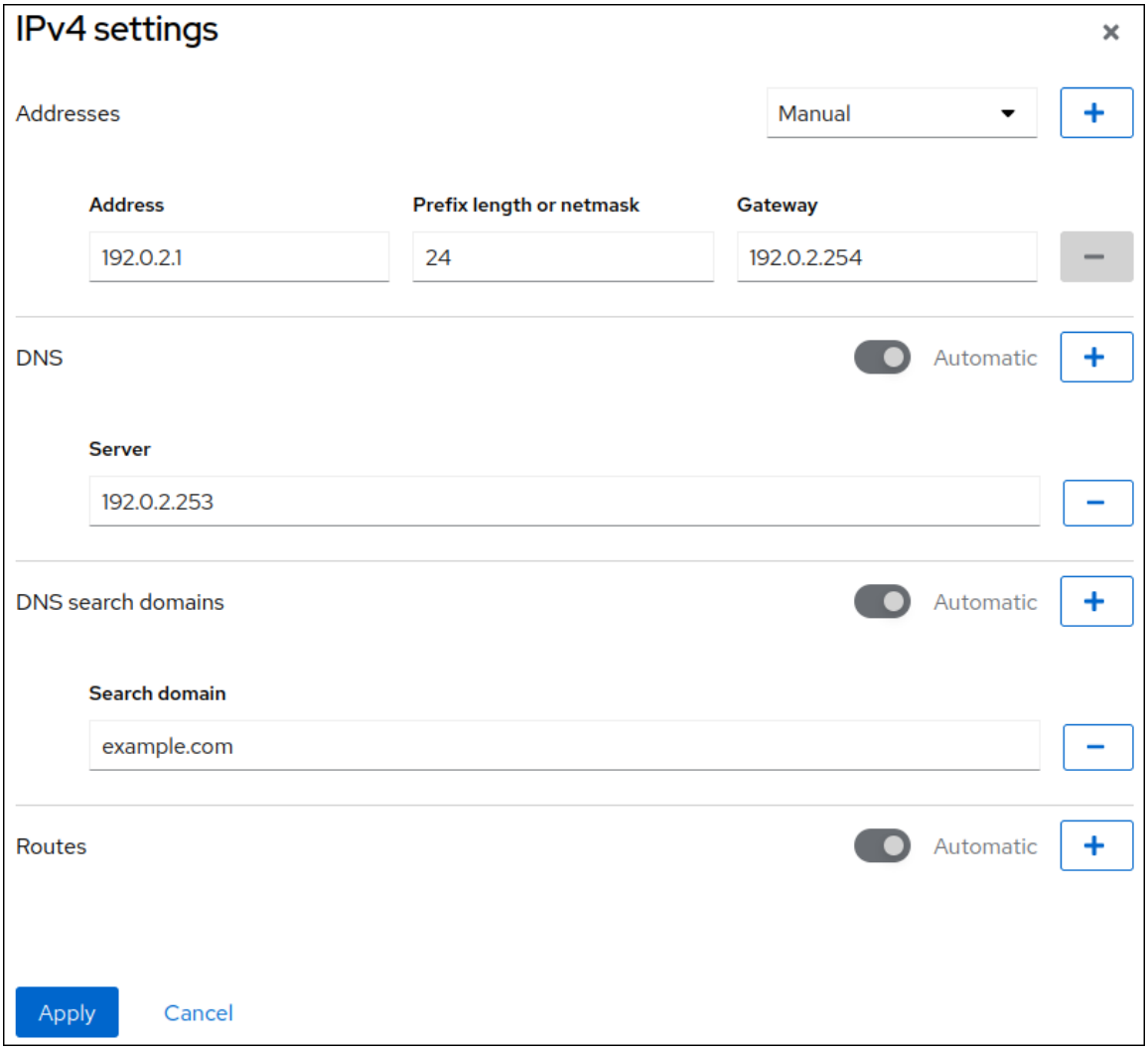
- Deux ou plusieurs périphériques réseau physiques ou virtuels sont installés sur le serveur.
- Pour utiliser des périphériques Ethernet comme ports du pont, les périphériques Ethernet physiques ou virtuels doivent être installés sur le serveur.
- Pour utiliser des périphériques team, bond ou VLAN comme ports de la passerelle, vous pouvez soit créer ces périphériques lors de la création de la passerelle, soit les créer à l'avance comme décrit dans la section :
  - Configuration d'une équipe réseau à l'aide de la console web RHEL
  - Configuration d'une liaison réseau à l'aide de la console web RHEL
  - Configuration du marquage VLAN à l'aide de la console web RHEL

Procédure

1. Sélectionnez l'onglet **Networking** dans le menu de navigation situé à gauche de l'écran.
2. Cliquez sur **Add bridge** dans la section **Interfaces**.
3. Saisissez le nom du dispositif de pont que vous souhaitez créer.
4. Sélectionnez les interfaces qui doivent être des ports du pont.
5. Facultatif : Activez la fonction **Spanning tree protocol (STP)** pour éviter les boucles de pont et les radiations de diffusion.



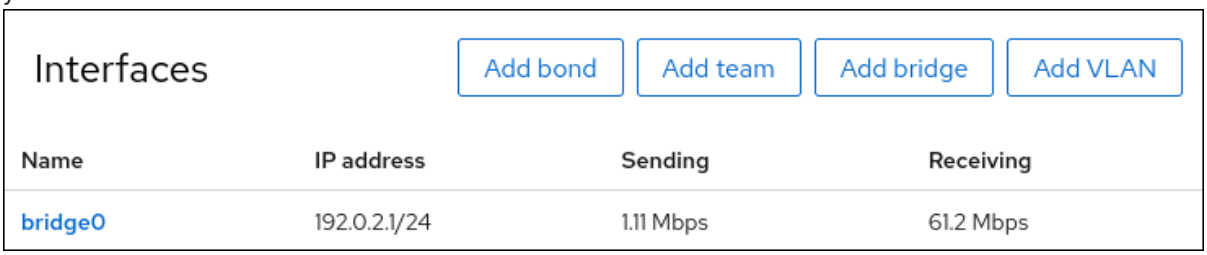
6. Cliquez sur **Appliquer**.
7. Par défaut, le pont utilise une adresse IP dynamique. Si vous souhaitez définir une adresse IP statique :
   a. Cliquez sur le nom du pont dans la section **Interfaces**.
   b. Cliquez sur **Edit** en regard du protocole que vous souhaitez configurer.
   c. Sélectionnez **Manual** à côté de **Addresses**, et entrez l'adresse IP, le préfixe et la passerelle par défaut.
   d. Dans la section **DNS**, cliquez sur le bouton et entrez l'adresse IP du serveur DNS. Répétez cette étape pour définir plusieurs serveurs DNS.
   e. Dans la section **DNS search domains**, cliquez sur le bouton et entrez le domaine de recherche.
   f. Si l'interface nécessite des routes statiques, configurez-les dans la section **Routes**.



g. Cliquez sur **Appliquer**

Vérification

1. Sélectionnez l'onglet **Networking** dans la navigation sur le côté gauche de l'écran, et vérifiez s'il y a du trafic entrant et sortant sur l'interface :



10.2. SUPPRESSION D'INTERFACES DU PONT À L'AIDE DE LA CONSOLE WEB

Les ponts de réseau peuvent comprendre plusieurs interfaces. Vous pouvez les retirer du pont. Chaque interface supprimée sera automatiquement transformée en interface autonome.

Apprenez à supprimer une interface réseau d'un pont logiciel créé dans le système RHEL 9.

Conditions préalables

- Avoir un pont avec plusieurs interfaces dans votre système.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Ouvrir **Networking**.
3. Cliquez sur le pont que vous souhaitez configurer.
4. Dans l'écran des paramètres du pont, faites défiler vers le bas jusqu'au tableau des ports (interfaces).
5. Sélectionnez une interface et cliquez sur le bouton **-**.

Verification steps

- Allez sur **Networking** pour vérifier que vous pouvez voir l'interface en tant qu'interface autonome dans la table **Interface members**.

10.3. SUPPRESSION DE PONTS DANS LA CONSOLE WEB

Vous pouvez supprimer un pont réseau logiciel dans la console web RHEL. Toutes les interfaces réseau incluses dans le pont seront automatiquement transformées en interfaces autonomes.

Conditions préalables

- Avoir un pont dans son système.

Procédure

1. Connectez-vous à la console web RHEL.
   Pour plus de détails, voir Connexion à la console web .
2. Ouvrez la section **Networking**.
3. Cliquez sur le pont que vous souhaitez configurer.
4. Cliquez sur **Delete**.

Verification steps

- Retournez sur **Networking** et vérifiez que toutes les interfaces réseau sont affichées dans le tableau **Interface members**.

Certaines interfaces qui faisaient auparavant partie du pont peuvent devenir inactives. Si nécessaire, activez-les et définissez manuellement les paramètres du réseau.

CHAPITRE 11. CONFIGURATION DES VLAN DANS LA CONSOLE WEB

Cette section décrit comment configurer un réseau local virtuel (VLAN). Un VLAN est un réseau logique au sein d'un réseau physique. L'interface VLAN marque les paquets avec l'ID VLAN lorsqu'ils passent par l'interface, et supprime les marques des paquets qui reviennent.

11.1. CONFIGURATION DU MARQUAGE VLAN À L'AIDE DE LA CONSOLE WEB RHEL

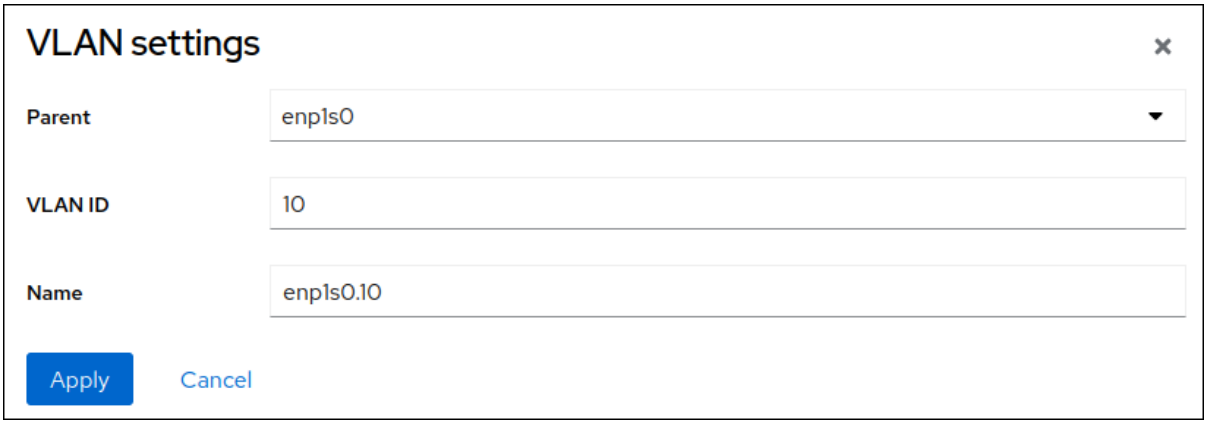
Utilisez la console web RHEL pour configurer le marquage VLAN si vous préférez gérer les paramètres du réseau à l'aide d'une interface basée sur un navigateur web.

Conditions préalables

- L'interface que vous prévoyez d'utiliser comme parent de l'interface VLAN virtuelle prend en charge les balises VLAN.
- Si vous configurez le VLAN au-dessus d'une interface de liaison :
  - Les ports de la liaison sont en place.
  - La liaison n'est pas configurée avec l'option **fail_over_mac=follow**. Un périphérique virtuel VLAN ne peut pas modifier son adresse MAC pour qu'elle corresponde à la nouvelle adresse MAC du parent. Dans ce cas, le trafic serait toujours envoyé avec l'adresse MAC source incorrecte.
  - Le lien n'est généralement pas censé obtenir des adresses IP à partir d'un serveur DHCP ou d'une auto-configuration IPv6. Assurez-vous que c'est le cas en désactivant les protocoles IPv4 et IPv6 qui créent le lien. Sinon, si la configuration automatique DHCP ou IPv6 échoue au bout d'un certain temps, l'interface risque d'être mise hors service.
- Le commutateur auquel l'hôte est connecté est configuré pour prendre en charge les balises VLAN. Pour plus de détails, consultez la documentation de votre commutateur.

Procédure

1. Sélectionnez l'onglet **Networking** dans le menu de navigation situé à gauche de l'écran.
2. Cliquez sur **Add VLAN** dans la section **Interfaces**.
3. Sélectionnez l'appareil parent.
4. Saisissez l'ID VLAN.
5. Saisissez le nom du périphérique VLAN ou conservez le nom généré automatiquement.



6. Cliquez sur **Appliquer**.

7. Par défaut, le dispositif VLAN utilise une adresse IP dynamique. Si vous souhaitez définir une adresse IP statique :

   a. Cliquez sur le nom du périphérique VLAN dans la section **Interfaces**.

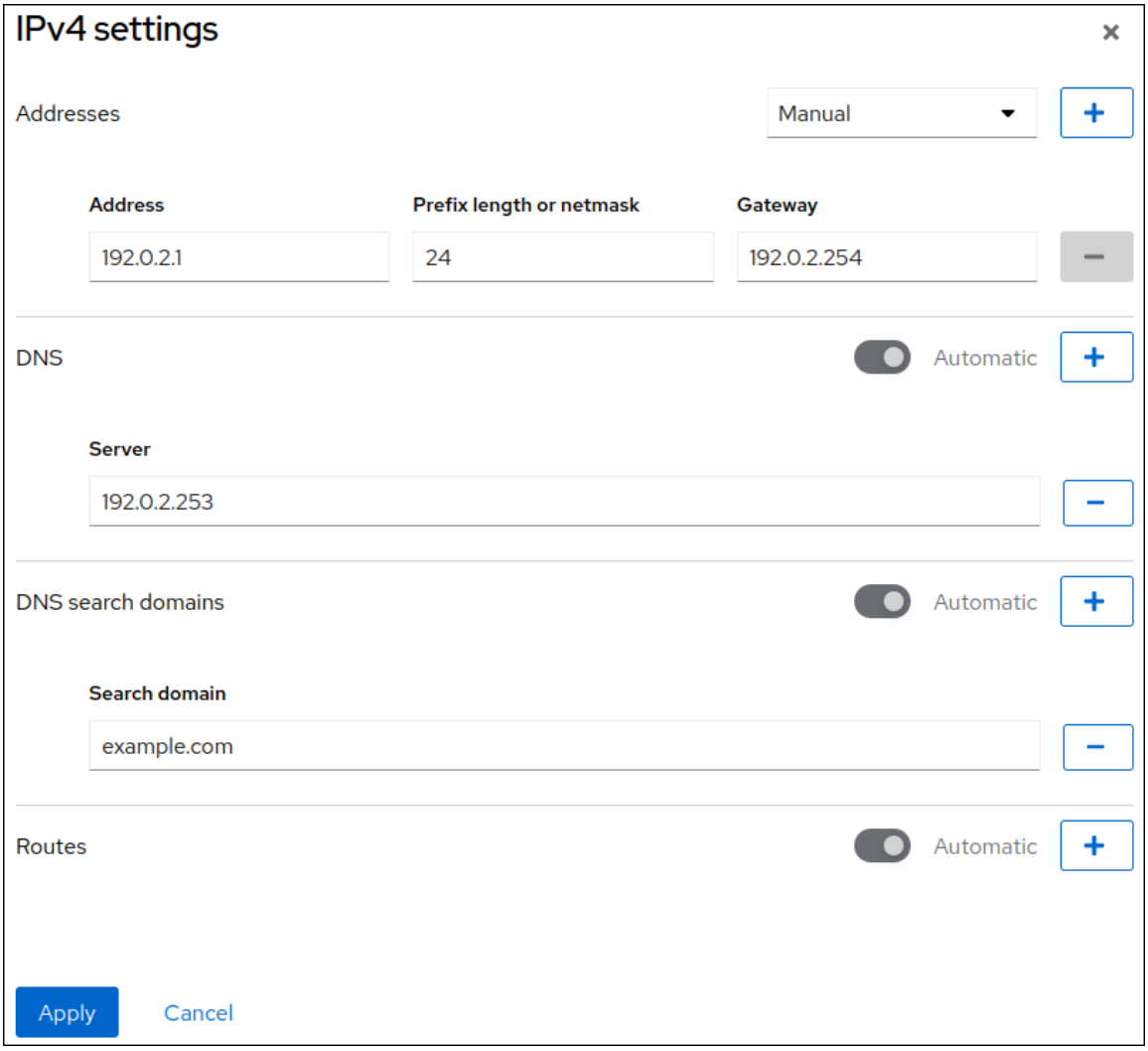
   b. Cliquez sur **Edit** en regard du protocole que vous souhaitez configurer.

   c. Sélectionnez **Manual** à côté de **Addresses**, et entrez l'adresse IP, le préfixe et la passerelle par défaut.

   d. Dans la section **DNS**, cliquez sur le bouton et entrez l'adresse IP du serveur DNS. Répétez cette étape pour définir plusieurs serveurs DNS.

   e. Dans la section **DNS search domains**, cliquez sur le bouton et entrez le domaine de recherche.

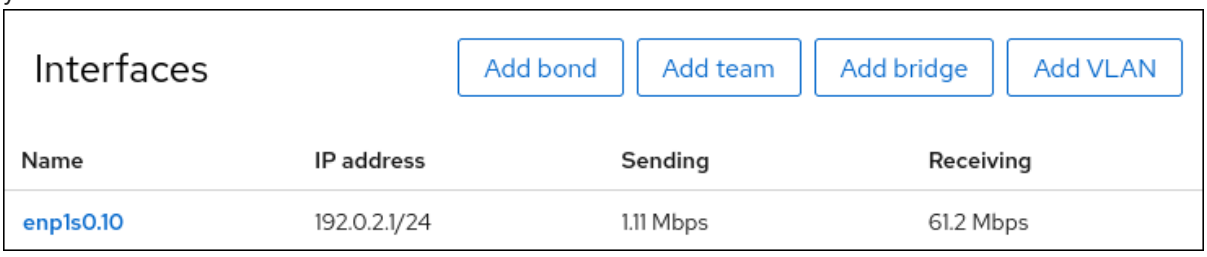
   f. Si l'interface nécessite des routes statiques, configurez-les dans la section **Routes**.



g. Cliquez sur **Appliquer**

Vérification

- Sélectionnez l'onglet **Networking** dans la navigation sur le côté gauche de l'écran, et vérifiez s'il y a du trafic entrant et sortant sur l'interface :



CHAPITRE 12. CONFIGURATION DU PORT D'ÉCOUTE DE LA CONSOLE WEB

Apprenez à autoriser de nouveaux ports ou à modifier les ports existants à l'aide de la console Web RHEL 9.

12.1. AUTORISER UN NOUVEAU PORT SUR UN SYSTÈME AVEC SELINUX ACTIF

Permet à la console web d'écouter sur un port sélectionné.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

- Pour les ports qui ne sont pas définis par une autre partie de SELinux, exécuter :

```
$ sudo semanage port -a -t websm_port_t -p tcp PORT_NUMBER
```

- Pour les ports qui sont déjà définis par une autre partie de SELinux, exécutez :

```
$ sudo semanage port -m -t websm_port_t -p tcp PORT_NUMBER
```

Les changements devraient prendre effet immédiatement.

12.2. AUTORISER UN NOUVEAU PORT SUR UN SYSTÈME AVEC FIREWALLD

Permet à la console web de recevoir des connexions sur un nouveau port.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.
- Le service **firewalld** doit être en cours d'exécution.

Procédure

1. Pour ajouter un nouveau numéro de port, exécutez la commande suivante :

```
$ sudo firewall-cmd --permanent --service cockpit --add-port=PORT_NUMBER/tcp
```

2. Pour supprimer l'ancien numéro de port du service **cockpit**, exécutez la commande suivante

```
$ sudo firewall-cmd --permanent --service cockpit --remove-port=OLD_PORT_NUMBER/tcp
```

IMPORTANT

Si vous n'exécutez que **firewall-cmd --service cockpit --add-port=PORT_NUMBER/tcp** sans l'option **--permanent**, votre modification disparaîtra lors du prochain rechargement de **firewalld** ou lors d'un redémarrage du système.

12.3. MODIFIER LE PORT DE LA CONSOLE WEB

Remplacer le protocole de contrôle de transmission (TCP) par défaut sur le port **9090** par un autre.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.
- Si votre système est protégé par SELinux, vous devez le paramétrer pour permettre à Cockpit d'écouter sur un nouveau port. Pour plus d'informations, voir Autoriser un nouveau port sur un système avec SELinux actif.
- Si vous avez configuré **firewalld** comme pare-feu, vous devez le paramétrer pour autoriser Cockpit à recevoir des connexions sur un nouveau port, pour plus d'informations, voir Autoriser un nouveau port sur un système avec **firewalld**.

Procédure

1. Modifiez le port d'écoute à l'aide de l'une des méthodes suivantes :
   a. En utilisant la commande **systemctl edit cockpit.socket**:
      i. Exécutez la commande suivante :

      ```
      $ sudo systemctl edit cockpit.socket
      ```

      Cela ouvrira le fichier **/etc/systemd/system/cockpit.socket.d/override.conf**.

      ii. Modifier le contenu de **override.conf** ou ajouter un nouveau contenu dans le format suivant :

      ```
      [Socket]
      ListenStream=
      ListenStream=PORT_NUMBER
      ```

   b. Vous pouvez également ajouter le contenu susmentionné au fichier **/etc/systemd/system/cockpit.socket.d/listen.conf**.
   Créez le répertoire **cockpit.socket.d.** et le fichier **listen.conf** s'ils n'existent pas encore.
2. Exécutez les commandes suivantes pour que les modifications soient prises en compte :

   ```
   $ sudo systemctl daemon-reload
   $ sudo systemctl restart cockpit.socket
   ```

   Si vous avez utilisé **systemctl edit cockpit.socket** à l'étape précédente, il n'est pas nécessaire d'exécuter **systemctl daemon-reload**.

Verification steps

- Pour vérifier que la modification a été effectuée avec succès, essayez de vous connecter à la console web avec le nouveau port.

CHAPITRE 13. GESTION DU PARE-FEU À L'AIDE DE LA CONSOLE WEB

Un pare-feu est un moyen de protéger les machines contre tout trafic indésirable provenant de l'extérieur. Il permet aux utilisateurs de contrôler le trafic réseau entrant sur les machines hôtes en définissant un ensemble de règles de pare-feu. Ces règles sont utilisées pour trier le trafic entrant et le bloquer ou l'autoriser.

Conditions préalables

- La console web RHEL 9 configure le service **firewalld**.
  Pour plus d'informations sur le service **firewalld**, voir Démarrer avec firewalld.

13.1. EXÉCUTION DU PARE-FEU À L'AIDE DE LA CONSOLE WEB

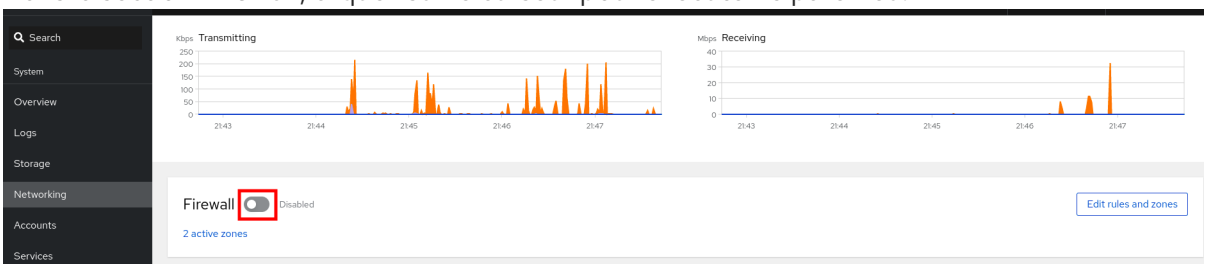
Cette section décrit où et comment exécuter le pare-feu système RHEL 9 dans la console Web.

NOTE

La console web RHEL 9 configure le service **firewalld**.

Procédure

1. Connectez-vous à la console web RHEL 9. Pour plus d'informations, voir Connexion à la console web.
2. Ouvrez la section **Networking**.
3. Dans la section **Firewall**, cliquez sur le curseur pour exécuter le pare-feu.



   Si vous ne voyez pas le curseur **Firewall**, connectez-vous à la console web avec les privilèges administratifs.

À ce stade, votre pare-feu fonctionne.

Pour configurer les règles du pare-feu, voir Activation des services sur le pare-feu à l'aide de la console web

13.2. ARRÊT DU PARE-FEU À L'AIDE DE LA CONSOLE WEB

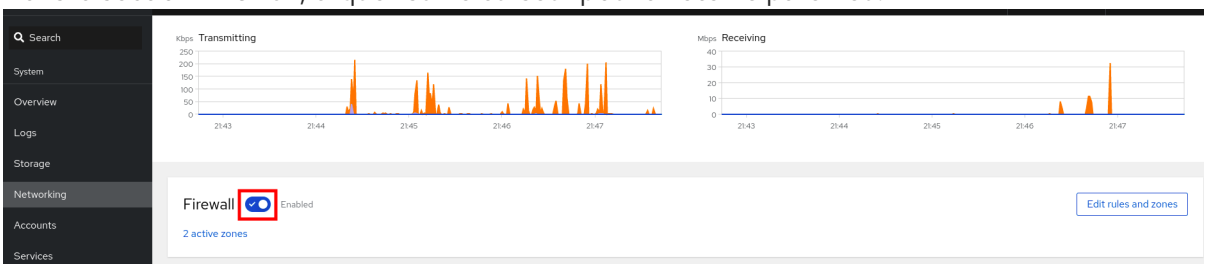
Cette section décrit où et comment arrêter le pare-feu du système RHEL 9 dans la console Web.

NOTE

La console web RHEL 9 configure le service **firewalld**.

Procédure

1. Connectez-vous à la console web RHEL 9. Pour plus d'informations, voir Connexion à la console web.
2. Ouvrez la section **Networking**.
3. Dans la section **Firewall**, cliquez sur le curseur pour arrêter le pare-feu.



Si vous ne voyez pas le curseur **Firewall**, connectez-vous à la console web avec les privilèges administratifs.

À ce stade, le pare-feu a été arrêté et ne sécurise pas votre système.

13.3. ZONES

firewalld peut être utilisé pour séparer les réseaux en différentes zones en fonction du niveau de confiance que l'utilisateur a décidé d'accorder aux interfaces et au trafic au sein de ce réseau. Une connexion ne peut faire partie que d'une seule zone, mais une zone peut être utilisée pour plusieurs connexions réseau.

NetworkManager notifie à **firewalld** la zone d'une interface. Vous pouvez assigner des zones aux interfaces avec :

- **NetworkManager**
- **firewall-config** outil
- **firewall-cmd** outil en ligne de commande
- La console web RHEL

Les trois derniers ne peuvent éditer que les fichiers de configuration appropriés de **NetworkManager**. Si vous changez la zone de l'interface à l'aide de la console web, **firewall-cmd** ou **firewall-config**, la demande est transmise à **NetworkManager** et n'est pas traitée par **firewalld**.

Les zones prédéfinies sont stockées dans le répertoire **/usr/lib/firewalld/zones/** et peuvent être appliquées instantanément à toute interface réseau disponible. Ces fichiers ne sont copiés dans le répertoire **/etc/firewalld/zones/** qu'après avoir été modifiés. Les paramètres par défaut des zones prédéfinies sont les suivants :

block

Toute connexion réseau entrante est rejetée avec un message icmp-host-prohibited pour **IPv4** et icmp6-adm-prohibited pour **IPv6**. Seules les connexions réseau initiées depuis l'intérieur du système sont possibles.

dmz

Pour les ordinateurs de votre zone démilitarisée qui sont accessibles au public avec un accès limité à votre réseau interne. Seules les connexions entrantes sélectionnées sont acceptées.

drop

Tous les paquets réseau entrants sont abandonnés sans notification. Seules les connexions réseau sortantes sont possibles.

external

À utiliser sur les réseaux externes où le masquage est activé, en particulier pour les routeurs. Vous ne faites pas confiance aux autres ordinateurs du réseau pour ne pas nuire à votre ordinateur. Seules les connexions entrantes sélectionnées sont acceptées.

home

À utiliser à la maison lorsque vous faites essentiellement confiance aux autres ordinateurs du réseau. Seules les connexions entrantes sélectionnées sont acceptées.

internal

À utiliser sur les réseaux internes lorsque vous faites essentiellement confiance aux autres ordinateurs du réseau. Seules les connexions entrantes sélectionnées sont acceptées.

public

À utiliser dans les lieux publics où vous ne faites pas confiance aux autres ordinateurs du réseau. Seules les connexions entrantes sélectionnées sont acceptées.

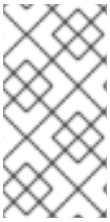
trusted

Toutes les connexions réseau sont acceptées.

work

À utiliser au travail lorsque vous faites essentiellement confiance aux autres ordinateurs du réseau. Seules les connexions entrantes sélectionnées sont acceptées.

L'une de ces zones est définie comme la zone *default*. Lorsque des connexions d'interface sont ajoutées à **NetworkManager**, elles sont affectées à la zone par défaut. Lors de l'installation, la zone par défaut dans **firewalld** est définie comme étant la zone **public**. La zone par défaut peut être modifiée.



NOTE

Les noms des zones du réseau doivent être explicites et permettre aux utilisateurs de prendre rapidement une décision raisonnable. Pour éviter tout problème de sécurité, examinez la configuration de la zone par défaut et désactivez tous les services inutiles en fonction de vos besoins et de l'évaluation des risques.

Ressources supplémentaires

- La page de manuel **firewalld.zone(5)**.

13.4. ZONES DANS LA CONSOLE WEB

La console web de Red Hat Enterprise Linux met en œuvre les principales fonctionnalités du service firewalld et vous permet de :

- Ajouter des zones de pare-feu prédéfinies à une interface particulière ou à une plage d'adresses IP
- Configurer des zones en sélectionnant des services dans la liste des services activés
- Désactiver un service en le retirant de la liste des services activés
- Supprimer une zone d'une interface

13.5. ACTIVATION DE ZONES À L'AIDE DE LA CONSOLE WEB

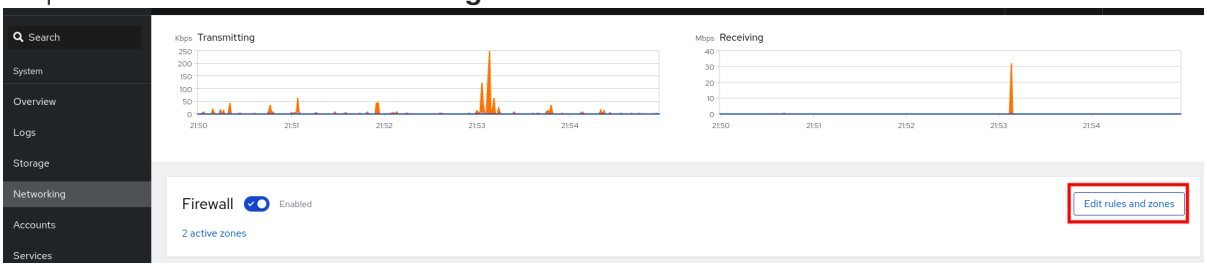
La console web vous permet d'appliquer des zones de pare-feu prédéfinies et existantes à une interface particulière ou à une plage d'adresses IP. Cette section décrit comment activer une zone sur une interface.

Conditions préalables

- La console web RHEL 9 a été installée. Pour plus de détails, voir le lien : https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/managing_systems_using_the_rhel_9_web_console/getting-started-with-the-rhel-9-web-console_system-management-using-the-rhel-9-web-console#installing-the-web-console_getting-started-with-the-rhel-9-web-consoleInstalling the web console].
- Le pare-feu doit être activé. Pour plus de détails, voir Exécuter le pare-feu à l'aide de la console web.

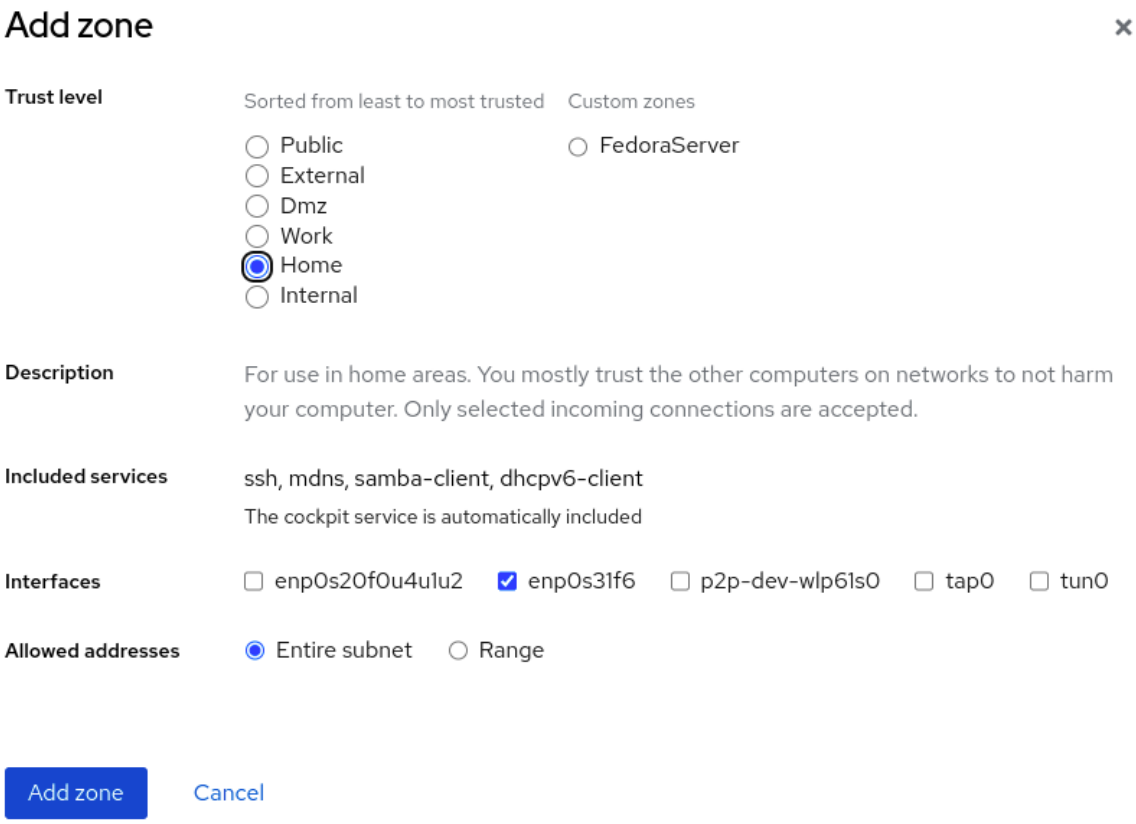
Procédure

1. Connectez-vous à la console web RHEL avec des privilèges administratifs. Pour plus d'informations, voir Connexion à la console web .
2. Cliquez sur **Networking**.
3. Cliquez sur le bouton **Modifier les règles et les zones**.

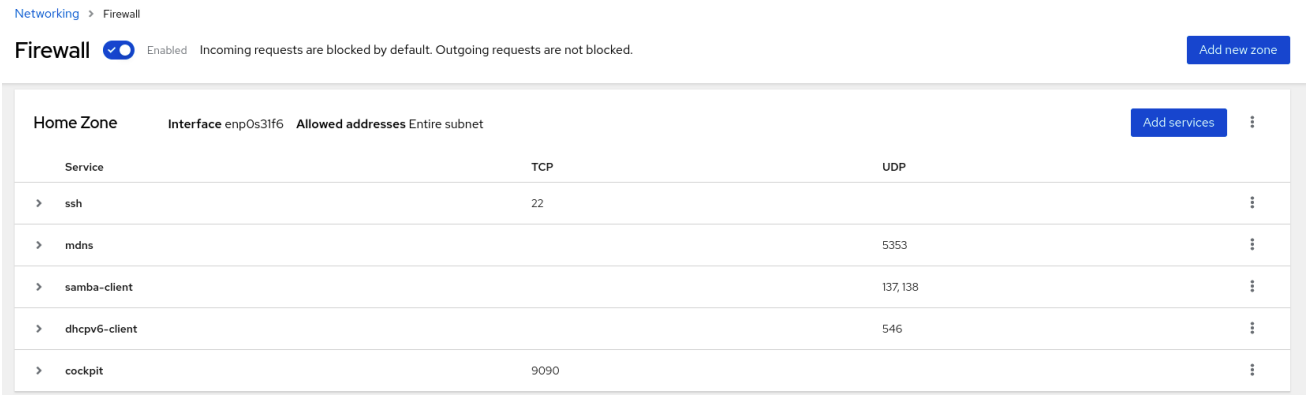


   Si vous ne voyez pas le bouton **Modifier les règles et les zones**, connectez-vous à la console web avec les privilèges d'administrateur.
4. Dans la section **Firewall**, cliquez sur **Add new zone**.
5. Dans la boîte de dialogue **Add zone**, sélectionnez une zone dans les options **Trust level**. Vous pouvez voir ici toutes les zones prédéfinies dans le service **firewalld**.
6. Dans la partie **Interfaces**, sélectionnez une ou plusieurs interfaces sur lesquelles la zone sélectionnée est appliquée.
7. Dans la partie **Allowed Addresses**, vous pouvez choisir si la zone est appliquée sur :
   - l'ensemble du sous-réseau
   - ou une série d'adresses IP dans le format suivant :
     - 192.168.1.0
     - 192.168.1.0/24
     - 192.168.1.0/24, 192.168.1.0

8. Cliquez sur le bouton **Ajouter une zone**.



Vérifiez la configuration sur **Firewall**.



13.6. ACTIVATION DE SERVICES SUR LE PARE-FEU À L'AIDE DE LA CONSOLE WEB

Par défaut, les services sont ajoutés à la zone de pare-feu par défaut. Si vous utilisez plusieurs zones de pare-feu sur plusieurs interfaces réseau, vous devez d'abord sélectionner une zone, puis ajouter le service avec le port.

La console web RHEL 9 affiche des services **firewalld** prédéfinis et vous pouvez les ajouter aux zones de pare-feu actives.

IMPORTANT

La console web RHEL 9 configure le service **firewalld**.

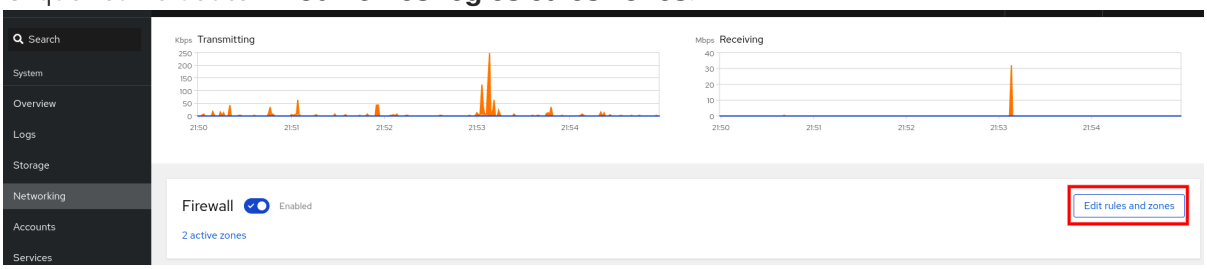
La console web n'autorise pas les règles génériques **firewalld** qui ne sont pas répertoriées dans la console web.

Conditions préalables

- La console web RHEL 9 a été installée. Pour plus de détails, voir Installation de la console web .
- Le pare-feu doit être activé. Pour plus de détails, voir Exécuter le pare-feu à l'aide de la console web.

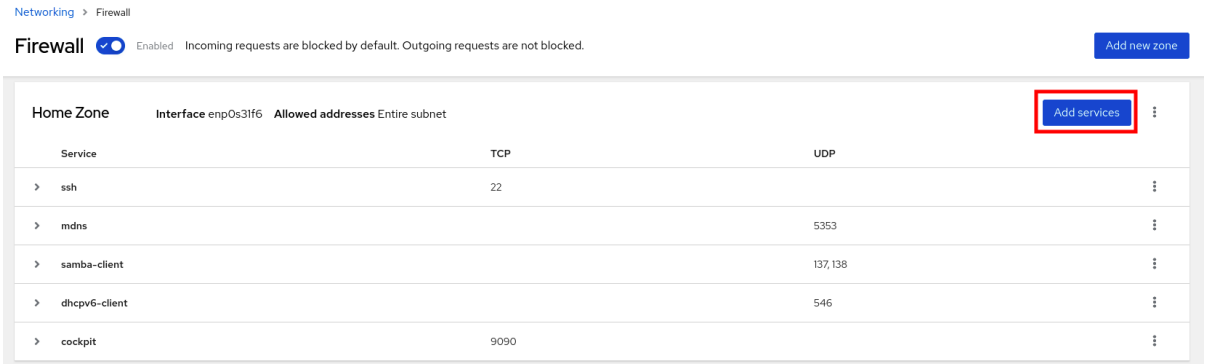
Procédure

1. Connectez-vous à la console web RHEL avec des privilèges d'administrateur. Pour plus d'informations, voir Connexion à la console web .
2. Cliquez sur **Networking**.
3. Cliquez sur le bouton **Modifier les règles et les zones**.

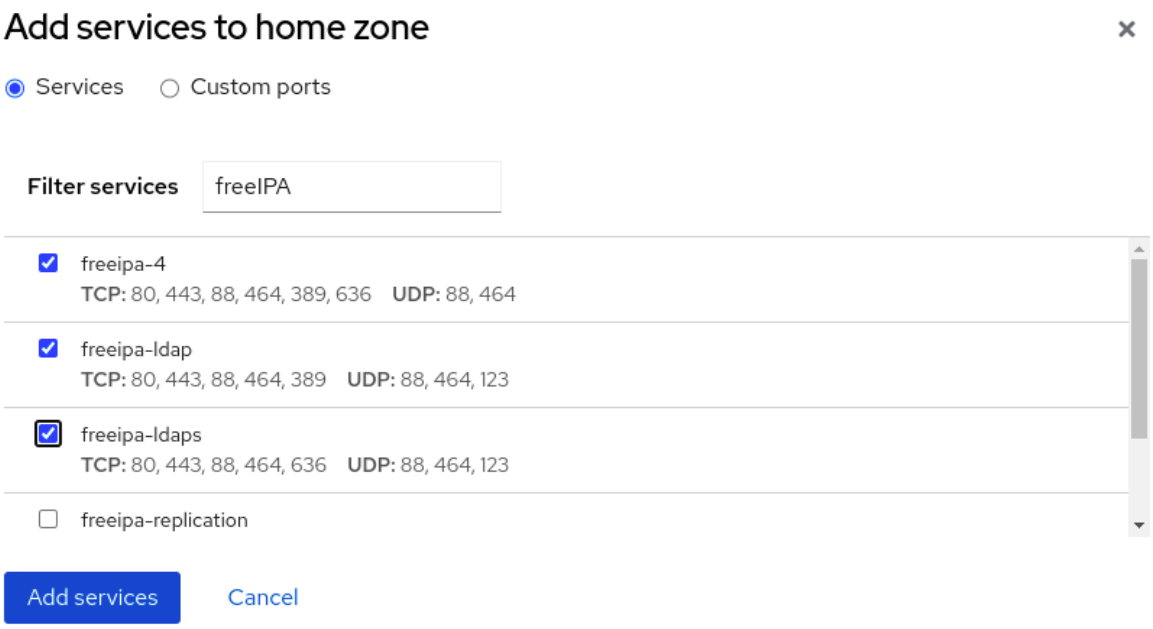


Si vous ne voyez pas le bouton **Modifier les règles et les zones**, connectez-vous à la console web avec les privilèges d'administrateur.

4. Dans la section **Firewall**, sélectionnez une zone pour laquelle vous souhaitez ajouter le service et cliquez sur **Add Services**.



5. Dans la boîte de dialogue **Add Services**, recherchez le service que vous souhaitez activer sur le pare-feu.
6. Activer les services souhaités.



7. Cliquez sur **Add Services**.

A ce stade, la console web RHEL 9 affiche le service dans la liste de **Services** de la zone.

13.7. CONFIGURATION DES PORTS PERSONNALISÉS À L'AIDE DE LA CONSOLE WEB

La console web vous permet d'ajouter :

- Services écoutant sur des ports standard : Activation de services sur le pare-feu à l'aide de la console web
- Services écoutant sur des ports personnalisés.

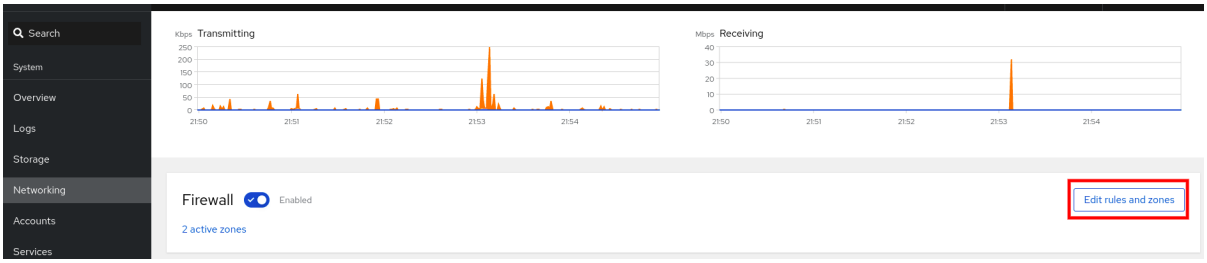
Cette section décrit comment ajouter des services avec des ports personnalisés configurés.

Conditions préalables

- La console web RHEL 9 a été installée. Pour plus de détails, voir Installation de la console web .
- Le pare-feu doit être activé. Pour plus de détails, voir Exécuter le pare-feu à l'aide de la console web.

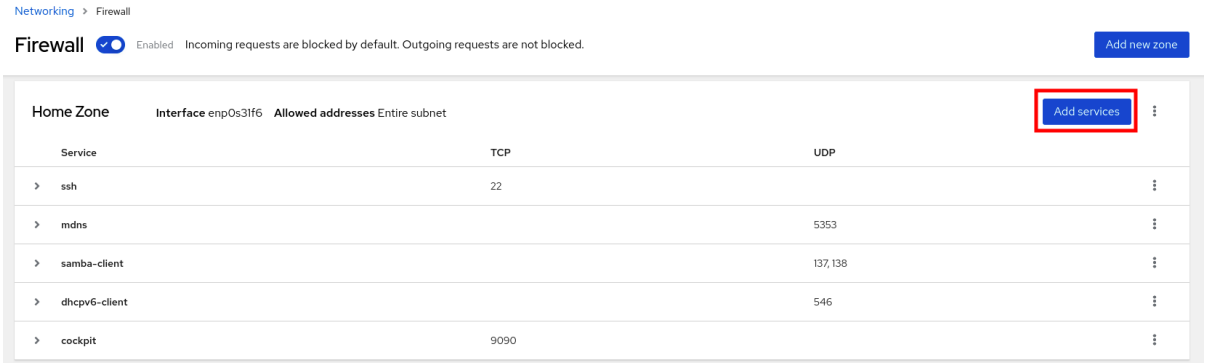
Procédure

1. Connectez-vous à la console web RHEL avec des privilèges d'administrateur. Pour plus d'informations, voir Connexion à la console web .
2. Cliquez sur **Networking**.
3. Cliquez sur le bouton **Modifier les règles et les zones**.



Si vous ne voyez pas le bouton **Modifier les règles et les zones**, connectez-vous à la console web avec les privilèges administratifs.

4. Dans la section **Firewall**, sélectionnez une zone pour laquelle vous souhaitez configurer un port personnalisé et cliquez sur **Add Services**.



5. Dans la boîte de dialogue **Add services**, cliquez sur le bouton radio **Ports personnalisés**.

6. Dans les champs TCP et UDP, ajoutez les ports selon les exemples. Vous pouvez ajouter des ports dans les formats suivants :

   - Numéros de port tels que 22
   - Plage de numéros de port, par exemple 5900-5910
   - Alias tels que nfs, rsync

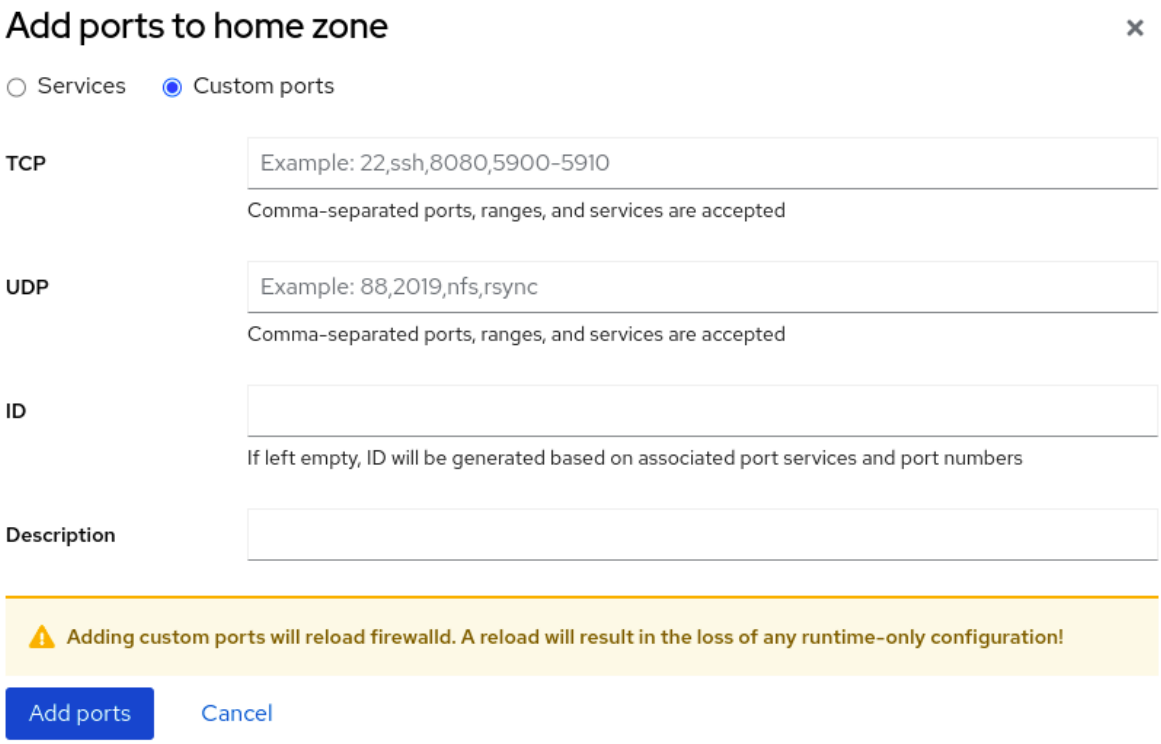
NOTE

Vous pouvez ajouter plusieurs valeurs dans chaque champ. Les valeurs doivent être séparées par une virgule et sans espace, par exemple : 8080,8081,http

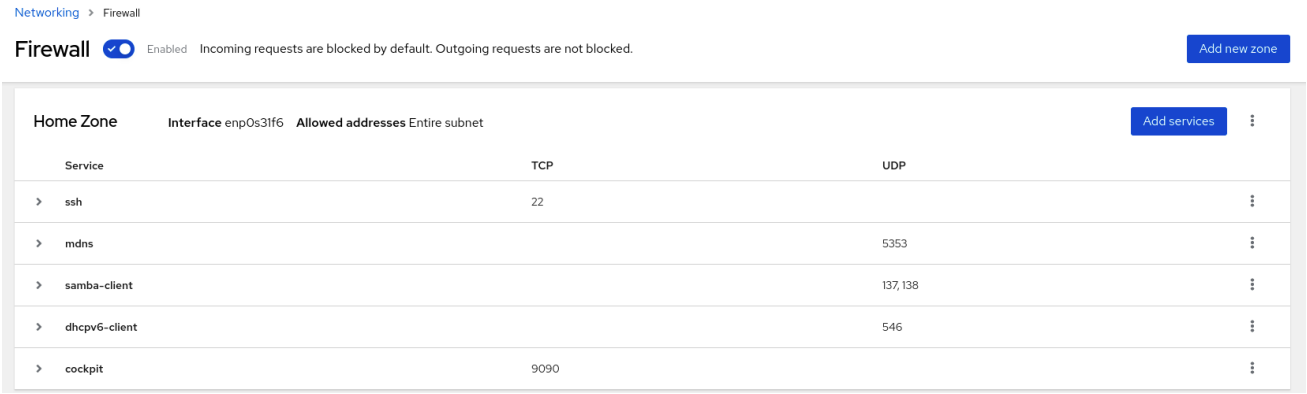
7. Après avoir ajouté le numéro de port dans le fichier **TCP**, le fichier **UDP** ou les deux, vérifiez le nom du service dans le champ **Name**.
   Le champ **Name** affiche le nom du service pour lequel ce port est réservé. Vous pouvez réécrire le nom si vous êtes sûr que ce port est libre d'utilisation et qu'aucun serveur n'a besoin de communiquer sur ce port.

8. Dans le champ **Name**, ajoutez un nom pour le service, y compris les ports définis.

9. Cliquez sur le bouton **Ajouter des ports**.



Pour vérifier les paramètres, allez sur la page **Firewall** et trouvez le service dans la liste des zones **Services**.



13.8. DÉSACTIVATION DE ZONES À L'AIDE DE LA CONSOLE WEB

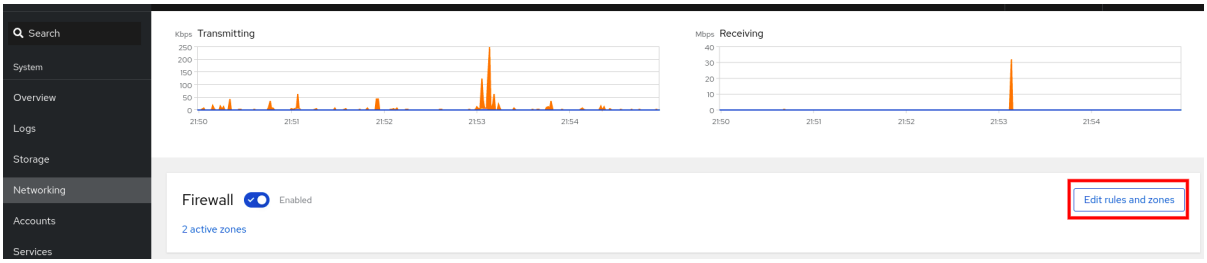
Cette section décrit comment désactiver une zone de pare-feu dans votre configuration de pare-feu à l'aide de la console web.

Conditions préalables

- La console web RHEL 9 a été installée. Pour plus de détails, voir Installation de la console web .

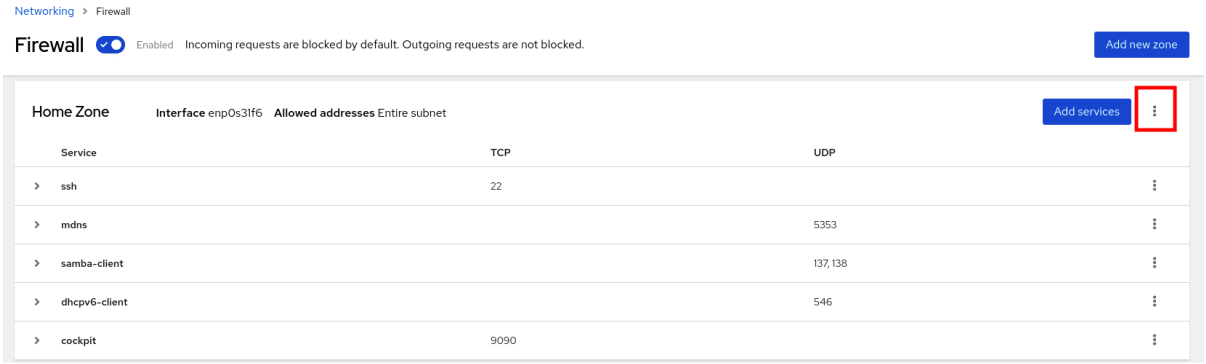
Procédure

1. Connectez-vous à la console web RHEL avec des privilèges d'administrateur. Pour plus d'informations, voir Connexion à la console web .
2. Cliquez sur **Networking**.
3. Cliquez sur le bouton **Modifier les règles et les zones**.



Si vous ne voyez pas le bouton **Modifier les règles et les zones**, connectez-vous à la console web avec les privilèges d'administrateur.

4. Cliquez sur l'icône **Options** dans la zone que vous souhaitez supprimer.



5. Cliquez sur **Delete**.

La zone est maintenant désactivée et l'interface n'inclut pas les services et ports ouverts qui ont été configurés dans la zone.

CHAPITRE 14. MISE EN PLACE DE POLITIQUES CRYPTOGRAPHIQUES À L'ÉCHELLE DU SYSTÈME DANS LA CONSOLE WEB

Vous pouvez choisir parmi des niveaux de politique cryptographique prédéfinis pour l'ensemble du système et passer de l'un à l'autre directement dans l'interface de la console web de Red Hat Enterprise Linux. Si vous définissez une politique personnalisée sur votre système, la console Web affiche la politique sur la page **Overview** ainsi que dans la fenêtre de dialogue **Change crypto policy**.

Conditions préalables

- La console web RHEL 9 a été installée. Pour plus de détails, voir Installation et activation de la console web.
- Vous disposez de privilèges d'administrateur.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Dans la carte **Configuration** de la page **Overview**, cliquez sur la valeur actuelle de votre police d'assurance à côté de **Crypto policy**.
3. Dans la fenêtre de dialogue **Change crypto policy**, cliquez sur le niveau de politique que vous souhaitez commencer à utiliser.
4. Cliquez sur le bouton **Appliquer et redémarrer**.

Vérification

- Connectez-vous à nouveau et vérifiez que la valeur de **Crypto policy** correspond à celle que vous avez sélectionnée.

CHAPITRE 15. APPLIQUER UN PLAYBOOK ANSIBLE GÉNÉRÉ

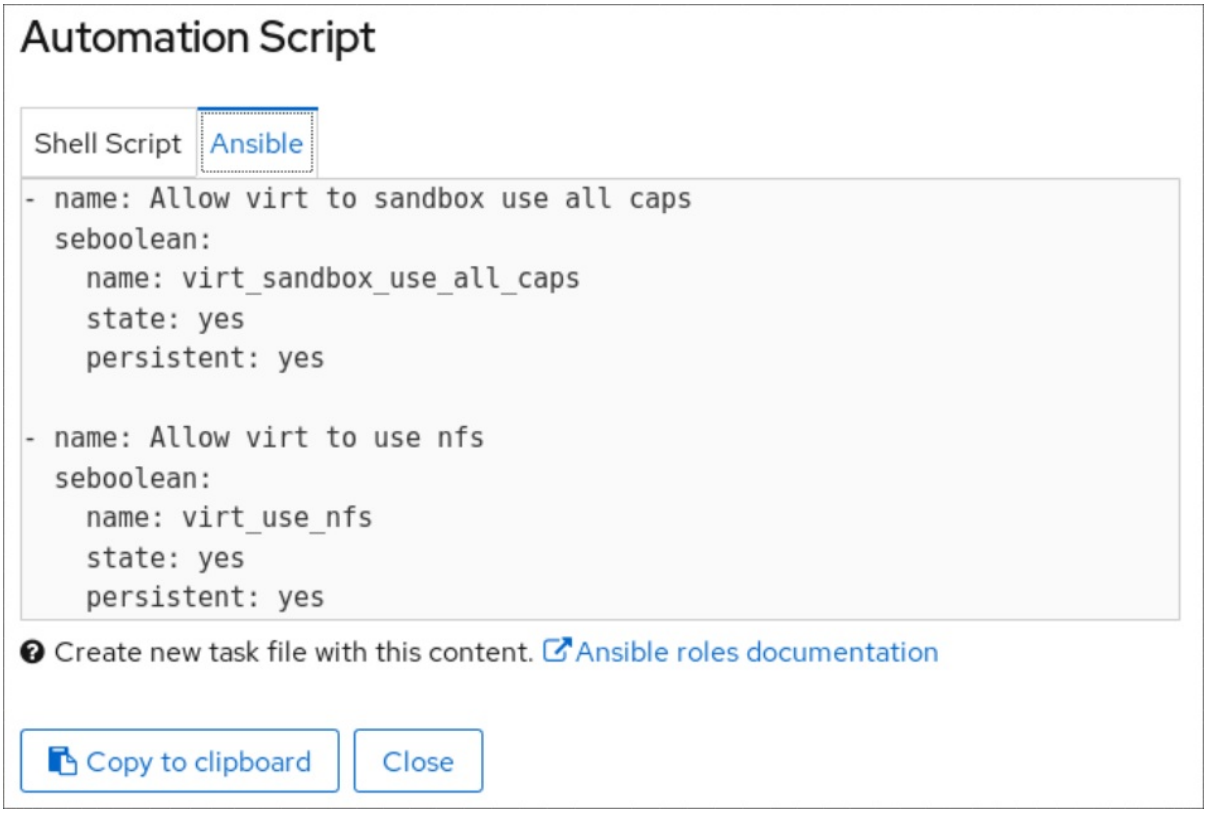
Lors de la résolution de problèmes avec SELinux, la console web est capable de générer un script shell ou un playbook Ansible que vous pouvez ensuite exporter et appliquer à d'autres machines.

Conditions préalables

- L'interface de la console web doit être installée et accessible.
  Pour plus de détails, voir Installation de la console web.

Procédure

1. Cliquez sur **SELinux**.
2. Cliquez sur "Voir le script d'automatisation" en haut à droite.
   Une fenêtre avec le script généré s'ouvre. Vous pouvez naviguer entre un script shell et un onglet d'options de génération de playbook Ansible.



3. Cliquez sur le bouton **Copier dans le presse-papiers** pour sélectionner le script ou le manuel de jeu et l'appliquer.

Vous disposez ainsi d'un script d'automatisation que vous pouvez appliquer à d'autres machines.

Ressources supplémentaires

- Résolution des problèmes liés à SELinux
- Déployer la même configuration SELinux sur plusieurs systèmes
- Pour plus de détails sur la commande **ansible-playbook**, voir la page de manuel **ansible-playbook(1)**.

CHAPITRE 16. GESTION DES PARTITIONS À L'AIDE DE LA CONSOLE WEB

Apprenez à gérer les systèmes de fichiers sur RHEL 9 à l'aide de la console Web.

Pour plus d'informations sur les systèmes de fichiers disponibles, voir la section Vue d'ensemble des systèmes de fichiers disponibles.

16.1. AFFICHAGE DES PARTITIONS FORMATÉES AVEC DES SYSTÈMES DE FICHIERS DANS LA CONSOLE WEB

La section **Storage** de la console web affiche tous les systèmes de fichiers disponibles dans la table **Filesystems**.

Cette section vous permet d'accéder à la liste des partitions formatées avec des systèmes de fichiers affichés dans la console web.

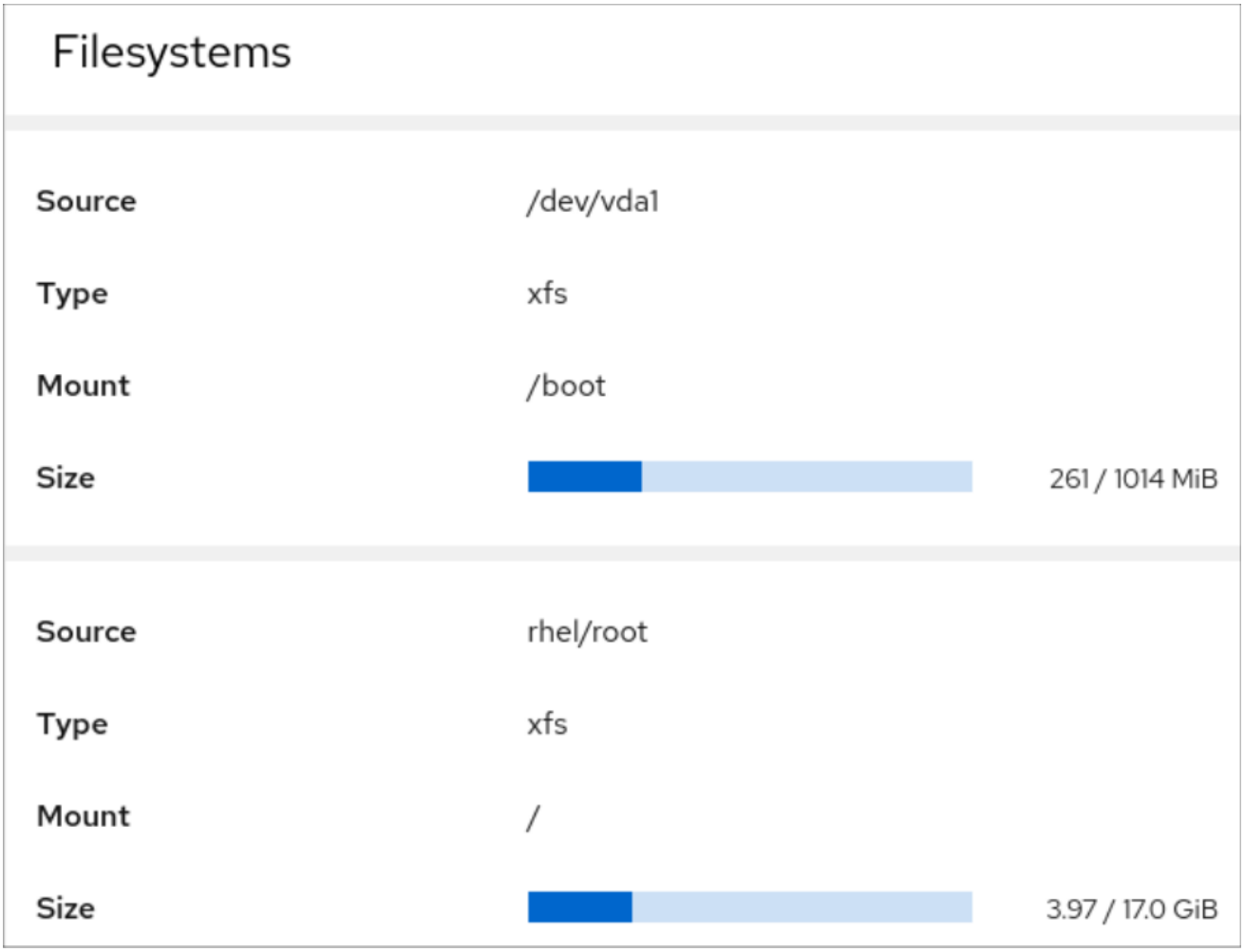
Conditions préalables

- Le paquetage **cockpit-storaged** est installé sur votre système.
- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL 9. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur l'onglet **Storage**.

Dans la table **Filesystems**, vous pouvez voir toutes les partitions disponibles formatées avec des systèmes de fichiers, leur nom, leur taille et l'espace disponible sur chaque partition.



16.2. CRÉATION DE PARTITIONS DANS LA CONSOLE WEB

Pour créer une nouvelle partition :

- Utiliser une table de partition existante
- Créer une partition

Conditions préalables

- Le paquetage **cockpit-storaged** est installé sur votre système.
- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.
- Un volume non formaté connecté au système, visible dans la table **Other Devices** de l'onglet **Storage**.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur l'onglet **Storage**.
3. Dans la table **Other Devices**, cliquez sur un volume dans lequel vous souhaitez créer la partition.

4. Dans la section **Content**, cliquez sur le bouton **Créer une partition**.
5. Dans la boîte de dialogue **Create partition**, sélectionnez la taille de la nouvelle partition.
6. Dans le menu déroulant **Erase**, sélectionnez :
   - **Don't overwrite existing data** - la console web RHEL ne réécrit que l'en-tête du disque. L'avantage de cette option est la rapidité du formatage.
   - **Overwrite existing data with zeros** - la console web RHEL réécrit tout le disque avec des zéros. Cette option est plus lente car le programme doit parcourir l'ensemble du disque, mais elle est plus sûre. Utilisez cette option si le disque contient des données et que vous devez les écraser.
7. Dans le menu déroulant **Type**, sélectionnez un système de fichiers :
   - **XFS** prend en charge les grands volumes logiques, le changement de disques physiques en ligne sans interruption de service et l'extension d'un système de fichiers existant. Laissez ce système de fichiers sélectionné si vous n'avez pas d'autre préférence.
   - **ext4** est pris en charge par le système de fichiers :
     - Volumes logiques
     - Commutation des lecteurs physiques en ligne sans interruption de service
     - Développement d'un système de fichiers
     - Réduction d'un système de fichiers

   Une option supplémentaire consiste à activer le chiffrement de la partition par LUKS (Linux Unified Key Setup), qui permet de chiffrer le volume à l'aide d'une phrase d'authentification.
8. Dans le champ **Name**, entrez le nom du volume logique.
9. Dans le menu déroulant **Mounting**, sélectionnez **Custom**.
   L'option **Default** ne garantit pas que le système de fichiers sera monté au prochain démarrage.
10. Dans le champ **Mount Point**, ajoutez le chemin de montage.
11. Sélectionnez **Mount at boot**.
12. Cliquez sur le bouton **Créer une partition**.
    Le formatage peut prendre plusieurs minutes en fonction de la taille du volume et des options de formatage sélectionnées.

    Une fois le formatage terminé, vous pouvez voir les détails du volume logique formaté dans l'onglet **Filesystem**.

Verification steps

- Pour vérifier que la partition a été ajoutée avec succès, passez à l'onglet **Storage** et vérifiez la table **Filesystems**.

16.3. SUPPRESSION DE PARTITIONS DANS LA CONSOLE WEB

La procédure suivante vous apprend à supprimer des partitions dans l'interface de la console web.

Conditions préalables

- Le paquetage **cockpit-storaged** est installé sur votre système.
- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.
- Démonter le système de fichiers de la partition.
  Pour plus d'informations sur le montage et le démontage des partitions, voir Montage et démontage des systèmes de fichiers dans la console web

Procédure

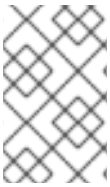
1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur l'onglet **Storage**.
3. Dans la table **Filesystems**, sélectionnez un volume dans lequel vous souhaitez supprimer la partition.
4. Dans la section **Content**, cliquez sur la partition que vous souhaitez supprimer.
5. La partition se déroule et vous pouvez cliquer sur le bouton **Supprimer**.
   La partition ne doit pas être montée ni utilisée.

Verification steps

- Pour vérifier que la partition a été supprimée avec succès, passez à l'onglet **Storage** et vérifiez la table **Content**.

16.4. MONTAGE ET DÉMONTAGE DE SYSTÈMES DE FICHIERS DANS LA CONSOLE WEB

Pour pouvoir utiliser les partitions sur les systèmes RHEL, vous devez monter un système de fichiers sur la partition en tant que périphérique.



NOTE

Vous pouvez également démonter un système de fichiers et le système RHEL cessera de l'utiliser. Le démontage du système de fichiers vous permet de supprimer, d'enlever ou de reformater des périphériques.

Conditions préalables

- Le paquetage **cockpit-storaged** est installé sur votre système.
- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.
- Si vous souhaitez démonter un système de fichiers, assurez-vous que le système n'utilise aucun fichier, service ou application stocké dans la partition.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur l'onglet **Storage**.
3. Dans la table **Filesystems**, sélectionnez un volume dans lequel vous souhaitez supprimer la partition.
4. Dans la section **Content**, cliquez sur la partition dont vous souhaitez monter ou démonter le système de fichiers.
5. Cliquez sur le bouton **Monter** ou **Démonter**.
   À ce stade, le système de fichiers a été monté ou démonté en fonction de votre action.

CHAPITRE 17. GESTION DES MONTAGES NFS DANS LA CONSOLE WEB

La console web RHEL 9 vous permet de monter des répertoires distants à l'aide du protocole NFS (Network File System).

NFS permet d'atteindre et de monter des répertoires distants situés sur le réseau et de travailler avec les fichiers comme si le répertoire était situé sur votre disque physique.

Conditions préalables

- La console web RHEL 9 a été installée.
  Pour plus de détails, voir Installation de la console web.
- Le paquetage **cockpit-storaged** est installé sur votre système.
- Nom ou adresse IP du serveur NFS.
- Chemin d'accès au répertoire sur le serveur distant.

17.1. CONNEXION DES MONTAGES NFS DANS LA CONSOLE WEB

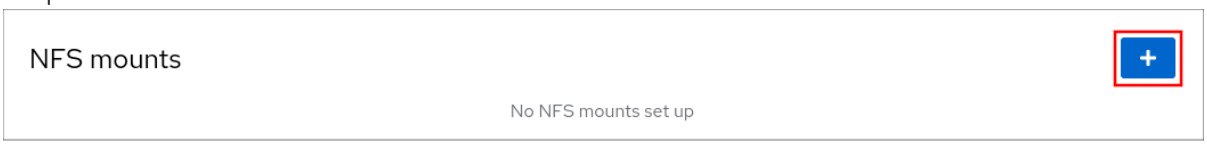
Connectez un répertoire distant à votre système de fichiers à l'aide de NFS.

Conditions préalables

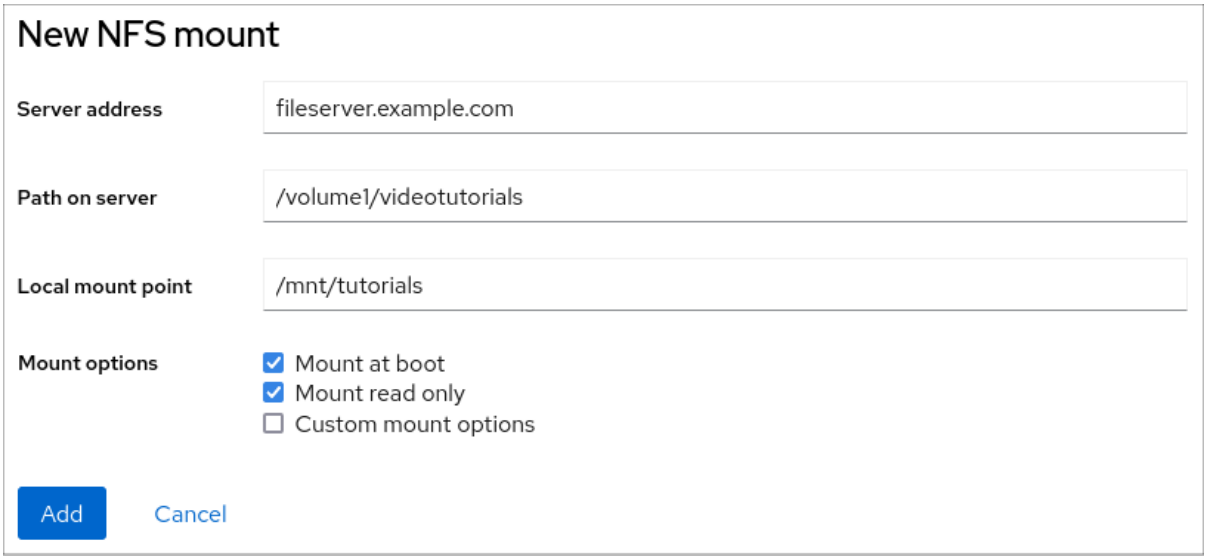
- Nom ou adresse IP du serveur NFS.
- Chemin d'accès au répertoire sur le serveur distant.

Procédure

1. Connectez-vous à la console web RHEL 9. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur **Storage**.
3. Cliquez sur dans la section **NFS mounts**.



4. Dans la boîte de dialogue **New NFS Mount**, entrez le serveur ou l'adresse IP du serveur distant.
5. Dans le champ **Path on Server**, entrez le chemin d'accès au répertoire que vous souhaitez monter.
6. Dans le champ **Local Mount Point**, entrez le chemin d'accès au répertoire dans votre système local.
7. Sélectionnez **Mount at boot**. Cela garantit que le répertoire sera accessible même après le redémarrage du système local.
8. Si vous ne souhaitez pas modifier le contenu, vous pouvez sélectionner **Mount read only**.



9. Cliquez sur **Add**.

Verification steps

- Ouvrez le répertoire monté et vérifiez que le contenu est accessible.

Pour dépanner la connexion, vous pouvez l'ajuster à l'aide des options de montage personnalisées .

17.2. PERSONNALISATION DES OPTIONS DE MONTAGE NFS DANS LA CONSOLE WEB

Modifier un montage NFS existant et ajouter des options de montage personnalisées.

Les options de montage personnalisées peuvent vous aider à dépanner la connexion ou à modifier les paramètres du montage NFS, par exemple en changeant les délais d'attente ou en configurant l'authentification.

Conditions préalables

- Ajout d'un montage NFS.

Procédure

1. Connectez-vous à la console web RHEL 9. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur **Storage**.
3. Cliquez sur le montage NFS que vous souhaitez ajuster.
4. Si le répertoire distant est monté, cliquez sur **Unmount**.
   Le répertoire ne doit pas être monté lors de la configuration des options de montage personnalisées. Dans le cas contraire, la console web n'enregistre pas la configuration, ce qui provoque une erreur.

1. Cliquez sur **Edit**.

1. Dans la boîte de dialogue **NFS Mount**, sélectionnez **Custom mount option**.

2. Saisissez les options de montage en les séparant par une virgule. Par exemple :
    - **nfsvers=4**- le numéro de version du protocole NFS
    - **soft**- le type de récupération après l'expiration d'une requête NFS
    - **sec=krb5**- sur le serveur NFS peuvent être sécurisés par l'authentification Kerberos. Le client et le serveur NFS doivent tous deux prendre en charge l'authentification Kerberos.

Pour obtenir une liste complète des options de montage NFS, entrez **man nfs** dans la ligne de commande.

1. Cliquez sur **Apply**.
2. Cliquez sur **Mount**.

Verification steps

- Ouvrez le répertoire monté et vérifiez que le contenu est accessible.

CHAPITRE 18. GESTION DES BAIES REDONDANTES DE DISQUES INDÉPENDANTS DANS LA CONSOLE WEB

Le système RAID (Redundant Arrays of Independent Disks) est un moyen d'organiser plusieurs disques en une seule unité de stockage. Le RAID protège les données stockées sur les disques contre les défaillances de ces derniers.

Le RAID utilise les stratégies de distribution des données suivantes :

- Miroir - les données sont copiées à deux endroits différents. Si un disque tombe en panne, vous disposez d'une copie et vos données ne sont pas perdues.
- Striping - les données sont réparties uniformément entre les disques.

Le niveau de protection dépend du niveau RAID.

La console web RHEL prend en charge les niveaux RAID suivants :

- RAID 0 (Stripe)
- RAID 1 (miroir)
- RAID 4 (parité dédiée)
- RAID 5 (parité distribuée)
- RAID 6 (Double Parité Distribuée)
- RAID 10 (bande de miroirs)

Avant de pouvoir utiliser des disques dans un RAID, vous devez.. :

- Créer un RAID.
- Le formater avec le système de fichiers.
- Montez le RAID sur le serveur.

Conditions préalables

- La console web RHEL 9 est installée et accessible. Pour plus de détails, voir Installation de la console web.
- Le paquetage **cockpit-storaged** est installé sur votre système.

18.1. CRÉATION D'UN RAID DANS LA CONSOLE WEB

Configurez le RAID dans la console web RHEL 9.

Conditions préalables

- Disques physiques connectés au système. Chaque niveau RAID nécessite un nombre différent de disques.

Procédure

1. Ouvrez la console web RHEL 9.
2. Cliquez sur **Storage**.
3. Cliquez sur l'icône de menu dans le tableau **Devices**.
4. Cliquez sur **Create RAID device**.
5. Dans la boîte de dialogue **Create RAID Device**, saisissez un nom pour le nouveau RAID.
6. Dans la liste déroulante **RAID Level**, sélectionnez le niveau de RAID que vous souhaitez utiliser.
7. Dans la liste déroulante **Chunk Size**, laissez la valeur prédéfinie telle quelle.
   La valeur **Chunk Size** indique la taille de chaque bloc pour l'écriture des données. Si la taille du bloc est de 512 KiB, le système écrit les premiers 512 KiB sur le premier disque, les deuxièmes 512 KiB sont écrits sur le deuxième disque et les troisièmes blocs sont écrits sur le troisième disque. Si vous avez trois disques dans votre RAID, le quatrième bloc de 512 KiB sera à nouveau écrit sur le premier disque.
8. Sélectionnez les disques que vous souhaitez utiliser pour le RAID.
9. Cliquez sur **Create**.

Verification steps

- Allez dans la section **Storage** et vérifiez que vous pouvez voir le nouveau RAID dans la boîte **RAID devices** et formatez-le.

Vous avez les options suivantes pour formater et monter le nouveau RAID dans la console web :

Formatage du RAID

Création de partitions sur la table de partition

Création d'un groupe de volumes au-dessus du RAID

18.2. FORMATAGE DU RAID DANS LA CONSOLE WEB

Formatez le nouveau périphérique RAID logiciel créé dans l'interface Web de RHEL 9.

Conditions préalables

- Les disques physiques sont connectés et visibles par RHEL 9.
- Le RAID est créé.
- Considérez le système de fichiers qui sera utilisé pour le RAID.
- Envisager la création d'une table de partitionnement.

Procédure

1. Ouvrez la console web RHEL 9.
2. Cliquez sur **Storage**.

3. Dans la boîte **RAID devices**, choisissez le RAID que vous souhaitez formater en cliquant dessus.
4. Dans l'écran des détails du RAID, descendez jusqu'à la partie **Content**.
5. Cliquez sur le RAID nouvellement créé.
6. Cliquez sur le bouton **Format**.
7. Dans la liste déroulante **Erase**, sélectionnez :
   - **Don't overwrite existing data** – la console web RHEL ne réécrit que l'en-tête du disque. L'avantage de cette option est la rapidité du formatage.
   - **Overwrite existing data with zeros** – la console web RHEL réécrit tout le disque avec des zéros. Cette option est plus lente car le programme doit parcourir l'ensemble du disque. Utilisez cette option si le RAID contient des données et que vous devez les réécrire.
8. Dans la liste déroulante **Type**, sélectionnez un système de fichiers XFS, si vous n'avez pas d'autre préférence.
9. Saisissez le nom du système de fichiers.
10. Dans la liste déroulante **Mounting**, sélectionnez **Custom**.
    L'option **Default** ne garantit pas que le système de fichiers sera monté au prochain démarrage.
11. Dans le champ **Mount Point**, ajoutez le chemin de montage.
12. Sélectionnez **Mount at boot**.
13. Cliquez sur le bouton **Format**.
    Le formatage peut prendre plusieurs minutes en fonction des options de formatage utilisées et de la taille du RAID.

    Après avoir terminé avec succès, vous pouvez voir les détails du RAID formaté dans l'onglet **Filesystem**.
14. Pour utiliser le RAID, cliquez sur **Mount**.

À ce stade, le système utilise le RAID monté et formaté.

18.3. CRÉATION D'UNE TABLE DE PARTITION SUR UN RAID À L'AIDE DE LA CONSOLE WEB

Formatez le RAID avec la table de partition sur le nouveau périphérique RAID logiciel créé dans l'interface RHEL 9.

Le RAID nécessite un formatage comme tout autre périphérique de stockage. Deux options s'offrent à vous :

- Formater le périphérique RAID sans partitions
- Créer une table de partition avec des partitions

Conditions préalables

- Les disques physiques sont connectés et visibles par .

- Le RAID est créé.
- Considérez le système de fichiers utilisé pour le RAID.
- Envisagez de créer une table de partitionnement.

Procédure

1. Ouvrez la console RHEL 9.
2. Cliquez sur **Storage**.
3. Dans la boîte **RAID devices**, sélectionnez le RAID que vous souhaitez modifier.
4. Dans l'écran des détails du RAID, descendez jusqu'à la partie **Content**.
5. Cliquez sur le RAID nouvellement créé.
6. Cliquez sur le bouton **Créer une table de partition**.
7. Dans la liste déroulante **Erase**, sélectionnez :
   - **Don't overwrite existing data** – la console web RHEL ne réécrit que l'en-tête du disque. L'avantage de cette option est la rapidité du formatage.
   - **Overwrite existing data with zeros** – la console web RHEL réécrit tout le RAID avec des zéros. Cette option est plus lente car le programme doit parcourir l'ensemble du RAID. Utilisez cette option si le RAID contient des données et que vous devez les réécrire.
8. Dans la liste déroulante **Partitioning**, sélectionnez :
   - Compatible avec les systèmes et les disques durs modernes > 2TB (GPT) - GUID Partition Table est un système de partitionnement moderne recommandé pour les RAID de grande taille comportant plus de quatre partitions.
   - Compatible avec tous les systèmes et appareils (MBR) - Le Master Boot Record fonctionne avec des disques d'une taille maximale de 2 To. Le MBR prend également en charge quatre partitions primaires au maximum.
9. Cliquez sur **Format**.

À ce stade, la table de partitionnement a été créée et vous pouvez créer des partitions.

Pour créer des partitions, voir Création de partitions sur le RAID à l'aide de la console Web .

18.4. CRÉATION DE PARTITIONS SUR UN RAID À L'AIDE DE LA CONSOLE WEB

Créez une partition dans la table de partition existante.

Conditions préalables

- La table de partition est créée. Pour plus d'informations, voir Création d'une table de partitions sur un RAID à l'aide de la console web

Procédure

1. Ouvrez la console web RHEL 9.
2. Cliquez sur **Storage**.
3. Dans la boîte **RAID devices**, cliquez sur le RAID que vous souhaitez modifier.
4. Dans l'écran des détails du RAID, descendez jusqu'à la partie **Content**.
5. Cliquez sur le RAID nouvellement créé.
6. Cliquez sur **Create Partition**.
7. Dans la boîte de dialogue **Create partition**, définissez la taille de la première partition.
8. Dans la liste déroulante **Erase**, sélectionnez :
   - **Don't overwrite existing data** – la console web RHEL ne réécrit que l'en-tête du disque. L'avantage de cette option est la rapidité du formatage.
   - **Overwrite existing data with zeros** – la console web RHEL réécrit tout le RAID avec des zéros. Cette option est plus lente car le programme doit parcourir l'ensemble du RAID. Utilisez cette option si le RAID contient des données et que vous devez les réécrire.
9. Dans la liste déroulante **Type**, sélectionnez un système de fichiers XFS, si vous n'avez pas d'autre préférence.
10. Saisissez un nom quelconque pour le système de fichiers. N'utilisez pas d'espaces dans le nom.
11. Dans la liste déroulante **Mounting**, sélectionnez **Custom**.
    L'option **Default** ne garantit pas que le système de fichiers sera monté au prochain démarrage.
12. Dans le champ **Mount Point**, ajoutez le chemin de montage.
13. Sélectionnez **Mount at boot**.
14. Cliquez sur **Create partition**.

Le formatage peut prendre plusieurs minutes en fonction des options de formatage utilisées et de la taille du RAID.

Après avoir terminé avec succès, vous pouvez continuer à créer d'autres partitions.

À ce stade, le système utilise un RAID monté et formaté.

18.5. CRÉATION D'UN GROUPE DE VOLUMES AU-DESSUS D'UN RAID À L'AIDE DE LA CONSOLE WEB

Construire un groupe de volumes à partir d'un RAID logiciel.

Conditions préalables

- Périphérique RAID, qui n'est pas formaté et monté.

Procédure

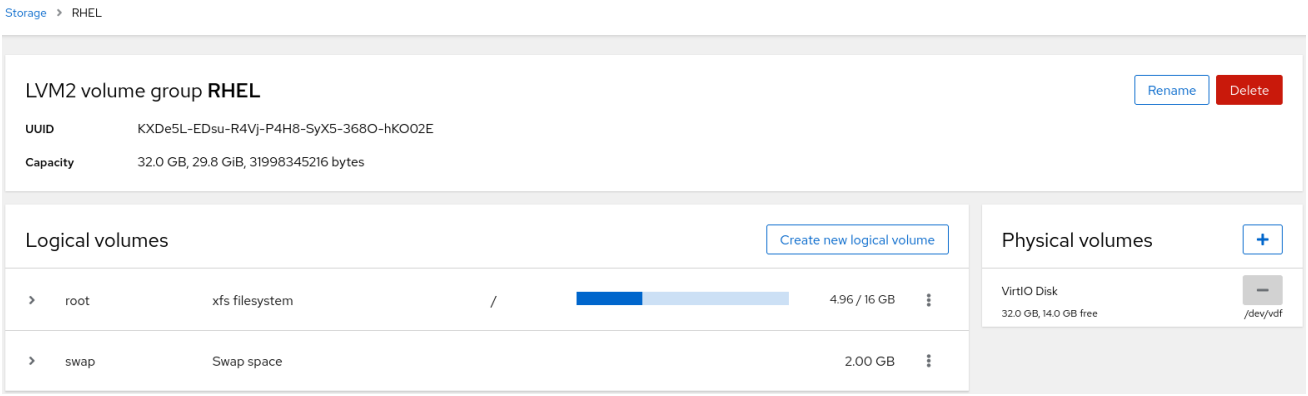
1. Ouvrez la console web RHEL 9.

2. Cliquez sur **Storage**.
3. Cliquez sur le bouton dans la boîte **Volume Groups**.
4. Dans la boîte de dialogue **Create Volume Group**, saisissez un nom pour le nouveau groupe de volumes.
5. Dans la liste **Disks**, sélectionnez un périphérique RAID.
   Si le RAID n'apparaît pas dans la liste, démontez-le du système. Le périphérique RAID ne doit pas être utilisé par le système RHEL 9.
6. Cliquez sur **Create**.

Le nouveau groupe de volumes a été créé et vous pouvez continuer à créer un volume logique.

CHAPITRE 19. CONFIGURATION DES VOLUMES LOGIQUES LVM À L'AIDE DE LA CONSOLE WEB

Red Hat Enterprise Linux 9 prend en charge le gestionnaire de volume logique LVM. Lorsque vous installez un Red Hat Enterprise Linux 9, il sera installé sur le LVM créé automatiquement lors de l'installation.



La capture d'écran montre la vue de la console web d'une installation propre d'un système RHEL 9 avec deux volumes logiques créés automatiquement pendant l'installation.

Pour en savoir plus sur les volumes logiques, suivez les sections décrites :

- Qu'est-ce que le gestionnaire de volume logique et quand l'utiliser ?
- Qu'est-ce qu'un groupe de volume et comment le créer ?
- Qu'est-ce qu'un volume logique et comment le créer ?
- Comment formater les volumes logiques ?
- Comment redimensionner les volumes logiques ?

Conditions préalables

- La console web RHEL 9 a été installée.
  Pour plus d'informations, voir Installation et activation de la console web .
- Le paquetage **cockpit-storaged** est installé sur votre système.
- Lecteurs physiques, périphériques RAID ou tout autre type de périphérique en mode bloc à partir duquel vous pouvez créer le volume logique.

19.1. LOGICAL VOLUME MANAGER DANS LA CONSOLE WEB

La console web RHEL 9 fournit une interface graphique permettant de créer des groupes de volumes LVM et des volumes logiques.

Les groupes de volumes créent une couche entre les volumes physiques et logiques. Ils permettent d'ajouter ou de supprimer des volumes physiques sans influencer le volume logique lui-même. Les groupes de volumes apparaissent comme un lecteur dont la capacité est constituée des capacités de tous les lecteurs physiques inclus dans le groupe.

Vous pouvez regrouper des lecteurs physiques en groupes de volumes dans la console web.

Les volumes logiques agissent comme un lecteur physique unique et sont construits au-dessus d'un groupe de volumes dans votre système.

Les principaux avantages des volumes logiques sont les suivants

- Meilleure flexibilité que le système de partitionnement utilisé sur votre disque physique.
- Possibilité de connecter plusieurs disques physiques dans un seul volume.
- Possibilité d'augmenter (croissance) ou de réduire (diminution) la capacité du volume en ligne, sans redémarrage.
- Possibilité de créer des instantanés.

Ressources supplémentaires

- Configuration et gestion des volumes logiques

19.2. CRÉATION DE GROUPES DE VOLUMES DANS LA CONSOLE WEB

Créer des groupes de volumes à partir d'un ou plusieurs lecteurs physiques ou d'autres périphériques de stockage.

Les volumes logiques sont créés à partir de groupes de volumes. Chaque groupe de volumes peut comprendre plusieurs volumes logiques.

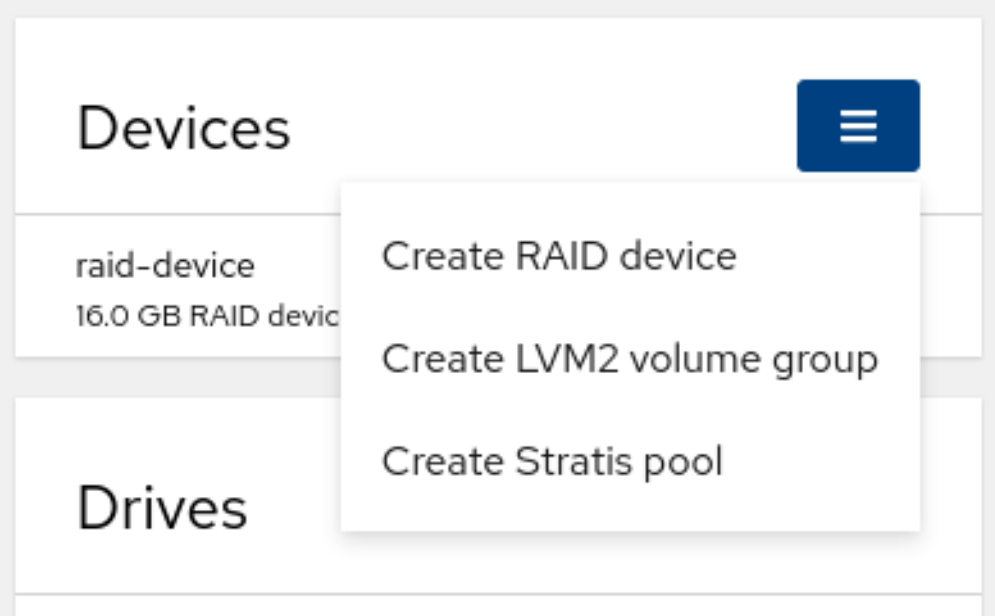
Pour plus d'informations, voir Gestion des groupes de volumes LVM .

Conditions préalables

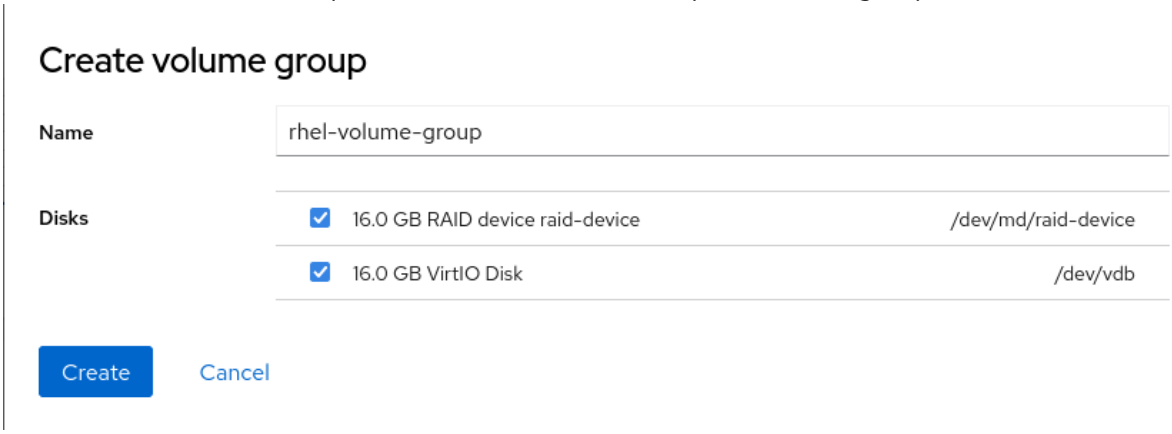
- Lecteurs physiques ou autres types de périphériques de stockage à partir desquels vous souhaitez créer des groupes de volumes.

Procédure

1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Stockage**.
3. Dans la section **Devices**, sélectionnez **Create LVM2 volume group** dans le menu déroulant.



4. Dans le champ **Name**, entrez un nom de groupe sans espace.
5. Sélectionnez les lecteurs que vous souhaitez combiner pour créer le groupe de volumes.

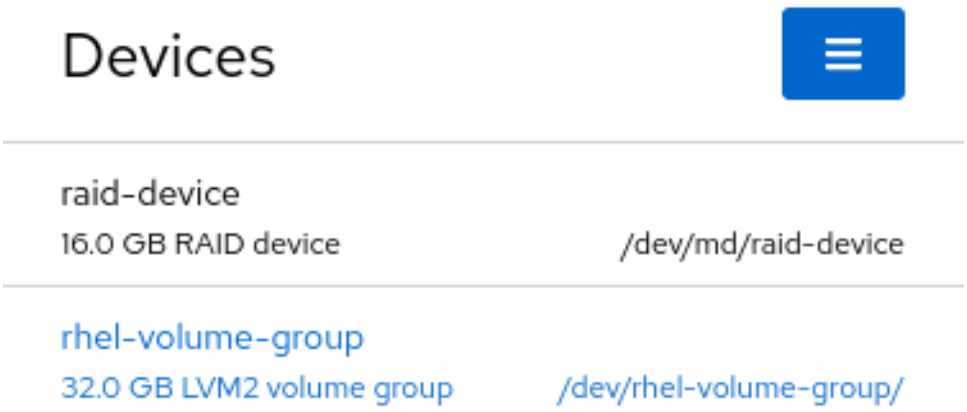


   Il peut arriver que vous ne puissiez pas voir les périphériques comme vous le souhaitez. La console web RHEL n'affiche que les périphériques de bloc inutilisés. Les périphériques utilisés sont, par exemple, les suivants

   - Appareils formatés avec un système de fichiers
   - Volumes physiques dans un autre groupe de volumes
   - Volumes physiques faisant partie d'un autre dispositif RAID logiciel
     Si vous ne voyez pas le périphérique, formatez-le pour qu'il soit vide et inutilisé.

6. Cliquez sur **Créer**.

La console Web ajoute le groupe de volumes dans la section **Devices**. Après avoir cliqué sur le groupe, vous pouvez créer des volumes logiques alloués à partir de ce groupe de volumes.



19.3. CRÉATION DE VOLUMES LOGIQUES DANS LA CONSOLE WEB

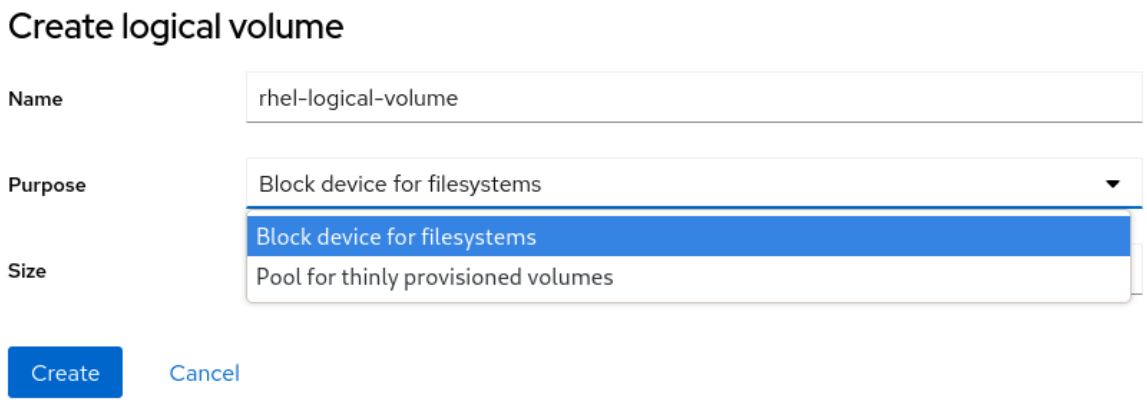
Les volumes logiques agissent comme des lecteurs physiques. Vous pouvez utiliser la console web RHEL 9 pour créer des volumes logiques LVM dans un groupe de volumes.

Conditions préalables

- Le paquetage **cockpit-storaged** est installé sur votre système.
- Groupe de volumes créé. Pour plus de détails, voir Création de groupes de volumes dans la console web.

Procédure

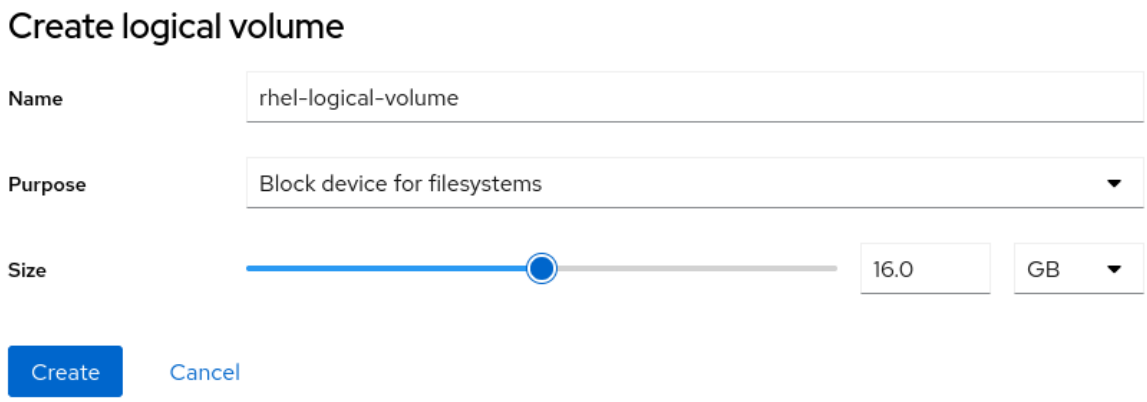
1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Stockage**.
3. Dans la section **Devices**, cliquez sur le groupe de volumes dans lequel vous souhaitez créer des volumes logiques.
4. Dans la section **Logical volumes**, cliquez sur **Créer un nouveau volume logique**.
5. Dans le champ **Name**, entrez un nom pour le nouveau volume logique sans espace.
6. Dans le menu déroulant **Purpose**, sélectionnez **Block device for filesystems**.
   Cette configuration permet de créer un volume logique dont la taille maximale est égale à la somme des capacités de tous les lecteurs inclus dans le groupe de volumes.



7. Définissez la taille du volume logique. Envisagez :

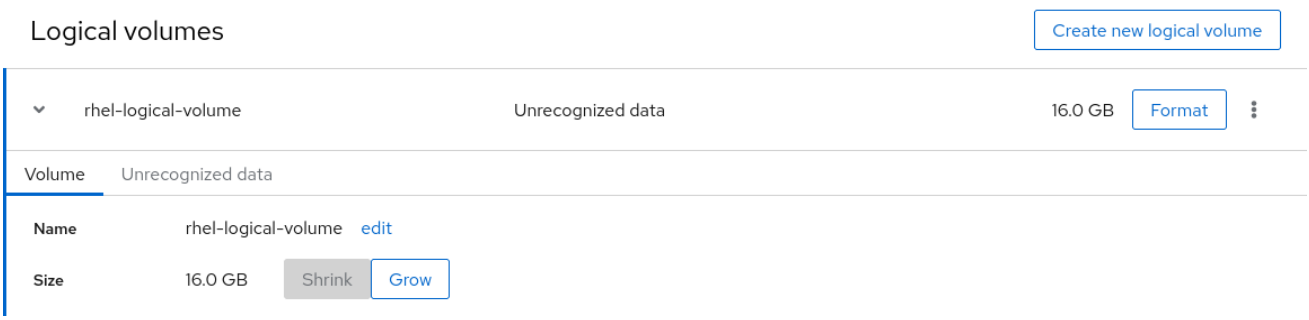
   - Espace dont le système utilisant ce volume logique aura besoin.
   - Nombre de volumes logiques à créer.

   Il n'est pas nécessaire d'utiliser tout l'espace. Si nécessaire, vous pouvez agrandir le volume logique ultérieurement.



8. Cliquez sur **Créer**.

Pour vérifier les paramètres, cliquez sur votre volume logique et vérifiez les détails.



À ce stade, le volume logique a été créé et vous devez créer et monter un système de fichiers avec le processus de formatage.

19.4. FORMATAGE DES VOLUMES LOGIQUES DANS LA CONSOLE WEB

Les volumes logiques se comportent comme des lecteurs physiques. Pour les utiliser, vous devez les formater avec un système de fichiers.

> **AVERTISSEMENT**
>
> Le formatage des volumes logiques efface toutes les données qu'ils contiennent.

Le système de fichiers que vous sélectionnez détermine les paramètres de configuration que vous pouvez utiliser pour les volumes logiques. Par exemple, certains systèmes de fichiers XFS ne prennent pas en charge la réduction des volumes. Pour plus d'informations, voir Redimensionnement des volumes logiques dans la console web.

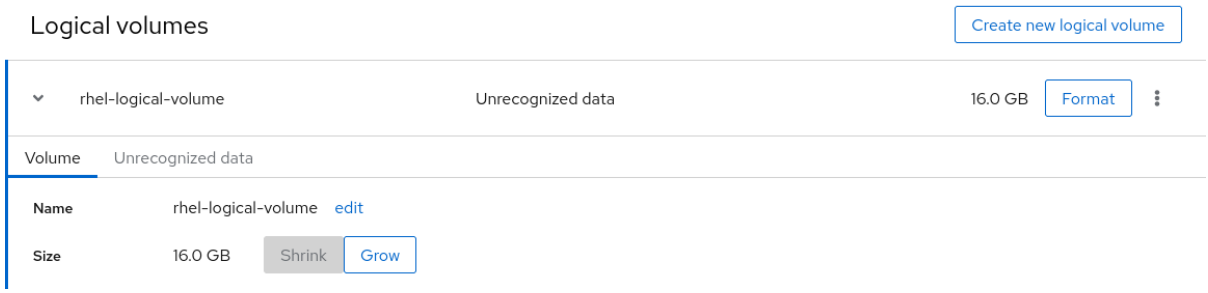
Les étapes suivantes décrivent la procédure de formatage des volumes logiques.

Conditions préalables

- Le paquetage **cockpit-storaged** est installé sur votre système.
- Volume logique créé. Pour plus de détails, voir Création de volumes logiques dans la console web.

Procédure

1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Stockage**.
3. Dans la section **Devices**, cliquez sur le groupe de volumes dans lequel le volume logique est placé.
4. Dans la section **Logical volumes**, cliquez sur **Format**.



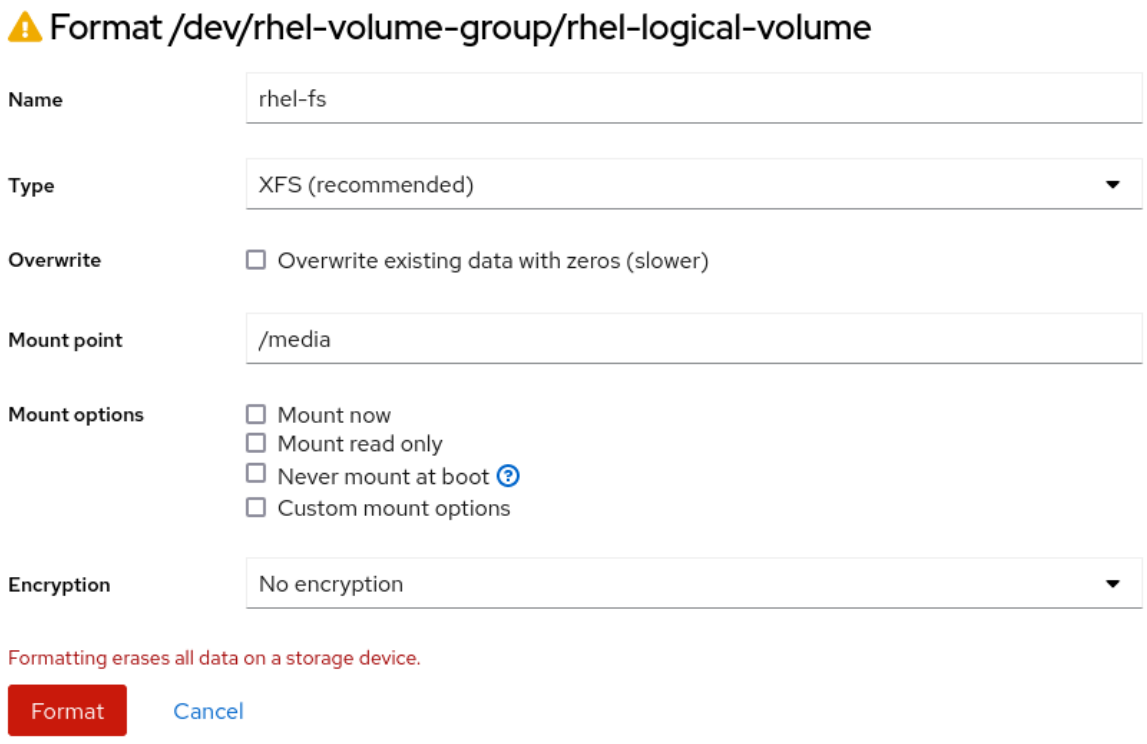
5. Dans le champ **Name**, entrez un nom pour le système de fichiers.
6. Dans le menu déroulant **Type**, sélectionnez un système de fichiers :
   - **XFS** prend en charge les grands volumes logiques, le changement de disques physiques en ligne sans interruption de service et l'extension d'un système de fichiers existant. Laissez ce système de fichiers sélectionné si vous n'avez pas d'autre préférence.

XFS ne permet pas de réduire la taille d'un volume formaté avec un système de fichiers XFS

- **ext4** est pris en charge par le système de fichiers :
  - Volumes logiques
  - Commutation des lecteurs physiques en ligne sans interruption de service
  - Développement d'un système de fichiers
  - Réduction d'un système de fichiers

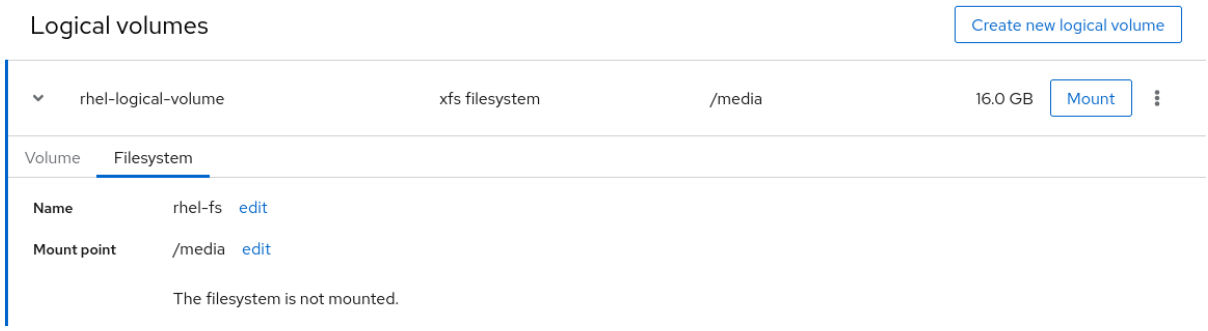
Vous pouvez également sélectionner une version avec le cryptage LUKS (Linux Unified Key Setup), qui vous permet de crypter le volume à l'aide d'une phrase de passe.

7. Sélectionnez l'option **Overwrite**:
   - **Don't overwrite existing data** – la console web RHEL ne réécrit que l'en-tête du disque. L'avantage de cette option est la rapidité du formatage.
   - **Overwrite existing data with zeros** – la console web RHEL réécrit tout le disque avec des zéros. Cette option est plus lente car le programme doit parcourir l'ensemble du disque. Utilisez cette option si le disque contient des données et que vous devez les écraser.
8. Dans le champ **Mount Point**, ajoutez le chemin de montage.



9. Cliquez sur **Format**.
   Le formatage peut prendre plusieurs minutes en fonction de la taille du volume et des options de formatage sélectionnées.

   Une fois le formatage terminé, vous pouvez voir les détails du volume logique formaté dans l'onglet **Filesystem**.



10. Pour utiliser le volume logique, cliquez sur **Monter**.

À ce stade, le système peut utiliser un volume logique monté et formaté.

19.5. REDIMENSIONNEMENT DES VOLUMES LOGIQUES DANS LA CONSOLE WEB

Découvrez comment étendre ou réduire les volumes logiques dans la console web RHEL 9.

La possibilité de redimensionner un volume logique dépend du système de fichiers utilisé. La plupart des systèmes de fichiers permettent d'étendre le volume en ligne (sans interruption de service).

Vous pouvez également réduire (diminuer) la taille des volumes logiques, si le volume logique contient un système de fichiers qui prend en charge la réduction. Cette fonction devrait être disponible, par exemple, dans les systèmes de fichiers ext3/ext4.

AVERTISSEMENT

Vous ne pouvez pas réduire les volumes qui contiennent des systèmes de fichiers GFS2 ou XFS.

Conditions préalables

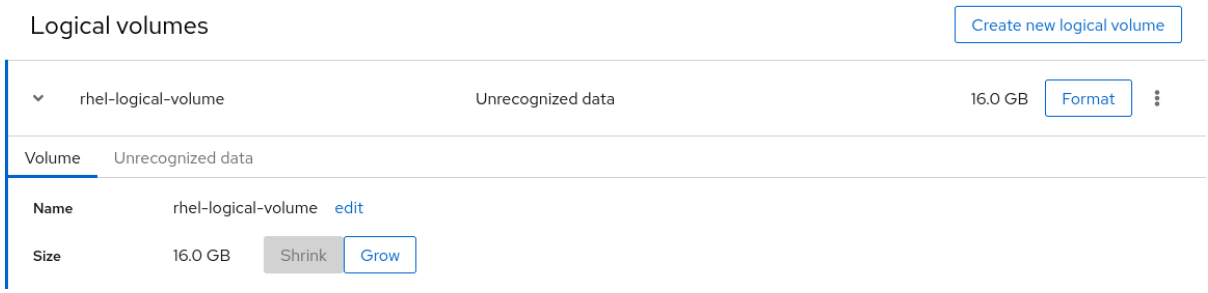
- Volume logique existant contenant un système de fichiers qui prend en charge le redimensionnement des volumes logiques.

Procédure

Les étapes suivantes décrivent la procédure à suivre pour augmenter un volume logique sans mettre le volume hors ligne :

1. Connectez-vous à la console web RHEL.
2. Cliquez sur **Stockage**.
3. Dans la section **Devices**, cliquez sur le groupe de volumes dans lequel le volume logique est placé.
4. Dans la section **Logical volumes**, cliquez sur le volume logique.

5. Dans l'onglet **Volume**, cliquez sur **Croître**.



6. Dans la boîte de dialogue **Grow logical volume**, réglez la taille du volume.

7. Cliquez sur " **Grow"**.

LVM augmente le volume logique sans interruption du système.

19.6. RESSOURCES SUPPLÉMENTAIRES

- Configuration et gestion des volumes logiques

CHAPITRE 20. CONFIGURATION DES VOLUMES LOGIQUES FINS À L'AIDE DE LA CONSOLE WEB

Les volumes logiques à faible provisionnement vous permettent d'allouer plus d'espace aux applications ou aux serveurs désignés que l'espace que les volumes logiques contiennent réellement.

Pour plus d'informations, voir Création de volumes snapshot à provisionnement fin .

Les sections suivantes décrivent :

- Création de pools pour les volumes logiques à provisionnement fin.
- Création de volumes logiques fins.
- Formatage de volumes logiques fins.

Conditions préalables

- La console web RHEL 9 a été installée.
  Pour plus de détails, voir Installation de la console web .
- Le paquetage **cockpit-storaged** est installé sur votre système.
- Lecteurs physiques ou autres types de périphériques de stockage à partir desquels vous souhaitez créer des groupes de volumes.

20.1. CRÉATION DE POOLS POUR LES VOLUMES LOGIQUES FINS DANS LA CONSOLE WEB

Créer un pool pour les volumes à provisionnement fin.

Conditions préalables

- Groupe de volume créé .

Procédure

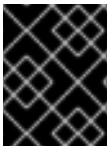
1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Storage**.
3. Cliquez sur le groupe de volumes dans lequel vous souhaitez créer des volumes restreints.
4. Cliquez sur **Create new Logical Volume**
5. Dans le champ **Name**, entrez un nom pour le nouveau pool de volumes légers sans espaces.
6. Dans le menu déroulant **Purpose**, sélectionnez **Pool for thin-provisioned volumes** Cette configuration vous permet de créer le thin volume.
7. Définir la taille du pool de volumes légers. Envisagez :
   - De combien de volumes fins aurez-vous besoin dans ce pool ?
   - Quelle est la taille prévue de chaque volume fin ?

Il n'est pas nécessaire d'utiliser tout l'espace. Si nécessaire, vous pouvez agrandir la piscine ultérieurement.

8. Cliquez sur **Create**.
   Le pool de volumes restreints a été créé et vous pouvez ajouter des volumes restreints.

20.2. CRÉATION DE VOLUMES LOGIQUES FINS DANS LA CONSOLE WEB

Créez un volume logique léger dans le pool. Le pool peut inclure plusieurs volumes logiques et chaque volume logique peut être aussi grand que le pool de volumes logiques lui-même.



IMPORTANT

L'utilisation de volumes fins nécessite une vérification régulière de l'espace physique libre du volume logique.

Conditions préalables

- Création d'un pool pour les volumes restreints.
  Pour plus de détails, voir Création de pools pour les volumes logiques fins dans la console Web .

Procédure

1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Storage**.
3. Cliquez sur le groupe de volumes dans lequel vous souhaitez créer des volumes restreints.
4. Cliquez sur la piscine souhaitée.
5. Cliquez sur **Create Thin Volume**.
6. Dans la boîte de dialogue **Create Thin Volume**, entrez un nom pour le volume fin sans espaces.
7. Définir la taille du volume fin.
8. Cliquez sur **Create**.

À ce stade, le volume logique fin a été créé et vous devez le formater.

20.3. FORMATAGE DES VOLUMES LOGIQUES DANS LA CONSOLE WEB

Les volumes logiques se comportent comme des lecteurs physiques. Pour les utiliser, vous devez les formater avec un système de fichiers.

AVERTISSEMENT

Le formatage des volumes logiques efface toutes les données qu'ils contiennent.

Le système de fichiers que vous sélectionnez détermine les paramètres de configuration que vous pouvez utiliser pour les volumes logiques. Par exemple, certains systèmes de fichiers XFS ne prennent pas en charge la réduction des volumes. Pour plus d'informations, voir Redimensionnement des volumes logiques dans la console web.

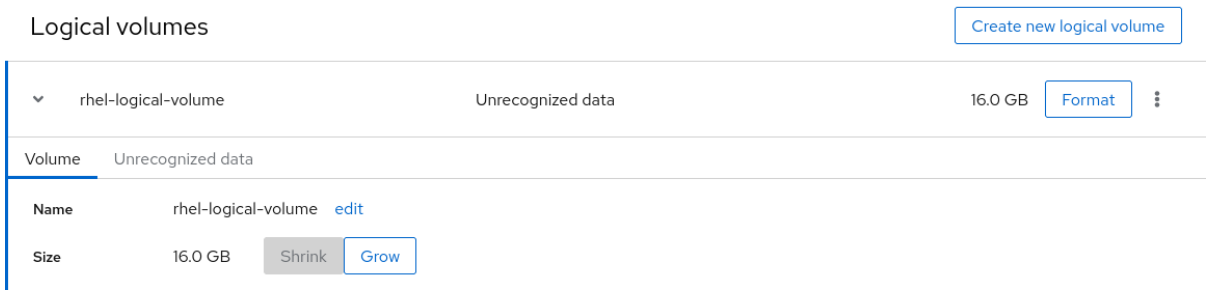
Les étapes suivantes décrivent la procédure de formatage des volumes logiques.

Conditions préalables

- Le paquetage **cockpit-storaged** est installé sur votre système.
- Volume logique créé. Pour plus de détails, voir Création de volumes logiques dans la console web.

Procédure

1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Stockage**.
3. Dans la section **Devices**, cliquez sur le groupe de volumes dans lequel le volume logique est placé.
4. Dans la section **Logical volumes**, cliquez sur **Format**.

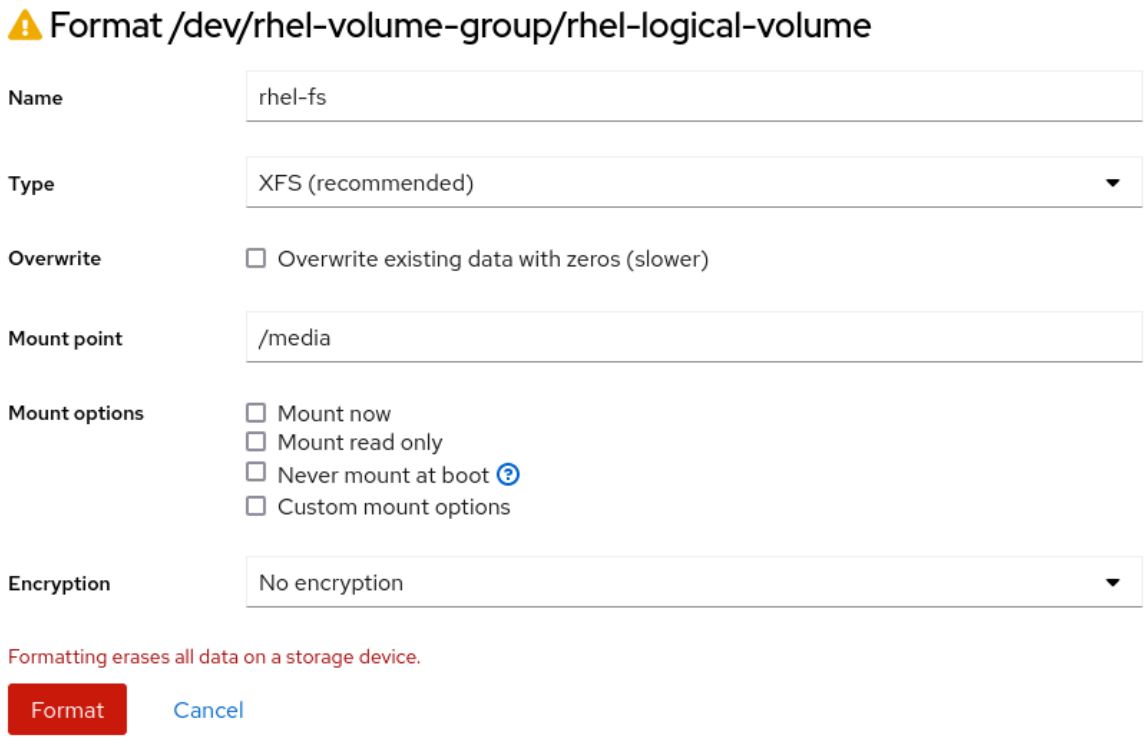


5. Dans le champ **Name**, entrez un nom pour le système de fichiers.
6. Dans le menu déroulant **Type**, sélectionnez un système de fichiers :
   - **XFS** prend en charge les grands volumes logiques, le changement de disques physiques en ligne sans interruption de service et l'extension d'un système de fichiers existant. Laissez ce système de fichiers sélectionné si vous n'avez pas d'autre préférence.
     XFS ne permet pas de réduire la taille d'un volume formaté avec un système de fichiers XFS
   - **ext4** est pris en charge par le système de fichiers :
     - Volumes logiques
     - Commutation des lecteurs physiques en ligne sans interruption de service

- Développement d'un système de fichiers
- Réduction d'un système de fichiers

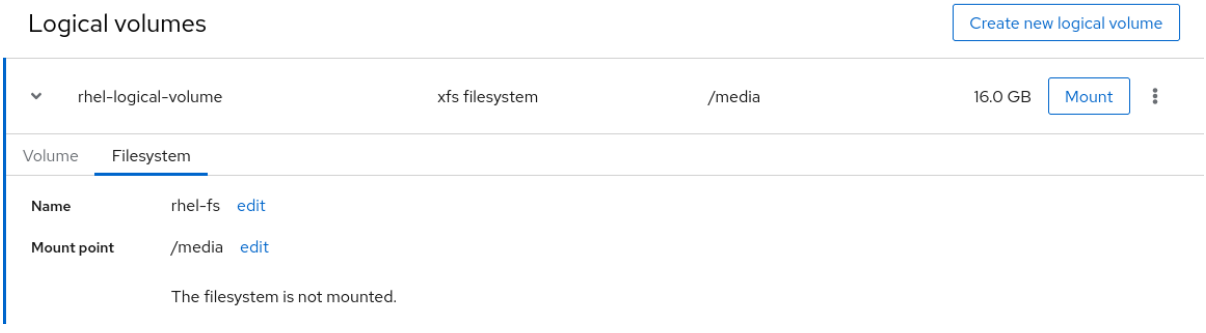
Vous pouvez également sélectionner une version avec le cryptage LUKS (Linux Unified Key Setup), qui vous permet de crypter le volume à l'aide d'une phrase de passe.

7. Sélectionnez l'option **Overwrite**:
   - **Don't overwrite existing data** – la console web RHEL ne réécrit que l'en-tête du disque. L'avantage de cette option est la rapidité du formatage.
   - **Overwrite existing data with zeros** – la console web RHEL réécrit tout le disque avec des zéros. Cette option est plus lente car le programme doit parcourir l'ensemble du disque. Utilisez cette option si le disque contient des données et que vous devez les écraser.
8. Dans le champ **Mount Point**, ajoutez le chemin de montage.



9. Cliquez sur **Format**.
   Le formatage peut prendre plusieurs minutes en fonction de la taille du volume et des options de formatage sélectionnées.

   Une fois le formatage terminé, vous pouvez voir les détails du volume logique formaté dans l'onglet **Filesystem**.



10. Pour utiliser le volume logique, cliquez sur **Monter**.

À ce stade, le système peut utiliser un volume logique monté et formaté.

CHAPITRE 21. MODIFICATION DES LECTEURS PHYSIQUES DANS LES GROUPES DE VOLUMES À L'AIDE DE LA CONSOLE WEB

Changez le lecteur d'un groupe de volumes à l'aide de la console Web RHEL 9.

Le changement des lecteurs physiques s'effectue selon les procédures suivantes :

- Ajout de lecteurs physiques à partir de volumes logiques.
- Suppression des lecteurs physiques des volumes logiques.

Conditions préalables

- La console web RHEL 9 a été installée.
  Pour plus de détails, voir Installation de la console web.
- Le paquetage **cockpit-storaged** est installé sur votre système.
- Un nouveau disque physique pour remplacer l'ancien ou celui qui est cassé.
- La configuration prévoit que les lecteurs physiques sont organisés dans un groupe de volumes.

21.1. AJOUT DE LECTEURS PHYSIQUES À DES GROUPES DE VOLUMES DANS LA CONSOLE WEB

La console web RHEL 9 vous permet d'ajouter un nouveau lecteur physique ou un autre type de volume au volume logique existant.

Conditions préalables

- Un groupe de volumes doit être créé.
- Un nouveau disque connecté à la machine.

Procédure

1. Connectez-vous à la console RHEL 9.
2. Cliquez sur **Storage**.
3. Dans la boîte **Volume Groups**, cliquez sur le groupe de volumes dans lequel vous souhaitez ajouter un volume physique.
4. Dans la boîte **Physical Volumes**, cliquez sur le bouton .
5. Dans la boîte de dialogue **Add Disks**, sélectionnez le lecteur préféré et cliquez sur **Add**.

Par conséquent, la console web RHEL 9 ajoute le volume physique.

Verification steps

- Vérifiez la section **Physical Volumes**, et le volume logique peut immédiatement commencer à écrire sur le disque.

21.2. SUPPRESSION DES LECTEURS PHYSIQUES DES GROUPES DE VOLUMES DANS LA CONSOLE WEB

Si un volume logique comprend plusieurs lecteurs physiques, vous pouvez supprimer l'un d'entre eux en ligne.

Le système déplace automatiquement toutes les données du lecteur à retirer vers d'autres lecteurs au cours du processus de retrait. Notez que cela peut prendre un certain temps.

La console web vérifie également s'il y a suffisamment d'espace pour retirer le lecteur physique.

Conditions préalables

- Un groupe de volumes avec plus d'un lecteur physique connecté.

Procédure

Les étapes suivantes décrivent comment supprimer un lecteur du groupe de volumes sans provoquer de panne dans la console Web RHEL 9.

1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur **Storage**.
3. Cliquez sur le groupe de volumes dans lequel se trouve le volume logique.
4. Dans la section **Physical Volumes**, localisez le volume préféré.
5. Cliquez sur le bouton **-**.
   La console web RHEL 9 vérifie si le volume logique dispose de suffisamment d'espace libre pour supprimer le disque. Si ce n'est pas le cas, vous ne pouvez pas retirer le disque et il est nécessaire d'en ajouter un autre au préalable. Pour plus d'informations, voir Ajout de disques physiques à des volumes logiques dans la console Web.

En conséquence, la console web RHEL 9 supprime le volume physique du volume logique créé sans provoquer de panne.

CHAPITRE 22. GESTION DES VOLUMES VIRTUAL DATA OPTIMIZER À L'AIDE DE LA CONSOLE WEB

Configurez le Virtual Data Optimizer (VDO) à l'aide de la console web RHEL 9.

Vous apprendrez à :

- Créer des volumes VDO
- Format des volumes VDO
- Extension des volumes VDO

Conditions préalables

- La console web RHEL 9 est installée et accessible. Pour plus de détails, voir Installation de la console web.
- Le paquetage **cockpit-storaged** est installé sur votre système.

22.1. VOLUMES VDO DANS LA CONSOLE WEB

Red Hat Enterprise Linux 9 prend en charge Virtual Data Optimizer (VDO).

VDO est une technologie de virtualisation de blocs qui combine :

Compression

Pour plus de détails, voir Activation ou désactivation de la compression dans VDO .

Déduplication

Pour plus de détails, voir Activation ou désactivation de la compression dans VDO .

Provisionnement fin

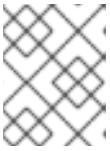
Pour plus d'informations, voir Création et gestion de volumes provisionnés (thin volumes).

Grâce à ces technologies, VDO :

- Économie d'espace de stockage en ligne
- Compression des fichiers
- Élimination des doublons
- Permet d'allouer plus d'espace virtuel que l'espace de stockage physique ou logique disponible
- Permet d'étendre le stockage virtuel en augmentant la capacité de stockage

La VDO peut être créée au-dessus de nombreux types de stockage. Dans la console web RHEL 9, vous pouvez configurer la VDO au-dessus de :

- LVM



NOTE

Il n'est pas possible de configurer la VDO sur des volumes à faible provisionnement.

- Physical volume
- RAID logiciel

Pour plus de détails sur l'emplacement de la VDO dans la pile de stockage, voir Configuration requise.

Ressources supplémentaires

- Pour plus d'informations sur la VDO, voir Déduplication et compression du stockage.

22.2. CRÉATION DE VOLUMES VDO DANS LA CONSOLE WEB

Créez un volume VDO dans la console web RHEL.

Conditions préalables

- Lecteurs physiques, LVM ou RAID à partir desquels vous souhaitez créer des VDO.

Procédure

1. Connectez-vous à la console web RHEL 9.
   Pour plus de détails, voir Connexion à la console web .
2. Cliquez sur **Storage**.
3. Cliquez sur le bouton dans la boîte **VDO Devices**.
4. Dans le champ **Name**, entrez le nom d'un volume VDO sans espace.
5. Sélectionnez le lecteur que vous souhaitez utiliser.
6. Dans la barre **Logical Size**, définissez la taille du volume VDO. Vous pouvez l'étendre plus de dix fois, mais réfléchissez à l'objectif pour lequel vous créez le volume VDO :
   - Pour les machines virtuelles actives ou le stockage en conteneur, utilisez une taille logique dix fois supérieure à la taille physique du volume.
   - Pour le stockage d'objets, utilisez une taille logique égale à trois fois la taille physique du volume.

   Pour plus de détails, voir Déploiement de la VDO .
7. Dans la barre **Index Memory**, allouez de la mémoire pour le volume VDO.
   Pour plus d'informations sur la configuration requise par VDO, voir Configuration requise.
8. Sélectionnez l'option **Compression**. Cette option permet de réduire efficacement différents formats de fichiers.
   Pour plus de détails, voir Activation ou désactivation de la compression dans VDO .
9. Sélectionnez l'option **Deduplication**.

Cette option permet de réduire la consommation des ressources de stockage en éliminant les copies multiples des blocs dupliqués. Pour plus de détails, voir Activation ou désactivation de la compression dans VDO.

10. [Facultatif] Si vous souhaitez utiliser le volume VDO avec des applications nécessitant une taille de bloc de 512 octets, sélectionnez **Use 512 Byte emulation**. Cette option réduit les performances du volume VDO, mais n'est que très rarement nécessaire. En cas de doute, laissez cette option désactivée.

11. Cliquez sur **Create**.

Verification steps

- Vérifiez que vous pouvez voir le nouveau volume VDO dans la section **Storage**. Vous pouvez ensuite le formater avec un système de fichiers.

22.3. FORMATAGE DES VOLUMES VDO DANS LA CONSOLE WEB

Les volumes VDO se comportent comme des lecteurs physiques. Pour les utiliser, vous devez les formater avec un système de fichiers.

AVERTISSEMENT

Le formatage de la VDO efface toutes les données du volume.

Les étapes suivantes décrivent la procédure de formatage des volumes VDO.

Conditions préalables

- Un volume VDO est créé. Pour plus d'informations, voir Création de volumes VDO dans la console web.

Procédure

1. Connectez-vous à la console web RHEL 9. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur **Storage**.
3. Cliquez sur le volume VDO.
4. Cliquez sur l'onglet **Unrecognized Data**.
5. Cliquez sur **Format**.
6. Dans le menu déroulant **Erase**, sélectionnez :

   Don’t overwrite existing data

   La console web RHEL réécrit uniquement l'en-tête du disque. L'avantage de cette option est la rapidité du formatage.

Overwrite existing data with zeros

La console web RHEL réécrit tout le disque avec des zéros. Cette option est plus lente car le programme doit parcourir l'ensemble du disque. Utilisez cette option si le disque contient des données et que vous devez les réécrire.

7. Dans le menu déroulant **Type**, sélectionnez un système de fichiers :

   - Le système de fichiers **XFS** prend en charge de grands volumes logiques, la commutation de lecteurs physiques en ligne sans interruption de service et la croissance. Laissez ce système de fichiers sélectionné si vous n'avez pas d'autre préférence.
     XFS ne prend pas en charge la réduction des volumes. Par conséquent, vous ne pourrez pas réduire un volume formaté avec XFS.

   - Le système de fichiers **ext4** prend en charge les volumes logiques, la commutation de lecteurs physiques en ligne sans interruption, la croissance et la réduction.

   Vous pouvez également sélectionner une version avec le cryptage LUKS (Linux Unified Key Setup), qui vous permet de crypter le volume à l'aide d'une phrase de passe.

8. Dans le champ **Name**, entrez le nom du volume logique.

9. Dans le menu déroulant **Mounting**, sélectionnez **Custom**.
   L'option **Default** ne garantit pas que le système de fichiers sera monté au prochain démarrage.

10. Dans le champ **Mount Point**, ajoutez le chemin de montage.

11. Sélectionnez **Mount at boot**.

12. Cliquez sur **Format**.
    Le formatage peut prendre plusieurs minutes en fonction des options de formatage utilisées et de la taille du volume.

    Après avoir terminé avec succès, vous pouvez voir les détails du volume VDO formaté dans l'onglet **Filesystem**.

13. Pour utiliser le volume VDO, cliquez sur **Mount**.

À ce stade, le système utilise le volume VDO monté et formaté.

22.4. EXTENSION DES VOLUMES VDO DANS LA CONSOLE WEB

Étendre les volumes VDO dans la console web RHEL 9.

Conditions préalables

- Le paquetage **cockpit-storaged** est installé sur votre système.
- Le volume VDO créé.

Procédure

1. Connectez-vous à la console web RHEL 9.
   Pour plus de détails, voir Connexion à la console web .

2. Cliquez sur **Storage**.

3. Cliquez sur votre volume VDO dans la boîte **VDO Devices**.
4. Dans les détails du volume VDO, cliquez sur le bouton **Croître**.
5. Dans la boîte de dialogue **Grow logical size of VDO**, augmentez la taille logique du volume VDO.
1. Cliquez sur **Grow**.

Verification steps

- Vérifiez les détails du volume VDO pour la nouvelle taille afin de vous assurer que les modifications ont été effectuées avec succès.

CHAPITRE 23. VERROUILLAGE DES DONNÉES AVEC UN MOT DE PASSE LUKS DANS LA CONSOLE WEB RHEL

Dans l'onglet **Storage** de la console web, vous pouvez désormais créer, verrouiller, déverrouiller, redimensionner et configurer des périphériques cryptés à l'aide du format LUKS (Linux Unified Key Setup) version 2.

Cette nouvelle version de LUKS offre :

- Des politiques de déverrouillage plus souples
- Une cryptographie plus forte
- Meilleure compatibilité avec les changements à venir

Conditions préalables

- La console web RHEL 9 a été installée. Pour plus de détails, voir Installation de la console web.
- Le paquetage **cockpit-storaged** est installé sur votre système.

23.1. CRYPTAGE DE DISQUE LUKS

Linux Unified Key Setup-on-disk-format (LUKS) fournit un ensemble d'outils qui simplifie la gestion des périphériques cryptés. Avec LUKS, vous pouvez chiffrer des périphériques en bloc et permettre à plusieurs clés d'utilisateur de déchiffrer une clé principale. Pour le chiffrement en bloc de la partition, utilisez cette clé principale.

Red Hat Enterprise Linux utilise LUKS pour effectuer le chiffrement du périphérique de bloc. Par défaut, l'option de chiffrement du périphérique de bloc n'est pas cochée lors de l'installation. Si vous sélectionnez l'option de chiffrer votre disque, le système vous demande une phrase de passe à chaque fois que vous démarrez l'ordinateur. Cette phrase de passe déverrouille la clé de chiffrement en bloc qui décrypte votre partition. Si vous souhaitez modifier la table de partition par défaut, vous pouvez sélectionner les partitions que vous souhaitez crypter. Cette option est définie dans les paramètres de la table de partitions.

Chiffres

Le chiffrement par défaut utilisé pour LUKS est **aes-xts-plain64**. La taille de clé par défaut de LUKS est de 512 bits. La taille de clé par défaut pour LUKS avec le mode **Anaconda** XTS est de 512 bits. Les codes disponibles sont les suivants :

- Norme de chiffrement avancée (AES)
- Twofish
- Serpent

LUKS effectue les opérations suivantes

- LUKS crypte des blocs entiers et est donc bien adapté à la protection du contenu des appareils mobiles tels que les supports de stockage amovibles ou les lecteurs de disques d'ordinateurs portables.

- Le contenu sous-jacent du bloc crypté est arbitraire, ce qui le rend utile pour crypter les périphériques d'échange. Cela peut également être utile pour certaines bases de données qui utilisent des périphériques de bloc spécialement formatés pour le stockage des données.
- LUKS utilise le sous-système de noyau existant pour le mappage de périphériques.
- LUKS permet de renforcer la phrase de passe, ce qui protège contre les attaques par dictionnaire.
- Les dispositifs LUKS contiennent plusieurs emplacements de clé, ce qui permet aux utilisateurs d'ajouter des clés de sauvegarde ou des phrases de passe.

LUKS n'est pas recommandé dans les cas suivants

- Les solutions de chiffrement de disque telles que LUKS ne protègent les données que lorsque le système est éteint. Une fois que le système est en marche et que LUKS a décrypté le disque, les fichiers qui s'y trouvent sont accessibles à tous ceux qui y ont accès.
- Scénarios nécessitant que plusieurs utilisateurs disposent de clés d'accès distinctes au même appareil. Le format LUKS1 offre huit emplacements de clé et le format LUKS2 en offre jusqu'à 32.
- Applications nécessitant un cryptage au niveau du fichier.

Ressources supplémentaires

- Page d'accueil du projet LUKS
- Spécification du format LUKS sur disque
- FIPS 197 : norme de cryptage avancée (AES)

23.2. CONFIGURATION DE LA PHRASE DE PASSE LUKS DANS LA CONSOLE WEB

Si vous souhaitez ajouter le chiffrement à un volume logique existant sur votre système, vous ne pouvez le faire qu'en formatant le volume.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.
- Le paquetage **cockpit-storaged** est installé sur votre système.
- Volume logique existant disponible sans cryptage.

Procédure

1. Connectez-vous à la console web RHEL 9.
   Pour plus de détails, voir Connexion à la console web .
2. Cliquez sur **Storage**.

3. Sélectionnez le périphérique de stockage que vous souhaitez formater.
4. Cliquez sur l'icône de menu et sélectionnez l'option **Format**.
5. Cochez la case **Encrypt data** pour activer le cryptage sur votre périphérique de stockage.
6. Définissez et confirmez votre nouvelle phrase de passe.
7. [Facultatif] Modifier d'autres options de cryptage.
8. Finaliser les paramètres de formatage.
9. Cliquez sur **Format**.

23.3. MODIFICATION DE LA PHRASE DE PASSE LUKS DANS LA CONSOLE WEB

Modifier une phrase de passe LUKS sur un disque ou une partition chiffré(e) dans la console Web.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.
- Le paquetage **cockpit-storaged** est installé sur votre système.

Procédure

1. Connectez-vous à la console web. Pour plus d'informations, voir Connexion à la console web .
2. Cliquez sur **Storage**
3. Dans le tableau des lecteurs, sélectionnez le disque contenant les données cryptées.
4. Dans **Content**, sélectionnez la partition cryptée.
5. Cliquez sur **Encryption**.
6. Dans le tableau **Keys**, cliquez sur l'icône du stylo.
7. Dans la fenêtre de dialogue **Change passphrase**:
   a. Saisissez votre phrase d'authentification actuelle.
   b. Saisissez votre nouvelle phrase d'authentification.
   c. Confirmez votre nouvelle phrase d'authentification.
8. Cliquez sur **Save**

CHAPITRE 24. GESTION DES MISES À JOUR LOGICIELLES DANS LA CONSOLE WEB

Apprendre à gérer les mises à jour logicielles dans la console web RHEL 9 et les moyens de les automatiser.

Le module de mise à jour des logiciels de la console web est basé sur l'utilitaire **dnf**. Pour plus d'informations sur la mise à jour des logiciels avec **dnf**, voir la section Mise à jour des paquets.

24.1. GESTION DES MISES À JOUR MANUELLES DE LOGICIELS DANS LA CONSOLE WEB

Cette section décrit comment mettre à jour manuellement votre logiciel à l'aide de la console web.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL 9.
   Pour plus de détails, voir Connexion à la console web.
2. Cliquez sur **Software Updates**.
   La liste des mises à jour disponibles est actualisée automatiquement si la dernière vérification remonte à plus de 24 heures. Pour déclencher une actualisation, cliquez sur le bouton **Vérifier les mises à jour**.
3. Appliquer les mises à jour. Vous pouvez consulter le journal des mises à jour pendant que la mise à jour est en cours.
   a. Pour installer toutes les mises à jour disponibles, cliquez sur le bouton **Installer toutes les mises à jour**.
   b. Si des mises à jour de sécurité sont disponibles, vous pouvez les installer séparément en cliquant sur le bouton **Installer les mises à jour de sécurité**.
   c. Si des mises à jour de kpatch sont disponibles, vous pouvez les installer séparément en cliquant sur le bouton **Installer les mises à jour de kpatch**.
4. Facultatif : vous pouvez activer le commutateur **Reboot after completion** pour un redémarrage automatique de votre système.
   Si vous effectuez cette étape, vous pouvez sauter les autres étapes de cette procédure.
5. Une fois que le système a appliqué les mises à jour, il vous est recommandé de redémarrer votre système.
   Nous recommandons cette opération surtout si la mise à jour inclut un nouveau noyau ou des services système que vous ne souhaitez pas redémarrer individuellement.
6. Cliquez sur **Ignore** pour annuler le redémarrage ou sur **Restart Now** pour redémarrer votre système.
   Après le redémarrage du système, connectez-vous à la console web et allez sur la page **Software Updates** pour vérifier que la mise à jour a réussi.

24.2. GESTION DES MISES À JOUR AUTOMATIQUES DE LOGICIELS DANS LA CONSOLE WEB

Dans la console web, vous pouvez choisir d'appliquer toutes les mises à jour, ou les mises à jour de sécurité, et également gérer la périodicité et l'heure de vos mises à jour automatiques.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL 9. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur **Software Updates**.
3. Dans le tableau **Settings**, cliquez sur le bouton **Modifier**.
4. Choisissez l'un des types de mises à jour automatiques. Vous pouvez choisir entre **Security updates only** ou **All updates**.
5. Pour modifier le jour de la mise à jour automatique, cliquez sur le menu déroulant **every day** et sélectionnez un jour spécifique.
6. Pour modifier l'heure de la mise à jour automatique, cliquez sur le champ **6:00** et sélectionnez ou tapez une heure spécifique.
7. Si vous souhaitez désactiver les mises à jour automatiques de logiciels, sélectionnez le type **No updates**.

24.3. GESTION DU REDÉMARRAGE À LA DEMANDE APRÈS L'APPLICATION DE MISES À JOUR LOGICIELLES DANS LA CONSOLE WEB

La fonction de redémarrage intelligent indique aux utilisateurs s'il est nécessaire de redémarrer l'ensemble du système après l'application d'une mise à jour logicielle ou s'il suffit de redémarrer certains services.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

Procédure

1. Connectez-vous à la console web RHEL 9. Pour plus d'informations, voir Connexion à la console web.
2. Cliquez sur **Software Updates**.
3. Appliquer une mise à jour de votre système.

4. Après une mise à jour réussie, cliquez sur **Reboot system...**, **Restart services...**, ou **Ignore**

5. Si vous décidez de l'ignorer, vous pouvez revenir au menu de redémarrage en effectuant l'une des opérations suivantes :

   a. Redémarrage :

      i. Cliquez sur le bouton **Redémarrer le système** dans le champ **Status** de la page **Software Updates**.

      ii. (Facultatif) Rédigez un message à l'intention des utilisateurs connectés.

      iii. Sélectionnez un délai dans le menu déroulant **Delay**.

      iv. Cliquez sur **Reboot**.

   b. Redémarrage des services :

      i. Cliquez sur le bouton **Redémarrer les services...** dans le champ **Status** de la page **Software Updates**.
      Vous verrez une liste de tous les services qui nécessitent un redémarrage.

      ii. Cliquez sur **Restart services**.
      Selon votre choix, le système redémarre ou vos services redémarrent.

24.4. APPLIQUER DES CORRECTIFS AVEC LE LIVE PATCHING DU NOYAU DANS LA CONSOLE WEB

La console web permet aux utilisateurs d'appliquer les correctifs de sécurité du noyau sans forcer les redémarrages en utilisant le cadre **kpatch**. La procédure suivante montre comment configurer le type de correctif préféré.

Conditions préalables

- La console web doit être installée et accessible. Pour plus de détails, voir Installation de la console web.

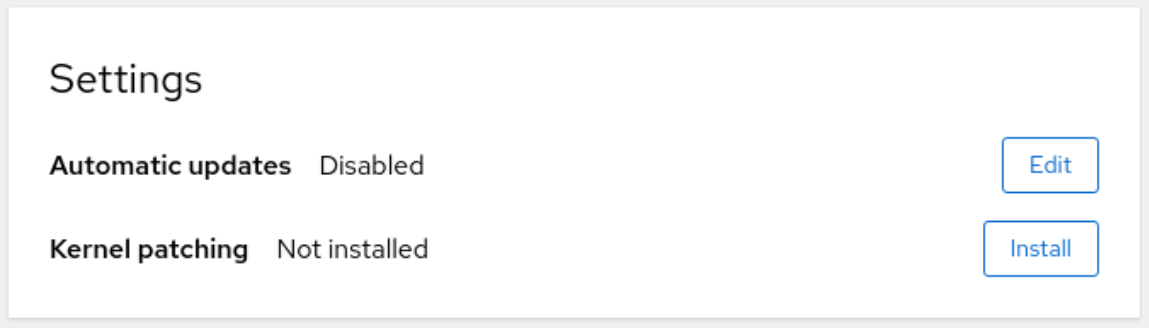
Procédure

1. Connectez-vous à la console web avec des privilèges administratifs. Pour plus d'informations, voir Connexion à la console web .

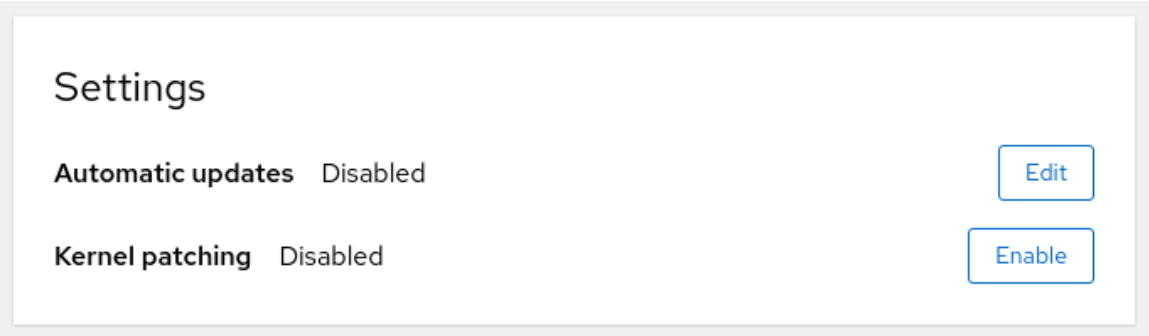
2. Cliquez sur **Software Updates**.

3. Vérifiez l'état des paramètres de correction du noyau.

   a. Si le correctif n'est pas installé, cliquez sur **Installer**.

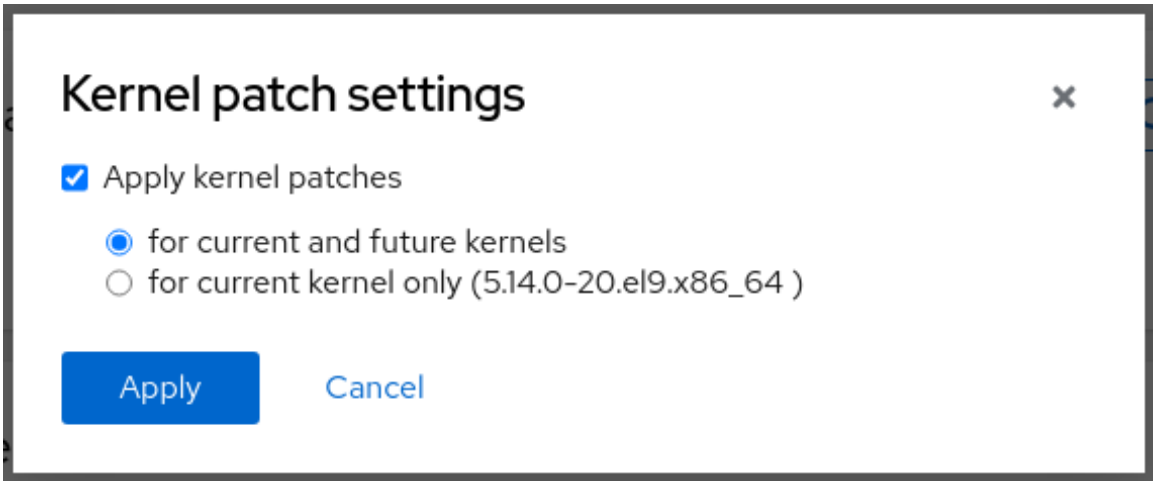


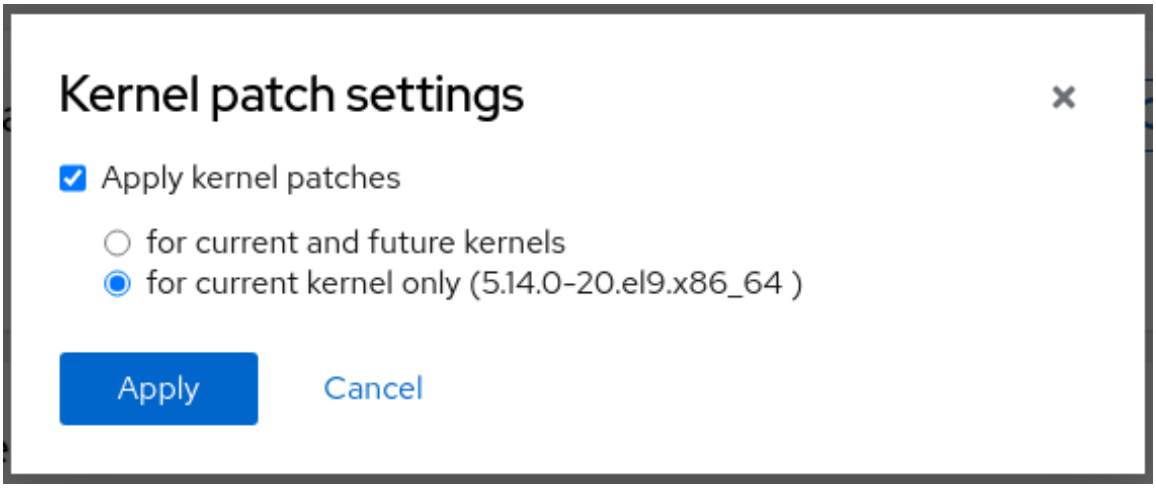
b. Pour activer le patching du noyau, cliquez sur **Activer**.



c. Cochez la case pour l'application des correctifs du noyau.

d. Sélectionnez si vous souhaitez appliquer des correctifs pour les noyaux actuels et futurs, ou pour le noyau actuel uniquement. Si vous choisissez de vous abonner à l'application de correctifs pour les futurs noyaux, le système appliquera également des correctifs pour les prochaines versions du noyau.

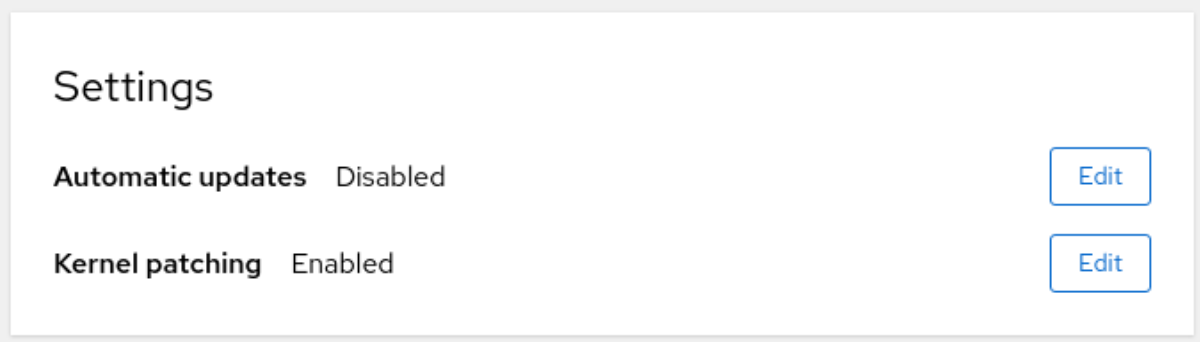




e. Cliquez sur **Appliquer**.

Vérification

- Vérifiez que le correctif du noyau est maintenant **Enabled** dans le tableau **Settings** de la section **Software updates**.



Ressources supplémentaires

- Application de correctifs avec le live patching du noyau

CHAPITRE 25. GESTION DES ABONNEMENTS DANS LA CONSOLE WEB

Gérez votre abonnement à Red Hat Enterprise Linux 9 à partir de la console web.

Pour obtenir un abonnement pour votre Red Hat Enterprise Linux, vous devez disposer d'un compte sur le portail client de Red Hat ou d'une clé d'activation.

Ce chapitre couvre les points suivants

- Gestion des abonnements dans la console web RHEL 9.
- Enregistrement des abonnements pour votre système dans la console web avec le nom d'utilisateur et le mot de passe Red Hat.
- Enregistrement des abonnements avec la clé d'activation.

Conditions préalables

- Abonnements achetés.
- Le système soumis à l'abonnement doit être connecté à l'internet car la console web doit communiquer avec le portail client de Red Hat.

25.1. GESTION DES ABONNEMENTS DANS LA CONSOLE WEB

La console Web de RHEL 9 fournit une interface permettant d'utiliser le Gestionnaire d'abonnements Red Hat installé sur votre système local.

Le gestionnaire d'abonnements se connecte au portail client de Red Hat et vérifie tous les abonnements disponibles :

- Abonnements actifs
- Abonnements expirés
- Abonnements renouvelés

Si vous souhaitez renouveler l'abonnement ou en obtenir un autre dans Red Hat Customer Portal, vous n'avez pas besoin de mettre à jour les données du Gestionnaire d'abonnements manuellement. Le Gestionnaire d'abonnements synchronise automatiquement les données avec Red Hat Customer Portal.

25.2. ENREGISTRER DES ABONNEMENTS AVEC DES INFORMATIONS D'IDENTIFICATION DANS LA CONSOLE WEB

Suivez les étapes suivantes pour enregistrer un Red Hat Enterprise Linux nouvellement installé avec les informations d'identification du compte à l'aide de la console Web RHEL.

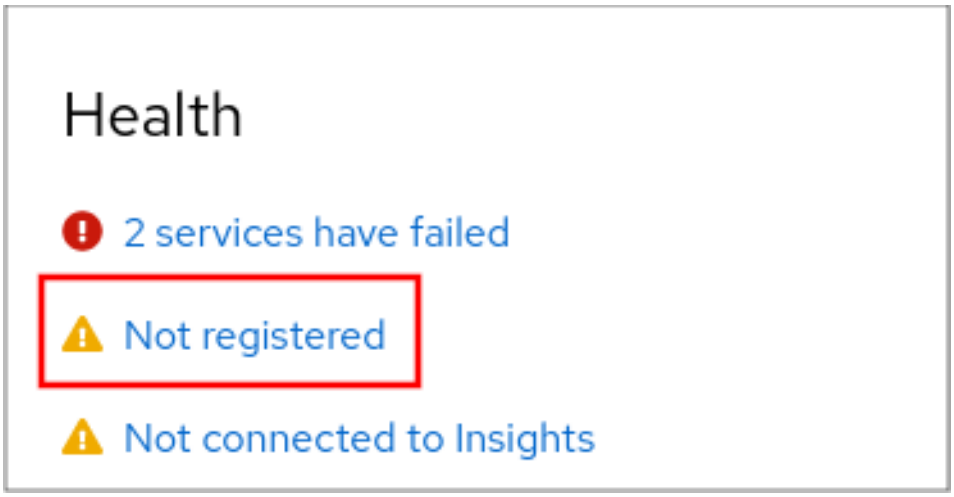
Conditions préalables

- Un compte utilisateur valide sur le portail client de Red Hat.
  Consultez la page Créer un login Red Hat .

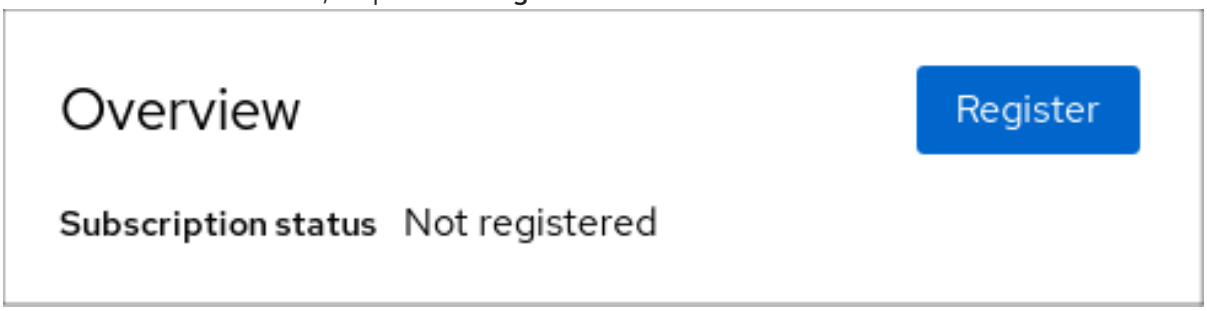
- Abonnement actif pour votre système RHEL.

Procédure

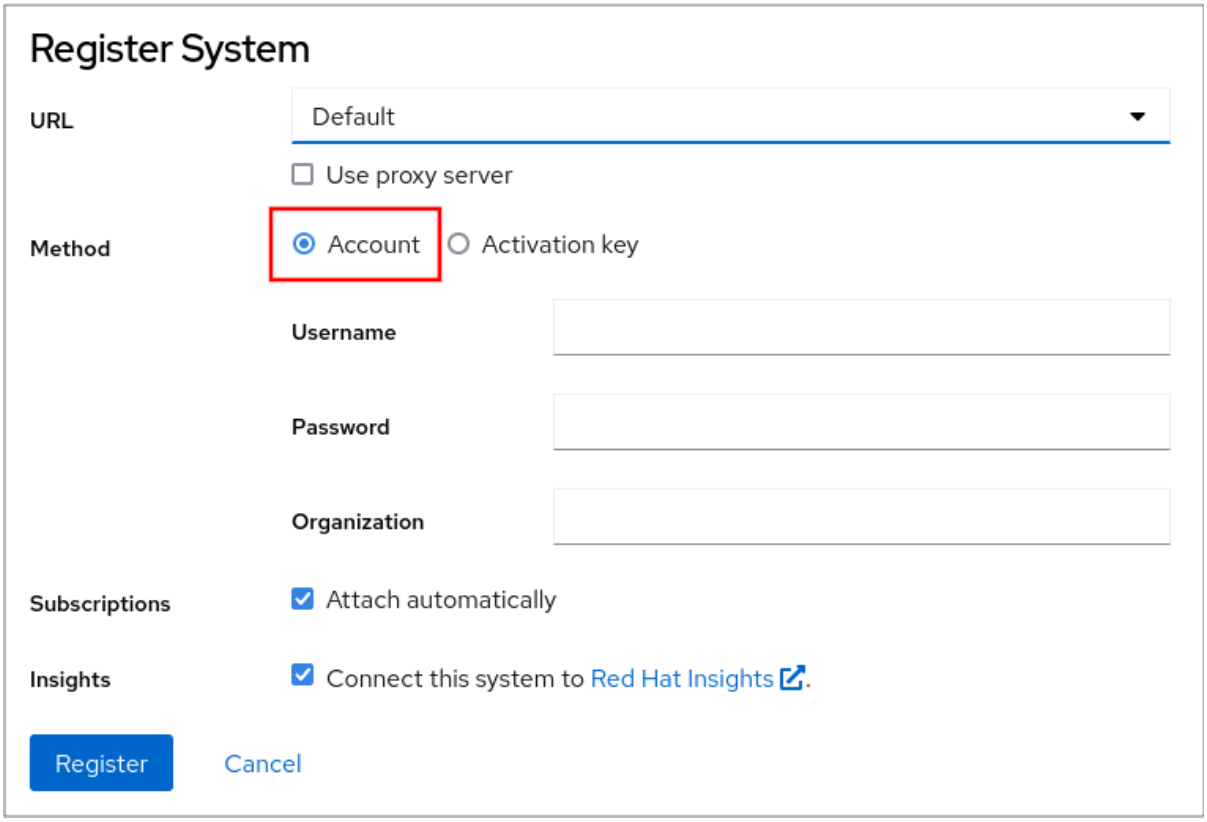
1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Dans le dossier **Health** de la page **Overview**, cliquez sur l'avertissement **Not registered**, ou cliquez sur **Subscriptions** dans le menu principal pour accéder à la page contenant vos informations d'abonnement.



3. Dans le dossier **Overview**, cliquez sur **Register**.



4. Dans la boîte de dialogue **Register system**, indiquez que vous souhaitez vous enregistrer en utilisant les informations d'identification de votre compte.



5. Entrez votre nom d'utilisateur.
6. Entrez votre mot de passe.
7. Si vous le souhaitez, vous pouvez saisir le nom ou l'identifiant de votre organisation.
   Si votre compte appartient à plus d'une organisation sur le portail client de Red Hat, vous devez ajouter le nom de l'organisation ou l'ID de l'organisation. Pour obtenir l'identifiant de l'organisation, adressez-vous à votre point de contact Red Hat.
   - Si vous ne souhaitez pas connecter votre système à Red Hat Insights, décochez la case **Insights**.
8. Cliquez sur le bouton **Enregistrer**.

À ce stade, votre système Red Hat Enterprise Linux a été enregistré avec succès.

25.3. ENREGISTRER DES ABONNEMENTS AVEC DES CLÉS D'ACTIVATION DANS LA CONSOLE WEB

Suivez les étapes suivantes pour enregistrer une nouvelle installation de Red Hat Enterprise Linux avec une clé d'activation à l'aide de la console Web RHEL.

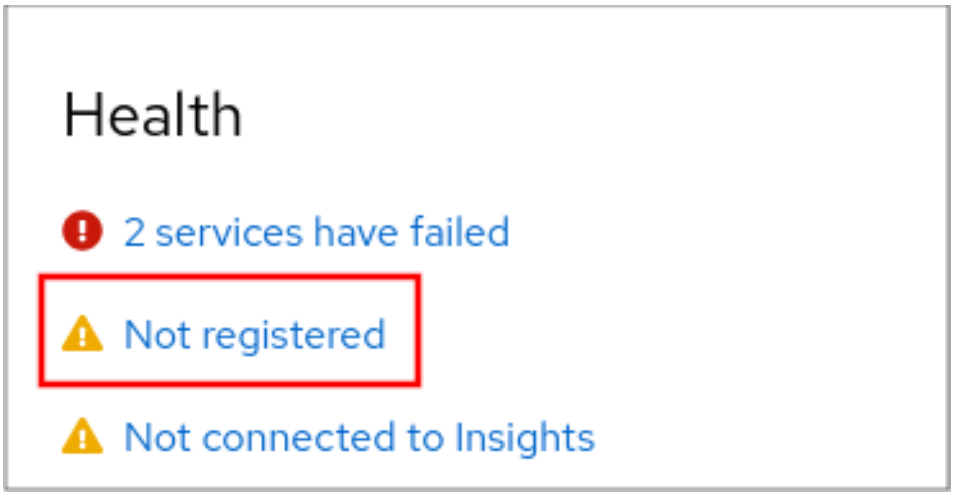
Conditions préalables

- Si vous n'avez pas de compte utilisateur dans le portail, votre fournisseur vous fournira la clé d'activation.

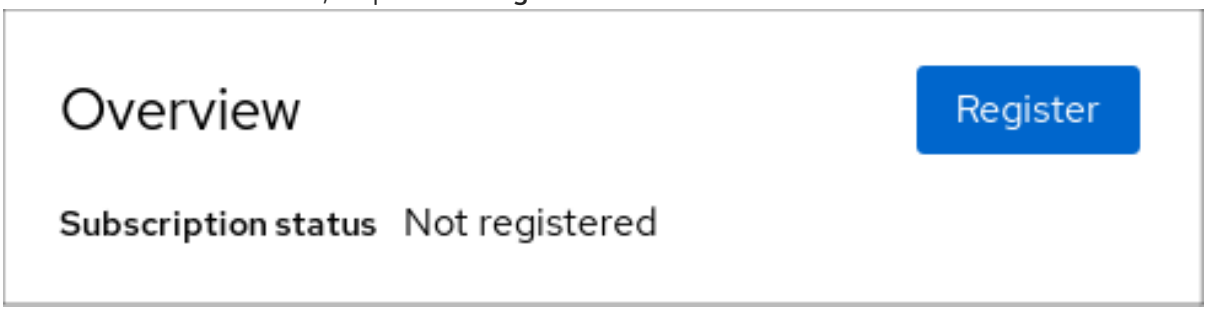
Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.

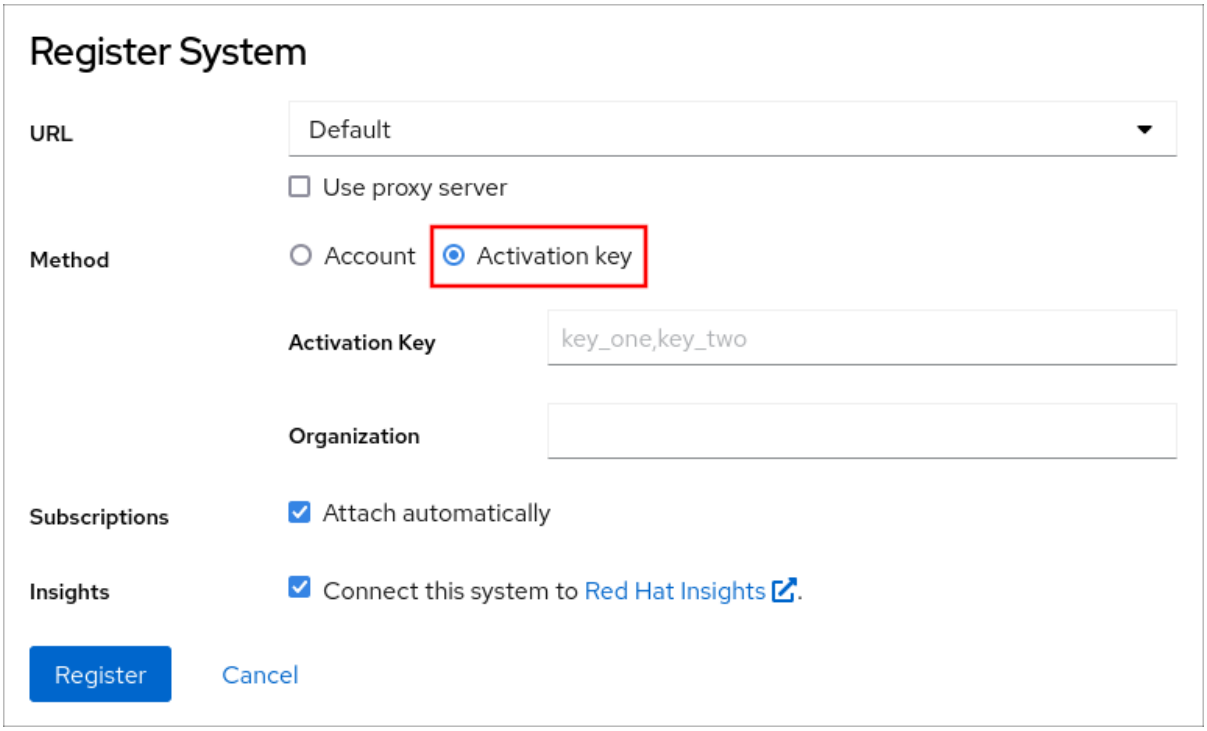
2. Dans le dossier **Health** de la page **Overview**, cliquez sur l'avertissement **Not registered**, ou cliquez sur **Subscriptions** dans le menu principal pour accéder à la page contenant vos informations d'abonnement.



3. Dans le dossier **Overview**, cliquez sur **Register**.



4. Dans la boîte de dialogue **Register system**, sélectionnez l'enregistrement à l'aide d'une clé d'activation.



5. Saisissez votre ou vos clés.

6. Saisissez le nom ou l'identifiant de votre organisation.
Pour obtenir l'identifiant de l'organisation, adressez-vous à votre point de contact Red Hat.

- Si vous ne souhaitez pas connecter votre système à Red Hat Insights, décochez la case **Insights**.

7. Cliquez sur le bouton **Enregistrer**.

À ce stade, votre système Red Hat Enterprise Linux a été enregistré avec succès.

CHAPITRE 26. CONFIGURATION DE KDUMP DANS LA CONSOLE WEB

Configurez et testez la configuration de **kdump** dans la console web de RHEL 9.

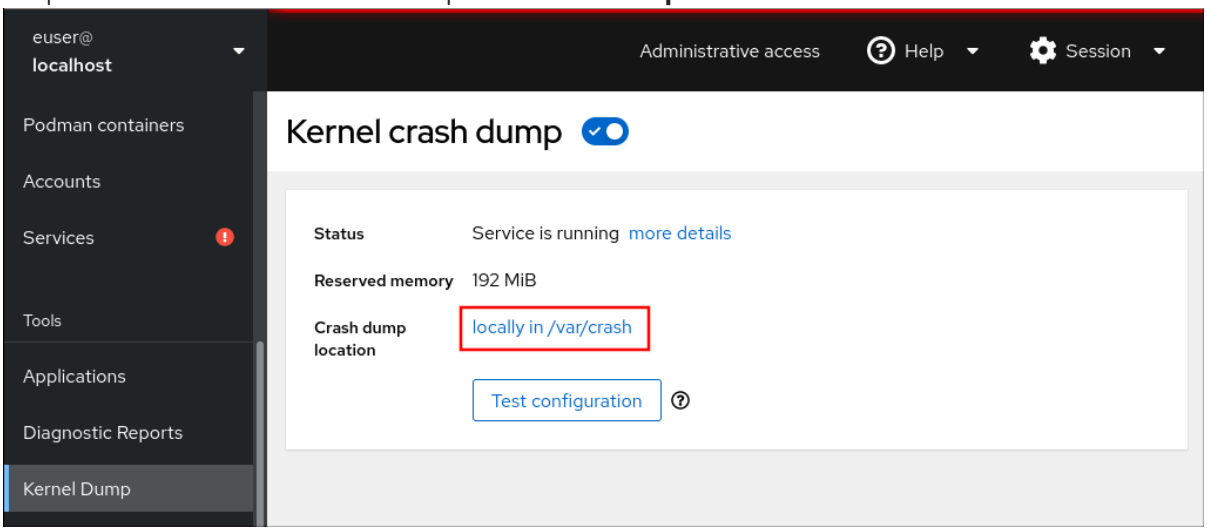
La console web fait partie de l'installation par défaut de RHEL 9 et permet d'activer ou de désactiver le service **kdump** au démarrage. En outre, la console web vous permet de configurer la mémoire réservée pour **kdump**; ou de sélectionner l'emplacement de sauvegarde de *vmcore* dans un format non compressé ou compressé.

26.1. CONFIGURER L'UTILISATION DE LA MÉMOIRE DE KDUMP ET L'EMPLACEMENT DE LA CIBLE DANS LA CONSOLE WEB

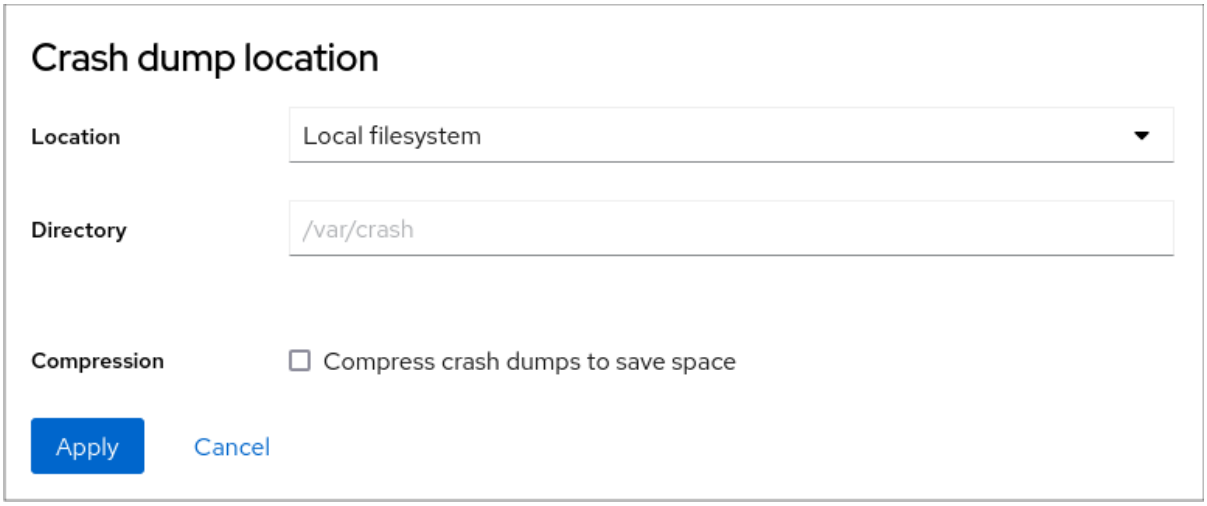
La procédure ci-dessous vous montre comment utiliser l'onglet **Kernel Dump** dans l'interface de la console web RHEL pour configurer la quantité de mémoire réservée au noyau **kdump**. La procédure décrit également comment spécifier l'emplacement cible du fichier dump **vmcore** et comment tester votre configuration.

Procédure

1. Ouvrez l'onglet **Kernel Dump** et démarrez le service **kdump**.
2. Configurez l'utilisation de la mémoire de **kdump** à l'aide de la ligne de commande.
3. Cliquez sur le lien situé à côté de l'option **Crash dump location**.



4. Sélectionnez l'option **Local Filesystem** dans le menu déroulant et indiquez le répertoire dans lequel vous souhaitez enregistrer le dump.

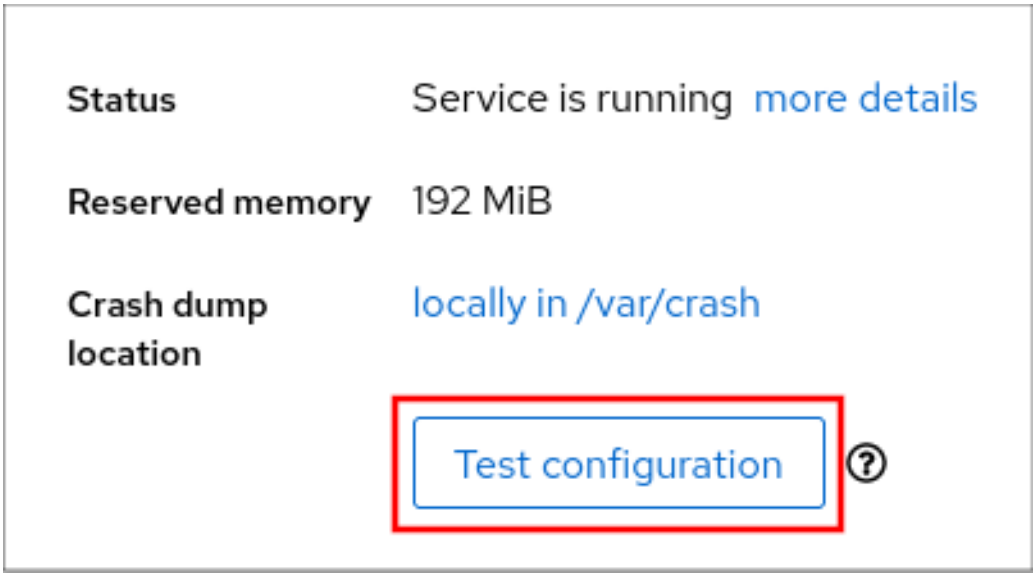


- Vous pouvez également sélectionner l'option **Remote over SSH** dans le menu déroulant pour envoyer le vmcore à une machine distante à l'aide du protocole SSH.
  Remplissez les champs **Server**, **ssh key**, et **Directory** avec l'adresse de la machine distante, l'emplacement de la clé ssh et un répertoire cible.
- Une autre possibilité consiste à sélectionner l'option **Remote over NFS** dans la liste déroulante et à remplir le champ **Mount** pour envoyer le noyau virtuel à une machine distante à l'aide du protocole NFS.

NOTE

Cochez la case **Compression** pour réduire la taille du fichier vmcore.

5. Testez votre configuration en plantant le noyau.



   a. Cliquez sur **Test configuration**.

   b. Dans le champ **Test kdump settings**, cliquez sur **Crash system**.

AVERTISSEMENT

Cette étape perturbe l'exécution du noyau et entraîne une panne du système et une perte de données.

Ressources supplémentaires

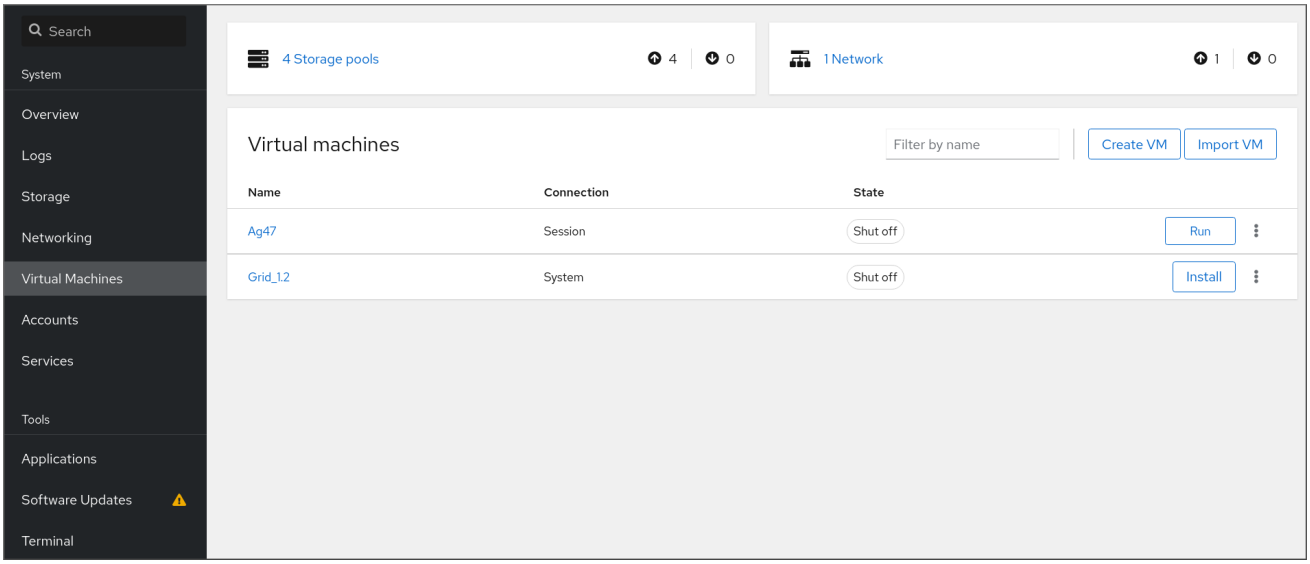
- Cibles kdump prises en charge
- Utiliser des communications sécurisées entre deux systèmes avec OpenSSH

26.2. RESSOURCES SUPPLÉMENTAIRES

- Commencer à utiliser la console web RHEL

CHAPITRE 27. MANAGING VIRTUAL MACHINES IN THE WEB CONSOLE

To manage virtual machines in a graphical interface on a RHEL 9 host, you can use the **Virtual Machines** pane in the RHEL 9 web console.



27.1. OVERVIEW OF VIRTUAL MACHINE MANAGEMENT USING THE WEB CONSOLE

The RHEL 9 web console is a web-based interface for system administration. As one of its features, the web console provides a graphical view of virtual machines (VMs) on the host system, and makes it possible to create, access, and configure these VMs.

Notez que pour utiliser la console web pour gérer vos machines virtuelles sur RHEL 9, vous devez d'abord installer un plug-in de console web pour la virtualisation.

Prochaines étapes

- Pour savoir comment activer la gestion des machines virtuelles dans votre console web, voir Configuration de la console web pour la gestion des machines virtuelles .
- Pour une liste complète des actions de gestion des machines virtuelles proposées par la console web, voir Fonctions de gestion des machines virtuelles disponibles dans la console web .

27.2. SETTING UP THE WEB CONSOLE TO MANAGE VIRTUAL MACHINES

Before using the RHEL 9 web console to manage virtual machines (VMs), you must install the web console virtual machine plug-in on the host.

Conditions préalables

- Ensure that the web console is installed and enabled on your machine.

```
# systemctl status cockpit.socket
cockpit.socket - Cockpit Web Service Socket
```

```
Loaded: loaded (/usr/lib/systemd/system/cockpit.socket
[...]
```

If this command returns **Unit cockpit.socket could not be found**, follow the Installing the web console document to enable the web console.

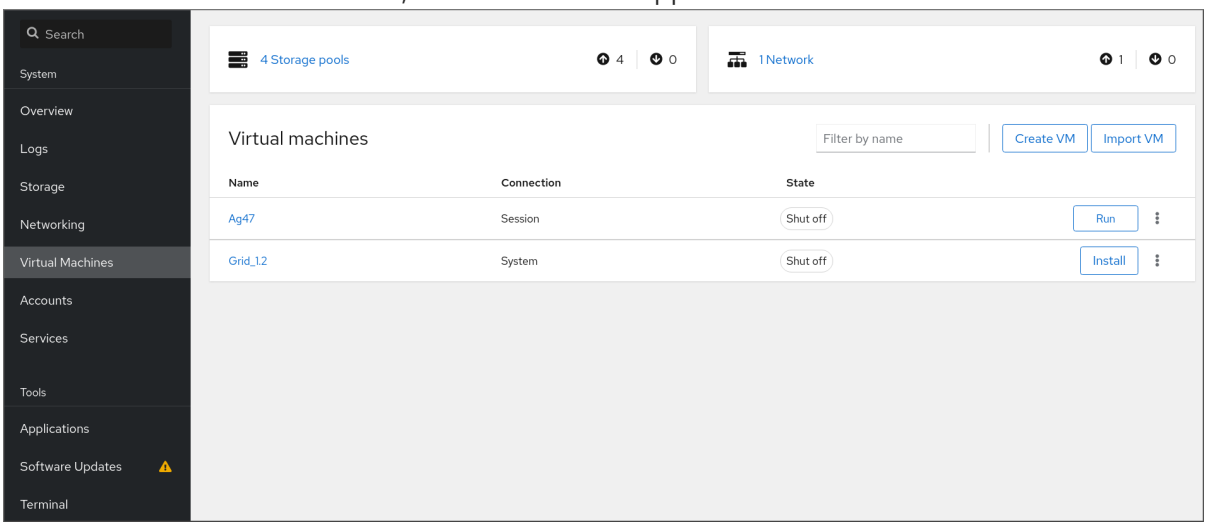
Procédure

- Install the **cockpit-machines** plug-in.

```
# dnf install cockpit-machines
```

Vérification

1. Access the web console, for example by entering the **https://localhost:9090** address in your browser.
2. Log in.
3. If the installation was successful, **Virtual Machines** appears in the web console side menu.



Ressources supplémentaires

- Gestion des systèmes à l'aide de la console web RHEL 9

27.3. RENAMING VIRTUAL MACHINES USING THE WEB CONSOLE

After create a virtual machine (VM), you might wish to rename the VM to avoid conflicts or assign a new unique name based on your use case. You can use the RHEL web console to rename the VM.

Conditions préalables

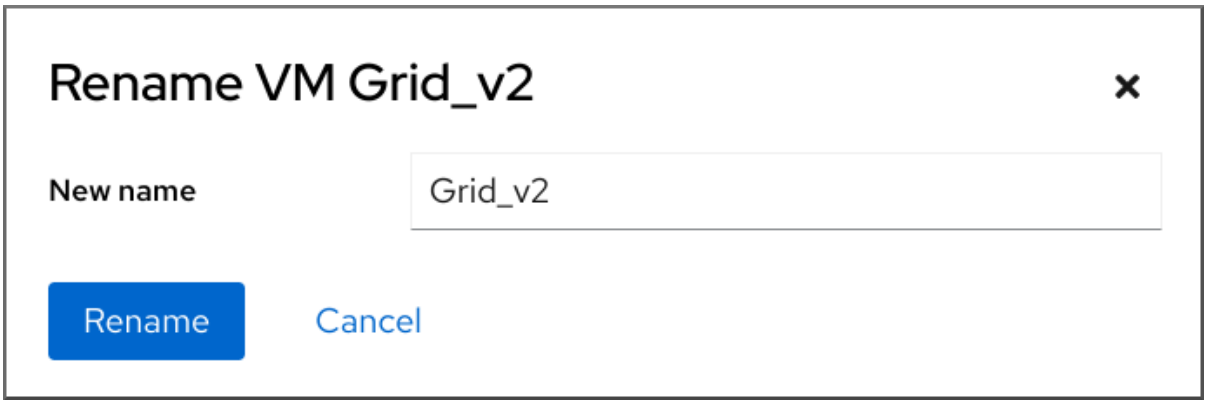
- Le plug-in VM de la console web est installé sur votre système.
- Ensure that the VM is shut down.

Procédure

1. In the **Virtual Machines** interface, click the Menu button ⋮ of the VM that you want to rename.

A drop down menu appears with controls for various VM operations.

2. Click **Rename**.
The Rename a VM dialog appears.



3. In the **New name** field, enter a name for the VM.
4. Click **Rename**.

Vérification

- The new VM name should appear in the **Virtual Machines** interface.

27.4. VIRTUAL MACHINE MANAGEMENT FEATURES AVAILABLE IN THE WEB CONSOLE

Using the RHEL 9 web console, you can perform the following actions to manage the virtual machines (VMs) on your system.

Tableau 27.1. Tâches VM pouvant être effectuées dans la console web RHEL 9

Tâche	Pour plus de détails, voir :
Create a VM and install it with a guest operating system	Créer des machines virtuelles et installer des systèmes d'exploitation invités à l'aide de la console web
Supprimer une VM.	Suppression de machines virtuelles à l'aide de la console web.
Start, shut down, and restart the VM	Démarrage des machines virtuelles à l'aide de la console web et Arrêt et redémarrage des machines virtuelles à l'aide de la console web
Connect to and interact with a VM using a variety of consoles	Interagir avec les machines virtuelles à l'aide de la console web
View a variety of information about the VM	Visualisation des informations sur les machines virtuelles à l'aide de la console web

Tâche	Pour plus de détails, voir :
Adjust the host memory allocated to a VM	Ajouter et supprimer la mémoire d'une machine virtuelle à l'aide de la console web
Manage network connections for the VM	Utilisation de la console web pour gérer les interfaces réseau des machines virtuelles
Manage the VM storage available on the host and attach virtual disks to the VM	Gestion du stockage pour les machines virtuelles
Configure the virtual CPU settings of the VM	Gérer les CPU virtuels à l'aide de la console web
Live migrate a VM	Migration en direct d'une machine virtuelle à l'aide de la console web
Renommer une VM	Renommer des machines virtuelles à l'aide de la console web
Partager des fichiers entre l'hôte et la VM	Partage de fichiers entre l'hôte et ses machines virtuelles
Manage host devices	Gestion des dispositifs virtuels à l'aide de la console web

CHAPITRE 28. GESTION DES SYSTÈMES DISTANTS DANS LA CONSOLE WEB

Connectez-vous aux systèmes distants et gérez-les dans la console web RHEL 9.

Le chapitre suivant décrit :

- La topologie optimale des systèmes connectés.
- Comment ajouter et supprimer des systèmes distants.
- Quand, pourquoi et comment utiliser les clés SSH pour l'authentification des systèmes distants.
- Comment configurer un client de console web pour permettre à un utilisateur authentifié par une carte à puce d'accéder à **SSH** à un hôte distant et d'accéder aux services qui s'y trouvent.

Conditions préalables

- Ouverture du service SSH sur les systèmes distants.

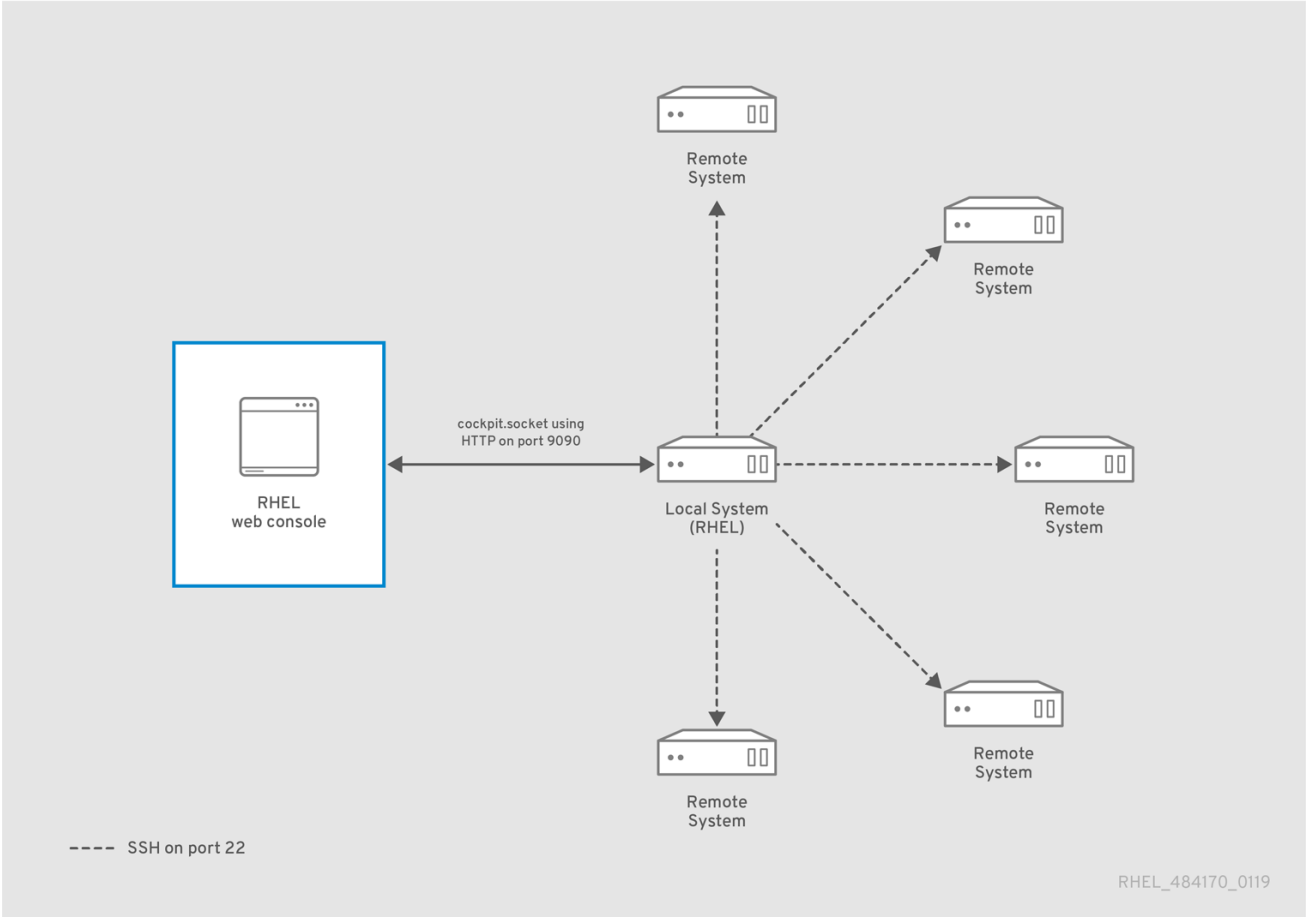
28.1. GESTIONNAIRE DE SYSTÈME À DISTANCE DANS LA CONSOLE WEB

L'utilisation de la console web RHEL 9 pour gérer des systèmes distants sur le réseau nécessite de prendre en compte la topologie des serveurs connectés.

Pour une sécurité optimale, Red Hat recommande la configuration de connexion suivante :

- Utiliser un système avec la console web comme hôte bastion. L'hôte bastion est un système dont le port HTTPS est ouvert.
- Tous les autres systèmes communiquent par SSH.

Lorsque l'interface web fonctionne sur l'hôte bastion, vous pouvez accéder à tous les autres systèmes via le protocole SSH en utilisant le port 22 dans la configuration par défaut.



28.2. AJOUTER DES HÔTES DISTANTS À LA CONSOLE WEB

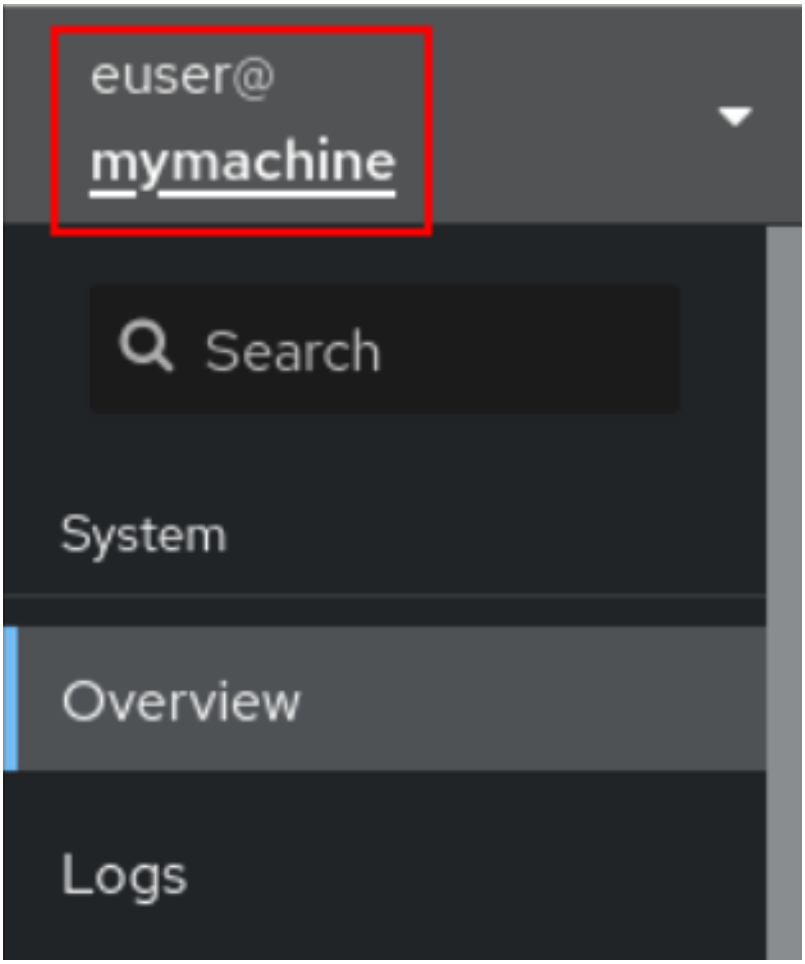
Cette section vous aide à connecter d'autres systèmes à l'aide d'un nom d'utilisateur et d'un mot de passe.

Conditions préalables

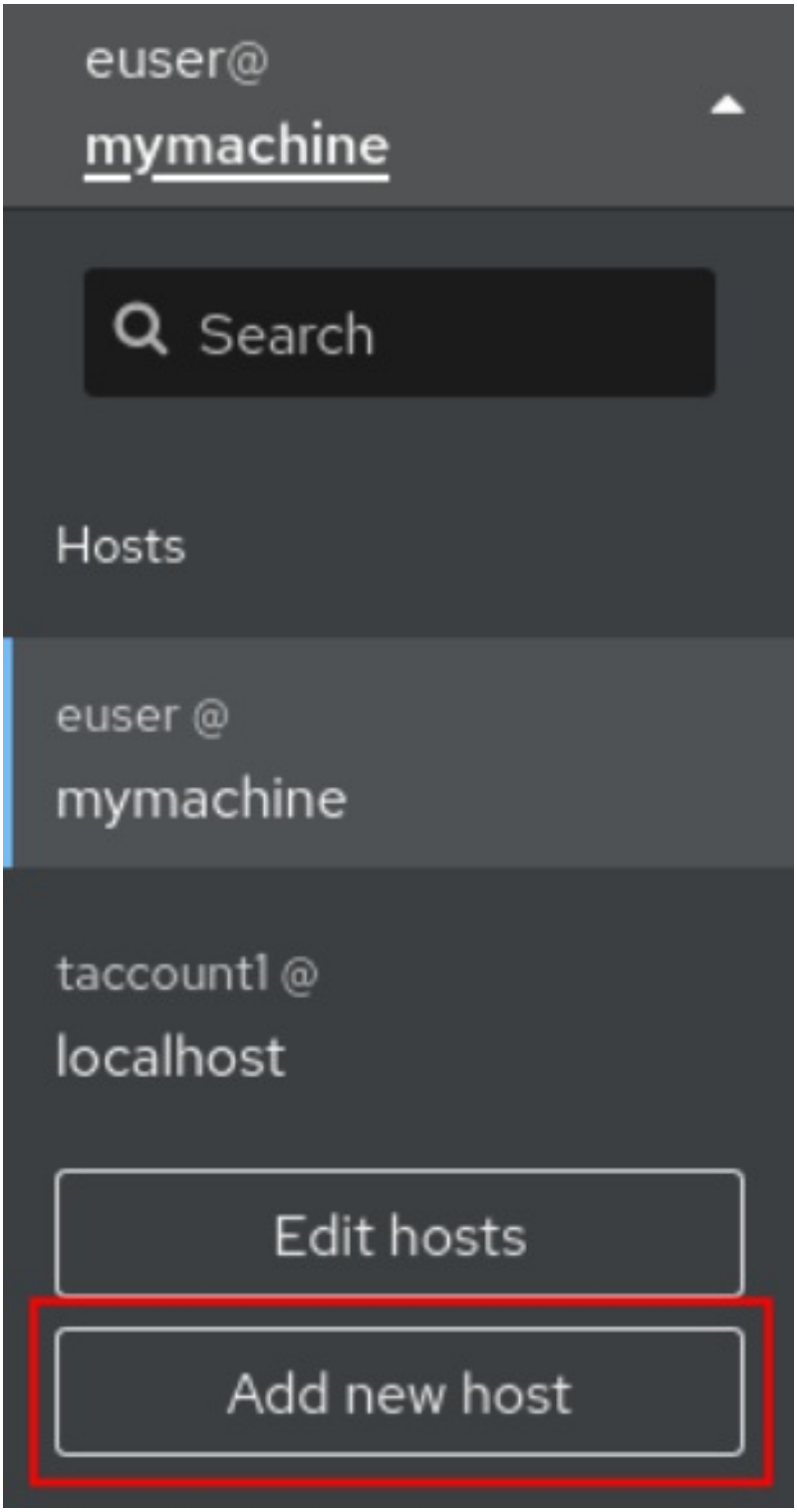
- Vous devez être connecté à la console web avec des privilèges d'administration. Pour plus d'informations, voir Connexion à la console web .

Procédure

1. Dans la console web RHEL 9, cliquez sur votre **username@hostname** dans le coin supérieur gauche de la page **Overview**.



2. Dans le menu déroulant, cliquez sur le bouton **Ajouter un nouvel hôte**.



3. Dans la boîte de dialogue **Add new host**, indiquez l'hôte que vous souhaitez ajouter.

4. (Facultatif) Ajoutez le nom d'utilisateur du compte auquel vous souhaitez vous connecter. Vous pouvez utiliser n'importe quel compte d'utilisateur du système distant. Toutefois, si vous utilisez les informations d'identification d'un compte d'utilisateur ne disposant pas de privilèges d'administration, vous ne pourrez pas effectuer de tâches d'administration.

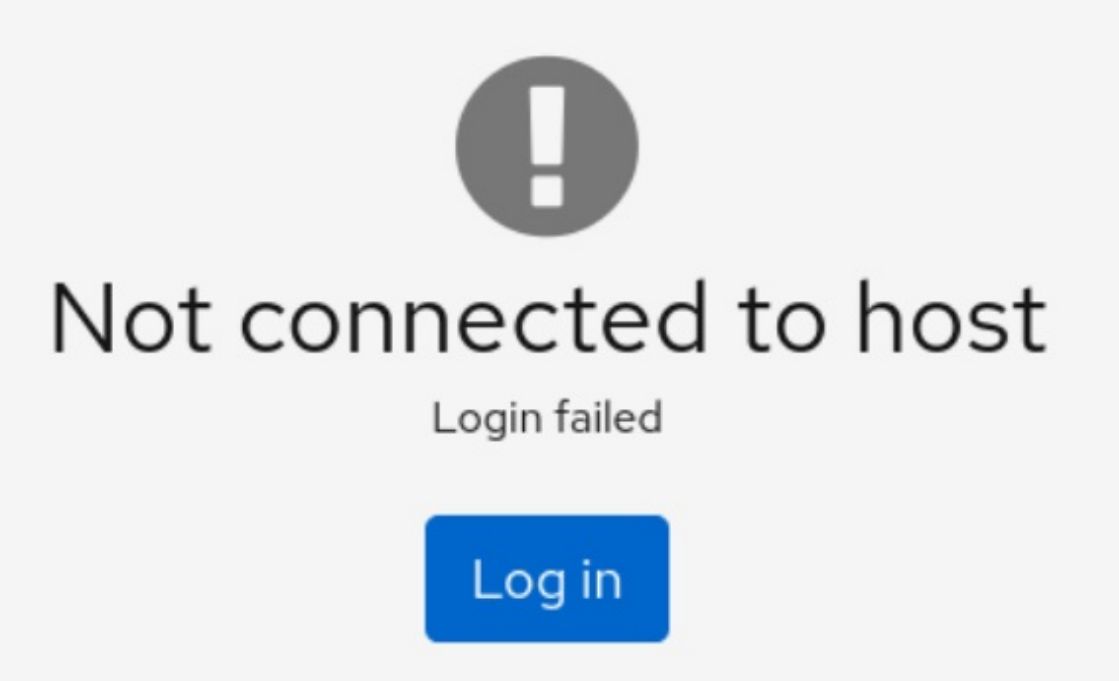
   Si vous utilisez les mêmes informations d'identification que pour votre système local, la console web authentifiera automatiquement les systèmes distants à chaque fois que vous vous connecterez. Toutefois, l'utilisation des mêmes informations d'identification sur plusieurs machines peut constituer un risque potentiel pour la sécurité.

5. (Facultatif) Cliquez sur le champ **Color** pour modifier la couleur du système.

6. Cliquez sur **Add**.
   Le nouvel hôte apparaîtra dans la liste des hôtes dans le menu déroulant **username@hostname**.

NOTE

La console web n'enregistre pas les mots de passe utilisés pour se connecter aux systèmes distants, ce qui signifie que vous devez vous connecter à nouveau après chaque redémarrage du système. La prochaine fois que vous vous connectez, cliquez sur le bouton **Connexion** situé sur l'écran principal du système distant déconnecté pour ouvrir la boîte de dialogue de connexion.



28.3. SUPPRESSION DES HÔTES DISTANTS DE LA CONSOLE WEB

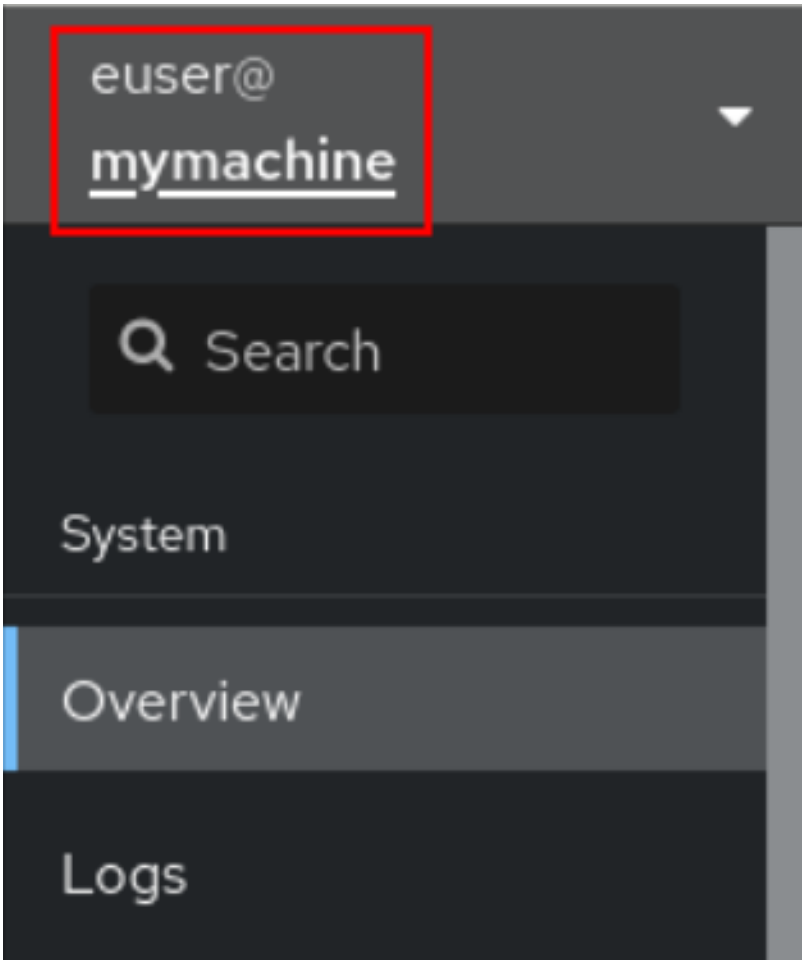
Cette section vous explique comment supprimer d'autres systèmes de la console web.

Conditions préalables

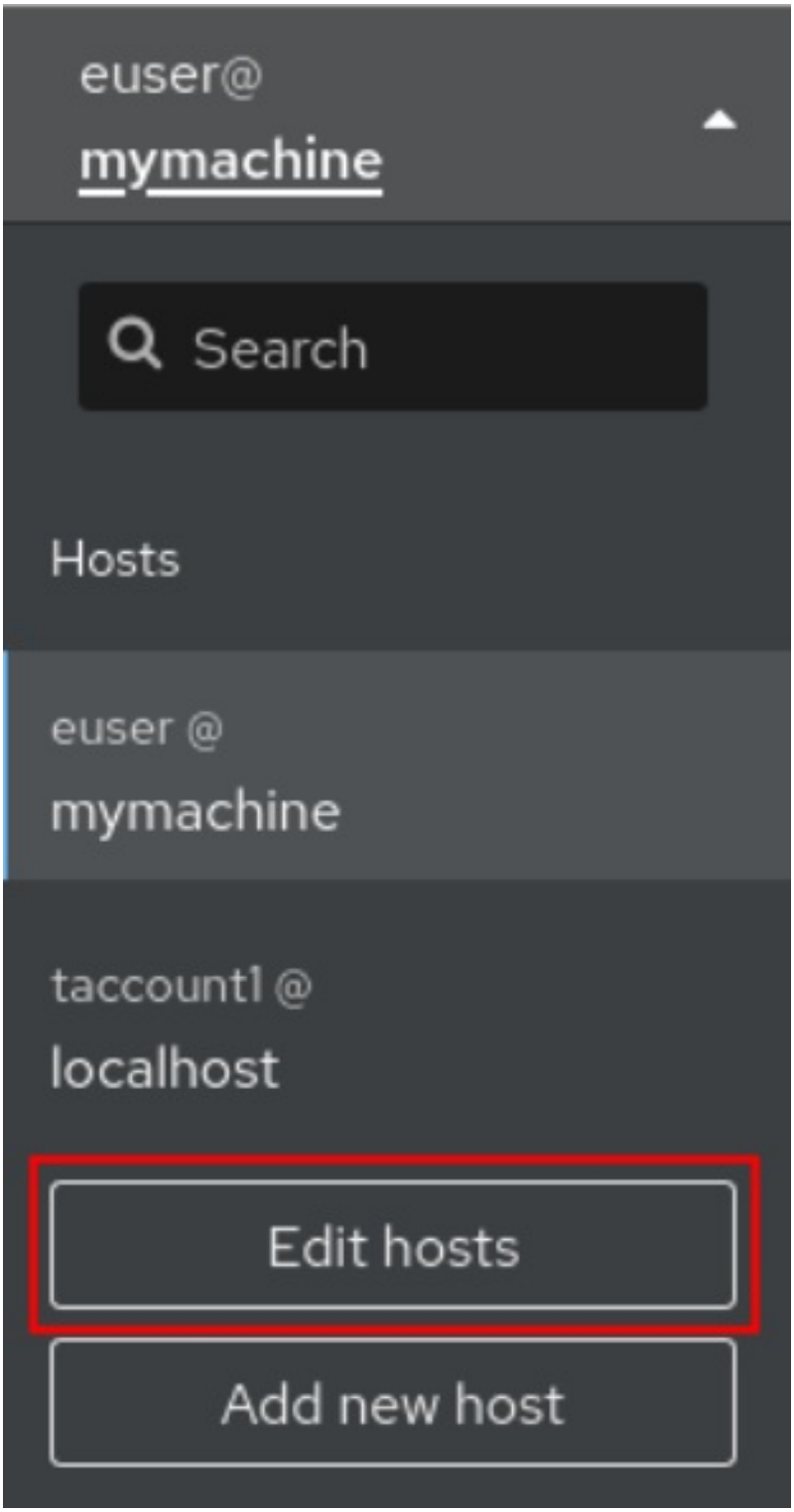
- Ajout de systèmes à distance.
  Pour plus de détails, voir Ajouter des hôtes distants à la console web .
- Vous devez être connecté à la console web avec des privilèges d'administrateur.
  Pour plus de détails, voir Connexion à la console web .

Procédure

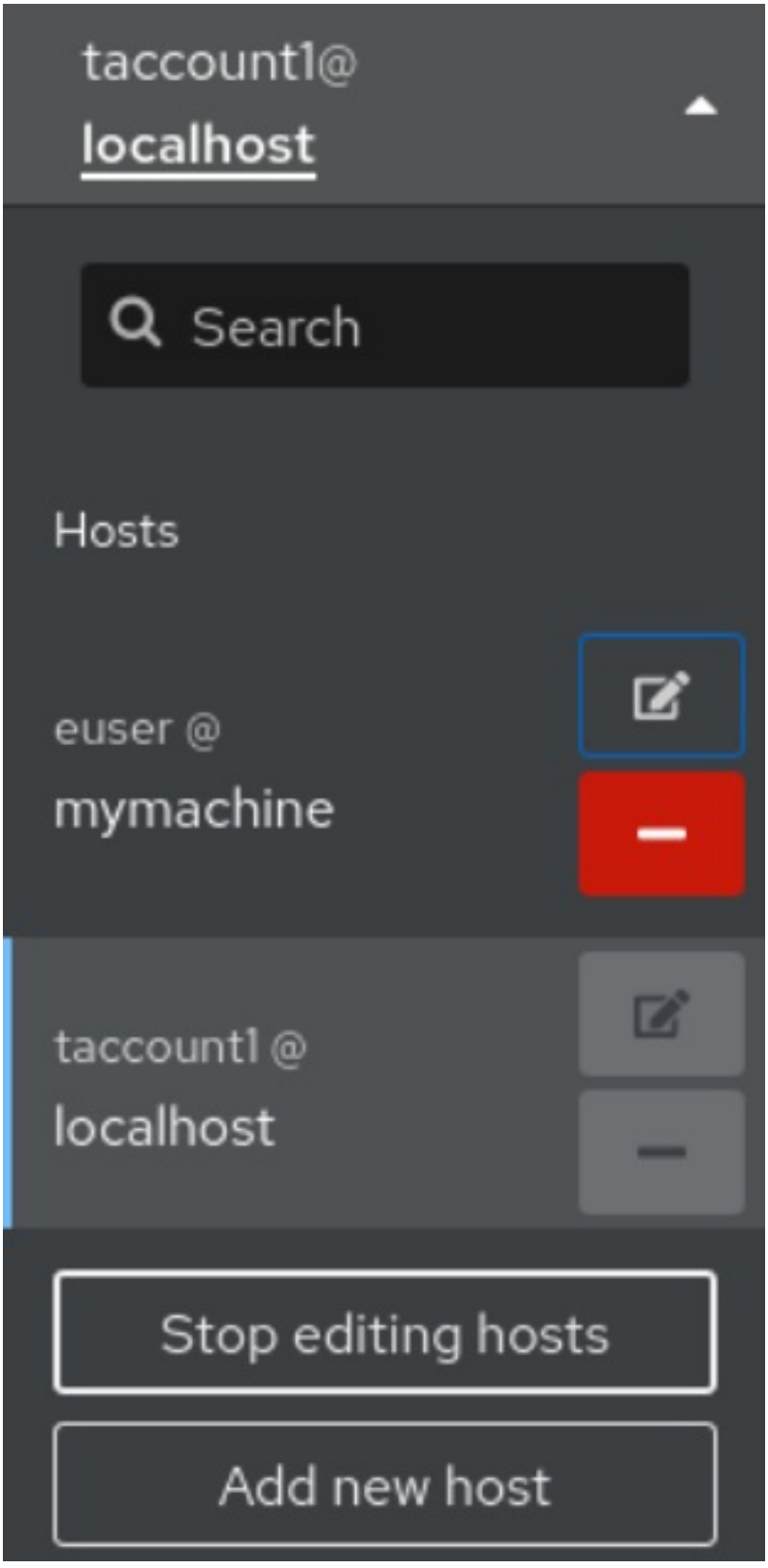
1. Connectez-vous à la console web RHEL 9.
2. Cliquez sur votre **username@hostname** dans le coin supérieur gauche de la page **Overview**.



3. Cliquez sur l'icône **Modifier les hôtes**.



4. Pour supprimer un hôte de la console web, cliquez sur le signe moins rouge **-** à côté de son nom d'hôte. Notez que vous ne pouvez pas supprimer un hôte auquel vous êtes actuellement connecté.



En conséquence, le serveur est supprimé de votre console web.

28.4. ACTIVATION DE LA CONNEXION SSH POUR UN NOUVEL HÔTE

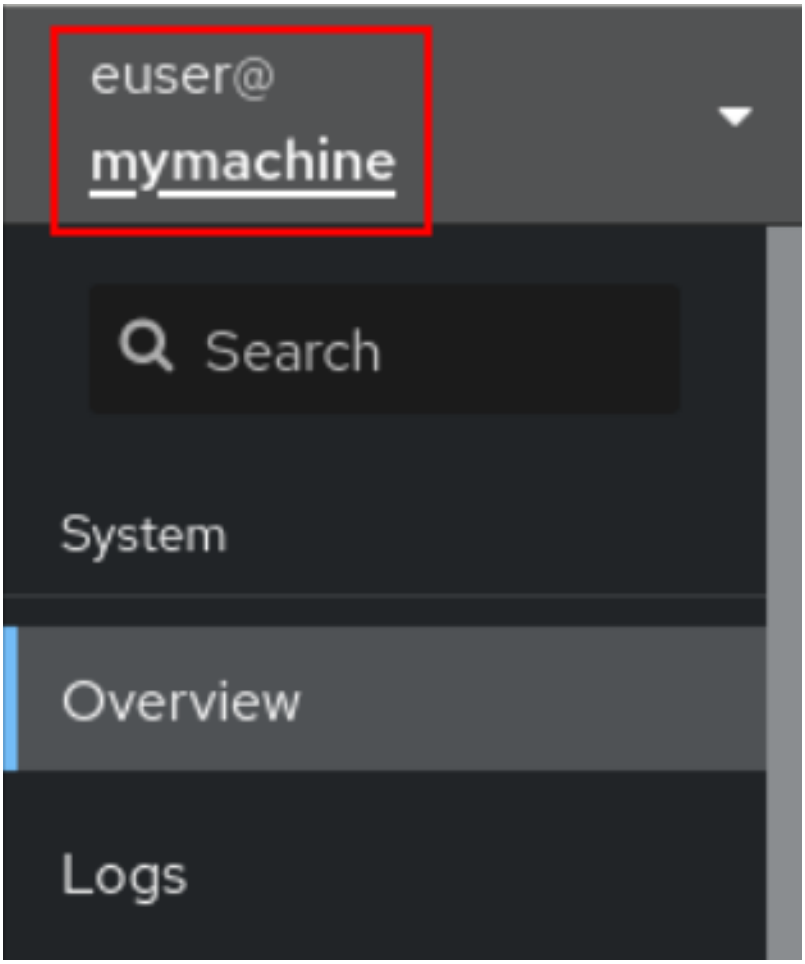
Lorsque vous ajoutez un nouvel hôte, vous pouvez également vous y connecter à l'aide d'une clé SSH. Si vous disposez déjà d'une clé SSH sur votre système, la console web utilisera la clé existante ; sinon, la console web peut créer une clé.

Conditions préalables

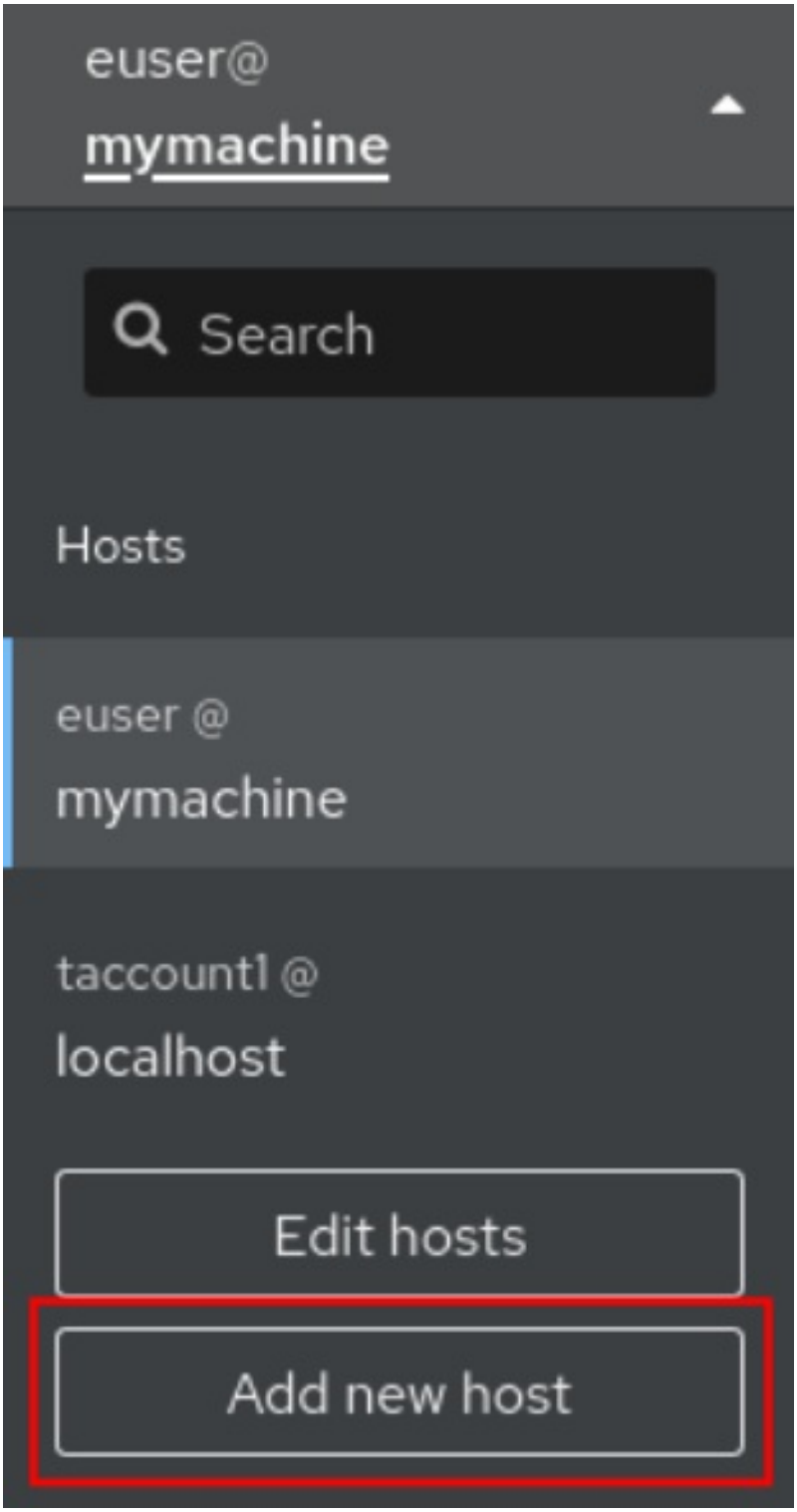
- Vous devez être connecté à la console web avec des privilèges d'administration.
  Pour plus de détails, voir Connexion à la console web .

Procédure

1. Dans la console web RHEL 9, cliquez sur votre **username@hostname** dans le coin supérieur gauche de la page **Overview**.



2. Dans le menu déroulant, cliquez sur le bouton **Ajouter un nouvel hôte**.



3. Dans la boîte de dialogue **Add new host**, indiquez l'hôte que vous souhaitez ajouter.

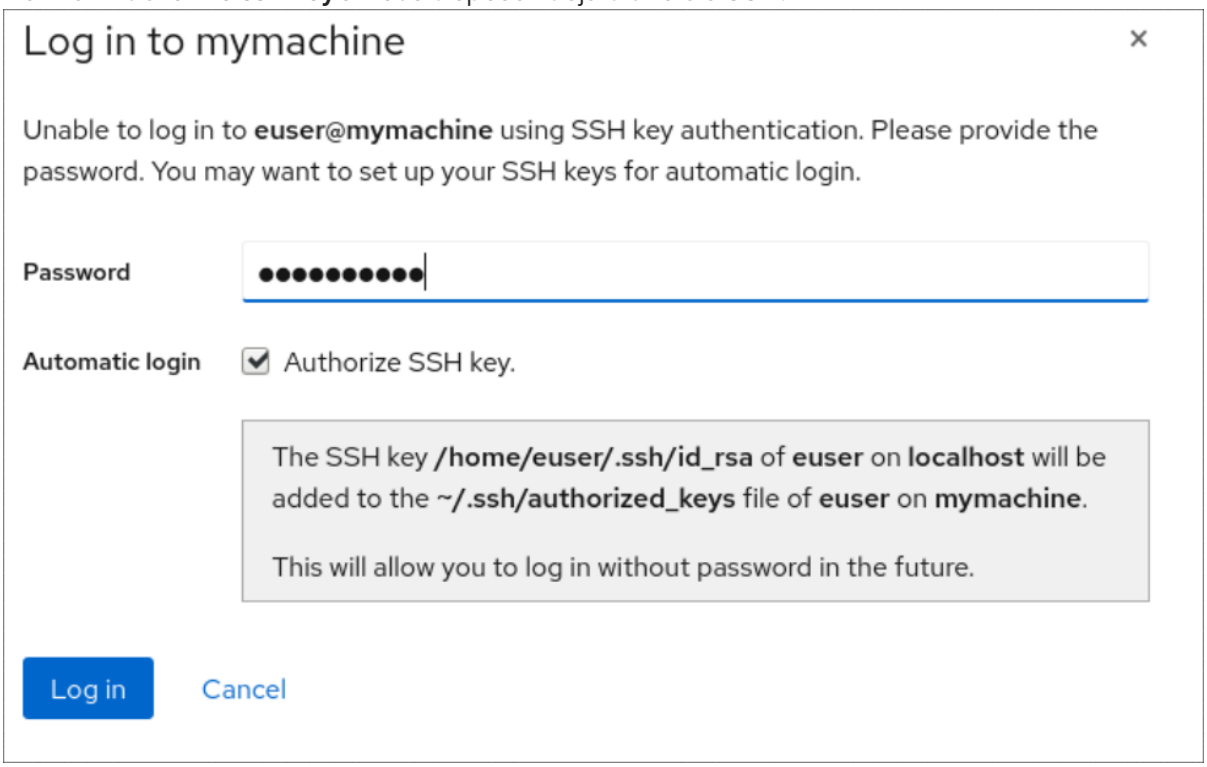
4. Ajoutez le nom d'utilisateur du compte auquel vous souhaitez vous connecter.
   Vous pouvez utiliser n'importe quel compte d'utilisateur du système distant. Toutefois, si vous utilisez les informations d'identification d'un compte d'utilisateur ne disposant pas de privilèges d'administration, vous ne pourrez pas effectuer de tâches d'administration.

5. (Facultatif) Cliquez sur le champ **Color** pour modifier la couleur du système.

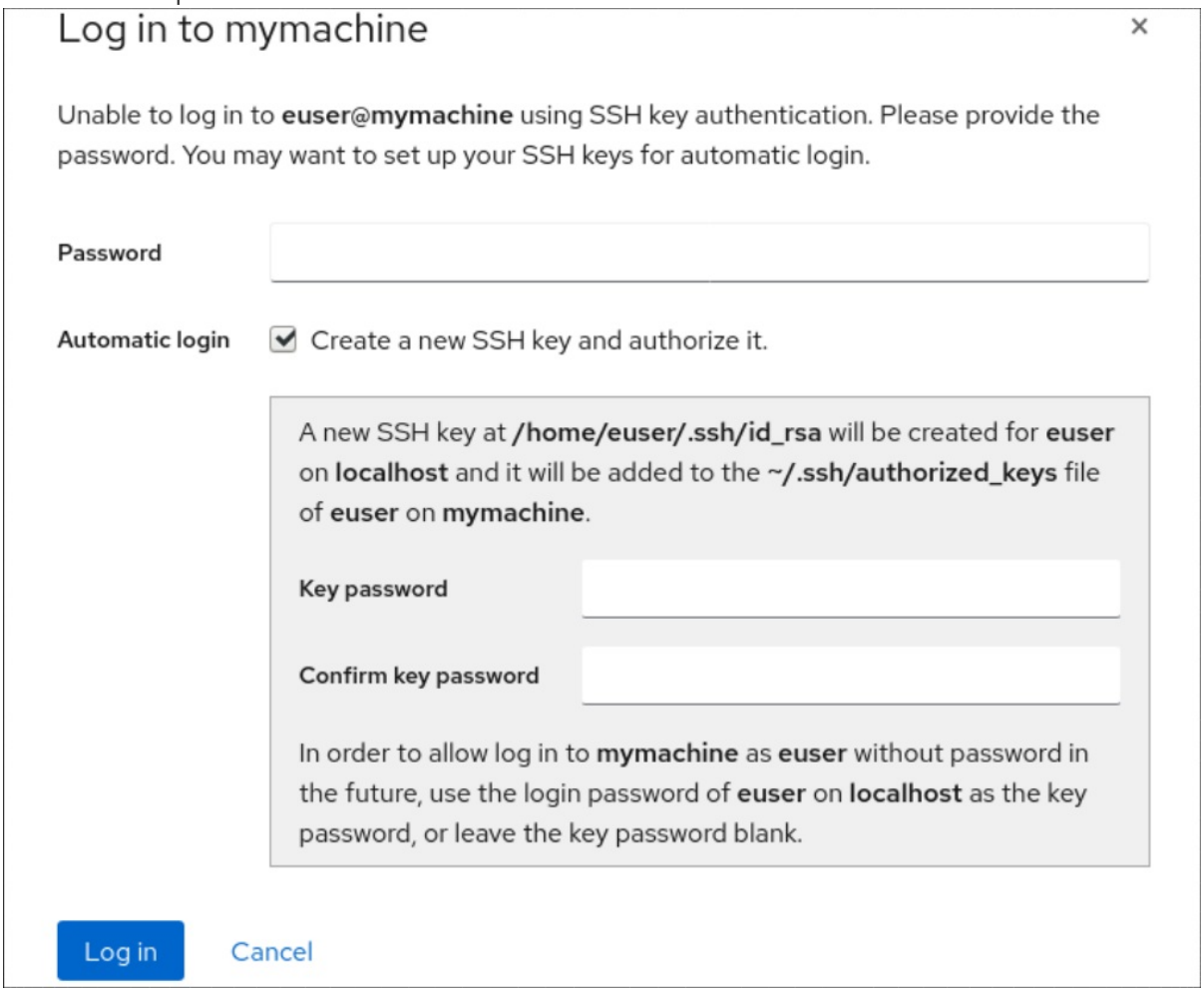
6. Cliquez sur **Add**.
   Une nouvelle fenêtre de dialogue apparaît pour demander un mot de passe.

7. Saisissez le mot de passe du compte utilisateur.

8. Vérifiez **Authorize ssh key** si vous disposez déjà d'une clé SSH.



9. Consultez **Create a new SSH key and authorize it** si vous n'avez pas de clé SSH. La console web la créera pour vous.



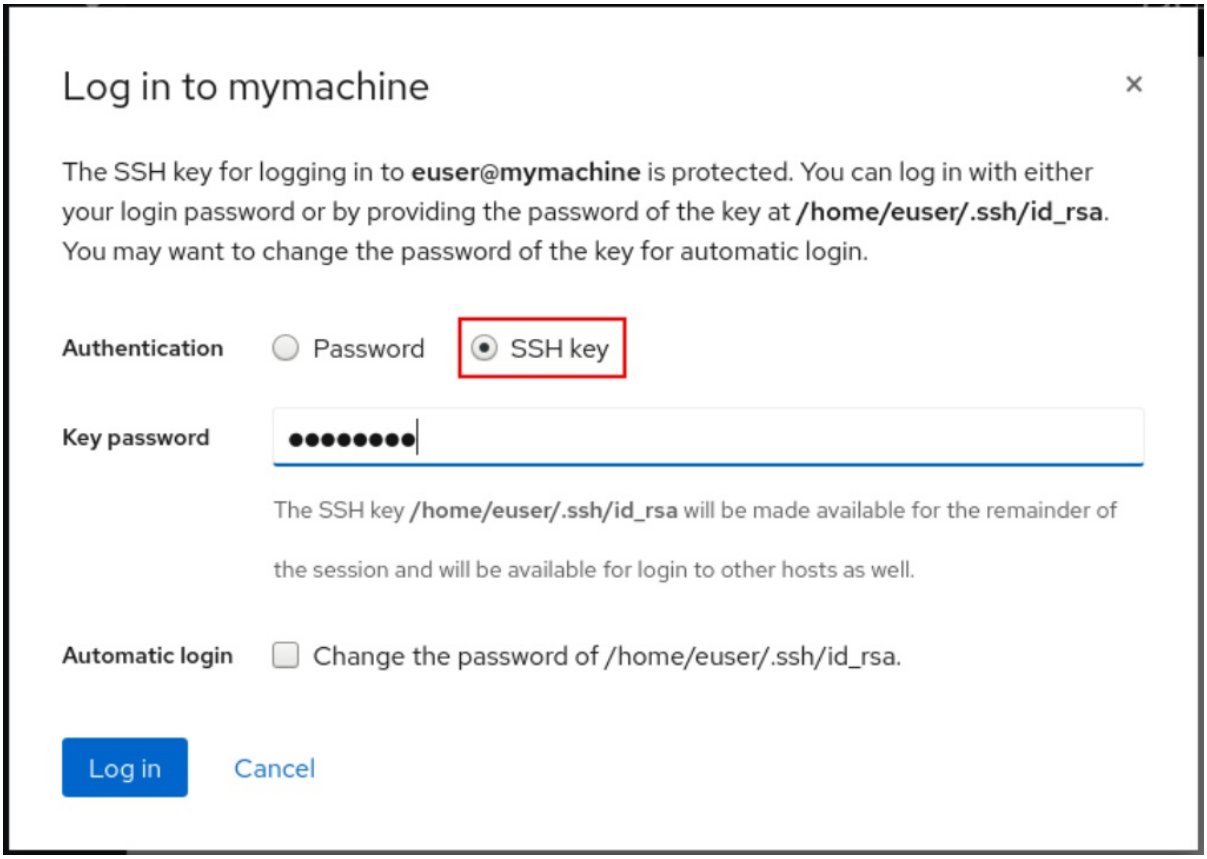
a. Ajouter un mot de passe pour la clé SSH.

b. Confirmer le mot de passe.

10. Cliquez sur **Log in**
Le nouvel hôte apparaîtra dans la liste des hôtes dans le menu déroulant **username@hostname**.

Verification steps

1. Déconnexion.
2. Se reconnecter.
3. Cliquez sur **Log in** dans l'écran **Not connected to host**
4. Sélectionnez **SSH key** comme option d'authentification.



5. Saisissez votre mot de passe clé.
6. Cliquez sur **Log in**.

Ressources supplémentaires

- Utiliser des communications sécurisées entre deux systèmes avec OpenSSH

28.5. DÉLÉGATION CONTRAINTE DANS LA GESTION DE L'IDENTITÉ

L'extension Service for User to Proxy (**S4U2proxy**) fournit un service qui obtient un ticket de service pour un autre service au nom d'un utilisateur. Cette fonctionnalité est connue sous le nom de **constrained delegation**. Le second service est généralement un mandataire qui effectue un travail pour

le compte du premier service, dans le contexte d'autorisation de l'utilisateur. L'utilisation de la délégation sous contrainte élimine la nécessité pour l'utilisateur de déléguer l'intégralité de son ticket d'attribution de ticket (TGT).

La gestion de l'identité (IdM) utilise traditionnellement la fonction Kerberos **S4U2proxy** pour permettre au serveur web d'obtenir un ticket de service LDAP au nom de l'utilisateur. Le système de confiance IdM-AD utilise également la délégation contrainte pour obtenir un principal **cifs**.

Vous pouvez utiliser la fonctionnalité **S4U2proxy** pour configurer un client de console Web afin de permettre à un utilisateur IdM authentifié avec une carte à puce d'effectuer les opérations suivantes :

- Exécuter des commandes avec des privilèges de superutilisateur sur l'hôte RHEL sur lequel le service de console web est exécuté sans qu'il soit demandé de s'authentifier à nouveau.
- Accédez à un hôte distant à l'aide de **SSH** et accédez aux services de l'hôte sans devoir vous authentifier à nouveau.

Ressources supplémentaires

- S4U2proxy
- Délégation sous contrainte de service

28.6. CONFIGURER UNE CONSOLE WEB POUR PERMETTRE À UN UTILISATEUR AUTHENTIFIÉ PAR UNE CARTE À PUCE DE SE CONNECTER EN SSH À UN HÔTE DISTANT SANS AVOIR À S'AUTHENTIFIER À NOUVEAU

Après vous être connecté à un compte d'utilisateur sur la console web RHEL, en tant qu'administrateur du système de gestion des identités (IdM), vous pouvez avoir besoin de vous connecter à des machines distantes en utilisant le protocole **SSH**. Vous pouvez utiliser la fonction de délégation restreinte pour utiliser **SSH** sans devoir vous authentifier à nouveau.

Cette procédure décrit comment configurer la console Web pour qu'elle utilise la délégation restreinte. Dans l'exemple ci-dessous, la session de la console web s'exécute sur l'hôte **myhost.idm.example.com** et est configurée pour accéder à l'hôte **remote.idm.example.com** en utilisant **SSH** au nom de l'utilisateur authentifié.

Conditions préalables

- Vous avez obtenu un ticket d'attribution de ticket (TGT) de l'IdM **admin**.
- **root** Vous avez accès à **remote.idm.example.com**.
- Le service de console web est présent dans l'IdM.
- L'hôte **remote.idm.example.com** est présent dans l'IdM.
- La console web a créé un ticket **S4U2Proxy** Kerberos dans la session de l'utilisateur. Pour vérifier que c'est bien le cas, connectez-vous à la console web en tant qu'utilisateur IdM, ouvrez la page **Terminal** et entrez :

```
$ klist
Ticket cache: FILE:/run/user/1894000001/cockpit-session-3692.ccache
Default principal: user@IDM.EXAMPLE.COM
```

```
Valid starting     Expires           Service principal
07/30/21 09:19:06 07/31/21 09:19:06
HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
07/30/21 09:19:06  07/31/21 09:19:06  krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM
        for client HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
```

Procédure

1. Créez une liste des hôtes cibles auxquels la règle de délégation peut accéder :
   a. Créer une cible de délégation de service :

```
$ ipa servicedelegationtarget-add cockpit-target
```

   b. Ajouter l'hôte cible à la cible de délégation :

```
$ ipa servicedelegationtarget-add-member cockpit-target \ --
principals=host/remote.idm.example.com@IDM.EXAMPLE.COM
```

2. Autoriser les sessions **cockpit** à accéder à la liste des hôtes cibles en créant une règle de délégation de service et en y ajoutant le principal Kerberos du service **HTTP**:
   a. Créer une règle de délégation de service :

```
$ ipa servicedelegationrule-add cockpit-delegation
```

   b. Ajoutez le client de la console web à la règle de délégation :

```
$ ipa servicedelegationrule-add-member cockpit-delegation \ --
principals=HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
```

   c. Ajouter la cible de délégation à la règle de délégation :

```
$ ipa servicedelegationrule-add-target cockpit-delegation \ --
servicedelegationtargets=cockpit-target
```

3. Activer l'authentification Kerberos sur l'hôte **remote.idm.example.com**:
   a. **SSH** à **remote.idm.example.com** comme **root**.
   b. Ouvrez le fichier **/etc/ssh/sshd_config** pour le modifier.
   c. Activez **GSSAPIAuthentication** en décommentant la ligne **GSSAPIAuthentication no** et en la remplaçant par **GSSAPIAuthentication yes**.
4. Redémarrez le service **SSH** sur **remote.idm.example.com** pour que les changements ci-dessus prennent effet immédiatement :

```
$ systemctl try-restart sshd.service
```

Ressources supplémentaires

- Connexion à la console web avec des cartes à puce

- Délégation contrainte dans la gestion de l'identité

28.7. UTILISER ANSIBLE POUR CONFIGURER UNE CONSOLE WEB AFIN DE PERMETTRE À UN UTILISATEUR AUTHENTIFIÉ PAR UNE CARTE À PUCE DE SE CONNECTER EN SSH À UN HÔTE DISTANT SANS AVOIR À S'AUTHENTIFIER À NOUVEAU

Après vous être connecté à un compte d'utilisateur sur la console web RHEL, en tant qu'administrateur du système de gestion des identités (IdM), vous pouvez avoir besoin de vous connecter à des machines distantes en utilisant le protocole **SSH**. Vous pouvez utiliser la fonction de délégation restreinte pour utiliser **SSH** sans devoir vous authentifier à nouveau.

Cette procédure décrit comment utiliser les modules **servicedelegationrule** et **servicedelegationtarget ansible-freeipa** pour configurer une console web afin d'utiliser la délégation contrainte. Dans l'exemple ci-dessous, la session de la console web s'exécute sur l'hôte **myhost.idm.example.com** et est configurée pour accéder à l'hôte **remote.idm.example.com** en utilisant **SSH** au nom de l'utilisateur authentifié.

Conditions préalables

- Le mot de passe de l'IdM **admin**.
- **root** accès à **remote.idm.example.com**.
- Le service de console web est présent dans l'IdM.
- L'hôte **remote.idm.example.com** est présent dans l'IdM.
- La console web a créé un ticket **S4U2Proxy** Kerberos dans la session de l'utilisateur. Pour vérifier que c'est bien le cas, connectez-vous à la console web en tant qu'utilisateur IdM, ouvrez la page **Terminal** et entrez :

```
$ klist
Ticket cache: FILE:/run/user/1894000001/cockpit-session-3692.ccache
Default principal: user@IDM.EXAMPLE.COM

Valid starting     Expires            Service principal
07/30/21 09:19:06 07/31/21 09:19:06
HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
07/30/21 09:19:06  07/31/21 09:19:06  krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM
        for client HTTP/myhost.idm.example.com@IDM.EXAMPLE.COM
```

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.

Procédure

1. Naviguez jusqu'à votre répertoire ***~/MyPlaybooks/*** répertoire :

```
$ cd ~/MyPlaybooks/
```

2. Créez un playbook **web-console-smart-card-ssh.yml** avec le contenu suivant :

   a. Créer une tâche qui assure la présence d'une cible de délégation :

```
---
- name: Playbook to create a constrained delegation target
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Ensure servicedelegationtarget web-console-delegation-target is present
    ipaservicedelegationtarget:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: web-console-delegation-target
```

   b. Ajouter une tâche qui ajoute l'hôte cible à la cible de délégation :

```
  - name: Ensure servicedelegationtarget web-console-delegation-target member
principal host/remote.idm.example.com@IDM.EXAMPLE.COM is present
    ipaservicedelegationtarget:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: web-console-delegation-target
      principal: host/remote.idm.example.com@IDM.EXAMPLE.COM
      action: member
```

   c. Ajouter une tâche qui assure la présence d'une règle de délégation :

```
  - name: Ensure servicedelegationrule delegation-rule is present
    ipaservicedelegationrule:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: web-console-delegation-rule
```

   d. Ajoutez une tâche qui garantit que le principal Kerberos du service client de la console Web est un membre de la règle de délégation contrainte :

```
  - name: Ensure the Kerberos principal of the web console client service is added to the
servicedelegationrule web-console-delegation-rule
    ipaservicedelegationrule:
      ipaadmin_password: "{{ ipaadmin_password }}"
      name: web-console-delegation-rule
      principal: HTTP/myhost.idm.example.com
      action: member
```

   e. Ajouter une tâche qui garantit que la règle de délégation contrainte est associée à la cible de délégation web-console-delegation-target :

```
  - name: Ensure a constrained delegation rule is associated with a specific delegation
```

```
target
  ipaservicedelegationrule:
    ipaadmin_password: "{{ ipaadmin_password }}"
    name: web-console-delegation-rule
    target: web-console-delegation-target
    action: member
```

3. Enregistrer le fichier.

4. Exécutez le playbook Ansible. Spécifiez le fichier du livre de jeu, le fichier contenant le mot de passe protégeant le fichier **secret.yml** et le fichier d'inventaire :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory web-console-smart-card-ssh.yml
```

5. Activer l'authentification Kerberos sur **remote.idm.example.com**:

   a. **SSH** à **remote.idm.example.com** comme **root**.

   b. Ouvrez le fichier **/etc/ssh/sshd_config** pour le modifier.

   c. Activez **GSSAPIAuthentication** en décommentant la ligne **GSSAPIAuthentication no** et en la remplaçant par **GSSAPIAuthentication yes**.

Ressources supplémentaires

- Connexion à la console web avec des cartes à puce
- Délégation contrainte dans la gestion de l'identité
- **README-servicedelegationrule.md** et **README-servicedelegationtarget.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**
- Exemples de playbooks dans les répertoires **/usr/share/doc/ansible-freeipa/playbooks/servicedelegationtarget** et **/usr/share/doc/ansible-freeipa/playbooks/servicedelegationrule**

CHAPITRE 29. CONFIGURATION DE L'AUTHENTIFICATION UNIQUE POUR LA CONSOLE WEB RHEL 9 DANS LE DOMAINE IDM

Apprenez à utiliser l'authentification unique (SSO) fournie par Identity Management (IdM) dans la console web RHEL 9.

Avantages :

- Les administrateurs de domaines IdM peuvent utiliser la console web RHEL 9 pour gérer les machines locales.
- Les utilisateurs disposant d'un ticket Kerberos dans le domaine IdM n'ont pas besoin de fournir d'identifiants de connexion pour accéder à la console web.
- Tous les hôtes connus du domaine IdM sont accessibles via SSH à partir de l'instance locale de la console web RHEL 9.
- La configuration du certificat n'est pas nécessaire. Le serveur web de la console bascule automatiquement sur un certificat émis par l'autorité de certification IdM et accepté par les navigateurs.

Ce chapitre couvre les étapes suivantes pour configurer le SSO pour la connexion à la console web RHEL :

1. Ajouter des machines au domaine IdM à l'aide de la console web RHEL 9.
   Pour plus d'informations, voir Joindre un système RHEL 9 à un domaine IdM à l'aide de la console Web.
2. Si vous souhaitez utiliser Kerberos pour l'authentification, vous devez obtenir un ticket Kerberos sur votre machine.
   Pour plus d'informations, voir Connexion à la console web à l'aide de l'authentification Kerberos .
3. Permet aux administrateurs du serveur IdM d'exécuter n'importe quelle commande sur n'importe quel hôte.
   Pour plus de détails, voir Activation de l'accès sudo aux administrateurs de domaine sur le serveur IdM

Conditions préalables

- La console web RHEL installée sur les systèmes RHEL 9.
  Pour plus de détails, voir Installation de la console web.
- Client IdM installé sur les systèmes dotés de la console web RHEL.
  Pour plus de détails, voir l'installation du client IdM.

29.1. JOINDRE UN SYSTÈME RHEL 9 À UN DOMAINE IDM À L'AIDE DE LA CONSOLE WEB

Vous pouvez utiliser la console Web pour joindre le système Red Hat Enterprise Linux 9 au domaine Identity Management (IdM).

Conditions préalables

- Le domaine IdM est en cours d'exécution et accessible à partir du client que vous souhaitez rejoindre.
- Vous disposez des informations d'identification de l'administrateur du domaine IdM.

Procédure

1. Connectez-vous à la console web RHEL.
   Pour plus de détails, voir Connexion à la console web .
2. Dans le champ **Configuration** de l'onglet **Overview**, cliquez sur **Join Domain**.
3. Dans la boîte de dialogue **Join a Domain**, entrez le nom d'hôte du serveur IdM dans le champ **Domain Address**.
4. Dans le champ **Domain administrator name**, entrez le nom d'utilisateur du compte d'administration IdM.
5. Dans le site **Domain administrator password**, ajoutez un mot de passe.
6. Cliquez sur **Join**.

Verification steps

1. Si la console web RHEL 9 n'a pas affiché d'erreur, le système a été joint au domaine IdM et vous pouvez voir le nom du domaine dans l'écran **System**.
2. Pour vérifier que l'utilisateur est membre du domaine, cliquez sur la page Terminal et tapez la commande **id**:

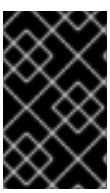
```
$ id
euid=548800004(example_user) gid=548800004(example_user)
groups=548800004(example_user) context=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
```

Ressources supplémentaires

- Planification de la gestion de l'identité
- Installation de la gestion des identités
- Gestion des utilisateurs, des groupes, des hôtes et des règles de contrôle d'accès de l'IdM

29.2. SE CONNECTER À LA CONSOLE WEB EN UTILISANT L'AUTHENTIFICATION KERBEROS

La procédure suivante décrit les étapes à suivre pour configurer le système RHEL 9 afin d'utiliser l'authentification Kerberos.



IMPORTANT

Avec SSO, vous n'avez généralement pas de privilèges administratifs dans la console web. Cela ne fonctionne que si vous avez configuré sudo sans mot de passe. La console web ne demande pas de mot de passe sudo de manière interactive.

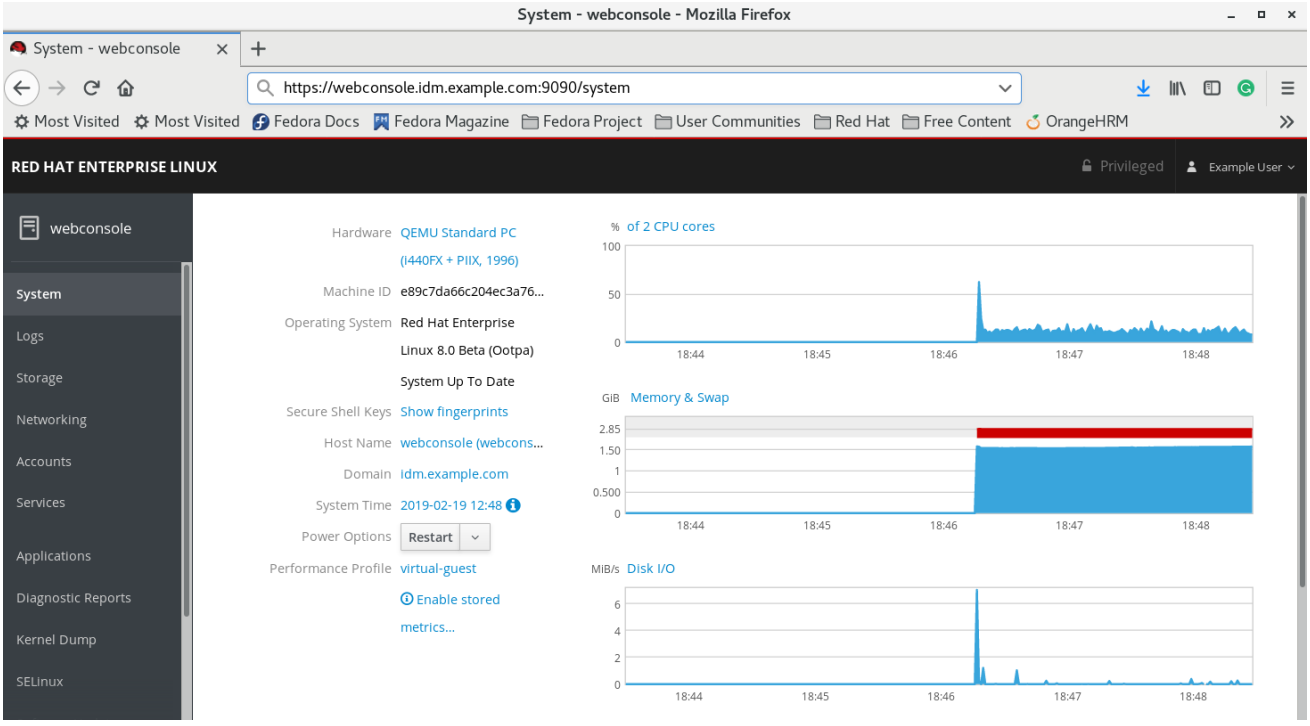
Conditions préalables

- Le domaine IdM fonctionne et est accessible dans l'environnement de votre entreprise. Pour plus d'informations, voir Joindre un système RHEL 9 à un domaine IdM à l'aide de la console Web.
- Activez le service **cockpit.socket** sur les systèmes distants auxquels vous souhaitez vous connecter et les gérer à l'aide de la console Web RHEL. Pour plus de détails, voir Installation de la console web .
- Si le système n'utilise pas de ticket Kerberos géré par le client SSSD, essayez de demander manuellement le ticket à l'aide de l'utilitaire **kinit**.

Procédure

Connectez-vous à la console web RHEL avec l'adresse suivante : **https://dns_name:9090**.

À ce stade, vous êtes connecté avec succès à la console web RHEL et vous pouvez commencer la configuration.



29.3. ACTIVATION DE L'ACCÈS SUDO AUX ADMINISTRATEURS DE DOMAINE SUR LE SERVEUR IDM

La procédure suivante décrit les étapes à suivre pour permettre aux administrateurs de domaine d'exécuter n'importe quelle commande sur n'importe quel hôte du domaine Identity Management (IdM).

Pour ce faire, activez l'accès sudo au groupe d'utilisateurs **admins** créé automatiquement lors de l'installation du serveur IdM.

Tous les utilisateurs ajoutés au groupe **admins** auront un accès sudo si vous exécutez le script **ipa-advise** sur le groupe.

Conditions préalables

- Le serveur utilise IdM 4.7.1 ou une version ultérieure.

Procédure

1. Se connecter au serveur IdM.
2. Exécutez le script ipa-advise :

```
$ ipa-advise enable-admins-sudo | sh -ex
```

Si la console n'affiche pas d'erreur, le groupe **admins** dispose des droits d'administration sur toutes les machines du domaine IdM.

CHAPITRE 30. CONFIGURATION DE L'AUTHENTIFICATION PAR CARTE À PUCE AVEC LA CONSOLE WEB POUR LES UTILISATEURS GÉRÉS DE MANIÈRE CENTRALISÉE

Configurer l'authentification par carte à puce dans la console web RHEL pour les utilisateurs qui sont gérés de manière centralisée par :

- Gestion de l'identité
- Active Directory, qui est relié à la gestion des identités dans le cadre de la confiance inter-forêts

Conditions préalables

- Le système pour lequel vous souhaitez utiliser l'authentification par carte à puce doit être membre d'un domaine Active Directory ou Identity Management.
- Le certificat utilisé pour l'authentification par carte à puce doit être associé à un utilisateur particulier dans Identity Management ou Active Directory.
  Pour plus de détails sur l'association d'un certificat à l'utilisateur dans la gestion des identités, voir Ajouter un certificat à une entrée utilisateur dans l'interface Web Id M ou Ajouter un certificat à une entrée utilisateur dans l'interface CLI IdM.

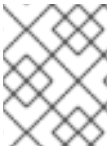
30.1. AUTHENTIFICATION PAR CARTE À PUCE POUR LES UTILISATEURS GÉRÉS DE MANIÈRE CENTRALISÉE

Une carte à puce est un dispositif physique qui peut fournir une authentification personnelle à l'aide de certificats stockés sur la carte. L'authentification personnelle signifie que vous pouvez utiliser les cartes à puce de la même manière que les mots de passe des utilisateurs.

Vous pouvez stocker les informations d'identification de l'utilisateur sur la carte à puce sous la forme d'une clé privée et d'un certificat. Un logiciel et un matériel spécifiques sont utilisés pour y accéder. Vous insérez la carte à puce dans un lecteur ou une prise USB et fournissez le code PIN de la carte à puce au lieu de votre mot de passe.

La gestion des identités (IdM) prend en charge l'authentification par carte à puce avec :

- Certificats d'utilisateur délivrés par l'autorité de certification de l'IdM.
- Certificats d'utilisateur émis par l'autorité de certification Active Directory Certificate Service (ADCS).



NOTE

Si vous souhaitez commencer à utiliser l'authentification par carte à puce, consultez la configuration matérielle requise : Prise en charge des cartes à puce dans RHEL8 .

30.2. INSTALLATION D'OUTILS DE GESTION ET D'UTILISATION DES CARTES À PUCE

Pour configurer votre carte à puce, vous avez besoin d'outils qui peuvent générer des certificats et les stocker sur une carte à puce.

Vous devez :

- Installez le paquet **gnutls-utils**, qui vous aide à gérer les certificats.
- Installez le paquetage **opensc**, qui fournit un ensemble de bibliothèques et d'utilitaires pour travailler avec des cartes à puce.
- Démarrez le service **pcscd**, qui communique avec le lecteur de cartes à puce.

Procédure

1. Installez les paquets **opensc** et **gnutls-utils**:

```
# dnf -y install opensc gnutls-utils
```

2. Démarrez le service **pcscd**.

```
# systemctl start pcscd
```

Vérifiez que le service **pcscd** est opérationnel.

30.3. PRÉPARATION DE VOTRE CARTE À PUCE ET TÉLÉCHARGEMENT DE VOS CERTIFICATS ET CLÉS SUR VOTRE CARTE À PUCE

Cette section décrit la configuration de la carte à puce avec l'outil **pkcs15-init**, qui vous aide à configurer :

- Effacer votre carte à puce
- Définition de nouveaux codes PIN et de clés de déblocage de code PIN (PUK) en option
- Création d'un nouvel emplacement sur la carte à puce
- Stockage du certificat, de la clé privée et de la clé publique dans la fente
- Si nécessaire, verrouiller les paramètres de la carte à puce, car certaines cartes à puce nécessitent ce type de finalisation

NOTE

L'outil **pkcs15-init** peut ne pas fonctionner avec toutes les cartes à puce. Vous devez utiliser les outils qui fonctionnent avec la carte à puce que vous utilisez.

Conditions préalables

- Le paquet **opensc**, qui comprend l'outil **pkcs15-init**, est installé.
  Pour plus de détails, voir Installation des outils de gestion et d'utilisation des cartes à puce .
- La carte est insérée dans le lecteur et connectée à l'ordinateur.
- Vous disposez de la clé privée, de la clé publique et du certificat à stocker sur la carte à puce. Dans cette procédure, **testuser.key**, **testuserpublic.key**, et **testuser.crt** sont les noms utilisés pour la clé privée, la clé publique et le certificat.

- Vous disposez du code PIN de l'utilisateur de votre carte à puce actuelle et du code PIN de l'agent de sécurité (SO-PIN).

Procédure

1. Effacez votre carte à puce et authentifiez-vous avec votre code PIN :

```
$ pkcs15-init --erase-card --use-default-transport-keys
Using reader with a card: Reader name
PIN [Security Officer PIN] required.
Please enter PIN [Security Officer PIN]:
```

   La carte a été effacée.

2. Initialisez votre carte à puce, définissez votre code PIN et PUK d'utilisateur, ainsi que le code PIN et PUK de votre responsable de la sécurité :

```
$ pkcs15-init --create-pkcs15 --use-default-transport-keys \
   --pin 963214 --puk 321478 --so-pin 65498714 --so-puk 784123
Using reader with a card: Reader name
```

   L'outil **pcks15-init** crée un nouvel emplacement sur la carte à puce.

3. Définir l'étiquette et l'ID d'authentification pour l'emplacement :

```
$ pkcs15-init --store-pin --label testuser \
   --auth-id 01 --so-pin 65498714 --pin 963214 --puk 321478
Using reader with a card: Reader name
```

   L'étiquette est définie sur une valeur lisible par l'homme, dans ce cas, **testuser**. L'adresse **auth-id** doit être composée de deux valeurs hexadécimales ; dans ce cas, elle est fixée à **01**.

4. Stockez et étiquetez la clé privée dans le nouvel emplacement de la carte à puce :

```
$ pkcs15-init --store-private-key testuser.key --label testuser_key \
   --auth-id 01 --id 01 --pin 963214
Using reader with a card: Reader name
```

NOTE

La valeur que vous indiquez pour **--id** doit être la même lorsque vous stockez votre clé privée et votre certificat à l'étape suivante. Il est recommandé de spécifier votre propre valeur pour **--id**, sinon l'outil calculera une valeur plus complexe.

5. Stockez et étiquetez le certificat dans le nouvel emplacement de la carte à puce :

```
$ pkcs15-init --store-certificate testuser.crt --label testuser_crt \
   --auth-id 01 --id 01 --format pem --pin 963214
Using reader with a card: Reader name
```

6. (Facultatif) Stockez et étiquetez la clé publique dans le nouvel emplacement de la carte à puce :

```
$ pkcs15-init --store-public-key testuserpublic.key
   --label testuserpublic_key --auth-id 01 --id 01 --pin 963214
Using reader with a card: Reader name
```

NOTE

Si la clé publique correspond à une clé privée ou à un certificat, indiquez le même ID que celui de la clé privée ou du certificat.

7. (Facultatif) Certaines cartes à puce exigent que vous finalisiez la carte en verrouillant les paramètres :

```
$ pkcs15-init -F
```

À ce stade, votre carte à puce comprend le certificat, la clé privée et la clé publique dans l'emplacement nouvellement créé. Vous avez également créé votre code PIN et PUK d'utilisateur ainsi que le code PIN et PUK de l'agent de sécurité.

30.4. ACTIVATION DE L'AUTHENTIFICATION PAR CARTE À PUCE POUR LA CONSOLE WEB

Pour pouvoir utiliser l'authentification par carte à puce dans la console web, activez l'authentification par carte à puce dans le fichier **cockpit.conf**.

En outre, vous pouvez désactiver l'authentification par mot de passe dans le même fichier.

Conditions préalables

- La console web RHEL a été installée.

Procédure

1. Connectez-vous à la console web RHEL avec des privilèges d'administrateur.
2. Cliquez sur **Terminal**.
3. Dans le site **/etc/cockpit/cockpit.conf**, le site **ClientCertAuthentication** est remplacé par le site **yes**:

```
[WebService]
ClientCertAuthentication = yes
```

4. Il est possible de désactiver l'authentification par mot de passe dans **cockpit.conf** avec :

```
[Basic]
action = none
```

Cette configuration désactive l'authentification par mot de passe et vous devez toujours utiliser la carte à puce.

5. Redémarrez la console web pour vous assurer que le site **cockpit.service** accepte la modification :

```
# systemctl restart cockpit
```

30.5. SE CONNECTER À LA CONSOLE WEB AVEC DES CARTES À PUCE

Vous pouvez utiliser des cartes à puce pour vous connecter à la console web.

Conditions préalables

- Un certificat valide stocké dans votre carte à puce et associé à un compte d'utilisateur créé dans un domaine Active Directory ou Identity Management.
- PIN pour déverrouiller la carte à puce.
- La carte à puce a été introduite dans le lecteur.

Procédure

1. Ouvrez votre navigateur web et ajoutez l'adresse de la console web dans la barre d'adresse.
   Le navigateur vous demande d'ajouter le code PIN protégeant le certificat stocké sur la carte à puce.
2. Dans la boîte de dialogue **Password Required**, saisissez le code PIN et cliquez sur **OK**.
3. Dans la boîte de dialogue **User Identification Request**, sélectionnez le certificat stocké dans la carte à puce.
4. Sélectionnez **Remember this decision**.
   Le système n'ouvre pas cette fenêtre la prochaine fois.

   NOTE

   Cette étape ne s'applique pas aux utilisateurs de Google Chrome.
5. Cliquez sur **OK**.

Vous êtes maintenant connecté et la console web affiche son contenu.

30.6. ACTIVATION DE SUDO SANS MOT DE PASSE POUR LES UTILISATEURS DE CARTES À PUCE

Une fois que vous vous êtes connecté à la console web avec un certificat, il se peut que vous deviez passer en mode administratif (privilèges de racine via **sudo**). Si votre compte utilisateur possède un mot de passe, vous pouvez l'utiliser pour vous authentifier sur **sudo**.

Comme alternative, si vous utilisez Red Hat Identity Management, vous pouvez déclarer l'authentification initiale du certificat de la console web comme étant de confiance pour l'authentification à **sudo**, SSH, ou d'autres services. À cette fin, la console Web crée automatiquement un ticket Kerberos S4U2Proxy dans la session de l'utilisateur.

Conditions préalables

- Gestion de l'identité

- Active Directory connecté à la confiance entre les forêts grâce à la gestion des identités
- Carte à puce configurée pour se connecter à la console web. Pour plus d'informations, voir Configuration de l'authentification par carte à puce avec la console web pour les utilisateurs gérés de manière centralisée.

Procédure

1. Définir des règles de délégation des contraintes pour dresser la liste des hôtes auxquels le ticket peut accéder.

   Exemple 30.1. Mise en place de règles de délégation de contraintes

   La session de la console web s'exécute sur l'hôte **host.example.com** et doit être autorisée à accéder à son propre hôte avec **sudo**. De plus, nous ajoutons un deuxième hôte de confiance - **remote.example.com**.

   - Créer la délégation suivante :
     - Exécutez les commandes suivantes pour ajouter une liste de machines cibles auxquelles une règle particulière peut accéder :

       ```
       # ipa servicedelegationtarget-add cockpit-target
       # ipa servicedelegationtarget-add-member cockpit-target \
         --principals=host/host.example.com@EXAMPLE.COM \
         --principals=host/remote.example.com@EXAMPLE.COM
       ```

     - Pour autoriser les sessions de la console web (HTTP/principal) à accéder à cette liste d'hôtes, exécutez les commandes suivantes :

       ```
       # ipa servicedelegationrule-add cockpit-delegation
       # ipa servicedelegationrule-add-member cockpit-delegation \
         --principals=HTTP/host.example.com@EXAMPLE.COM
       # ipa servicedelegationrule-add-target cockpit-delegation \
         --servicedelegationtargets=cockpit-target
       ```

2. Activer l'authentification GSS dans les services correspondants :

   a. Pour sudo, activez le module **pam_sss_gss** dans le fichier **/etc/sssd/sssd.conf**:

      i. En tant que root, ajoutez une entrée pour votre domaine dans le fichier de configuration **/etc/sssd/sssd.conf**.

      ```
      [domain/example.com]
      pam_gssapi_services = sudo, sudo-i
      ```

      ii. Activez le module dans le fichier **/etc/pam.d/sudo** sur la première ligne.

      ```
      auth sufficient pam_sss_gss.so
      ```

   b. Pour SSH, mettez à jour l'option **GSSAPIAuthentication** du fichier **/etc/ssh/sshd_config** en **yes**.

AVERTISSEMENT

Le ticket S4U délégué n'est pas transmis aux hôtes SSH distants lorsque l'on s'y connecte depuis la console web. L'authentification sudo sur un hôte distant avec votre ticket ne fonctionnera pas.

Vérification

1. Connectez-vous à la console web à l'aide d'une carte à puce.
2. Cliquez sur le bouton **Limited access**.
3. Authentifiez-vous à l'aide de votre carte à puce.

OU

1. Essayez de vous connecter à un autre hôte avec SSH.

30.7. LIMITATION DES SESSIONS D'UTILISATEURS ET DE LA MÉMOIRE POUR ÉVITER UNE ATTAQUE DOS

L'authentification par certificat est protégée en séparant et en isolant les instances du serveur web **cockpit-ws** contre les attaquants qui veulent se faire passer pour un autre utilisateur. Cependant, cela introduit un risque d'attaque par déni de service (DoS) : Un attaquant distant pourrait créer un grand nombre de certificats et envoyer un grand nombre de requêtes HTTPS à **cockpit-ws**, chacune utilisant un certificat différent.

Pour éviter ce déni de service, les ressources collectives de ces instances de serveur web sont limitées. Par défaut, les limites du nombre de connexions et de l'utilisation de la mémoire sont fixées à 200 threads et à une limite de mémoire de 75 % (soft) / 90 % (hard).

La procédure suivante décrit la protection des ressources en limitant le nombre de connexions et la mémoire.

Procédure

1. Dans le terminal, ouvrez le fichier de configuration **system-cockpithttps.slice**:

```
# systemctl edit system-cockpithttps.slice
```

2. Limitez les **TasksMax** à *100* et les **CPUQuota** à *30%*:

```
[Slice]
# change existing value
TasksMax=100
# add new restriction
CPUQuota=30%
```

3. Pour appliquer les modifications, redémarrez le système :

```
# systemctl daemon-reload
# systemctl stop cockpit
```

Désormais, les nouvelles limites de mémoire et de session utilisateur protègent le serveur web **cockpit-ws** contre les attaques DoS.

CHAPITRE 31. GESTION DES IMAGES DE CONTENEURS À L'AIDE DE LA CONSOLE WEB RHEL

Vous pouvez utiliser l'interface web de la console web RHEL pour extraire, élaguer ou supprimer vos images de conteneur.

31.1. CONDITIONS PRÉALABLES

- Console web installée et accessible. Voir Installation de la console web et Connexion à la console web.
- Installation du module complémentaire **cockpit-podman**:

```
# dnf install cockpit-podman
```

31.2. EXTRACTION D'IMAGES DE CONTENEURS DANS LA CONSOLE WEB

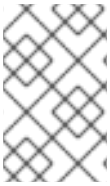
Vous pouvez télécharger des images de conteneurs sur votre système local et les utiliser pour créer vos conteneurs.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Images**, cliquez sur le menu débordant dans le coin supérieur droit et sélectionnez **Download new image**.
3. La boîte de dialogue **Search for an image**apparaît.
4. Dans le champ **Search for**, entrez le nom de l'image ou spécifiez sa description.
5. Dans la liste déroulante **in**, sélectionnez le registre à partir duquel vous souhaitez extraire l'image.
6. Facultatif. Dans le champ **Tag**, entrez la balise de l'image.
7. Cliquez sur **Télécharger**

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Vous pouvez voir l'image nouvellement téléchargée dans le tableau **Images**.



NOTE

Vous pouvez créer un conteneur à partir de l'image téléchargée en cliquant sur **Créer un conteneur** dans le tableau **Images**. Pour créer le conteneur, suivez les étapes 3.-8. de la section Création de conteneurs dans la console Web .

31.3. ÉLAGUER LES IMAGES DE CONTENEURS DANS LA CONSOLE WEB

Vous pouvez supprimer toutes les images inutilisées sur lesquelles aucun conteneur n'est basé.

Conditions préalables

- Au moins une image de conteneur est tirée.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Images**, cliquez sur le menu débordant dans le coin supérieur droit et sélectionnez **Prune unused images**.
3. La fenêtre pop-up avec la liste des images apparaît. Cliquez sur **Prune** pour confirmer votre choix.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Les images supprimées ne doivent pas figurer dans le tableau **Images**.

31.4. SUPPRESSION D'IMAGES DE CONTENEURS DANS LA CONSOLE WEB

Vous pouvez supprimer l'image.

Conditions préalables

- Au moins une image de conteneur est tirée.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Images**, sélectionnez l'image que vous souhaitez supprimer, puis cliquez sur le menu déroulant et sélectionnez **Delete**.
3. La fenêtre pop-up apparaît. Cliquez sur **Delete tagged images** pour confirmer votre choix.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Le conteneur supprimé ne doit pas figurer dans le tableau **Images**.

CHAPITRE 32. GÉRER LES CONTENEURS À L'AIDE DE LA CONSOLE WEB RHEL

Vous pouvez utiliser l'interface web de la console web RHEL pour gérer vos conteneurs et pods. Vous pouvez créer des conteneurs dans la console web RHEL en tant qu'utilisateur non root ou root.

- En tant que *root user*, vous pouvez créer des conteneurs système avec des privilèges et des options supplémentaires.
- En tant qu'utilisateur de *non-root*, vous avez deux possibilités :
  - Connectez-vous à la console web avec *limited privileges*, puis créez des conteneurs d'utilisateurs.
  - Connectez-vous à la console web avec *administrative privileges*, puis vous pouvez créer les deux types de conteneurs - les conteneurs utilisateur et les conteneurs système.

Pour plus de détails sur l'accès limité et l'accès administratif, voir Connexion à la console web . Pour plus d'informations sur les différences entre les conteneurs avec et sans racine, voir Considérations spéciales pour les conteneurs sans racine.

32.1. CONDITIONS PRÉALABLES

- Console web installée et accessible. Voir Installation de la console web et Connexion à la console web.
- Installation du module complémentaire **cockpit-podman**:

```
# dnf install cockpit-podman
```

32.2. CRÉER DES CONTENEURS DANS LA CONSOLE WEB

Vous pouvez créer un conteneur et ajouter des mappages de ports, des volumes, des variables d'environnement, des contrôles de santé, etc.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Cliquez sur **Créer un conteneur**.
3. Dans le champ **Name**, entrez le nom de votre conteneur.
4. Fournissez les informations souhaitées dans l'onglet **Details**.
   - *Available only with the administrative access* : Sélectionnez le propriétaire du conteneur : Système ou Utilisateur.
   - Dans la liste déroulante **Image**, sélectionnez ou recherchez l'image du conteneur dans les registres sélectionnés.
     - Facultatif. Cochez la case **Pull latest image**pour extraire la dernière image du conteneur.

- Le champ **Command** indique la commande. Vous pouvez modifier la commande par défaut si nécessaire.
    - Facultatif. Cochez la case **With terminal** pour exécuter votre conteneur avec un terminal.
- Le champ **Memory limit** indique la limite de mémoire pour le conteneur. Pour modifier la limite de mémoire par défaut, cochez la case et indiquez la limite.
- *Available only for system containers*: Dans le site **CPU shares field**, spécifiez la quantité relative de temps CPU. La valeur par défaut est 1024. Cochez la case pour modifier la valeur par défaut.
- *Available only for system containers*: Dans le menu déroulant **Restart policy**, sélectionnez l'une des options suivantes :
    - Non (valeur par défaut) : Aucune action.
    - En cas d'échec : Redémarre un conteneur en cas d'échec.
    - Toujours : Redémarre le conteneur lorsqu'on le quitte ou après le démarrage du système.

5. Fournissez les informations souhaitées dans l'onglet **Integration**.
    - Cliquez sur **Add port mapping** pour ajouter un mappage de port entre le conteneur et le système hôte.
        - Saisissez l'adresse IP, le port de l'hôte, le port du conteneur et le protocole.
    - Cliquez sur **Ajouter un volume** pour ajouter un volume.
        - Saisissez le chemin d'accès de l'hôte, le chemin d'accès du conteneur. Vous pouvez cocher la case Inscriptible pour créer un volume inscriptible. Dans la liste déroulante SELinux, sélectionnez l'une des options suivantes : Pas d'étiquette, Partagé ou Privé.
    - Cliquez sur **Ajouter une variable** pour ajouter une variable d'environnement.
        - Saisissez la clé et la valeur.
6. Fournissez les informations souhaitées dans l'onglet **Health check**.
    - Dans les champs **Command**, entrez la commande healthcheck.
    - Spécifier les options de contrôle de santé :
        - Intervalle (30 secondes par défaut)
        - Délai d'attente (30 secondes par défaut)
        - Période de démarrage
        - Nombre de tentatives (3 par défaut) pour la commande "Healthcheck"
7. Cliquez sur **Créer et exécuter** pour créer et exécuter le conteneur.

NOTE

Vous pouvez cliquer sur **Créer** pour ne créer que le conteneur.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Vous pouvez voir le nouveau conteneur créé dans le tableau **Containers**.

32.3. INSPECTION DES CONTENEURS DANS LA CONSOLE WEB

Vous pouvez afficher des informations détaillées sur le conteneur.

Conditions préalables

- Un conteneur a été créé.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Cliquez sur l'icône de la flèche **>** pour voir les détails du conteneur.
   - Dans l'onglet **Details**, vous pouvez voir l'ID du conteneur, l'image, la commande, Created (date de création du conteneur) et son état.
     - *Available only for system containers*: Vous pouvez également voir l'adresse IP, l'adresse MAC et l'adresse de la passerelle.
   - Dans l'onglet **Integration**, vous pouvez voir les variables d'environnement, les mappages de ports et les volumes.
   - Dans l'onglet **Log**, vous pouvez voir les journaux des conteneurs.
   - Dans l'onglet **Console**, vous pouvez interagir avec le conteneur à l'aide de la ligne de commande.

32.4. CHANGER L'ÉTAT DES CONTENEURS DANS LA CONSOLE WEB

Vous pouvez modifier le statut du conteneur.

Conditions préalables

- Un conteneur a été créé.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Containers**, sélectionnez le conteneur que vous souhaitez modifier et cliquez sur le menu de débordement pour sélectionner l'action que vous souhaitez effectuer :
   - **Start**
   - **Stop**
   - **Force stop**
   - **Restart**

- **Force restart**
- **Pause**
- **Rename**

32.5. COMMITER DES CONTENEURS DANS LA CONSOLE WEB

Vous pouvez créer une nouvelle image basée sur l'état actuel du conteneur.

Conditions préalables

- Un conteneur a été créé.

Procédure

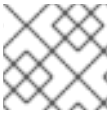
1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Containers**, sélectionnez le conteneur que vous souhaitez modifier, puis cliquez sur le menu de débordement et sélectionnez **Commit**.
3. Dans le formulaire **Commit container**, ajoutez les détails suivants :
   - Dans le champ **New image name**, saisissez le nom de l'image.
   - Facultatif : dans le champ **Tag**, saisissez la balise.
   - Facultatif : dans le champ **Author**, saisissez votre nom.
   - Facultatif : dans le champ **Command**, modifiez la commande si nécessaire.
   - Optionnel : Cochez les options dont vous avez besoin :
     - Mise en pause du conteneur lors de la création de l'image : Le conteneur et ses processus sont mis en pause pendant la création de l'image.
     - Use legacy Docker format : si vous n'utilisez pas le format d'image Docker, c'est le format OCI qui est utilisé.
4. Cliquez sur **Commit**.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Vous pouvez voir l'image nouvellement créée dans le tableau **Images**.

32.6. CRÉATION D'UN POINT DE CONTRÔLE DE CONTENEUR DANS LA CONSOLE WEB

À l'aide de la console web, vous pouvez définir un point de contrôle sur un conteneur en cours d'exécution ou une application individuelle et stocker son état sur le disque.



NOTE

La création d'un point de contrôle n'est disponible que pour les conteneurs système.

Conditions préalables

- Un conteneur est en cours d'exécution.

Procédure

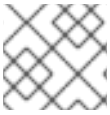
1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Containers**, sélectionnez le conteneur que vous souhaitez modifier et cliquez sur le menu de l'icône de débordement et sélectionnez **Checkpoint**.
3. Facultatif. Dans le formulaire **Checkpoint container**, cochez les options dont vous avez besoin :
   - Keep all temporary checkpoint files : conserver tous les fichiers temporaires de logs et de statistiques créés par CRIU pendant le checkpoint. Ces fichiers ne sont pas supprimés en cas d'échec du point de contrôle, afin de permettre un débogage ultérieur.
   - Leave running after writing checkpoint to disk : laisser le conteneur fonctionner après l'écriture du point de contrôle au lieu de l'arrêter.
   - Prise en charge de la préservation des connexions TCP établies
4. Cliquez sur **Point de contrôle**.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Sélectionnez le conteneur que vous avez contrôlé, cliquez sur l'icône du menu de débordement et vérifiez qu'il y a une option **Restore**.

32.7. RESTAURATION D'UN POINT DE CONTRÔLE DE CONTENEUR DANS LA CONSOLE WEB

Vous pouvez utiliser les données sauvegardées pour restaurer le conteneur après un redémarrage à l'endroit même où il a été contrôlé.



NOTE

La création d'un point de contrôle n'est disponible que pour les conteneurs système.

Conditions préalables

- Un conteneur a été contrôlé.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Containers**, sélectionnez le conteneur que vous souhaitez modifier, puis cliquez sur le menu de débordement et sélectionnez **Restore**.
3. Facultatif. Dans le formulaire **Restore container**, cochez les options dont vous avez besoin :

- Conserver tous les fichiers de points de contrôle temporaires : Keep all temporary log and statistics files created by CRIU during checkpointing. Ces fichiers ne sont pas supprimés en cas d'échec du point de contrôle, afin de permettre un débogage ultérieur.
- Restauration avec des connexions TCP établies
- Ignorer l'adresse IP si elle est définie de manière statique : Si le conteneur a été démarré avec une adresse IP, le conteneur restauré tente également d'utiliser cette adresse IP et la restauration échoue si cette adresse IP est déjà utilisée. Cette option est applicable si vous avez ajouté le mappage de port dans l'onglet Intégration lors de la création du conteneur.
- Ignorer l'adresse MAC si elle est définie de manière statique : Si le conteneur a été démarré avec une adresse MAC, le conteneur restauré tente également d'utiliser cette adresse MAC et la restauration échoue si cette adresse MAC est déjà utilisée.

4. Cliquez sur **Restaurer**.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Vous pouvez voir que le conteneur restauré dans la table **Containers** est en cours d'exécution.

32.8. SUPPRESSION DE CONTENEURS DANS LA CONSOLE WEB

Vous pouvez supprimer le conteneur.

Conditions préalables

- Un conteneur existe.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Containers**, sélectionnez le conteneur que vous souhaitez supprimer, puis cliquez sur le menu de débordement et sélectionnez **Delete**.
3. La fenêtre pop-up apparaît. Cliquez sur **Delete** pour confirmer votre choix.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Le conteneur supprimé ne doit pas figurer dans le tableau **Containers**.

32.9. CRÉATION DE PODS DANS LA CONSOLE WEB

Vous pouvez créer des pods dans l'interface de la console web RHEL.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Cliquez sur **Créer un pod**.
3. Fournissez les informations souhaitées dans le formulaire **Create pod**:

- *Available only with the administrative access* : Sélectionnez le propriétaire du conteneur : Système ou Utilisateur.
- Dans le champ **Name**, entrez le nom de votre conteneur.
- Cliquez sur **Add port mapping** pour ajouter un mappage de port entre le conteneur et le système hôte.
  - Saisissez l'adresse IP, le port de l'hôte, le port du conteneur et le protocole.
- Cliquez sur **Ajouter un volume** pour ajouter un volume.
  - Saisissez le chemin d'accès de l'hôte, le chemin d'accès du conteneur. Vous pouvez cocher la case Inscriptible pour créer un volume inscriptible. Dans la liste déroulante SELinux, sélectionnez l'une des options suivantes : Pas d'étiquette, Partagé ou Privé.

4. Cliquez sur **Créer**.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Vous pouvez voir le nouveau pod créé dans le tableau **Containers**.

32.10. CRÉER DES CONTENEURS DANS LE POD DANS LA CONSOLE WEB

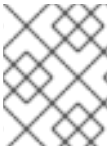
Vous pouvez créer un conteneur dans un pod.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Cliquez sur **Créer un conteneur dans un pod**.
3. Suivez les étapes 3.-8. dans Création de conteneurs dans la console web .

NOTE

Le propriétaire d'un conteneur est le même que celui d'un pod.



NOTE

Dans le module, vous pouvez inspecter les conteneurs, modifier leur état, les valider ou les supprimer.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Vous pouvez voir le nouveau conteneur créé dans le pod sous le tableau **Containers**.

32.11. CHANGER L'ÉTAT DES PODS DANS LA CONSOLE WEB

Vous pouvez modifier le statut du pod.

Conditions préalables

- Une nacelle a été créée.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Containers**, sélectionnez le pod que vous souhaitez modifier et cliquez sur le menu déroulant pour sélectionner l'action que vous souhaitez effectuer :
   - **Start**
   - **Stop**
   - **Force stop**
   - **Restart**
   - **Force restart**
   - **Pause**

32.12. SUPPRESSION DE PODS DANS LA CONSOLE WEB

Vous pouvez supprimer le pod.

Conditions préalables

- Une nacelle existe.

Procédure

1. Cliquez sur **Podman containers** dans le menu principal.
2. Dans le tableau **Containers**, sélectionnez le module que vous souhaitez supprimer, cliquez sur le menu déroulant et sélectionnez **Delete**.
3. La fenêtre pop-up apparaît. Cliquez sur **Delete** pour confirmer votre choix.

AVERTISSEMENT

Tous les conteneurs d'une nacelle seront enlevés.

Vérification

- Cliquez sur **Podman containers** dans le menu principal. Le pod supprimé ne doit pas figurer dans le tableau **Containers**.