Red Hat Enterprise Linux 9

RHEL 9 웹 콘솔을 사용하여 시스템 관리

Guide

Last Updated: 2022-07-03

Red Hat Enterprise Linux 9 RHEL 9 웹 콘솔을 사용하여 시스템 관리

Guide

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

법적 공지

초록

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서, 웹 속성에서 문제가 있는 용어를 교체하기 위해 최선을 다하고 있습니다. 먼저 마스터(master), 슬레이브(slave), 블랙리스트(blacklist), 화이트리스트(whitelist) 등 네 가지 용어를 교체하고 있습니다. 이러한 변경 작업은 작업 범위가 크므로 향후 여러 릴리스에 걸쳐 점차 구현할 예정입니다. 자세한 내용은 CTO Chris Wright의 메시지 를 참조하십시오.

RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견을 보내 주십시오. 문서를 개선할 수 있는 방법에 관해 알려주십시오.

- 특정 문구에 대한 간단한 의견 작성 방법은 다음과 같습니다.
  1. 문서가 *Multi-page HTML* 형식으로 표시되는지 확인합니다. 또한 문서 오른쪽 상단에 피드백 버튼이 있는지 확인합니다.
  2. 마우스 커서를 사용하여 주석 처리하려는 텍스트 부분을 강조 표시합니다.
  3. 강조 표시된 텍스트 아래에 표시되는 피드백 추가 팝업을 클릭합니다.
  4. 표시된 지침을 따릅니다.
- Bugzilla를 통해 피드백을 제출하려면 새 티켓을 생성하십시오.
  1. Bugzilla 웹 사이트로 이동하십시오.
  2. 구성 요소로 문서를 사용합니다.
  3. 설명 필드에 문서 개선을 위한 제안 사항을 기입하십시오. 관련된 문서의 해당 부분 링크를 알려주십시오.
  4. 버그 제출을 클릭합니다.

1장. RHEL 웹 콘솔 사용하기

Red Hat Enterprise Linux 9에 웹 콘솔을 설치하고 RHEL 9 웹 콘솔에서 원격 호스트를 추가하고 모니터링하는 방법을 알아봅니다.

사전 요구 사항

- Red Hat Enterprise Linux 9 설치.
- 네트워킹이 활성화되어 있습니다.
- 적절한 서브스크립션이 첨부된 등록된 시스템입니다.

1.1. RHEL 웹 콘솔이란 무엇입니까?

RHEL 웹 콘솔은 로컬 시스템뿐만 아니라 네트워크 환경에 있는 Linux 서버를 관리하고 모니터링하도록 설계된 Red Hat Enterprise Linux 웹 기반 인터페이스입니다.

RHEL 웹 콘솔을 사용하면 다음과 같은 다양한 관리 작업을 수행할 수 있습니다.

- 서비스 관리
- 사용자 계정 관리
- 시스템 서비스 관리 및 모니터링
- 네트워크 인터페이스 및 방화벽 구성
- 시스템 로그 검토
- 가상 머신 관리
- 진단 보고서 생성
- 커널 덤프 구성 설정
- SELinux 구성
- 소프트웨어 업데이트
- 시스템 서브스크립션 관리

RHEL 웹 콘솔은 터미널에서와 동일한 시스템 API를 사용하며 터미널에서 수행된 작업은 RHEL 웹 콘솔에 즉시 반영됩니다.

네트워크 환경에서 시스템 로그와 성능이 그래프로 표시되는 것을 모니터링할 수 있습니다. 또한 웹 콘솔에서 직접 또는 터미널을 통해 설정을 직접 변경할 수 있습니다.

1.2. 웹 콘솔 설치 및 활성화

RHEL 9 웹 콘솔에 액세스하려면 먼저 **cockpit.socket** 서비스를 활성화합니다.

Red Hat Enterprise Linux 9에는 다양한 설치 변형에 기본적으로 설치된 RHEL 9 웹 콘솔이 포함되어 있습니다. 시스템에 없는 경우 cockpit **.socket** 서비스를 활성화하기 전에 **cockpit** 패키지를 설치합니다.

절차

1. 웹 콘솔이 설치 변형에 기본적으로 설치되지 않은 경우 **cockpit** 패키지를 수동으로 설치합니다.

```
# dnf install cockpit
```

2. 웹 서버를 실행하는 **cockpit.socket** 서비스를 활성화하고 시작합니다.

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

3. 웹 콘솔이 기본적으로 설치 변형에 설치되지 않고 사용자 지정 방화벽 프로필을 사용하는 경우 **cockpit** 서비스를 **firewalld** 에 추가하여 방화벽에서 포트 9090을 엽니다.

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

검증 단계

- 이전 설치 및 구성을 확인하려면 웹 콘솔을 엽니다.

1.3. 웹 콘솔에 로그인

시스템 사용자 이름과 암호를 사용하여 RHEL 웹 콘솔에 처음 로그인하려면 이 절차의 단계를 사용합니다.

사전 요구 사항

- 웹 콘솔을 여는 데 다음 브라우저 중 하나를 사용하십시오.
  - Mozilla Firefox 52 이상
  - Google Chrome 57 이상
  - Microsoft Edge 16 이상
- 시스템 사용자 계정 자격 증명
  RHEL 웹 콘솔은 **/etc/pam.d/cockpit** 에 있는 특정 PAM 스택을 사용합니다. PAM을 사용한 인증을 사용하면 시스템의 모든 로컬 계정의 사용자 이름 및 암호를 사용하여 로그인할 수 있습니다.

절차

1. 웹 브라우저에서 웹 콘솔을 열고 다음 주소를 입력합니다.

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

참고

이렇게 하면 로컬 머신의 로그가 기록됩니다. 원격 시스템의 웹 콘솔에 로그인하려면 다음을 참조하십시오. 1.4절. "원격 머신에서 웹 콘솔에 연결"

자체 서명된 인증서를 사용하는 경우 브라우저가 경고를 발행합니다. 인증서를 확인하고 로그인을 계속하려면 보안 예외를 수락합니다.

콘솔은 **/etc/cockpit/ws-certs.d** 디렉터리에서 인증서를 로드하고 알파벳순으로 **.cert** 확장자가 있는 마지막 파일을 사용합니다. 보안 예외를 부여하지 않으려면 CA(인증 기관)에서 서명한 인증서를 설치합니다.

2. 로그인 화면에서 시스템 사용자 이름과 암호를 입력합니다.
3. **Log In**(로그인)을 클릭합니다.

인증에 성공하면 RHEL 웹 콘솔 인터페이스가 열립니다.

참고

제한된 액세스와 관리 액세스 간에 전환하려면 웹 콘솔 페이지의 상단 패널에서 **access** 또는 **Limited** 액세스를 클릭합니다. 관리 액세스 권한을 받으려면 사용자 암호를 제공해야 합니다.

1.4. 원격 머신에서 웹 콘솔에 연결

모든 클라이언트 운영 체제에서 웹 콘솔 인터페이스와 휴대 전화 또는 독점에서 웹 콘솔 인터페이스에 연결할 수 있습니다.

사전 요구 사항

- 지원되는 인터넷 브라우저가 있는 장치 (예:
  - Mozilla Firefox 52 이상
  - Google Chrome 57 이상
  - Microsoft Edge 16 이상
- 설치 및 액세스 가능한 웹 콘솔을 사용하여 액세스하려는 RHEL 9 서버

절차

1. 웹 브라우저를 엽니다.
2. 원격 서버의 주소를 다음 형식 중 하나로 입력합니다.
   a. 서버의 호스트 이름: **https://server.hostname.example.com:port_number**.
   예를 들어 다음과 같습니다.

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

   b. 서버의 IP 주소 사용: **https://server.IP_address:port_number**
   예를 들어 다음과 같습니다.

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

3. 로그인 인터페이스가 열리면 RHEL 시스템 자격 증명을 사용하여 로그인합니다.

1.5. 일회성 암호를 사용하여 웹 콘솔에 로그인

시스템이 활성화된 OTP(Identity Management) 도메인의 일부인 경우 OTP(단일 암호) 구성을 사용하면 OTP를 사용하여 RHEL 웹 콘솔에 로그인할 수 있습니다.

중요

시스템이 활성화된 OTP 구성이 활성화된 IdM(Identity Management) 도메인의 일부인 경우에만 일회성 암호를 사용하여 로그인할 수 있습니다.

사전 요구 사항

- RHEL 웹 콘솔이 설치되었습니다.
- OTP 구성이 활성화된 ID 관리 서버
- OTP 토큰을 생성하는 구성된 하드웨어 또는 소프트웨어 장치입니다.

절차

1. 브라우저에서 RHEL 웹 콘솔을 엽니다.
   - 로컬: **https://localhost:PORT_NUMBER**
   - 서버 호스트 이름을 원격으로 사용: **https://example.com:PORT_NUMBER**
   - 서버 IP 주소를 원격으로 사용: **https://EXAMPLE.SERVER.IP.ADDR:PORT_NUMBER**
     자체 서명된 인증서를 사용하는 경우 브라우저가 경고를 발행합니다. 인증서를 확인하고 로그인을 계속하려면 보안 예외를 수락합니다.

     콘솔은 **/etc/cockpit/ws-certs.d** 디렉터리에서 인증서를 로드하고 알파벳순으로 **.cert** 확장자가 있는 마지막 파일을 사용합니다. 보안 예외를 부여하지 않으려면 CA(인증 기관)에서 서명한 인증서를 설치합니다.
2. 로그인 창이 열립니다. 로그인 창에서 시스템 사용자 이름과 암호를 입력합니다.
3. 장치에서 일회성 암호를 생성합니다.
4. 암호를 확인한 후 웹 콘솔 인터페이스에 표시되는 새 필드에 일회성 암호를 입력합니다.
5. 로그인을 클릭합니다.
6. 로그인에 성공하면 웹 콘솔 인터페이스의 개요 페이지로 이동합니다.

1.6. 웹 콘솔을 사용하여 시스템 재부팅

웹 콘솔을 사용하여 웹 콘솔이 연결된 RHEL 시스템을 다시 시작할 수 있습니다.

사전 요구 사항

- 웹 콘솔이 설치되고 액세스할 수 있습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. RHEL 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 개요 페이지에서 **Reboot** (재부팅) 버튼을 클릭합니다.

3. 사용자가 시스템에 로그인한 경우 **Reboot** (재부팅) 대화 상자에서 다시 시작 이유를 작성합니다.
4. 선택 사항: **Delay** 드롭다운 목록에서 재부팅 지연에 대한 시간 간격을 선택합니다.
5. **Reboot** (재부팅)를 클릭합니다.

1.7. 웹 콘솔을 사용하여 시스템 종료

웹 콘솔을 사용하여 웹 콘솔이 연결된 RHEL 시스템을 종료할 수 있습니다.

사전 요구 사항

- 웹 콘솔이 설치되고 액세스할 수 있습니다.

절차

1. RHEL 웹 콘솔에 로그인합니다.
2. 개요를 클릭합니다.
3. 재시작 드롭다운 목록에서 **Shut Down** 을 선택합니다.
4. 시스템에 로그인한 사용자가 있으면 **Shut Down** 대화 상자에서 종료 이유를 작성합니다.
5. 선택 사항: 드롭다운 목록에서 시간 간격을 선택합니다.
6. **Shut Down** 을 클릭합니다.

1.8. 웹 콘솔을 사용하여 시간 설정 구성

시간대를 설정하고 NTP(Network Time Protocol) 서버와 시스템 시간을 동기화할 수 있습니다.

사전 요구 사항

- 웹 콘솔이 설치되고 액세스할 수 있습니다.

절차

1. RHEL 웹 콘솔에 로그인합니다.
2. 개요 에서 현재 시스템 시간을 클릭합니다.
3. 시스템 시간 변경 대화 상자에서 필요한 경우 시간대를 변경합니다.
4. 설정 시간 드롭다운 메뉴에서 다음 중 하나를 선택합니다.

수동
: NTP 서버 없이 시간을 수동으로 설정해야 하는 경우 이 옵션을 사용합니다.

NTP 서버 자동 사용
: 이 옵션은 사전 설정된 NTP 서버와 자동으로 시간을 동기화하는 기본 옵션입니다.

특정 **NTP** 서버 자동 사용
: 이 옵션은 시스템을 특정 NTP 서버와 동기화해야 하는 경우에만 사용합니다. DNS 이름 또는 서버의 IP 주소를 지정합니다.

5. 변경을 클릭합니다.

- 시스템 탭에 표시되는 시스템 시간을 확인합니다.

1.9. 웹 콘솔을 사용하여 CPU 보안 문제를 방지하기 위해 SMT 비활성화

CPU SMT를 악용하는 공격의 경우 SMT(Simultaneous Multi Threading)를 비활성화합니다. SMT를 비활성화하면 L1TF 또는 MDS와 같은 보안 취약점을 완화할 수 있습니다.

중요

SMT를 비활성화하면 시스템 성능이 저하될 수 있습니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. RHEL 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 개요 탭에서 **System information** 필드를 찾아 **View hardware details**를 클릭합니다.
3. **CPU Security** (CPU 보안) 줄에서 **Mitigations** 를 클릭합니다.
   이 링크가 없으면 시스템에서 SMT를 지원하지 않으므로 보안 취약점이 발생하지 않습니다.
4. **CPU Security Toggles** 표에서 **Disable** 동시 멀티스레딩**(nosmt)** 옵션을 선택합니다.
5. 저장 및 재부팅 버튼을 클릭합니다.

시스템을 다시 시작한 후 CPU는 더 이상 SMT를 사용하지 않습니다.

추가 리소스

- L1TF - L1 터미널 Fault 공격 - CVE-2018-3620 및 CVE-2018-3646
- MDS - Microarchitectural Data Sampling - CVE-2018-12130, CVE-2018-12126, CVE-2018-12127, CVE-2019-11091

1.10. 로그인 페이지에 배너 추가

회사 또는 기관은 때때로 컴퓨터 사용이 적정한 목적을 위한 것이며, 사용자는 감시의 대상이 되고, 모든 사람이 통과할 수 있음을 경고해야 합니다. 로그인하기 전에 경고가 표시되어야 합니다. SSH와 유사하게 웹 콘솔은 로그인 화면에 배너 파일의 내용을 선택적으로 표시할 수 있습니다. 웹 콘솔 세션에서 배너를 사용하려면 **/etc/cockpit/cockpit.conf** 파일을 수정해야 합니다. 이 파일은 필요하지 않으며 수동으로 생성해야 할 수도 있습니다.

사전 요구 사항

- 웹 콘솔이 설치되고 액세스할 수 있습니다.
- sudo 권한이 있어야 합니다.

절차

1. 아직 기본 설정의 텍스트 편집기에서 **/etc/issue.cockpit** 파일을 만듭니다. 표시할 콘텐츠를 파일에 배너로 추가합니다.
   파일 내용과 표시된 콘텐츠 사이에 다시 포맷되지 않으므로 파일에 매크로를 포함하지 마십시오. 의도한 줄 바꿈을 사용합니다. ASCII Art를 사용할 수 있습니다.

2. 파일을 저장합니다.

3. 기본 설정의 텍스트 편집기에서 **/etc/cockpit/** 디렉토리에 **cockpit.conf** 파일을 열거나 만듭니다.

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

4. 파일에 다음 텍스트를 추가합니다.

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

5. 파일을 저장합니다.

6. 변경 사항을 적용하려면 웹 콘솔을 다시 시작하십시오.

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

검증 단계

- 웹 콘솔 로그인 화면을 다시 열어 배너가 표시되는지 확인합니다.

예 **1.1.** 로그인 페이지에 예제 배너 추가

1. 텍스트 편집기를 사용하여 원하는 텍스트로 **/etc/issue.cockpit** 파일을 생성합니다.

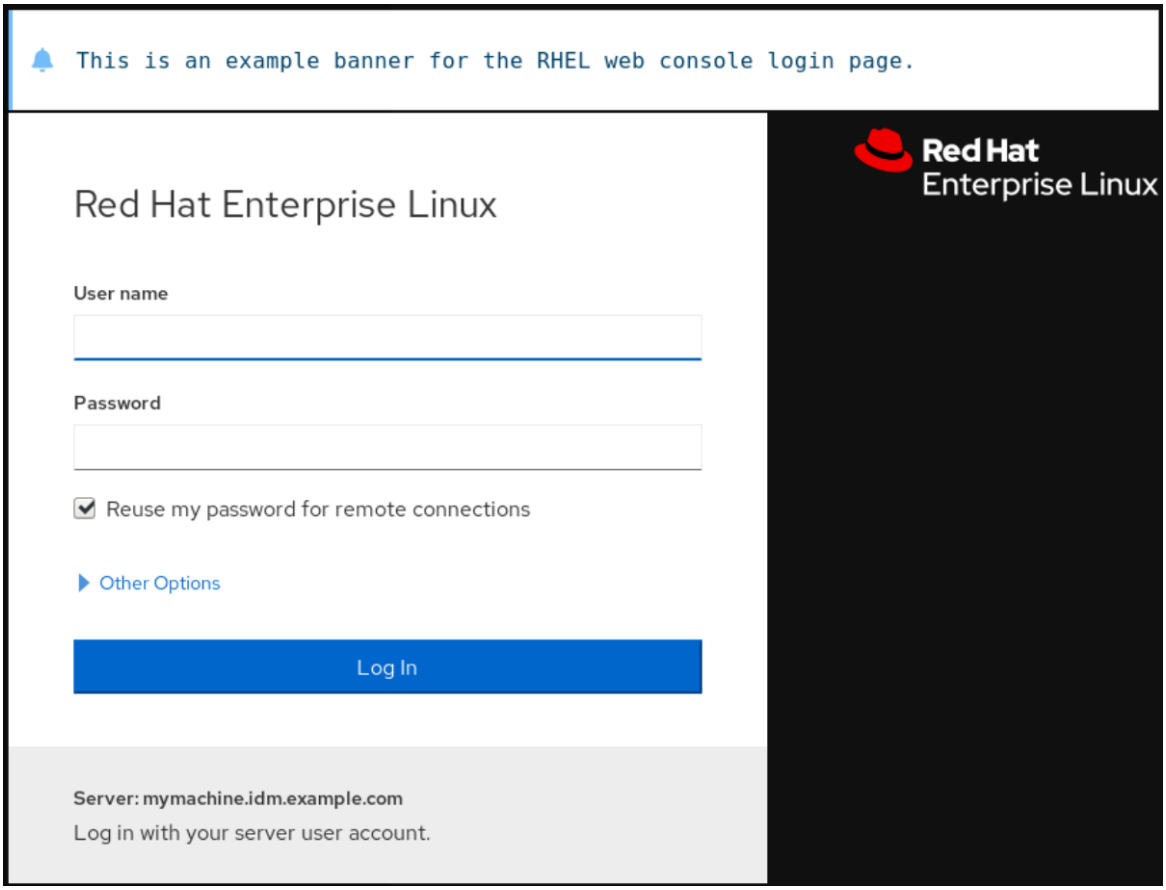
```
This is an example banner for the RHEL web console login page.
```

2. **/etc/cockpit/cockpit.conf** 파일을 열거나 만들고 다음 텍스트를 추가합니다.

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

3. 웹 콘솔을 다시 시작합니다.

4. 웹 콘솔 로그인 화면을 다시 엽니다.



1.11. 웹 콘솔에서 자동 유휴 잠금 구성

기본적으로 웹 콘솔 인터페이스에는 유휴 시간 제한이 설정되어 있지 않습니다. 시스템에서 유휴 타임아웃을 활성화하려면 **/etc/cockpit/cockpit.conf** 설정 파일을 수정하여 이 작업을 수행할 수 있습니다. 이 파일은 필요하지 않으며 수동으로 생성해야 할 수도 있습니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다.
- sudo 권한이 있어야 합니다.

절차

1. 기본 설정의 텍스트 편집기에서 **/etc/cockpit/** 디렉토리에 **cockpit.conf** 파일을 열거나 만듭니다.

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

2. 파일에 다음 텍스트를 추가합니다.

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

   몇 분 안에 **X** 를 선택한 기간 동안 숫자로 바꿉니다.

3. 파일을 저장합니다.
4. 변경 사항을 적용하려면 웹 콘솔을 다시 시작하십시오.

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

검증 단계

- 세션이 설정된 시간 후에 로그되는지 확인합니다.

2장. 웹 콘솔에서 호스트 이름 구성

Red Hat Enterprise Linux 웹 콘솔을 사용하여 웹 콘솔이 연결된 시스템에서 다양한 형식의 호스트 이름을 구성하는 방법을 알아봅니다.

2.1. 호스트 이름

호스트 이름은 시스템을 식별합니다. 기본적으로 호스트 이름은 **localhost** 로 설정되지만 변경할 수 있습니다.

호스트 이름은 다음 두 부분으로 구성됩니다.

호스트 이름

이는 시스템을 식별하는 고유한 이름입니다.

도메인

네트워크에서 시스템을 사용할 때 및 IP 주소 대신 이름을 사용할 때 호스트 이름 뒤에 있는 접미사로 도메인을 추가합니다.

연결된 도메인 이름을 FQDN(정규화된 도메인 이름)이라고 합니다. 예: **mymachine.example.com**

호스트 이름은 **/etc/hostname** 파일에 저장됩니다.

2.2. 웹 콘솔에서 호스트 이름

RHEL 웹 콘솔에서 상당히 호스트 이름을 구성할 수 있습니다. 예의 호스트 이름은 대문자, 공백 등을 사용하는 호스트 이름입니다.

예의 호스트 이름은 웹 콘솔에 표시되지만 호스트 이름과 일치하지 않아도 됩니다.

> 예 **2.1.** 웹 콘솔의 호스트 이름 형식
>
> 호스트 이름
>
> 내 머신
>
> 호스트 이름
>
> **mymachine**
>
> 실제 호스트 이름 **- FQDN(**정규화된 도메인 이름**)**
>
> **mymachine.idm.company.com**

2.3. 웹 콘솔을 사용하여 호스트 이름 설정

이 절차에서는 웹 콘솔에서 실제 호스트 이름 또는 예의 호스트 이름을 설정합니다.

사전 요구 사항

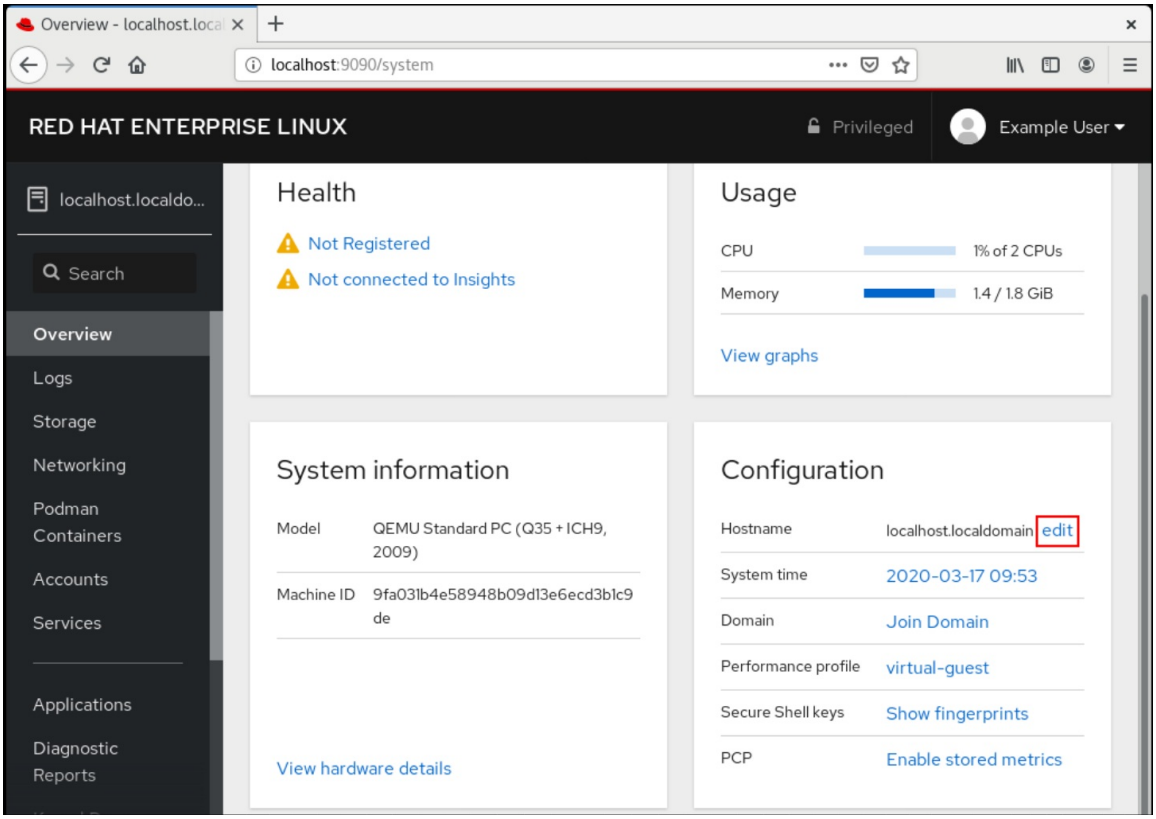
- 웹 콘솔이 설치되고 액세스할 수 있습니다.

절차

1. 웹 콘솔에 로그인합니다.

2. 개요를 클릭합니다.

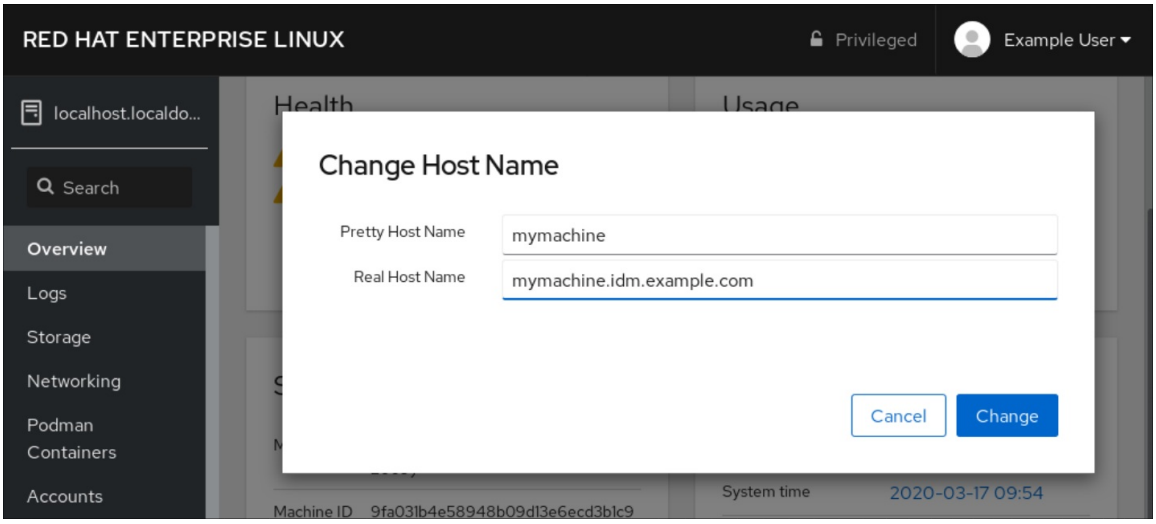
3. 현재 호스트 이름 옆에 있는 편집을 클릭합니다.



4. 호스트 이름 변경 대화 상자에서 **Pretty Host Name** 필드에 호스트 이름을 입력합니다.

5. **Real Host Name** 필드는 도메인 이름을 예의 이름에 연결합니다.
가상 호스트 이름과 일치하지 않는 경우 실제 호스트 이름을 수동으로 변경할 수 있습니다.

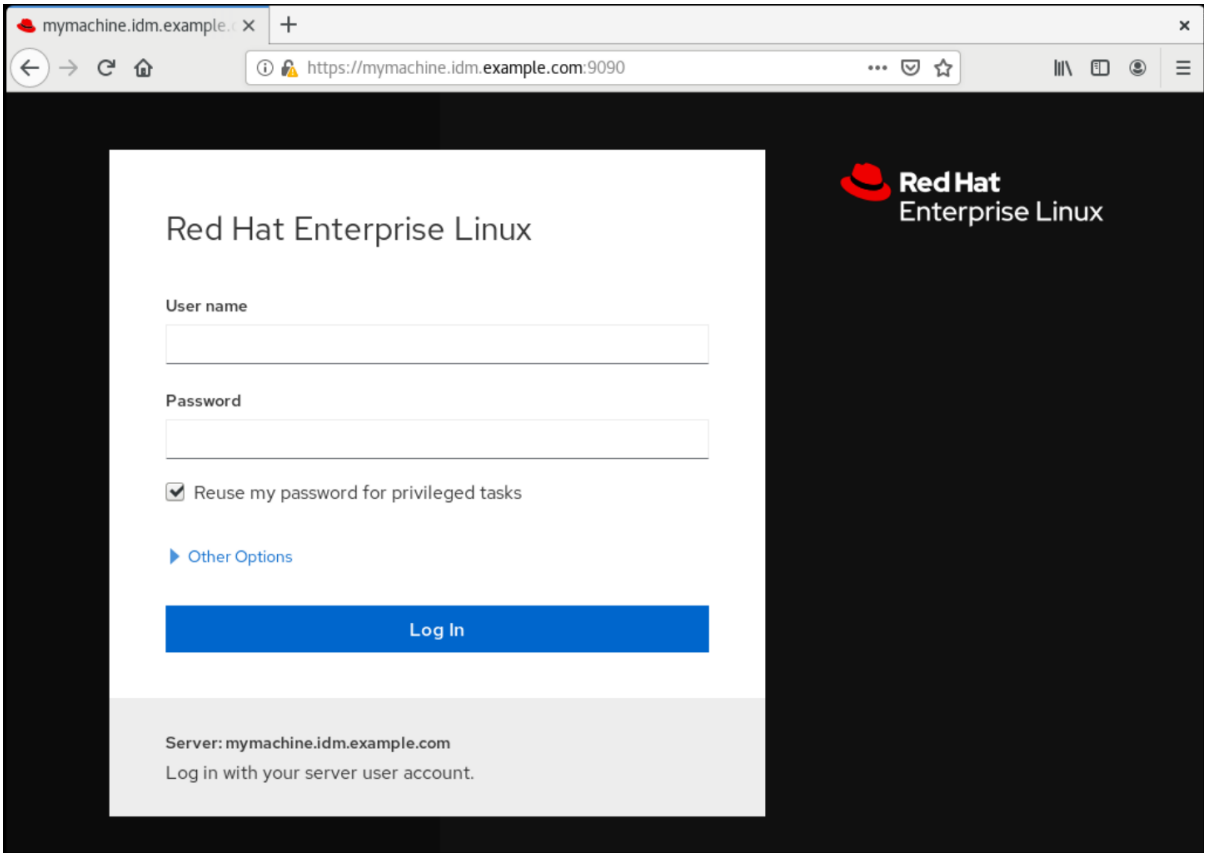
6. 변경을 클릭합니다.



검증 단계

1. 웹 콘솔에서 로그아웃합니다.

2. 브라우저의 주소 표시줄에 새 호스트 이름으로 주소를 입력하여 웹 콘솔을 다시 엽니다.


mymachine.idm.example.
https://mymachine.idm.example.com:9090
Red Hat Enterprise Linux
Red Hat Enterprise Linux
User name
Password
Reuse my password for privileged tasks
Other Options
Log In
Server: mymachine.idm.example.com
Log in with your server user account.

3장. RED HAT 웹 콘솔 애드온

RHEL 웹 콘솔에 애드온을 설치하고 사용할 수 있는 애드온 애플리케이션을 확인합니다.

3.1. 애드온 설치

cockpit 패키지는 기본적으로 Red Hat Enterprise Linux의 일부입니다. 애드온 애플리케이션을 사용하려면 별도로 설치해야 합니다.

사전 요구 사항

- **cockpit** 패키지를 설치하고 활성화했습니다.

절차

- 애드온을 설치합니다.

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

3.2. RHEL 웹 콘솔용 애드온

다음 표에는 RHEL 웹 콘솔에 사용할 수 있는 애드온 애플리케이션이 나열되어 있습니다.

기능 이름	패키지 이름	사용법
composer	cockpit-composer	사용자 정의 OS 이미지 빌드
Machine	cockpit-machines	libvirt 가상 머신 관리
PackageKit	cockpit-packagekit	소프트웨어 업데이트 및 애플리케이션 설치 (일반적으로 기본적으로 설치됨)
PCP	cockpit-pcp	지속적 및 보다 세밀한 성능 데이터 (UI에서 필요에 따라 설치)
podman	cockpit-podman	podman 컨테이너 관리
세션 기록	cockpit-session-recording	사용자 세션 기록 및 관리

4장. 웹 콘솔을 사용하여 시스템 성능 최적화

RHEL 웹 콘솔에서 성능 프로파일을 설정하여 선택한 작업에 대한 시스템의 성능을 최적화하는 방법을 알아봅니다.

4.1. 웹 콘솔에서 성능 튜닝 옵션

Red Hat Enterprise Linux 9는 다음 작업을 위해 시스템을 최적화하는 여러 성능 프로필을 제공합니다.

- 데스크탑을 사용하는 시스템
- 처리량 성능
- 대기 시간 성능
- 네트워크 성능
- 전력 소비 감소
- 가상 머신

tuned 서비스는 선택한 프로필과 일치하도록 시스템 옵션을 최적화합니다.

웹 콘솔에서 시스템에서 사용하는 성능 프로필을 설정할 수 있습니다.

추가 리소스

- TuneD 시작하기

4.2. 웹 콘솔에서 성능 프로파일 설정

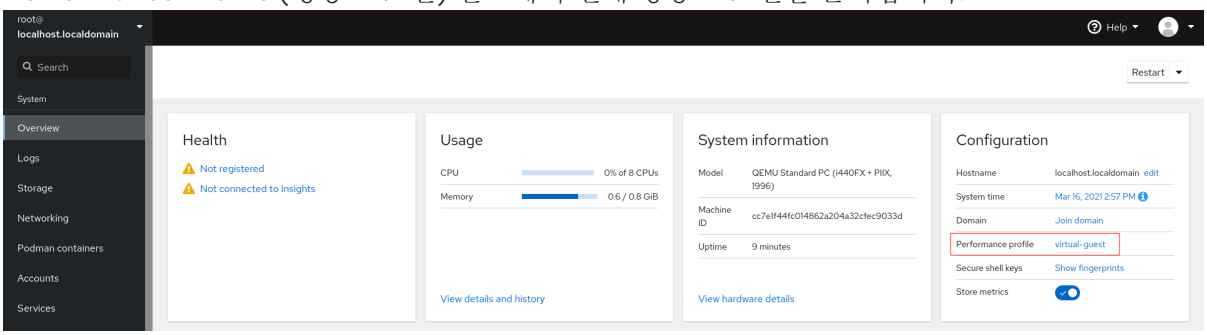
이 절차에서는 웹 콘솔을 사용하여 선택한 작업의 시스템 성능을 최적화합니다.

사전 요구 사항

- 웹 콘솔이 설치되어 액세스 가능한지 확인합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

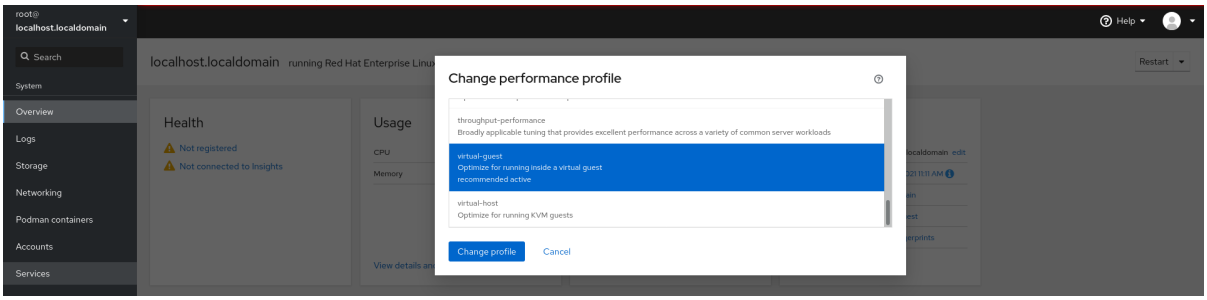
절차

1. RHEL 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 개요를 클릭합니다.
3. **Performance Profile** (성능 프로필) 필드에서 현재 성능 프로필을 클릭합니다.



4. 필요한 경우 성능 프로필 변경 대화 상자에서 프로필을 변경합니다.

5. 프로필 변경을 클릭합니다.



검증 단계

- 이제 개요 탭에 선택한 성능 프로필이 표시됩니다.

4.3. 웹 콘솔을 사용하여 성능 모니터링

Red Hat의 웹 콘솔에서는 문제 해결을 위해 Utilization Saturation and Errors(USE) 방법을 사용합니다. 새로운 성능 지표 페이지에는 최신 데이터와 함께 데이터 기록 보기가 있습니다.

여기서는 리소스 사용률 및 포화 상태에 대한 이벤트, 오류 및 그래픽 표시를 볼 수 있습니다.

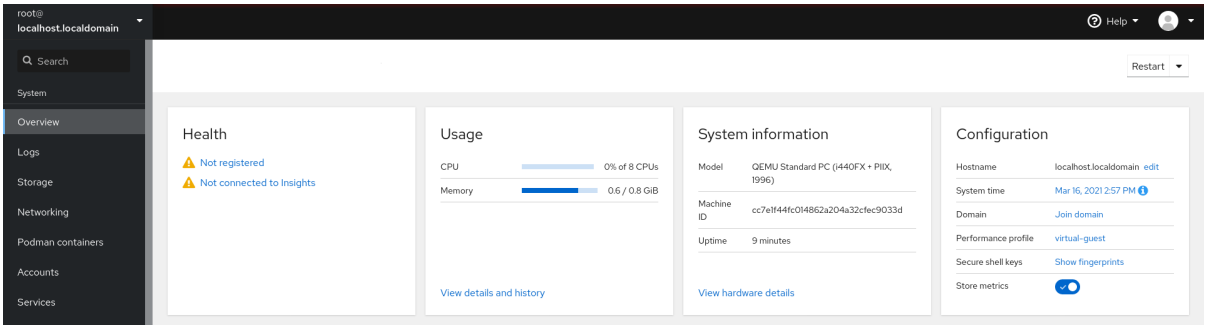
사전 요구 사항

1. 웹 콘솔이 설치되어 액세스 가능한지 확인합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
2. performance 지표를 수집할 수 있는 **cockpit-pcp** 패키지를 설치합니다.

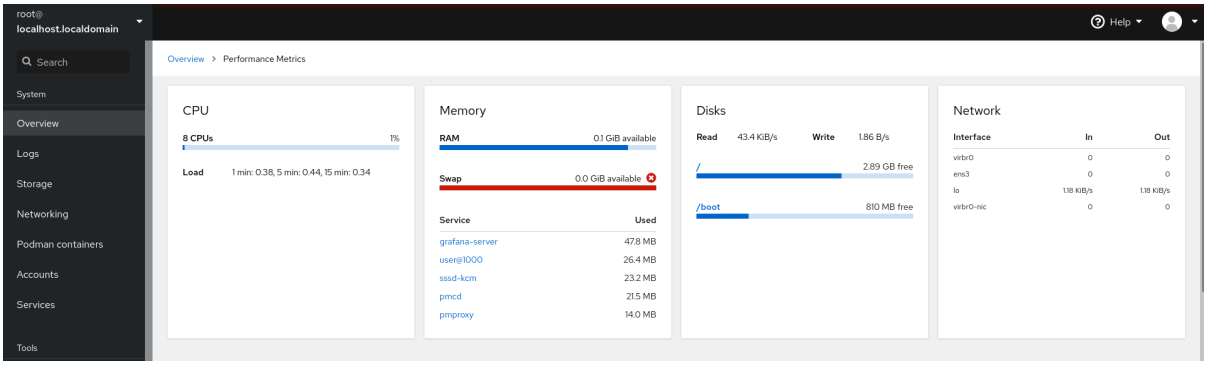
```
# dnf install cockpit-pcp
```

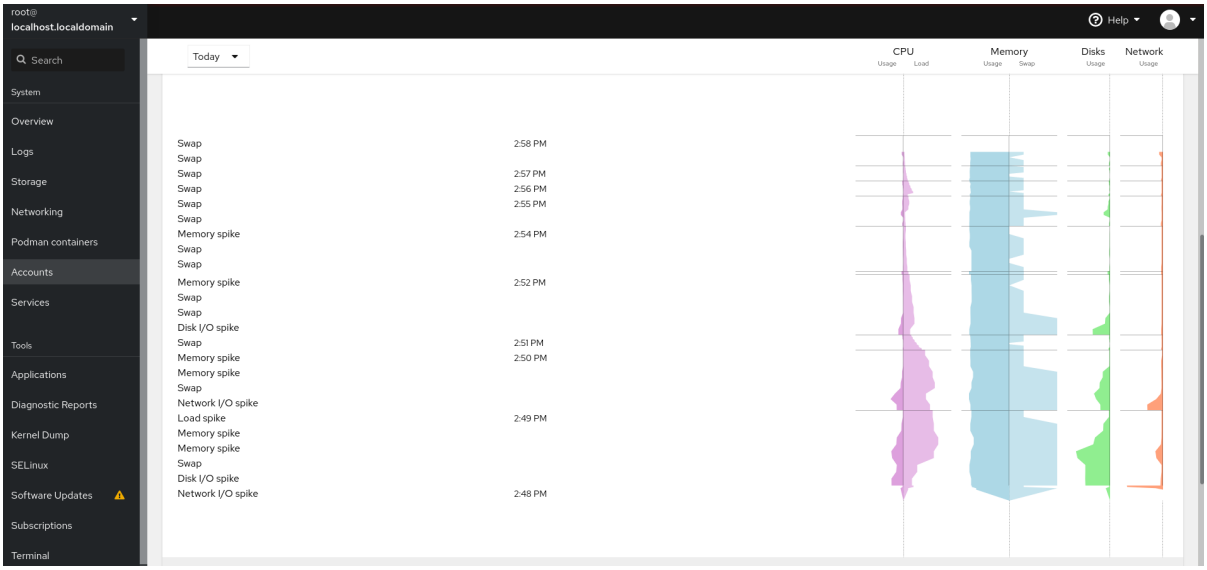
절차

1. RHEL 9 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 개요를 클릭합니다.



3. 보기 세부 정보 및 기록을클릭하여 성능 지표 를 확인합니다.


root@
localhost.localdomain
Help
Search
Overview
Performance Metrics
System
Overview
Logs
Storage
Networking
Podman containers
Accounts
Services
Tools
CPU
8 CPUs
1%
Load
1 min: 0.38, 5 min: 0.44, 15 min: 0.34
Memory
RAM
0.1 GiB available
Swap
0.0 GiB available
Service
Used
grafana-server
47.8 MB
user@1000
26.4 MB
sssd-kcm
23.2 MB
pmcd
21.5 MB
pmproxy
14.0 MB
Disks
Read
43.4 KiB/s
Write
1.86 B/s
/
2.89 GB free
/boot
810 MB free
Network
Interface
In
Out
virbr0
0
0
ens3
0
0
lo
1.18 KiB/s
1.18 KiB/s
virbr0-nic
0
0


root@
localhost.localdomain
Help
Search
Today
CPU
Usage
Load
Memory
Usage
Swap
Disks
Usage
Network
Usage
System
Overview
Logs
Storage
Networking
Podman containers
Accounts
Services
Tools
Applications
Diagnostic Reports
Kernel Dump
SELinux
Software Updates
Subscriptions
Terminal
Swap
2:58 PM
Swap
Swap
2:57 PM
Swap
2:56 PM
Swap
2:55 PM
Swap
Memory spike
2:54 PM
Swap
Swap
Memory spike
2:52 PM
Swap
Swap
Disk I/O spike
Swap
2:51 PM
Memory spike
2:50 PM
Memory spike
Swap
Network I/O spike
Load spike
2:49 PM
Memory spike
Memory spike
Swap
Disk I/O spike
Network I/O spike
2:48 PM

5장. 웹 콘솔에서 로그 검토

RHEL 웹 콘솔에서 로그에 액세스, 검토 및 필터링하는 방법을 알아봅니다.

5.1. 웹 콘솔에서 로그 검토

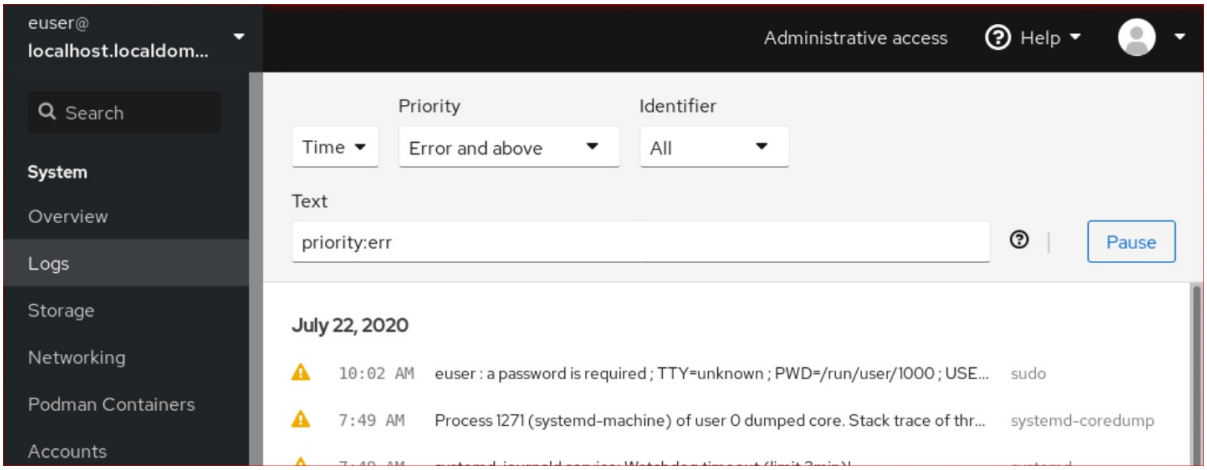
RHEL 9 웹 콘솔 로그 섹션은 **journalctl** 유틸리티의 UI입니다. 이 섹션에서는 웹 콘솔 인터페이스에서 시스템 로그에 액세스하는 방법을 설명합니다.

사전 요구 사항

- RHEL 9 웹 콘솔이 설치되었습니다.
  자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. RHEL 웹 콘솔에 로그인합니다.
   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 로그를 클릭합니다.



3. 목록에서 선택한 로그 항목을 클릭하여 로그 항목 세부 정보를 엽니다.

참고

일시 중지 버튼을 사용하여 새 로그 항목이 표시되지 않도록 일시 중지할 수 있습니다. 새 로그 항목을 다시 시작하면 웹 콘솔은 **Pause** 버튼을 사용한 후 보고된 모든 로그 항목을 로드합니다.

시간, 우선 순위 또는 식별자로 로그를 필터링할 수 있습니다. 자세한 내용은 웹 콘솔에서 로그 필터링을 참조하십시오.

5.2. 웹 콘솔에서 로그 필터링

이 섹션에서는 웹 콘솔에서 로그 항목을 필터링하는 방법을 보여줍니다.

사전 요구 사항

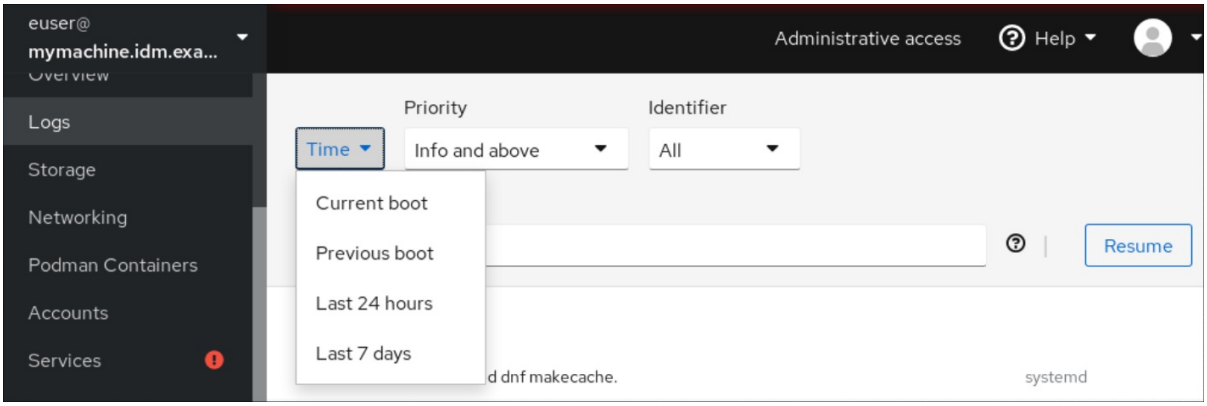
- 웹 콘솔 인터페이스를 설치하고 액세스할 수 있어야 합니다.
  자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

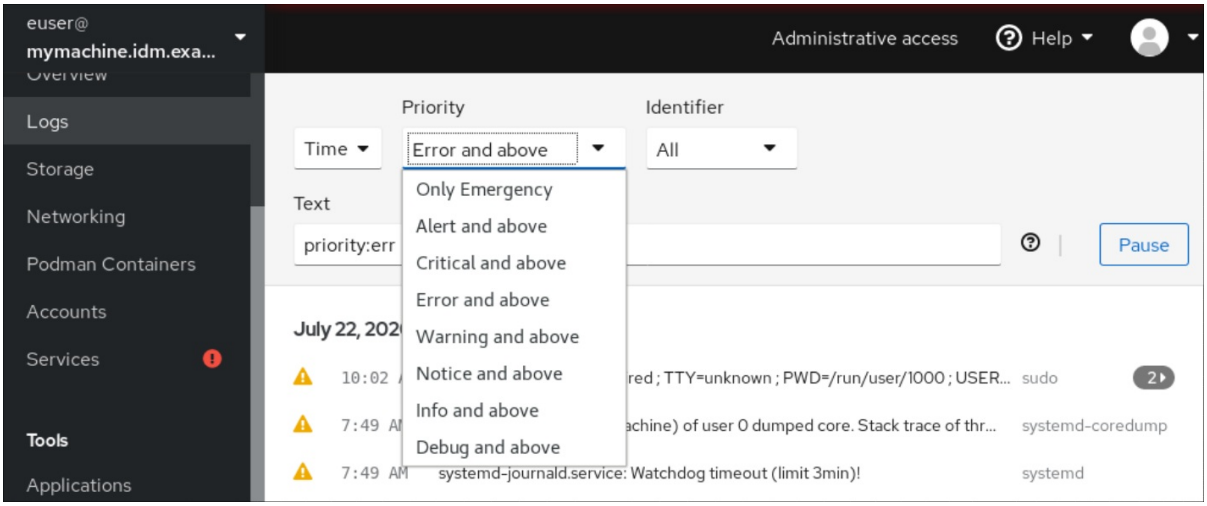
1. RHEL 9 웹 콘솔에 로그인합니다.
   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 로그를 클릭합니다.

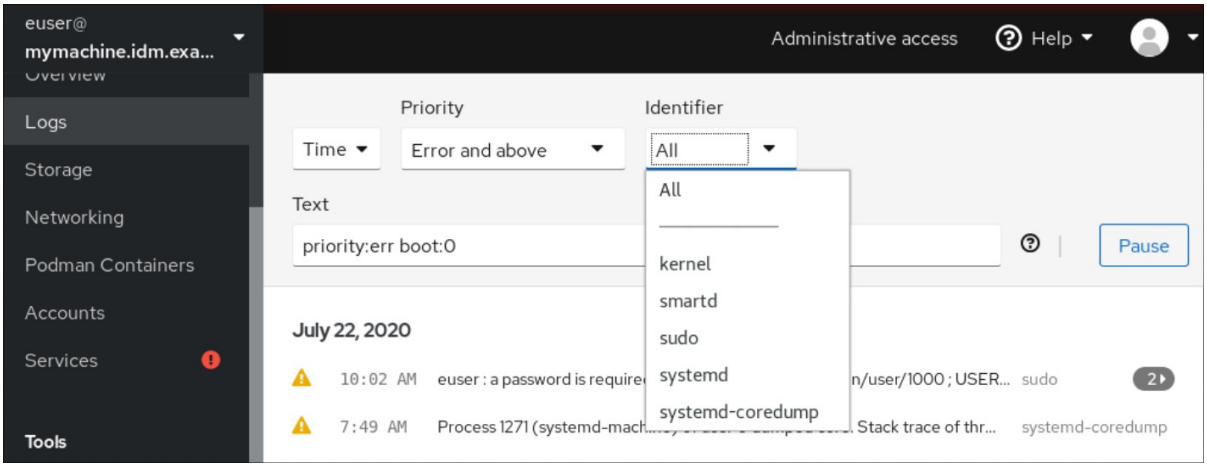
3. 기본적으로 웹 콘솔에는 최신 로그 항목이 표시됩니다. 특정 시간 범위로 필터링하려면 시간 드롭다운 메뉴를 클릭하고 선호하는 옵션을 선택합니다.



4. 오류 및 위의 심각도 로그 목록은 기본적으로 표시됩니다. 다른 우선 순위로 필터링하려면 오류 및 위의 드롭다운 메뉴를 클릭하고 기본 우선 순위를 선택합니다.



5. 기본적으로 웹 콘솔은 모든 식별자에 대한 로그를 표시합니다. 특정 식별자에 대한 로그를 필터링하려면 모든 드롭다운 메뉴를 클릭하고 식별자를 선택합니다.



6. 로그 항목을 열려면 선택한 로그를 클릭합니다.

5.3. 웹 콘솔에서 로그를 필터링하기 위한 텍스트 검색 옵션

텍스트 검색 옵션 기능은 로그를 필터링하기 위한 다양한 옵션을 제공합니다. 텍스트 검색을 사용하여 로그를 필터링하려면 세 개의 드롭다운 메뉴에 정의된 사전 정의된 옵션을 사용하거나 전체 검색을 직접 입력할 수 있습니다.

드롭다운 메뉴

검색의 주요 매개변수를 지정하는 데 사용할 수 있는 드롭다운 메뉴는 세 가지가 있습니다.

- 시간: 이 드롭다운 메뉴에는 다양한 검색 범위에 대한 사전 정의된 검색이 포함되어 있습니다.
- **Priority**: 이 드롭다운 메뉴에서는 다른 우선 순위 수준의 옵션을 제공합니다. **journalctl --priority** 옵션에 해당합니다. 기본 우선순위 값은 **Error**이고 위의 입니다. 다른 우선 순위를 지정하지 않을 때마다 설정됩니다.
- 식별자: 이 드롭다운 메뉴에서 필터링할 식별자를 선택할 수 있습니다. **journalctl --identifier** 옵션에 해당합니다.

Quantifiers

검색을 지정하는 데 사용할 수 있는 여섯 개의 쿼터가 있습니다. 로그 테이블 필터링의 옵션에서 다릅니다.

로그 필드

특정 로그 필드를 검색하려면 해당 콘텐츠와 함께 필드를 지정할 수 있습니다.

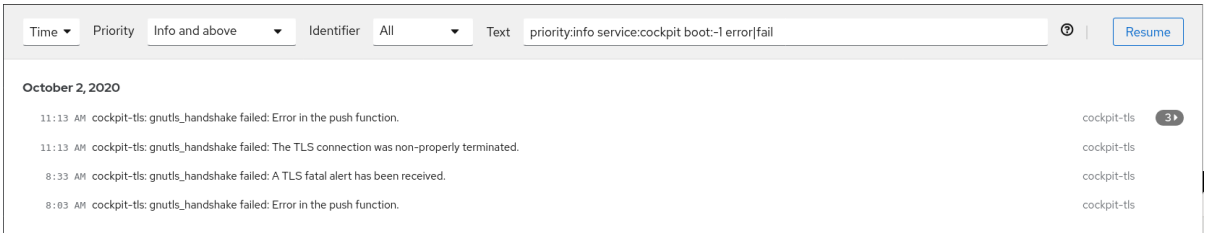
로그 메시지에서 자유 형식 텍스트 검색

로그 메시지에서 선택한 텍스트 문자열을 필터링할 수 있습니다. 문자열은 정규식의 형태일 수도 있습니다.

고급 로그 필터링 I

2020년 10월 22일 자정, 저널 필드 'JOB_TYPE'에서 발생한 'systemd'로 식별된 모든 로그 메시지를 필터링합니다. 'start' 또는 'restart).

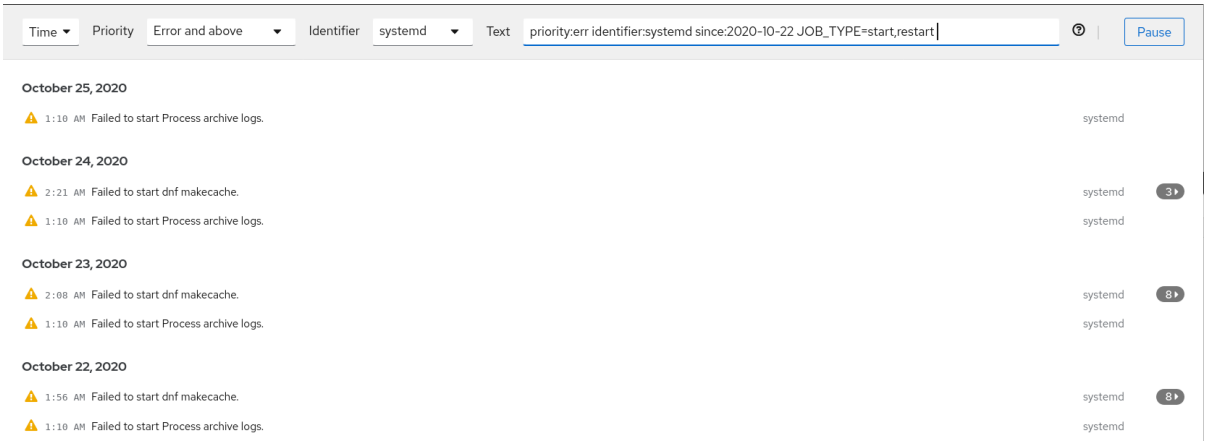
1. **identifier:2020-10-22 JOB_TYPE=start**부터 **search** 필드에 입력합니다.
2. 결과를 확인하십시오.



고급 로그 필터링 II

마지막 전에 부팅에서 발생한 'cockpit.service' systemd 장치에서 온 모든 로그 메시지를 필터링하고 메시지 본문에는 "error" 또는 "fail"가 포함됩니다.

1. **service:cockpit boot:-1 error|fail** to the search field를 입력합니다.
2. 결과를 확인하십시오.



5.4. 웹 콘솔에서 텍스트 검색 상자를 사용하여 로그를 필터링

텍스트 검색 상자를 사용하면 다른 매개변수에 따라 로그를 필터링할 수 있습니다. 검색에서는 필터링 드롭다운 메뉴, quantifiers, 로그 필드 및 자유 형식 문자열 검색을 사용하여 결합합니다.

사전 요구 사항

- 웹 콘솔 인터페이스를 설치하고 액세스할 수 있어야 합니다.
  자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. RHEL 웹 콘솔에 로그인합니다.
   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 로그를 클릭합니다.

3. 드롭다운 메뉴를 사용하여 세 가지 주요 quantifiers(시간 범위, 우선 순위 및 식별자)를 지정합니다.
   Priority quantifier는 항상 값을 가져야 합니다. 지정하지 않으면 오류 및 위의 우선 순위를 자동으로 필터링합니다. 텍스트 검색 상자에 반영한 옵션이 있는지 확인합니다.

4. 필터링할 로그 필드를 지정합니다.
   여러 로그 필드를 추가할 수 있습니다.

5. 자유 형식 문자열을 사용하여 다른 항목을 검색할 수 있습니다. 검색 상자에는 정규 표현식도 사용할 수 있습니다.

5.5. 로그 필터링 옵션

웹 콘솔에서 로그를 필터링하는 데 사용할 수 있는 **journalctl** 옵션은 여러 가지가 있습니다. 이 옵션은 유용할 수 있습니다. 이 중 일부는 웹 콘솔 인터페이스의 드롭다운 메뉴의 일부로 이미 설명되어 있습니다.

표 5.1. 테이블

옵션 이름	사용법	참고

옵션 이름	사용법	참고
priority	메시지 우선 순위로 출력을 필터링합니다. 단일 숫자 또는 텍스트 로그 수준을 사용합니다. 로그 수준은 일반적인 syslog 로그 수준입니다. 단일 로그 수준을 지정하면 이 로그 수준의 모든 메시지 또는 더 중요한 로그 수준이 표시됩니다.	**Priority** 드롭다운 메뉴에서 다룹니다.
identifier	지정된 syslog 식별자 SYSLOG_IDENTIFIER의 메시지를 표시합니다. 여러 번 지정할 수 있습니다.	**Identifier** 드롭다운 메뉴에 적용됩니다.
팔로우	가장 최근 저널 항목만 표시하고 저널에 추가할 때 새 항목을 지속적으로 출력합니다.	드롭다운에는 포함되지 않습니다.
service	지정된 **systemd** 유닛의 메시지를 표시합니다. 여러 번 지정할 수 있습니다.	드롭다운에 포함되지 않습니다. **journalctl --unit** 매개변수에 해당합니다.
boot	특정 부팅의 메시지를 표시합니다. 양의 정수는 저널이 시작될 때부터 부팅을 조회하며, equal-or-less-than 0 정수는 저널이 끝날 때부터 부팅됩니다. 따라서 1은 일기적 순서로 저널에 있는 첫 번째 부팅을 의미합니다. 2는 두 번째 순서와 같습니다. -0은 마지막 부팅 전의 부팅 -1이고 마지막 부팅 전의 부팅은 -1입니다.	**시간** 드롭다운 메뉴에서 **현재 부팅** 또는 **이전 부팅** 으로만 적용됩니다. 다른 옵션은 수동으로 작성해야 합니다.
이후	지정된 날짜 또는 지정된 날짜보다 오래된 항목 또는 지정된 날짜보다 오래된 항목을 각각 표시합니다. 날짜 사양은 "2012-10-30 18:17:16" 형식이어야 합니다. 시간 부분이 생략되면 "00:00:00"으로 가정합니다. 초 구성 요소만 생략하면 ":00"이라고 가정합니다. 날짜 구성 요소가 생략되면 현재 날짜로 간주됩니다. 또는 "오늘", "today", "tomorrow"는 현재 일 전의 00:00:00을 나타냅니다. "now"는 현재 시간을 나타냅니다. "now"는 현재 시간을 나타냅니다. 마지막으로 상대 시간을 각각 현재 시간 전 또는 이후의 시간을 나타내는 "-" 또는 "+"로 접두사로 지정할 수 있습니다.	드롭다운에는 포함되지 않습니다.

6장. 웹 콘솔에서 사용자 계정 관리

RHEL 웹 콘솔은 시스템 사용자 계정을 추가, 편집, 제거하기 위한 인터페이스를 제공합니다.

이 섹션을 읽은 후에는 다음을 알 수 있습니다.

- 기존 계정이 들어오는 위치.
- 새 계정을 추가하는 방법
- 암호 만료를 설정하는 방법.
- 사용자 세션을 종료하는 방법 및 시기.

사전 요구 사항

- 관리자 권한이 할당된 계정을 사용하여 RHEL 웹 콘솔에 로그인하십시오. 자세한 내용은 웹 콘솔에 로깅을참조하십시오.

6.1. 웹 콘솔에서 관리되는 시스템 사용자 계정

RHEL 웹 콘솔에 사용자 계정을 표시하면 다음을 수행할 수 있습니다.

- 시스템에 액세스할 때 사용자를 인증합니다.
- 시스템에 대한 액세스 권한을 설정합니다.

RHEL 웹 콘솔에는 시스템에 있는 모든 사용자 계정이 표시됩니다. 따라서 웹 콘솔에 처음 로그인한 직후에 하나 이상의 사용자 계정이 표시될 수 있습니다.

RHEL 웹 콘솔에 로그인한 후 다음 작업을 수행할 수 있습니다.

- 새 사용자 계정 생성.
- 매개 변수를 변경합니다.
- 계정 잠금.
- 사용자 세션을 종료합니다.

6.2. 웹 콘솔을 사용하여 새 계정 추가

다음 단계를 사용하여 시스템에 사용자 계정을 추가하고 RHEL 웹 콘솔을 통해 계정에 관리 권한을 설정합니다.

사전 요구 사항

- RHEL 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. RHEL 웹 콘솔에 로그인합니다.
2. 계정 을 클릭합니다.

3. **Create New Account** 를 클릭합니다.

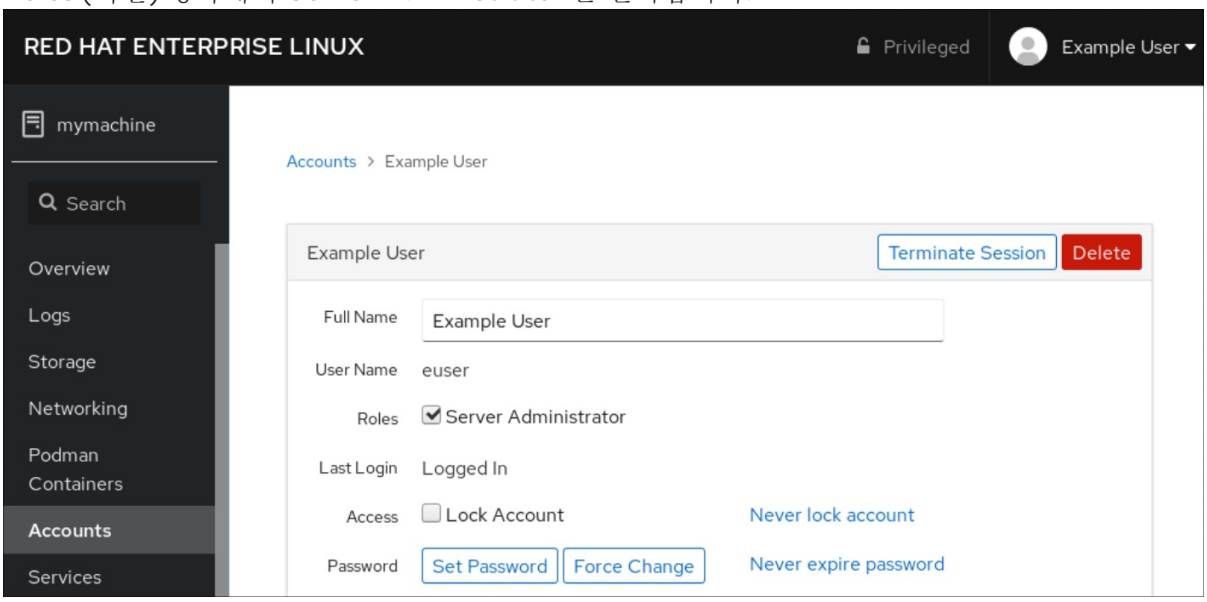
1. 전체 이름 필드에 사용자의 전체 이름을 입력합니다.
RHEL 웹 콘솔에서는 전체 이름의 사용자 이름을 자동으로 제안하고 사용자 이름 필드에 채웁니다. 첫 번째 이름의 첫 글자와 전체 이름으로 구성된 원래 명명 규칙을 사용하지 않으려면 제안을 업데이트합니다.

2. 암호/확인 필드에 암호를 입력하고 암호가 올바른지 확인하기 위해 다시 입력합니다.
필드 아래에 배치된 색상 표시줄에는 입력한 암호의 보안 수준이 표시되어 약한 암호로 사용자를 만들 수 없습니다.

1. 만들기 를 클릭하여 설정을 저장하고 대화 상자를 닫습니다.

2. 새로 생성된 계정을 선택합니다.

3. **Roles** (역할) 항목에서 **Server Administrator** 를 선택합니다.



이제 계정 설정에서 새 계정을 볼 수 있으며 자격 증명을 사용하여 시스템에 연결할 수 있습니다.

6.3. 웹 콘솔에서 암호 만료 적용

기본적으로 사용자 계정은 암호가 만료되지 않도록 설정했습니다. 정의된 일수 후에 만료되도록 시스템 암호를 설정할 수 있습니다. 암호가 만료되면 다음 로그인 시도에서 암호 변경을 요청합니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.

2. 계정 을 클릭합니다.

3. 암호 만료를 적용할 사용자 계정을 선택합니다.

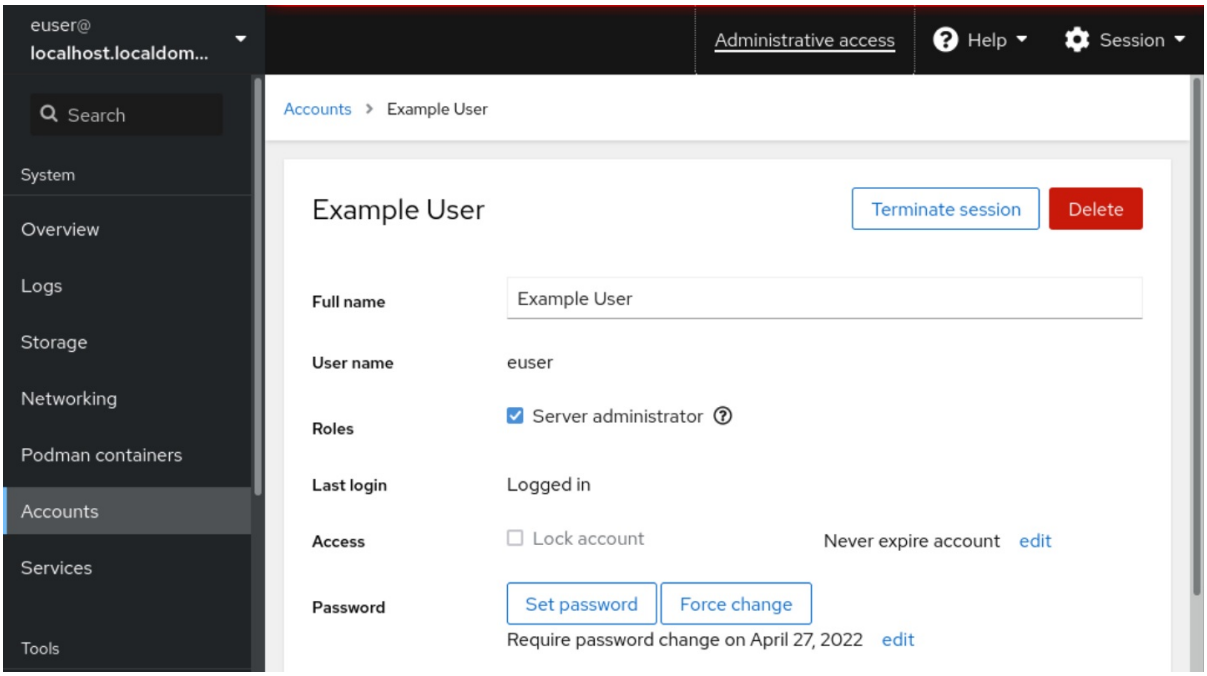
4. 사용자 계정 설정에서 두 번째 편집 을 클릭합니다.

5. 암호 만료 대화 상자에서 **must require password change every ...**을 선택합니다. **days**을(를) 입력하고 암호가 만료된 날 수를 나타내는 양의 정수 숫자를 입력합니다.

6. 변경을 클릭합니다.

검증 단계

- 암호 만료가 설정되었는지 확인하려면 계정 설정을 엽니다.
  RHEL 9 웹 콘솔에는 만료 날짜가 있는 링크가 표시됩니다.



6.4. 웹 콘솔에서 사용자 세션 종료

사용자는 시스템에 로그인할 때 사용자 세션을 생성합니다. 사용자 세션 종료는 시스템에서 사용자를 로그아웃하는 것을 의미합니다. 시스템 업그레이드와 같이 구성 변경에 민감한 관리 작업을 수행해야 하는 경우 유용할 수 있습니다.

RHEL 9 웹 콘솔의 각 사용자 계정에서 현재 사용 중인 웹 콘솔 세션을 제외하고 계정의 모든 세션을 종료할 수 있습니다. 이렇게 하면 시스템에 대한 액세스 권한을 금지할 수 있습니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.
2. 계정 을 클릭합니다.
3. 세션을 종료할 사용자 계정을 클릭합니다.
4. **Terminate Session** 을 클릭합니다.
   Terminate Session 버튼이 비활성화되어 있는 경우 사용자는 시스템에 로그인하지 않습니다.

   RHEL 웹 콘솔은 세션을 종료합니다.

7장. 웹 콘솔에서 서비스 관리

RHEL 웹 콘솔 인터페이스에서 시스템 서비스를 관리하는 방법을 알아봅니다. 서비스를 활성화 또는 비활성화하거나 서비스를 다시 시작하거나 다시 로드하거나 자동 시작을 관리할 수 있습니다.

7.1. 웹 콘솔에서 시스템 서비스 활성화 또는 비활성화

이 절차에서는 웹 콘솔 인터페이스를 사용하여 시스템 서비스를 활성화하거나 비활성화합니다.

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다.
  자세한 내용은 웹 콘솔 설치를 참조하십시오.

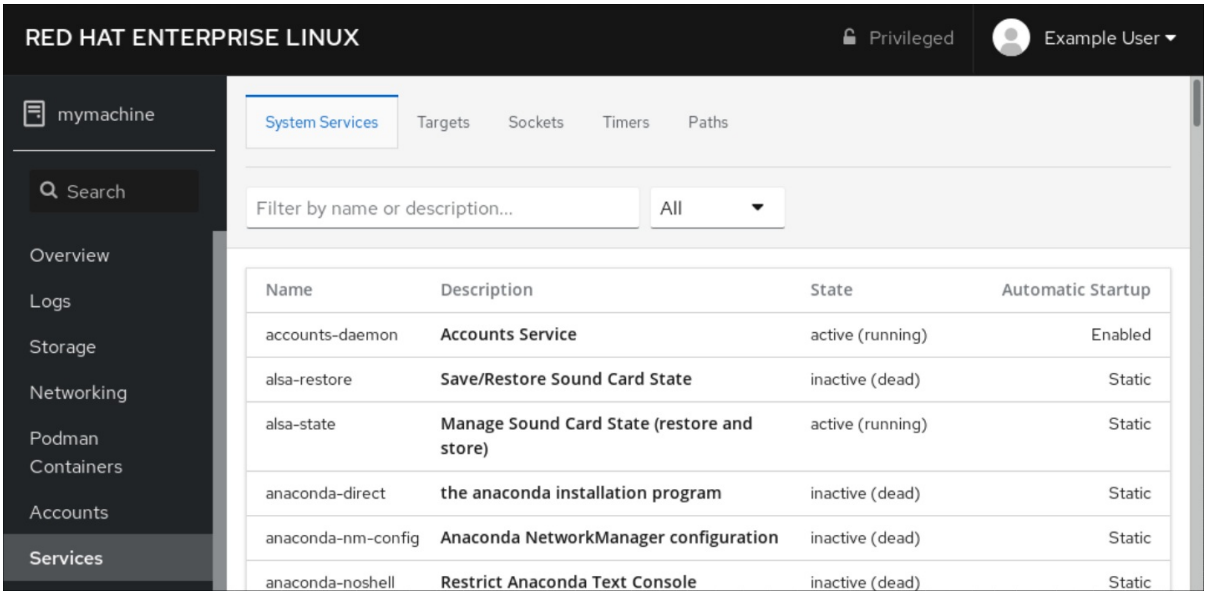
절차

이름 또는 설명으로 서비스를 필터링하고 **Enabled, Disabled** 또는 **Static** 자동 시작으로도 필터링할 수 있습니다. 인터페이스는 서비스의 현재 상태와 최근 로그를 표시합니다.

1. 관리자 권한으로 **RHEL** 웹 콘솔에 로그인합니다.
   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 왼쪽의 웹 콘솔 메뉴에서 **Services** (서비스)를 클릭합니다.

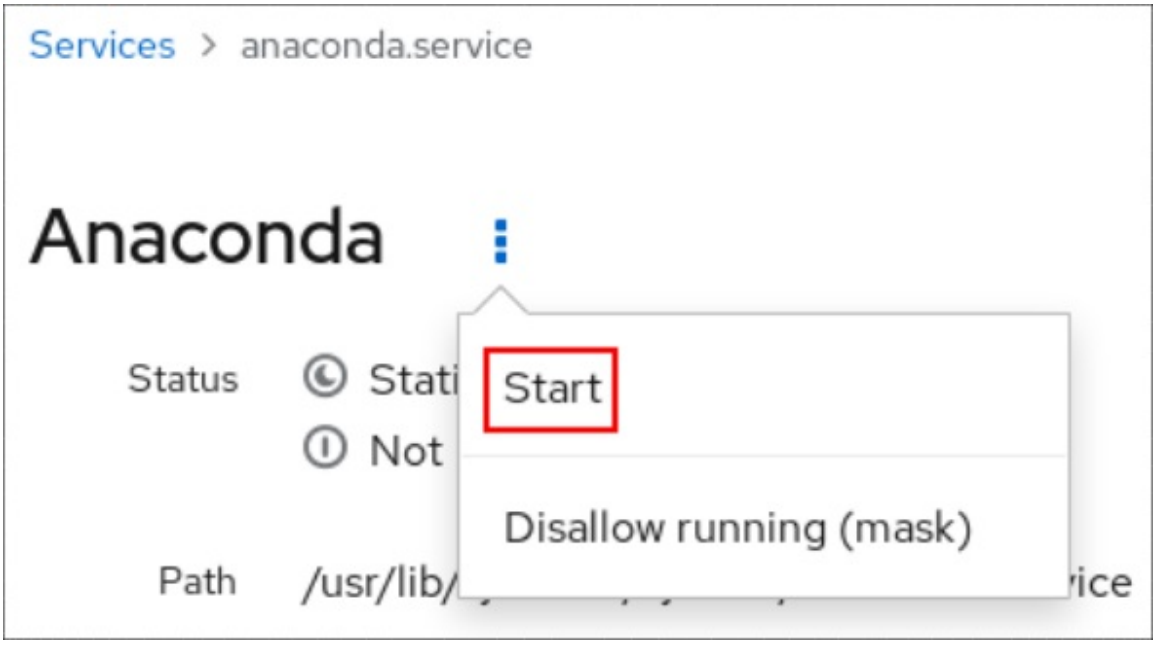
3. 서비스 의 기본 탭은**System Services** 입니다. 대상, 소켓, 타이머 또는 경로를 관리하려면 상단 메뉴의 해당 탭으로 전환합니다.



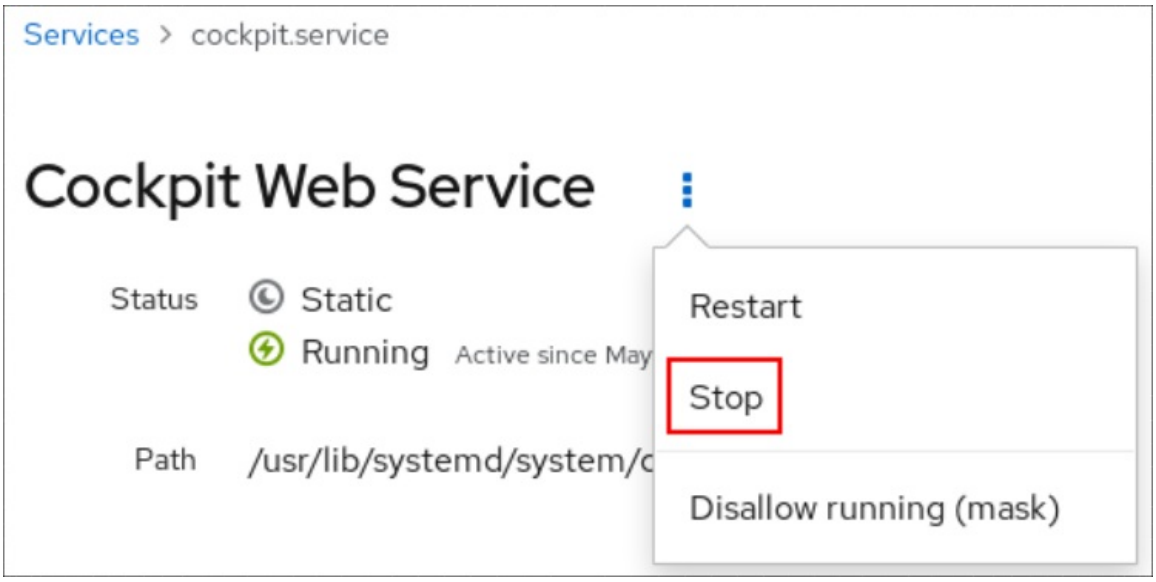
4. 서비스 설정을 열려면 목록에서 선택한 서비스를 클릭합니다. **State** 열을 확인하여 활성 또는 비활성 상태인 서비스를 확인할 수 있습니다.

5. 서비스를 활성화하거나 비활성화합니다.

   - 비활성 서비스를 활성화하려면 **Start** (시작) 버튼을 클릭합니다.



- 활성 서비스를 비활성화하려면 중지 버튼을 클릭합니다.



7.2. 웹 콘솔에서 시스템 서비스 다시 시작

이 절차에서는 웹 콘솔 인터페이스를 사용하여 시스템 서비스를 다시 시작합니다.

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다.
  자세한 내용은 웹 콘솔 설치를 참조하십시오.

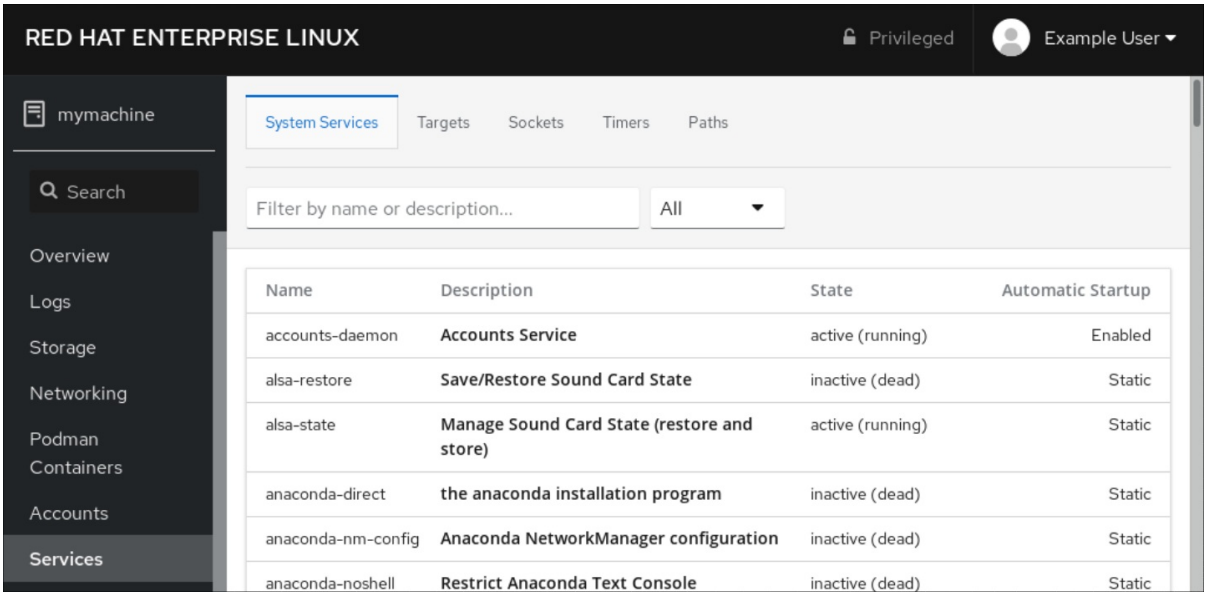
절차

이름 또는 설명으로 서비스를 필터링하고 **Enabled, Disabled** 또는 **Static** 자동 시작으로도 필터링할 수 있습니다. 인터페이스는 서비스의 현재 상태와 최근 로그를 표시합니다.

1. 관리자 권한으로 **RHEL** 웹 콘솔에 로그인합니다.
   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

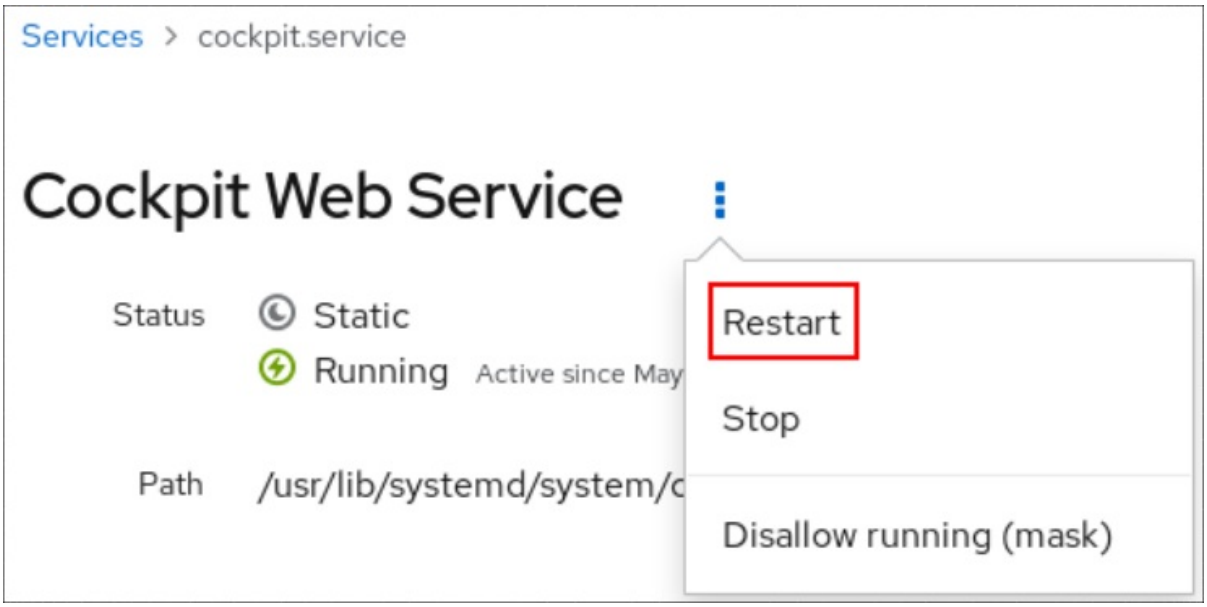
2. 왼쪽의 웹 콘솔 메뉴에서 **Services** (서비스)를 클릭합니다.

3. 서비스 의 기본 탭은**System Services** 입니다. 대상, 소켓, 타이머 또는 경로를 관리하려면 상단 메뉴의 해당 탭으로 전환합니다.



4. 서비스 설정을 열려면 목록에서 선택한 서비스를 클릭합니다.

5. 서비스를 다시 시작하려면 재시작 버튼을 클릭합니다.



8장. 웹 콘솔을 사용하여 네트워크 본딩 구성

RHEL 9 웹 콘솔에서 네트워크 본딩의 작동 방식 및 네트워크 본딩을 구성하는 방법을 알아봅니다.

참고

RHEL 9 웹 콘솔은 NetworkManager 서비스를 기반으로 빌드됩니다.

자세한 내용은 네트워킹 관리를 위한 NetworkManager 시작하기 를 참조하십시오.

사전 요구 사항

- RHEL 9 웹 콘솔이 설치 및 활성화되어 있습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

8.1. 네트워크 본딩 이해

네트워크 본딩은 네트워크 인터페이스를 결합하거나 집계하여 처리량 또는 중복성이 높은 논리 인터페이스를 제공하는 방법입니다.

active-backup,balance-tlb 및 **balance-alb** 모드에는 네트워크 스위치의 특정 구성이 필요하지 않습니다. 그러나 다른 본딩 모드에서는 링크를 집계하도록 스위치를 구성해야 합니다. 예를 들어, Cisco 스위치는 0, 2 및 3 모드의 경우, 4 모드인 경우 LACP(Link Aggregation Control Protocol) 및 InstallPlan Channel 이 필요합니다.

자세한 내용은 스위치 및 **Linux** 이더넷 본딩 드라이버 **HOWTO** 설명서를 참조하십시오.

중요

장애 조치 메커니즘과 같은 특정 네트워크 본딩 기능은 네트워크 스위치 없이 직접 케이블 연결을 지원하지 않습니다. 자세한 내용은 크로스 오버 케이블을 사용하여 직접 연결과 함께 **Is bonding supported with direct connection**을참조하십시오. **KCS** 솔루션

8.2. 본딩 모드

RHEL 9에는 몇 가지 모드 옵션이 있습니다. 각 모드 옵션은 특정 로드 밸런싱 및 내결함성에 따라 특성화됩니다. 결합된 인터페이스의 동작은 모드에 따라 다릅니다. 본딩 모드는 내결함성, 로드 밸런싱 또는 둘 다를 제공합니다.

로드 밸런싱 모드

- 라운드 로빈: 첫 번째 사용 가능한 인터페이스에서 마지막 인터페이스로 패킷을 순차적으로 전송합니다.

내결함성 모드

- 활성 백업**:** 기본 인터페이스가 실패하는 경우에만 백업 인터페이스 중 하나를 대체합니다**.** 활성 인터페이스에서 사용하는 **MAC** 주소만 볼 수 있습니다**.**

- **broadcast:** 모든 전송은 모든 인터페이스에서 전송됩니다**.**

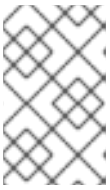
참고

브로드캐스트는 모든 결합된 인터페이스에서 네트워크 트래픽이 크게 증가합니다**.**

내결함성 및 로드 밸런싱 모드

- **XOR:** 대상 **MAC** 주소는 **modulo** 해시를 사용하는 인터페이스 간에 동일하게 배포됩니다**.** 각 인터페이스는 동일한 **MAC** 주소 그룹을 제공합니다**.**

- **802.3ad: IEEE 802.3ad** 동적 링크 집계 정책을 설정합니다**.** 동일한 속도 및 **duplex** 설정을 공유하는 집계 그룹을 만듭니다**.** 활성 집계기의 모든 인터페이스에서 전송 및 수신**.**



참고

이 모드에서는 **802.3ad** 호환 가능한 스위치가 필요합니다**.**

- 적응형 전송 로드 밸런싱**:** 발신 트래픽은 각 인터페이스의 현재 부하에 따라 배포됩니다**.** 현재 인터페이스에서 들어오는 트래픽을 수신합니다**.** 수신 인터페이스가 실패하면 다른 인터페이스는 실패한 인터페이스의 **MAC** 주소를 인수합니다**.**

- **Adaptive** 로드 밸런싱**: IPv4** 트래픽에 대한 전송 및 수신 부하 분산을 포함합니다**.**

ARP(Address Resolution Protocol) 협상을 통해 로드 밸런싱을 수행할 수 있으므로 본딩 구성에서 **Link Monitoring** 을 **ARP** 로 설정해야 합니다**.**

8.3. 웹 콘솔을 사용하여 새 본딩 추가

웹 콘솔을 사용하여 두 개 이상의 네트워크 인터페이스에서 **active-backup** 본딩을 구성합니다**.**

다른 네트워크 본딩 모드도 유사하게 구성할 수 있습니다.

사전 요구 사항

- 서버에 두 개 이상의 네트워크 카드가 설치되어 있습니다.
- 네트워크 카드가 스위치에 연결되어 있습니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 네트워킹을 엽니다.
3. **Add Bond** 버튼을 클릭합니다.
4. 본딩 설정 대화 상자에서 새 본딩의 이름을 입력합니다.
5. **Members** 필드에서 본딩 멤버여야 하는 인터페이스를 선택합니다.
6. **[선택 사항] MAC** 드롭 다운 목록에서 이 인터페이스에 사용할 **MAC** 주소를 선택합니다.

   MAC 필드를 비워 두면 본딩에서 드롭 다운 목록에 나열된 주소 중 하나를 가져옵니다.
7. 모드 드롭다운 목록에서 모드를 선택합니다.

   자세한 내용은 네트워크 본딩 모드를 참조하십시오.
8. 활성 백업을 선택하는 경우 기본 인터페이스를 선택합니다.

9. **Link Monitoring** (연결 모니터링) 드롭다운 메뉴에서 **MII** 옵션을 그대로 둡니다.

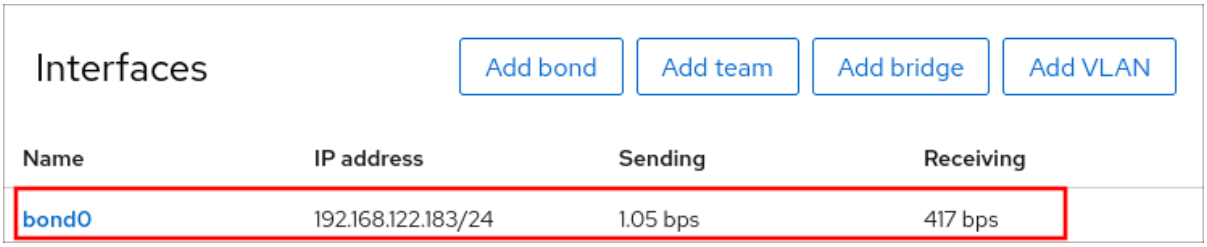
   적응형 로드 밸런싱 모드만 이 옵션을 **ARP** 로 전환해야 합니다.

10. **Monitoring Interval,Link up delay, Link down delay** 필드는 밀리초 단위 값을 포함합니다. 있는 그대로 두십시오. 문제 해결 목적으로만 값을 변경합니다.

11. 적용을 클릭합니다.

검증 단계

- 본딩이 올바르게 작동하는지 확인하려면 **Networking** (네트워킹) 섹션으로 이동하여 **Interfaces** (인터페이스) 테이블의 전송 및 수신자 열에 네트워크 활동이 표시되는지 확인합니다.



8.4. 웹 콘솔을 사용하여 본딩에 인터페이스 추가

네트워크 본딩에는 여러 인터페이스가 포함될 수 있으며 언제든지 인터페이스를 추가하거나 제거할 수 있습니다.

기존 본딩에 네트워크 인터페이스를 추가하는 방법을 알아봅니다.

사전 요구 사항

- 웹 콘솔을 사용하여 새 본딩 추가에 설명된 대로 여러 인터페이스가 구성된 본딩 사용

절차

1. 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 네트워킹을 엽니다.

3. **Interfaces** (인터페이스) 표에서 구성할 본딩을 클릭합니다.

4. 본딩 설정 화면에서 멤버 테이블(인터페이스)까지 아래로 스크롤합니다.

5. **Add member drop down** 아이콘을 클릭합니다.

6. 드롭다운 메뉴에서 인터페이스를 선택하고 클릭합니다.

검증 단계

- 선택한 인터페이스가 본딩 설정 화면의 **Interface members** 테이블에 표시되는지 확인합니다.

8.5. 웹 콘솔을 사용하여 본딩에서 인터페이스 제거 또는 비활성화

네트워크 본딩에는 여러 인터페이스가 포함될 수 있습니다. 장치를 변경해야 하는 경우 본딩에서 특정 인터페이스를 제거하거나 비활성화할 수 있으며 이는 활성 인터페이스의 나머지 부분과 함께 작동합니다.

본딩에 포함된 인터페이스 사용을 중지하려면 다음을 수행할 수 있습니다.

- 본딩에서 인터페이스를 제거합니다.

- 인터페이스를 일시적으로 비활성화합니다. 인터페이스는 본딩의 일부를 유지하지만, 다시 활성화할 때까지 본딩은 사용하지 않습니다.

사전 요구 사항

- 웹 콘솔을 사용하여 새 본딩 추가에 설명된 대로 여러 인터페이스가 구성된 본딩 사용

절차

1. **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 네트워킹을 엽니다.
3. 구성할 본딩을 클릭합니다.
4. 본딩 설정 화면에서 포트 테이블(인터페이스)까지 아래로 스크롤합니다.
5. 인터페이스를 선택하고 제거하거나 비활성화합니다.
   - 인터페이스를 제거하려면 **-** 버튼을 클릭합니다.
   - 인터페이스를 비활성화하거나 활성화하려면 선택한 인터페이스 옆에 있는 스위치를 토글합니다.

선택한 상황에 따라 웹 콘솔은 본딩에서 인터페이스를 제거하거나 비활성화하여 네트워킹 섹션에서 독립 실행형 인터페이스로 다시 볼 수 있습니다.

8.6. 웹 콘솔을 사용하여 본딩 제거 또는 비활성화

웹 콘솔을 사용하여 네트워크 본딩을 제거하거나 비활성화합니다. 본딩을 비활성화하면 인터페이스는 본딩에 그대로 유지되지만 네트워크 트래픽에는 본딩이 사용되지 않습니다.

사전 요구 사항

- 웹 콘솔에는 기존 본딩이 있습니다.

절차

1. 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 네트워킹을 엽니다.

3. 제거할 본딩을 클릭합니다.

4. 본딩 설정 화면에서 전환기를 전환하거나 삭제 버튼을 클릭하여 본딩을 비활성화하거나 활성화하여 본딩을 영구적으로 제거할 수 있습니다.

검증 단계

- 네트워킹 으로 돌아가서 본딩의 모든 인터페이스가 이제 독립 실행형 인터페이스인지 확인합니다.

9장. 웹 콘솔을 사용하여 네트워크 팀 구성

네트워크 본딩의 작동 방식, 네트워크 팀과 네트워크 본딩 간의 차이점 및 웹 콘솔에서 구성 가능성에 대해 알아보십시오.

다음에 대한 지침을 찾을 수도 있습니다.

- 새 네트워크 팀 추가
- 기존 네트워크 팀에 새 인터페이스 추가
- 기존 네트워크 팀에서 인터페이스 제거
- 네트워크 팀 제거

중요

Red Hat Enterprise Linux 9에서는 네트워크 티밍이 더 이상 사용되지 않습니다. 대안으로 네트워크 본딩 드라이버를 사용하는 것이 좋습니다. 자세한 내용은 네트워크 본딩 구성을 참조하십시오.

사전 요구 사항

- **RHEL** 웹 콘솔이 설치 및 활성화되었습니다.

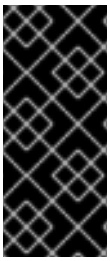
  자세한 내용은 웹 콘솔 설치를 참조하십시오.

9.1. 네트워크 티밍 이해

네트워크 티밍은 네트워크 인터페이스를 결합하거나 집계하여 처리량 또는 중복성이 높은 논리 인터페이스를 제공하는 기능입니다.

네트워크 티밍은 커널 드라이버를 사용하여 패킷 흐름을 빠르게 처리하는 것은 물론, 다른 작업을 위한 사용자 공간 라이브러리 및 서비스를 구현합니다. 이렇게 하면 네트워크 티밍은 부하 분산 및 중복성 요구

사항을 위한 쉽게 확장 가능하고 확장 가능한 솔루션입니다.



중요

장애 조치 메커니즘과 같은 특정 네트워크 티밍 기능은 네트워크 스위치 없이 직접 케이블 연결을 지원하지 않습니다. 자세한 내용은 크로스 오버 케이블을 사용하여 직접 연결에 지원되는 본딩을 참조하십시오.

9.2. 네트워크 티밍 및 본딩 기능 비교

네트워크 팀 및 네트워크 본딩에서 지원되는 기능에 대해 알아보십시오.

기능	네트워크 본딩	네트워크 팀
브로드캐스트 Tx 정책	있음	있음
라운드 로빈 Tx 정책	있음	있음
active-backup Tx 정책	있음	있음
LACP (802.3ad) 지원	예 (활성 전용)	있음
해시 기반 Tx 정책	있음	있음
사용자가 해시 함수를 설정할 수 있습니다.	없음	있음
TX 로드 밸런싱 지원(TLB)	있음	있음
LACP 해시 포트 선택	있음	있음
LACP 지원 로드 밸런싱	없음	있음
ethtool 링크 모니터링	있음	있음
ARP 링크 모니터링	있음	있음
NS/NA (IPv6) 링크 모니터링	없음	있음
포트 up/down delay	있음	있음
포트 우선순위 및 고정("기본" 옵션 개선)	없음	있음
별도의 포트별 링크 모니터링 설정	없음	있음

기능	네트워크 본딩	네트워크 팀
다중 링크 모니터링 설정	제한됨	있음
Lockless Tx/Rx 경로	아니요(rwlock)	예 (Rcus)
VLAN 지원	있음	있음
사용자 공간 런타임 제어	제한됨	있음
사용자 공간의 논리	없음	있음
확장성	하드	쉬움
모듈 설계	없음	있음
성능 오버헤드	낮음 (LOW)	매우 낮은
D-Bus 인터페이스	없음	있음
다중 장치 스택	있음	있음
LLDP를 사용하는 제로 구성	없음	(계획으로)
NetworkManager 지원	있음	있음

9.3. 웹 콘솔을 사용하여 새 팀 추가

웹 콘솔을 사용하여 두 개 이상의 네트워크 인터페이스에서 새로운 활성 백업 네트워크 팀을 구성합니다.

사전 요구 사항

- 서버에 두 개 이상의 네트워크 카드가 설치되어 있습니다.
- 네트워크 카드가 스위치에 연결되어 있습니다.

절차

1. 웹 콘솔에 로그인합니다.

자세한 내용은 웹 콘솔에 로깅을참조하십시오.

2. **Networking** 탭으로 이동합니다.

3. **Add Team (**팀 추가**)** 버튼을 클릭합니다.

4. 팀 설정 영역에서 새 팀의 매개 변수를 구성합니다.

   a. 팀 장치의 이름을 이름 필드에 추가합니다.

   b. **Ports (**포트**)** 필드에서 팀에 추가할 모든 네트워크 인터페이스를 선택합니다.

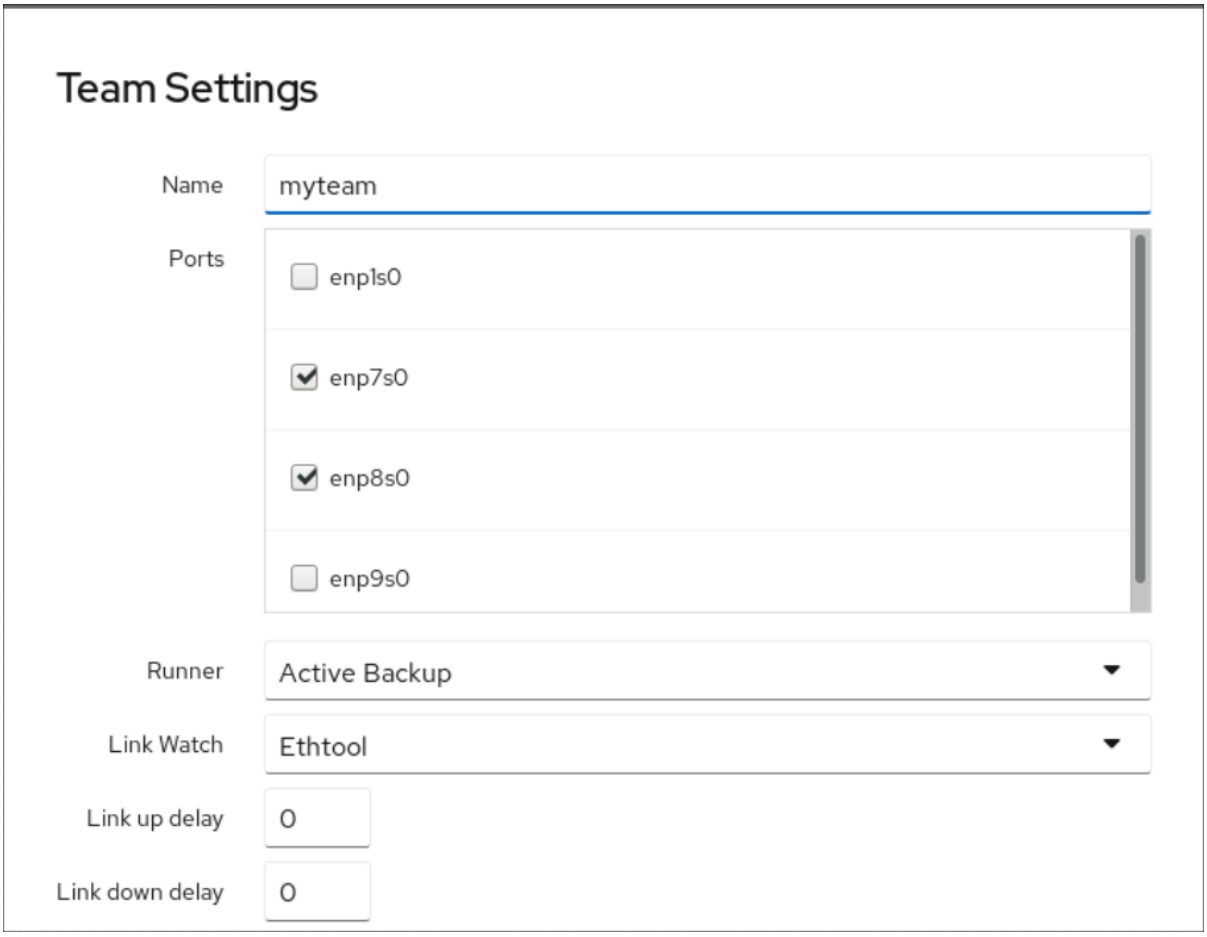
   c. **Runner** 드롭다운 메뉴에서 러너를 선택합니다.

   d. **Link Watch** 드롭다운 메뉴에서 링크를 선택합니다.

      i. **Ethtool** 을 선택하는 경우 링크 업 지연 및 링크 다운 지연을 설정합니다.

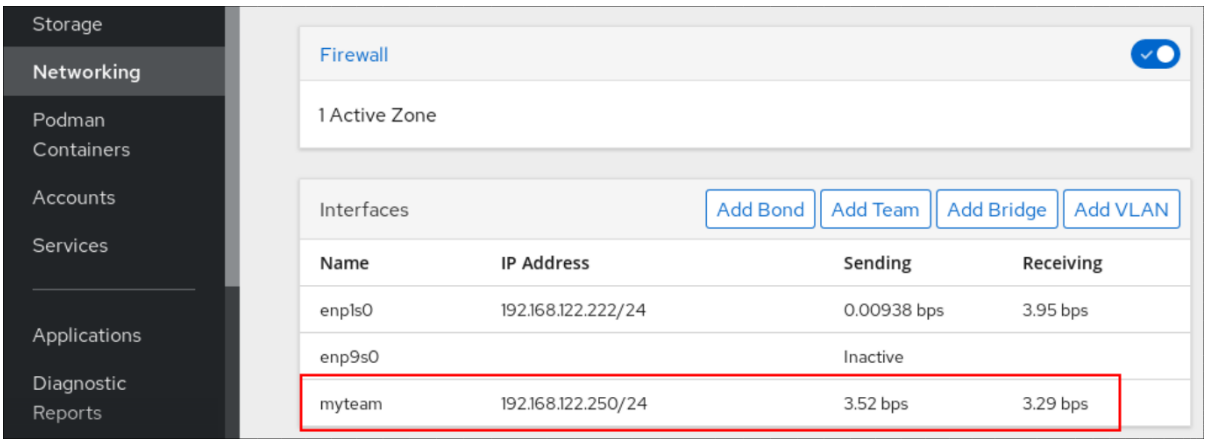
      ii. **ARP Ping** 또는 **NSNA Ping** 을 선택하는 경우 **ping** 간격과 **ping** 대상을 설정합니다.

5. 적용을클릭합니다.



검증 단계

1. **Networking** 탭으로 이동하여 **Interfaces(**인터페이스**)** 테이블의 전송 및 회수 열에 네트워크 활동이 표시되는지 확인합니다**.**



추가 리소스

- 네트워크 팀 러너

9.4. 웹 콘솔을 사용하여 팀에 새 인터페이스 추가

네트워크 팀은 여러 인터페이스를 포함할 수 있으며 언제든지 인터페이스를 추가하거나 제거할 수 있습니다. 다음 섹션에서는 기존 팀에 새 네트워크 인터페이스를 추가하는 방법을 설명합니다.

사전 요구 사항

- 네트워크 팀이 구성되어 있습니다.

절차

1. 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

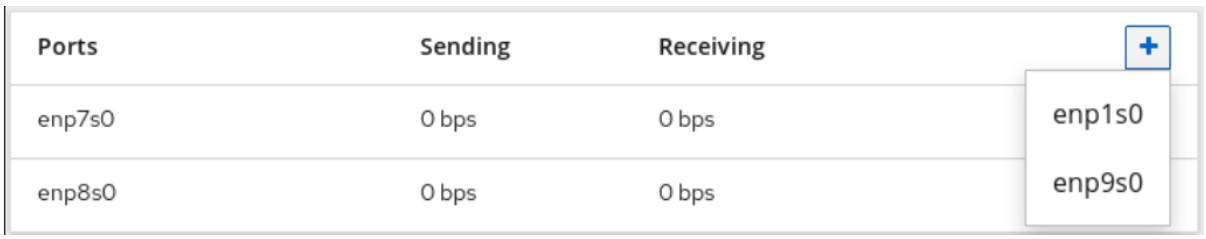
2. 네트워킹 탭으로 전환합니다.

3. **Interfaces** (인터페이스) 표에서 구성할 팀을 클릭합니다.

4. 팀 설정 창에서 **Ports** 테이블까지 아래로 스크롤합니다.

5. **+** 아이콘을 클릭합니다.

6. 드롭다운 목록에서 추가할 인터페이스를 선택합니다.



RHEL 웹 콘솔은 인터페이스를 팀에 추가합니다.

9.5. 웹 콘솔을 사용하여 팀에서 인터페이스 제거 또는 비활성화

네트워크 팀에는 여러 인터페이스가 포함될 수 있습니다. 장치를 변경해야 하는 경우 네트워크 팀에서 특정 인터페이스를 제거하거나 비활성화할 수 있으며 이는 나머지 활성 인터페이스와 함께 작동합니다.

팀에 포함된 인터페이스 사용을 중지하는 방법에는 두 가지가 있습니다.

- 팀에서 인터페이스 제거
- 일시적으로 인터페이스를 비활성화합니다. 그런 다음 인터페이스는 팀의 일부를 유지하지만 다시 활성화할 때까지 팀은 사용하지 않습니다.

사전 요구 사항

- 호스트에 여러 인터페이스가 있는 네트워크 팀이 있습니다.

절차

1. **RHEL** 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 네트워킹 탭으로 전환합니다.

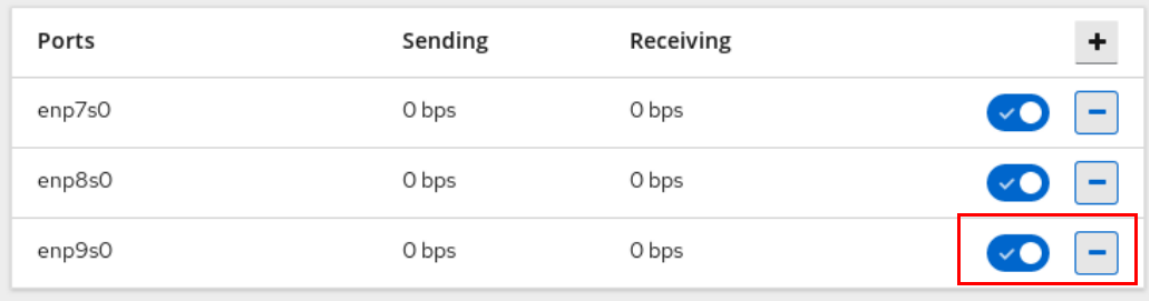
3. 구성할 팀을 클릭합니다.

4. 팀 설정 창에서 포트(인터페이스) 테이블까지 아래로 스크롤합니다.

5. 인터페이스를 선택하고 제거하거나 비활성화합니다.

a. **ON/OFF (**켜짐/꺼짐**)** 버튼을 **Off**로 전환하여 인터페이스를 비활성화합니다.

b. 인터페이스를 제거하려면 **-** 아이콘을 클릭합니다.



사용자 선택에 따라 웹 콘솔은 인터페이스를 제거하거나 비활성화합니다. 인터페이스를 제거하면 **Networking** 에서 독립 실행형 인터페이스로 사용할 수 있습니다.

9.6. 웹 콘솔을 사용하여 팀 제거 또는 비활성화

웹 콘솔을 사용하여 네트워크 팀을 제거하거나 비활성화합니다. 팀만 비활성화하면 팀의 인터페이스는 그대로 유지되지만 팀은 네트워크 트래픽에 사용되지 않습니다.

사전 요구 사항

- 네트워크 팀이 호스트에 구성되어 있습니다.

절차

1. 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 네트워킹 탭으로 전환합니다.

3. 제거 또는 비활성화하려는 팀을 클릭합니다.

4.

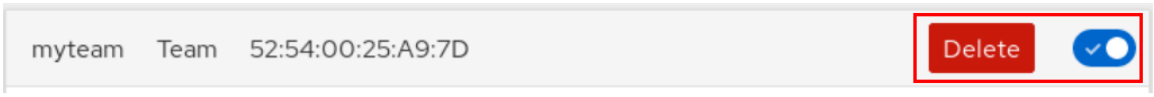
선택한 팀을 제거하거나 비활성화합니다.

a.

삭제 버튼을 클릭하여 팀을 제거할 수 있습니다.

b.

ON/OFF (켜짐/꺼짐**)** 스위치를 비활성화된 위치로 이동하여 팀을 비활성화할 수 있습니다.



검증 단계

- 팀을 제거한 경우 **Networking** 으로 이동하여 팀의 모든 인터페이스가 이제 독립 실행형 인터페이스로 나열되는지 확인합니다.

10장. 웹 콘솔에서 네트워크 브리지 구성

네트워크 브리지는 동일한 범위의 **IP** 주소를 사용하여 여러 인터페이스를 하나의 서브넷에 연결하는 데 사용됩니다.

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치 및 활성화되어 있습니다.

  자세한 내용은 웹 콘솔 설치를 참조하십시오.

10.1. 웹 콘솔에서 브리지 추가

웹 콘솔을 사용하여 여러 네트워크 인터페이스에 소프트웨어 브릿지를 만듭니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 네트워킹을 엽니다.

3. 브리지 추가 버튼을 클릭합니다.

4. 브리지 설정 대화 상자에서 새 브리지의 이름을 입력합니다.

5. 포트 필드에서 하나의 서브넷에 배치할 인터페이스를 선택합니다.

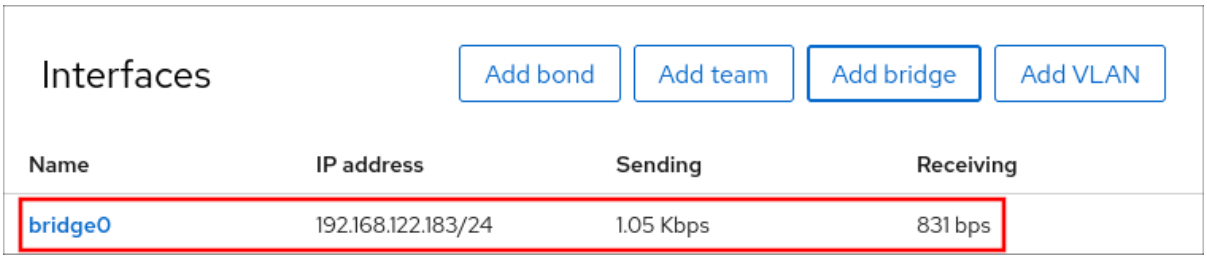
6. 필요한 경우 스파**nning Tree Protocol (STP)** 을 선택하여 브리지 루프 및 브로드캐스트를 방지할 수 있습니다.

7. 생성을 클릭합니다.

검증 단계

1. 네트워킹 으로 이동하여 새 브래그가 **Interfaces (**인터페이스**)** 테이블에 표시되는지 확인합니다**.**

2. 새 브리지 행의 전송 및 회수 열에서 값을 확인합니다**.**



브리지를 통해 **0**바이트가 전송되고 수신되었음을 확인할 수 있는 경우 연결이 올바르게 작동하지 않고 네트워크 설정을 조정해야 합니다**.**

10.2. 웹 콘솔에서 고정 IP 주소 구성

시스템의 **IP** 주소는 **DHCP** 서버에서 자동으로 풀에서 할당하거나 **IP** 주소를 수동으로 구성할 수 있습니다**. IP** 주소는 **DHCP** 서버 설정의 영향을 받지 않습니다**.**

RHEL 웹 콘솔을 사용하여 네트워크 브리지의 정적 **IPv4** 주소를 구성하는 방법을 알아봅니다**.**

절차

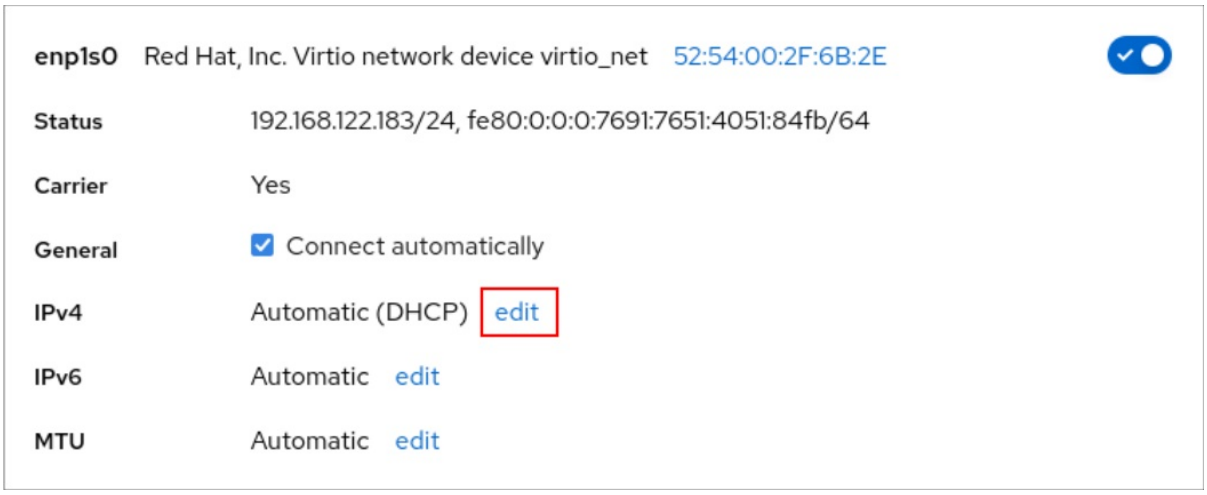
1. **RHEL** 웹 콘솔에 로그인합니다**.**

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오**.**

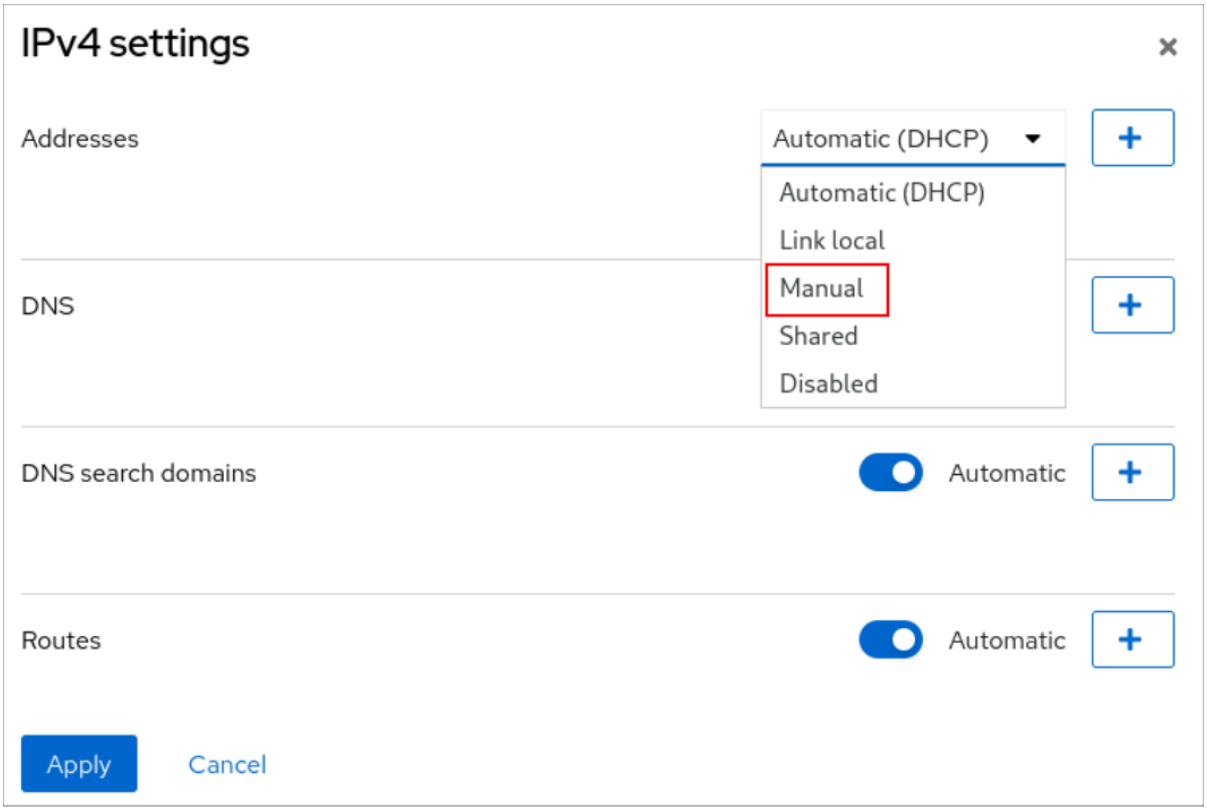
2. 네트워킹 섹션을 엽니다**.**

3. 고정 **IP** 주소를 설정할 인터페이스를 클릭합니다**.**

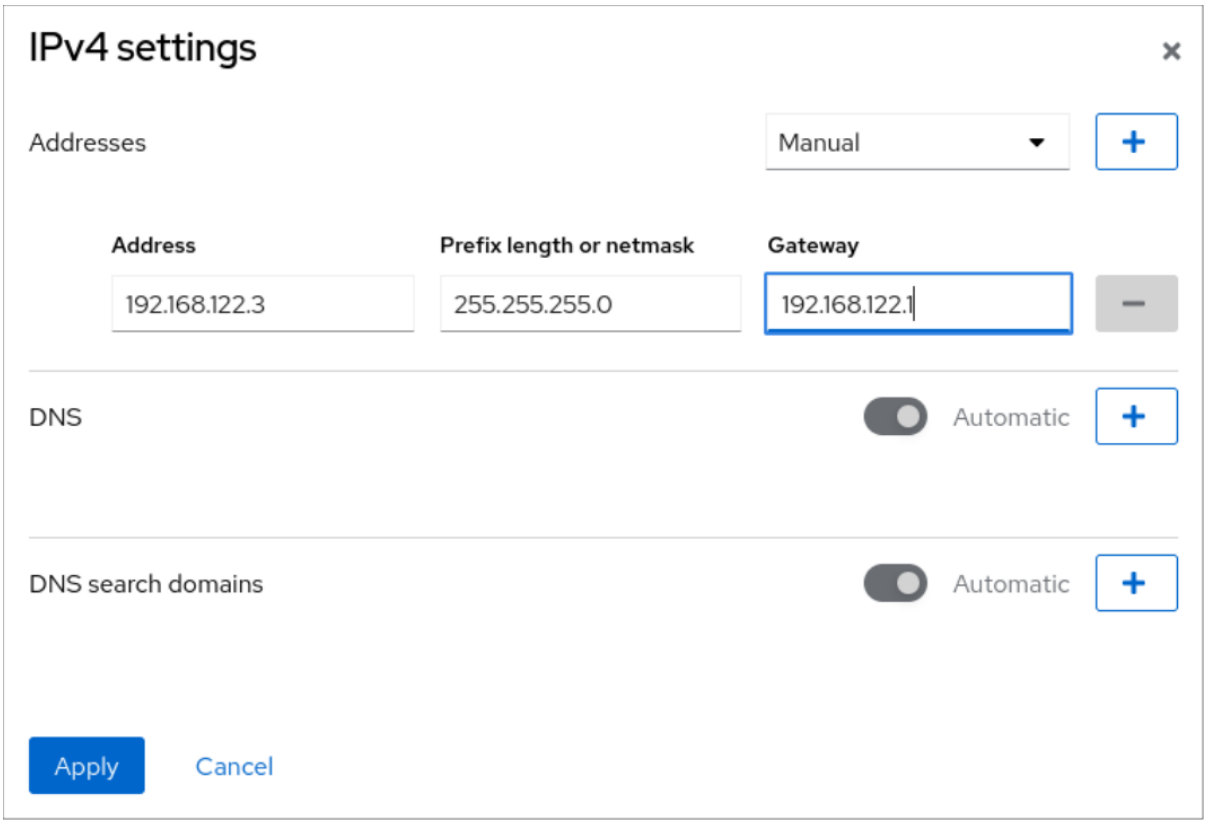
4. 인터페이스 세부 정보 화면의 **IPv4** 행에서 편집 을 클릭합니다.



5. **IPv4** 설정 대화 상자의 주소 드롭다운 목록에서 **Manual** 을 선택합니다.



6. **Addresses** 필드에 원하는 **IP** 주소, 넷마스크 및 게이트웨이를 입력합니다.



7. 적용을 클릭합니다.

검증 단계

- 브리지 세부 정보 표의 **IPv4** 행에 새 고정 **IP** 주소가 표시되는지 확인합니다.

10.3. 웹 콘솔을 사용하여 브리지에서 인터페이스 제거

네트워크 브릿지에는 여러 인터페이스가 포함될 수 있습니다. 브리지에서 제거할 수 있습니다. 제거된 각 인터페이스는 독립 실행형 인터페이스로 자동으로 변경됩니다.

RHEL 9 시스템에서 생성된 소프트웨어 브릿지에서 네트워크 인터페이스를 제거하는 방법을 알아봅니다.

사전 요구 사항

- 시스템에 여러 인터페이스가 있는 브리지 사용.

절차

1. **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 네트워킹을 엽니다.
3. 구성할 브리지를 클릭합니다.
4. 브리지 설정 화면에서 포트 테이블(인터페이스)까지 아래로 스크롤합니다.
5. 인터페이스를 선택하고 **-** 버튼을 클릭합니다.

검증 단계

- 네트워킹 으로 이동하여 인터페이스 멤버 테이블에서 인터페이스를 독립 실행형 인터페이스로 볼 수 있는지 확인합니다.

10.4. 웹 콘솔에서 브리지 삭제

RHEL 웹 콘솔에서 소프트웨어 네트워크 브릿지를 삭제할 수 있습니다. 브리지에 포함된 모든 네트워크 인터페이스는 독립 실행형 인터페이스로 자동으로 변경됩니다.

사전 요구 사항

- 시스템에 브리지가 있어야 합니다.

절차

1. **RHEL** 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 네트워킹 섹션을 엽니다.

3. 구성할 브리지를 클릭합니다.

4. 삭제를 클릭합니다.

검증 단계

- 네트워킹 으로 돌아가서 모든 네트워크 인터페이스가 인터페이스 멤버 테이블에 표시되는지 확인합니다.

이전에 브리지의 일부인 일부 인터페이스는 비활성 상태가 될 수 있습니다. 필요한 경우 이를 활성화하고 네트워크 매개 변수를 수동으로 설정합니다.

11장. 웹 콘솔에서 VLAN 구성

VLAN(Virtual LAN)은 단일 물리적 이더넷 인터페이스에서 생성된 가상 네트워크입니다. 각 **VLAN**은 고유한 양의 정수를 나타내는 **ID**로 정의되며 독립 실행형 인터페이스로 작동합니다.

RHEL 웹 콘솔에서 **VLAN**을 생성하는 방법을 알아봅니다.

사전 요구 사항

- **RHEL** 웹 콘솔이 설치되어 액세스할 수 있습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- 시스템에 네트워크 인터페이스가 있어야 합니다.

절차

1. **RHEL** 웹 콘솔에 로그인합니다.

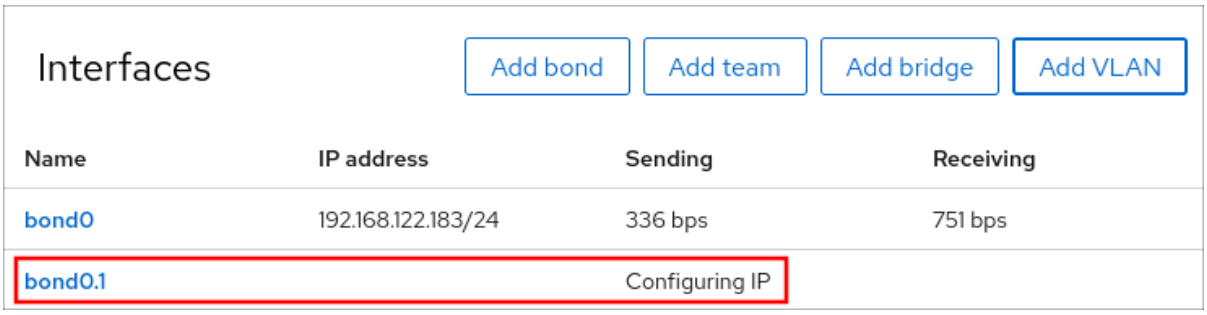
   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 네트워킹을 엽니다.
3. **VLAN** 추가 버튼을 클릭합니다.
4. **VLAN** 설정 대화 상자에서 **VLAN**을 생성할 실제 인터페이스를 선택합니다.
5. **VLAN ID**를 입력하거나 사전 정의된 번호를 사용합니다.
6. 이름 필드에는 상위 인터페이스와 **VLAN ID**로 구성된 사전 정의된 이름을 볼 수 있습니다. 필요하지 않은 경우 이름을 그대로 둡니다.

7. 적용을 클릭합니다.

검증 단계

- **Networking** (네트워킹)으로 이동하여 새 **VLAN**이 **Interfaces** (인터페이스) 테이블에 표시되는지 확인합니다.



네트워크 설정을 구성하려면 표에 새로 생성된 **VLAN**을 클릭합니다.

12장. 웹 콘솔 청취 포트 구성

RHEL 9 웹 콘솔을 사용하여 새 포트를 허용하거나 기존 포트를 변경하는 방법을 알아봅니다.

12.1. 활성 SELINUX로 시스템의 새 포트 허용

웹 콘솔을 활성화하여 선택한 포트에서 수신 대기합니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

- SELinux의 다른 부분에서 정의되지 않은 포트의 경우 다음을 실행합니다.

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

- SELinux의 다른 부분에서 이미 정의된 포트의 경우 다음을 실행합니다.

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

변경 사항은 즉시 적용됩니다.

12.2. FIREWALLD를 사용하여 시스템에서 새 포트 허용

웹 콘솔을 활성화하여 새 포트에서 연결을 수신합니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- firewalld 서비스가 실행 중이어야 합니다.

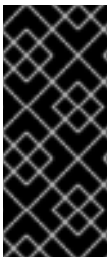
절차

1. 새 포트 번호를 추가하려면 다음 명령을 실행합니다.

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

2. **cockpit** 서비스에서 이전 포트 번호를 제거하려면 다음을 실행합니다.

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



중요

--permanent 옵션 없이 **firewall-cmd --service cockpit --add-port=PORT_NUMBER/tcp** 만 실행하면 **firewalld** 또는 시스템 재부팅이 다시 로드되면 변경 사항이 사라집니다.

12.3. 웹 콘솔 포트 변경

포트 **9090** 의 기본 **TCP(Transmission Control Protocol)**를 다른 하나로 변경합니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- **SELinux**가 시스템을 보호하는 경우 **Cockpit**이 새 포트에서 수신 대기하도록 설정해야 합니다. 자세한 내용은 활성 **SELinux**를 사용하여 시스템에서 새 포트 허용 을 참조하십시오.
- **firewalld** 를 방화벽으로 구성한 경우 새 포트에서 **Cockpit** 수신 연결을 허용하도록 설정해야 합니다. 자세한 내용은 **firewalld**를 사용하여 시스템에서 새 포트 허용 을 참조하십시오.

절차

1. 다음 방법 중 하나로 수신 대기 포트를 변경합니다.

   a. **systemctl edit cockpit.socket** 명령을 사용하여 다음을 수행합니다.

i. 다음 명령을 실행합니다.

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

그러면 **/etc/systemd/system/cockpit.socket.d/override.conf** 파일이 열립니다.

ii. **override.conf** 의 내용을 수정하거나 다음 형식으로 새 콘텐츠를 추가합니다.

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

b. 또는 위에 언급된 내용을 **/etc/systemd/system/cockpit.socket.d/listen.conf** 파일에 추가합니다.

cockpit.socket.d. 디렉터리가 없는 경우 **listen.conf** 파일을 생성합니다.

2. 변경 사항을 적용하려면 다음 명령을 실행합니다.

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

이전 단계에서 **systemctl edit cockpit.socket** 을 사용한 경우 **systemctl daemon-reload** 를 실행할 필요가 없습니다.

검증 단계

- 변경 사항이 성공했는지 확인하려면 새 포트를 사용하여 웹 콘솔에 연결하십시오.

13장. 웹 콘솔을 사용하여 방화벽 관리

방화벽은 원치 않는 트래픽으로부터 컴퓨터를 외부로부터 보호하는 방법입니다. 사용자가 방화벽 규칙 세트를 정의하여 호스트 시스템에서 들어오는 네트워크 트래픽을 제어할 수 있습니다. 이러한 규칙은 들어오는 트래픽을 정렬하고 차단하거나 를 허용하는 데 사용됩니다.

사전 요구 사항

- **RHEL 9** 웹 콘솔은 **firewalld** 서비스를 구성합니다.

  firewalld 서비스에 대한 자세한 내용은 **firewalld** 시작하기를 참조하십시오.

13.1. 웹 콘솔을 사용하여 방화벽 실행

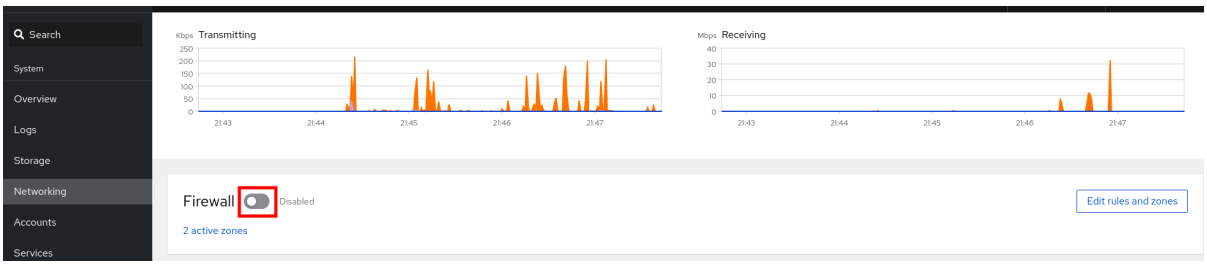
이 섹션에서는 웹 콘솔에서 **RHEL 9** 시스템 방화벽을 실행하는 위치와 방법에 대해 설명합니다.

참고

RHEL 9 웹 콘솔은 **firewalld** 서비스를 구성합니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 네트워킹 섹션을 엽니다.
3. 방화벽 섹션에서 슬라이더를 클릭하여 방화벽을 실행합니다.



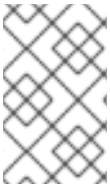
방화벽 슬라이더가 표시되지 않으면 관리 권한을 사용하여 웹 콘솔에 로그인합니다.

이 단계에서는 방화벽이 실행 중입니다.

방화벽 규칙을 구성하려면 웹 콘솔을 사용하여 방화벽에서 서비스 활성화를참조하십시오.

13.2. 웹 콘솔을 사용하여 방화벽 중지

이 섹션에서는 웹 콘솔에서 **RHEL 9** 시스템 방화벽을 중지하는 위치와 방법에 대해 설명합니다.

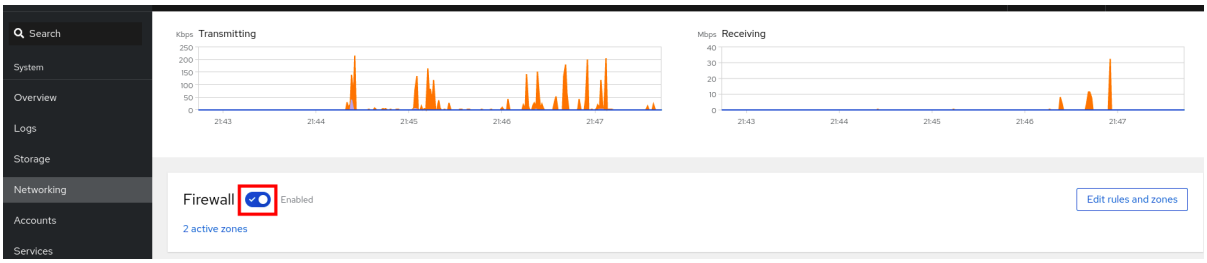


참고

RHEL 9 웹 콘솔은 **firewalld** 서비스를 구성합니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 네트워킹 섹션을 엽니다.
3. 방화벽 섹션에서 슬라이더를 클릭하여 방화벽을 중지합니다.**In the Firewall section, click the slider to stop the firewall.**



방화벽 슬라이더가 표시되지 않으면 관리 권한을 사용하여 웹 콘솔에 로그인합니다.

이 단계에서는 방화벽이 중지되었으며 사용자 시스템을 보호하지 않습니다.

13.3. 영역

firewalld 는 사용자가 해당 네트워크 내의 인터페이스와 트래픽에 배치하기로 결정한 신뢰 수준에 따라 네트워크를 다른 영역으로 분리하는 데 사용할 수 있습니다. 연결은 하나의 영역에만 속할 수 있지만, 여러 네트워크 연결에 영역을 사용할 수 있습니다.

NetworkManager 는 인터페이스 영역을 **firewalld** 에 알립니다. 다음을 사용하여 인터페이스에 영역을 할당할 수 있습니다.

- **NetworkManager**
- **firewall-config** 도구
- **firewall-cmd** 명령줄 도구
- **RHEL** 웹 콘솔

후자의 세 가지는 적절한 **NetworkManager** 구성 파일만 편집할 수 있습니다. 웹 콘솔, **firewall-cmd** 또는 **firewall-config** 를 사용하여 인터페이스의 영역을 변경하면 요청이 **NetworkManager** 로 전달되고**firewalld** 에서 처리되지 않습니다.

사전 정의된 영역은 **/usr/lib/firewalld/zones/** 디렉터리에 저장되며 사용 가능한 모든 네트워크 인터페이스에 즉시 적용할 수 있습니다. 이러한 파일은 수정된 후에만 **/etc/firewalld/zones/** 디렉토리에 복사됩니다. 사전 정의된 영역의 기본 설정은 다음과 같습니다.

블록

들어오는 네트워크 연결은 **IPv4** 및 **IPv6** 용으로 **icmp6-adm-prohibited**에 대한 **icmp-host-prohibited** 메시지와 함께 거부됩니다. 시스템 내에서 시작된 네트워크 연결만 가능합니다.

dmz

내부 네트워크에 대한 제한된 액세스 권한으로 공개적으로 액세스할 수 있는 내구성 있는 영역의 컴퓨터의 경우. 선택한 들어오는 연결만 허용됩니다.

drop

들어오는 모든 네트워크 패킷은 알림 없이 삭제됩니다. 발신 네트워크 연결만 가능합니다.

external

특히 라우터의 경우 마스커레이딩이 활성화된 외부 네트워크에서 사용합니다. 네트워크의 다른 컴퓨터를 신뢰하지 않고 컴퓨터를 손상시키지 않습니다. 선택한 들어오는 연결만 허용됩니다.

집

대부분 네트워크에있는 다른 컴퓨터를 신뢰할 때 집에서 사용하기 위해. 선택한 들어오는 연결만 허용됩니다.

internal

내부 네트워크에서 사용되는 경우 네트워크의 다른 컴퓨터를 대부분 신뢰할 수 있습니다. 선택한 들어오는 연결만 허용됩니다.

공개

네트워크의 다른 컴퓨터를 신뢰하지 않는 공공 영역에서 사용하기 위해. 선택한 들어오는 연결만 허용됩니다.

trusted

모든 네트워크 연결이 허용됩니다.

work

네트워크의 다른 컴퓨터를 대부분 신뢰할 수 있는 작업에서 사용하기 위해 선택한 들어오는 연결만 허용됩니다.

이러한 영역 중 하나는 *기본* 영역으로 설정됩니다. **NetworkManager** 에 인터페이스 연결이 추가되면 기본 영역에 할당됩니다. 설치 시 **firewalld** 의 기본 영역이 공개 영역으로 설정됩니다. 기본 영역을 변경할 수 있습니다.

참고

네트워크 영역 이름은 설명적이어야 하며 사용자가 신속하게 합리적인 결정을 내릴 수 있도록 해야 합니다. 보안 문제를 방지하려면 기본 영역 구성을 검토하고 요구 사항 및 위험 평가에 따라 불필요한 서비스를 비활성화합니다.

추가 리소스

- **firewalld.zone(5)** 도움말 페이지.

13.4. 웹 콘솔의 영역

Red Hat Enterprise Linux 웹 콘솔은 **firewalld** 서비스의 주요 기능을 구현하고 다음을 수행할 수 있습니다.

- 특정 인터페이스 또는 **IP** 주소 범위에 사전 정의된 방화벽 영역 추가
- 활성화된 서비스 목록으로 서비스를 선택하여 영역 구성
- 활성화된 서비스 목록에서 이 서비스를 제거하여 서비스를 비활성화합니다.
- 인터페이스에서 영역 제거

13.5. 웹 콘솔을 사용하여 영역 활성화

웹 콘솔을 사용하면 특정 인터페이스 또는 범위의 **IP** 주소에 사전 정의된 및 기존 방화벽 영역을 적용할 수 있습니다. 이 섹션에서는 인터페이스에서 영역을 활성화하는 방법에 대해 설명합니다.

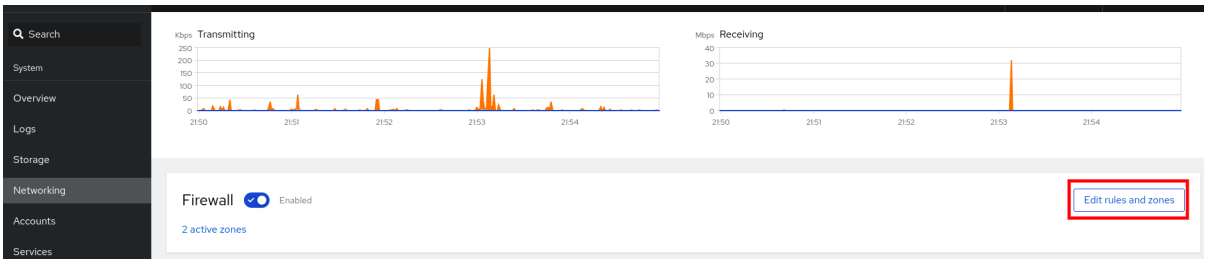
사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- 방화벽을 활성화해야 합니다. 자세한 내용은 웹 콘솔을 사용하여 방화벽 실행을 참조하십시오.

절차

1. 관리 권한을 사용하여 **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 네트워킹을 클릭합니다.

3. 규칙 및 영역 편집 버튼을 클릭합니다.



규칙 및 영역 편집 버튼이 표시되지 않으면 관리자 권한을 사용하여 웹 콘솔에 로그인합니다.

4. 방화벽 섹션에서 새 영역 추가 를 클릭합니다.

5. 영역 추가 대화 상자의 신뢰 수준 옵션에서 영역을 선택합니다.

여기에서 **firewalld** 서비스에서 사전 정의된 모든 영역을 볼 수 있습니다.

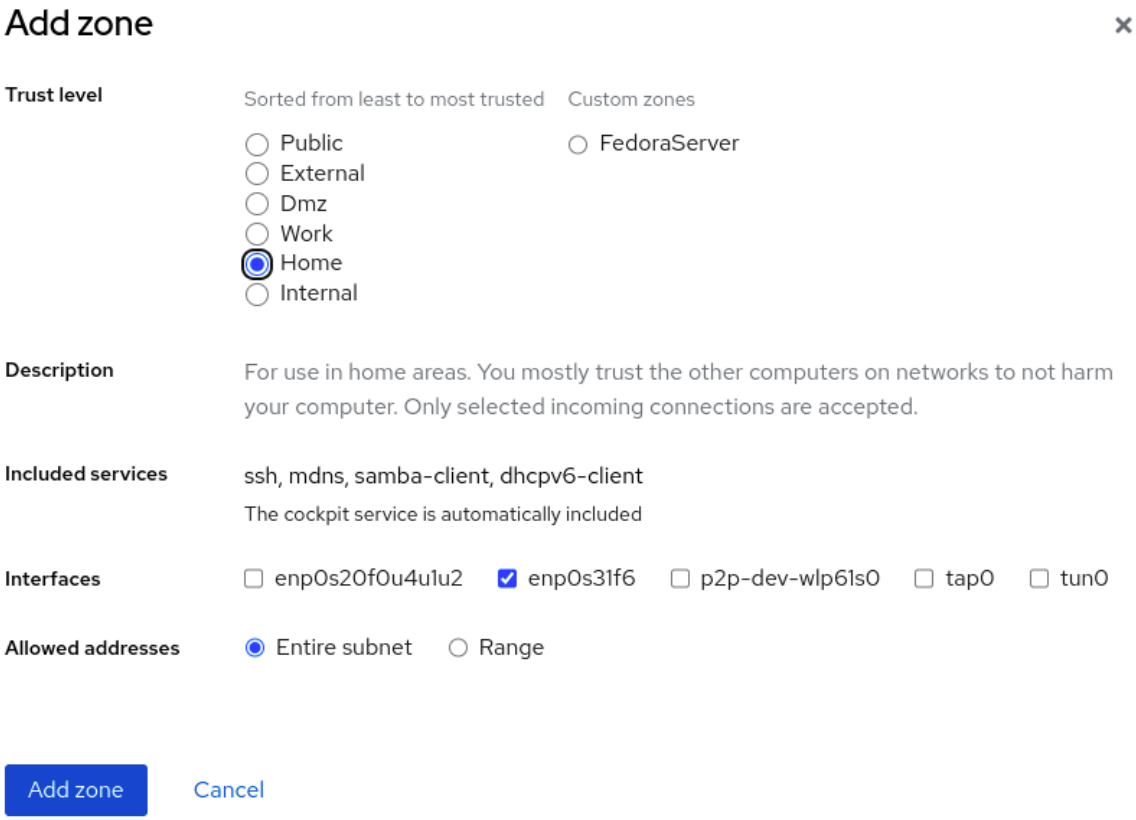
6. **Interfaces** (인터페이스) 부분에서 선택한 영역이 적용되는 인터페이스 또는 인터페이스를 선택합니다.

7. 허용된 주소 부분에서는 영역이 적용되는지 선택할 수 있습니다.

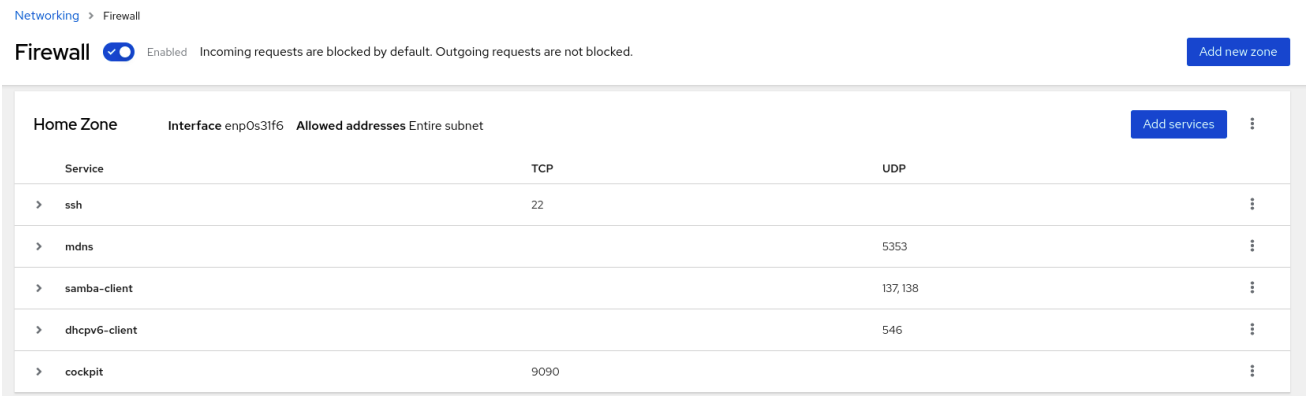
- 전체 서브넷
- 다음 형식의 **IP** 주소 범위:
  - **192.168.1.0**
  - **192.168.1.0/24**

- **192.168.1.0/24, 192.168.1.0**

8. **Add zone** 버튼을 클릭합니다.



방화벽 에서 구성을 확인합니다.



13.6. 웹 콘솔을 사용하여 방화벽에서 서비스 활성화

기본적으로 서비스는 기본 방화벽 영역에 추가됩니다. 더 많은 네트워크 인터페이스에서 방화벽 영역을 더 사용하는 경우 먼저 영역을 선택하고 포트를 사용하여 서비스를 추가해야 합니다.

RHEL 9 웹 콘솔은 사전 정의된 **firewalld** 서비스를 표시하며 활성 방화벽 영역에 추가할 수 있습니다.

중요

RHEL 9 웹 콘솔은 **firewalld** 서비스를 구성합니다.

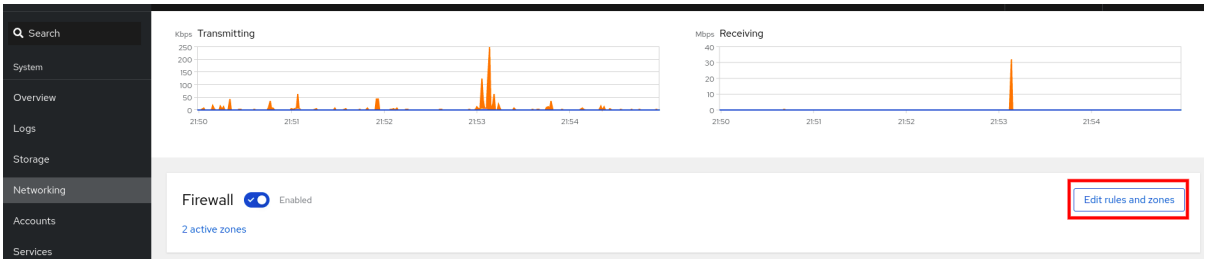
웹 콘솔에서는 웹 콘솔에 나열되지 않은 일반 **firewalld** 규칙을 허용하지 않습니다.

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- 방화벽을 활성화해야 합니다. 자세한 내용은 웹 콘솔을 사용하여 방화벽 실행을 참조하십시오.

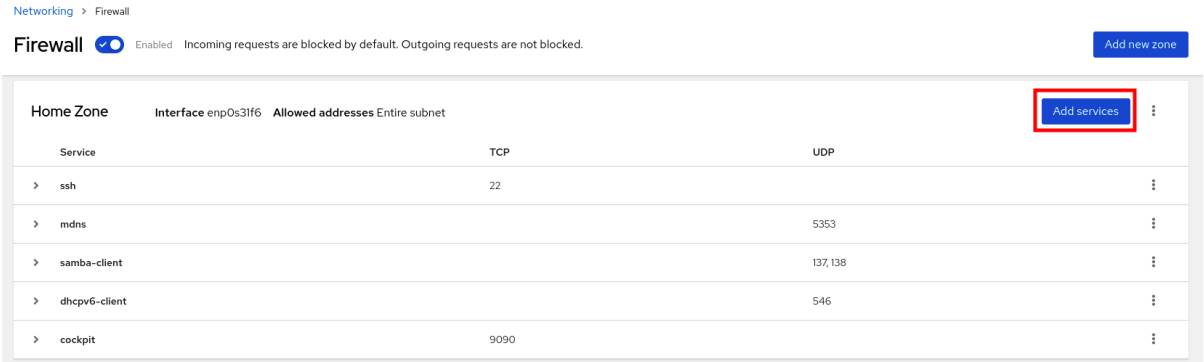
절차

1. 관리자 권한으로 **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 네트워킹을 클릭합니다.
3. 규칙 및 영역 편집 버튼을 클릭합니다.



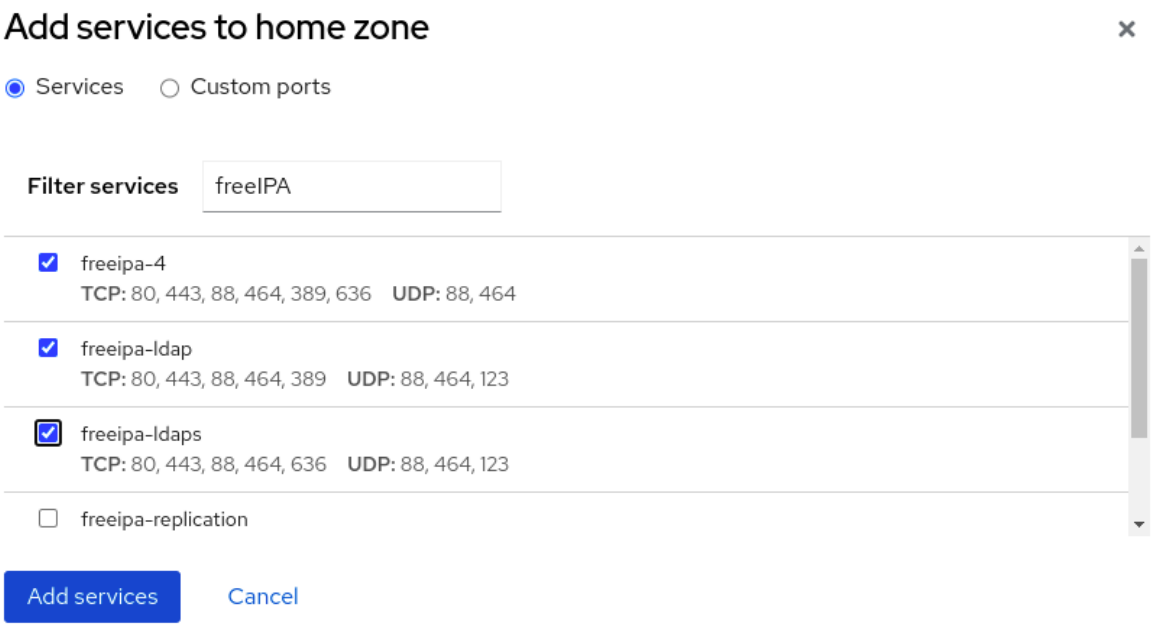
규칙 및 영역 편집 버튼이 표시되지 않으면 관리자 권한을 사용하여 웹 콘솔에 로그인합니다.

4. 방화벽 섹션에서 서비스를 추가할 영역을 선택하고 서비스 추가 를 클릭합니다.



5. 서비스 추가 대화 상자에서 방화벽에서 활성화할 서비스를 찾습니다.

6. 원하는 서비스를 활성화합니다.



7. 서비스 추가를 클릭합니다.

이때 **RHEL 9** 웹 콘솔은 영역의 서비스 목록에 서비스를 표시합니다.

13.7. 웹 콘솔을 사용하여 사용자 정의 포트 구성

웹 콘솔을 사용하면 다음을 추가할 수 있습니다.

- 표준 포트에서 수신 대기 중인 서비스: 웹 콘솔을 사용하여 방화벽에서 서비스 활성화
- 사용자 지정 포트에서 수신 대기하는 서비스.

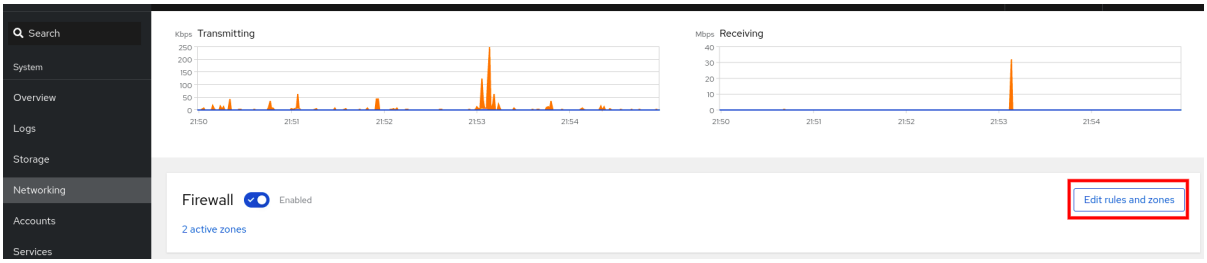
이 섹션에서는 사용자 지정 포트가 구성된 서비스를 추가하는 방법에 대해 설명합니다.

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- 방화벽을 활성화해야 합니다. 자세한 내용은 웹 콘솔을 사용하여 방화벽 실행을 참조하십시오.

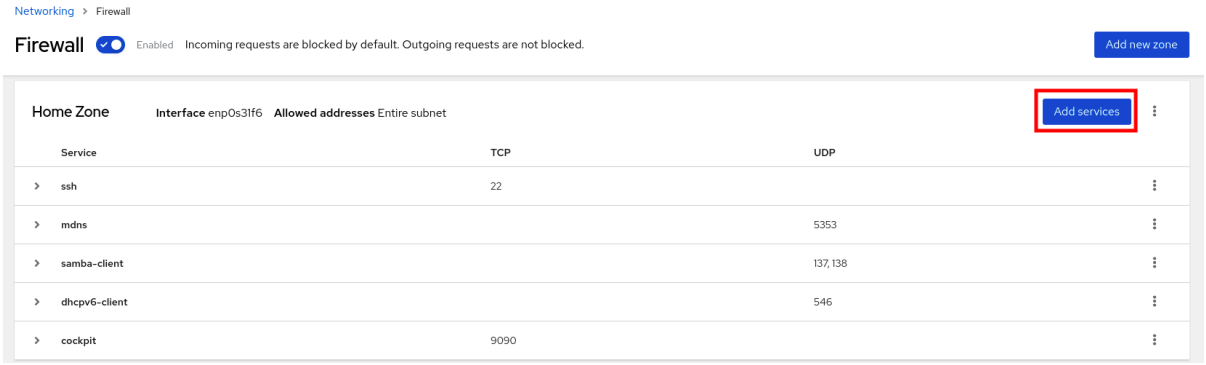
절차

1. 관리자 권한으로 **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 네트워킹을 클릭합니다.
3. 규칙 및 영역 편집 버튼을 클릭합니다.



규칙 및 영역 편집 버튼이 표시되지 않으면 관리자 권한으로 웹 콘솔에 로그인합니다.

4. 방화벽 섹션에서 사용자 지정 포트를 구성할 영역을 선택하고 서비스 추가 를 클릭합니다.



5. 서비스 추가 대화 상자에서 **Custom Ports** (사용자 지정 포트) 라디오 버튼을 클릭합니다.

6. **TCP** 및 **UDP** 필드에서 예제에 따라 포트를 추가합니다. 다음 형식으로 포트를 추가할 수 있습니다.

- 포트 번호(예: **22**)
- **5900-5910**과 같은 포트 번호 범위
- **nfs, rsync**와 같은 별칭

참고

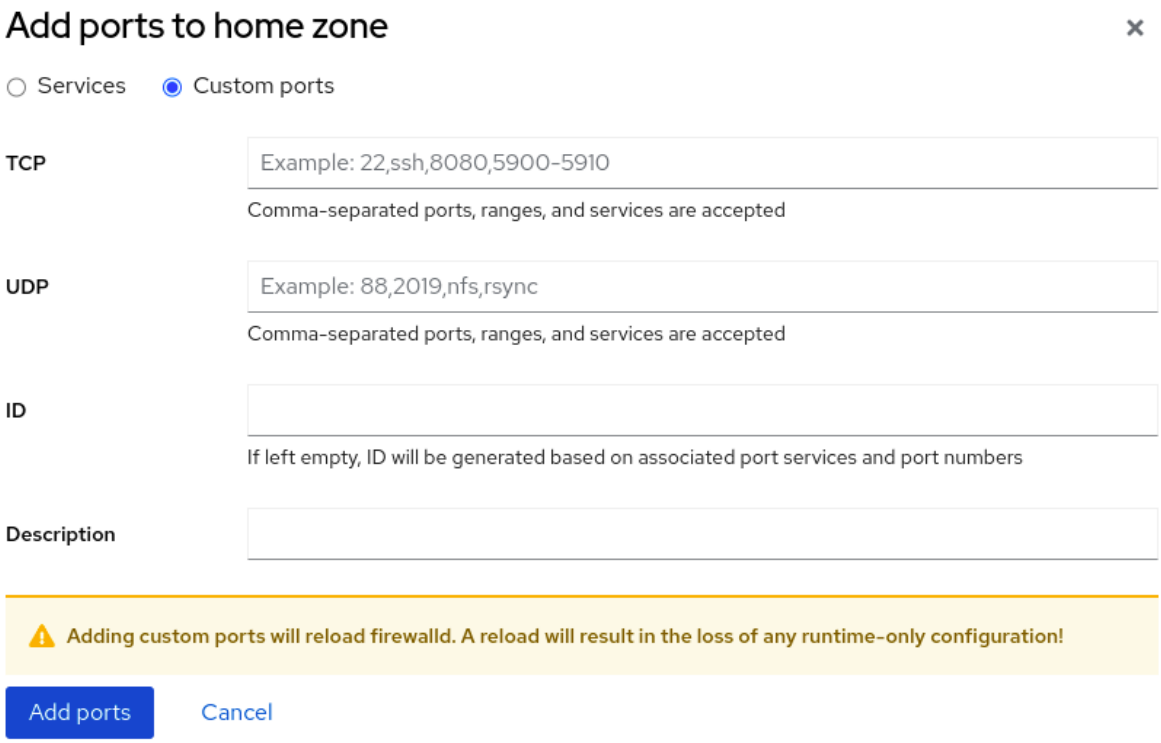
각 필드에 여러 값을 추가할 수 있습니다. 값은 쉼표로, 공백 없이 구분해야 합니다. 예를 들면 다음과 같습니다. **8080,8081,http**

7. **TCP** 및/또는 **UDP** 필드에 포트 번호를 추가한 후 이름 필드에서 서비스 이름을 확인합니다.

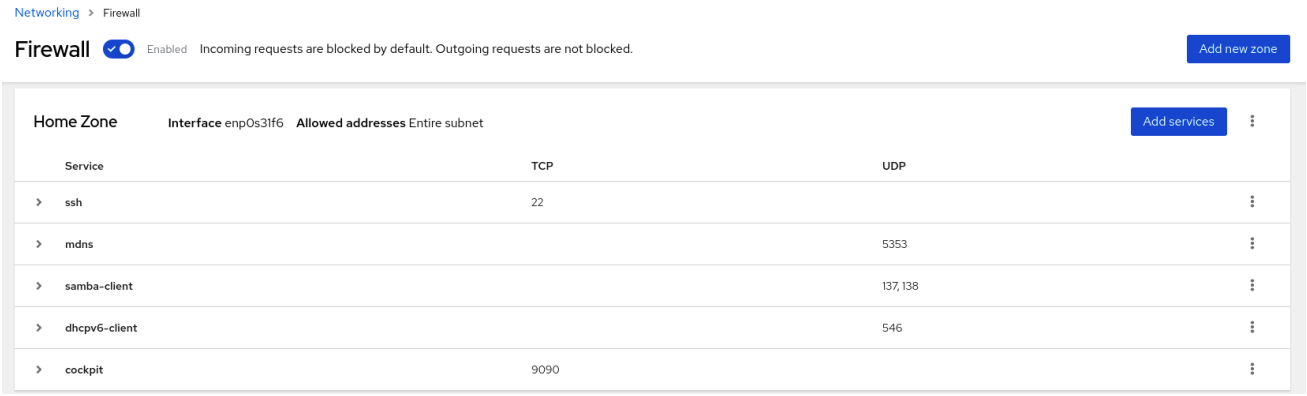
Name 필드에는 이 포트가 예약된 서비스 이름이 표시됩니다. 이 포트가 사용할 수 있고 서버가 이 포트에서 통신할 필요가 없는 경우 이름을 다시 작성할 수 있습니다.

8. 이름 필드에 정의된 포트를 포함하여 서비스의 이름을 추가합니다.

9. **Add Ports** 버튼을 클릭합니다.



설정을 확인하려면 방화벽 페이지로 이동하여 영역 서비스 목록에서 서비스를 찾습니다.



13.8. 웹 콘솔을 사용하여 영역 비활성화

이 섹션에서는 웹 콘솔을 사용하여 방화벽 구성에서 방화벽 영역을 비활성화하는 방법을 설명합니다.

사전 요구 사항

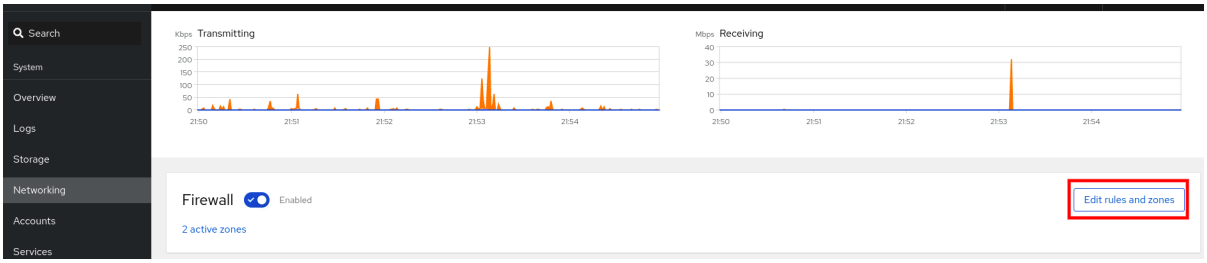
- **RHEL 9** 웹 콘솔이 설치되었습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. 관리자 권한으로 **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

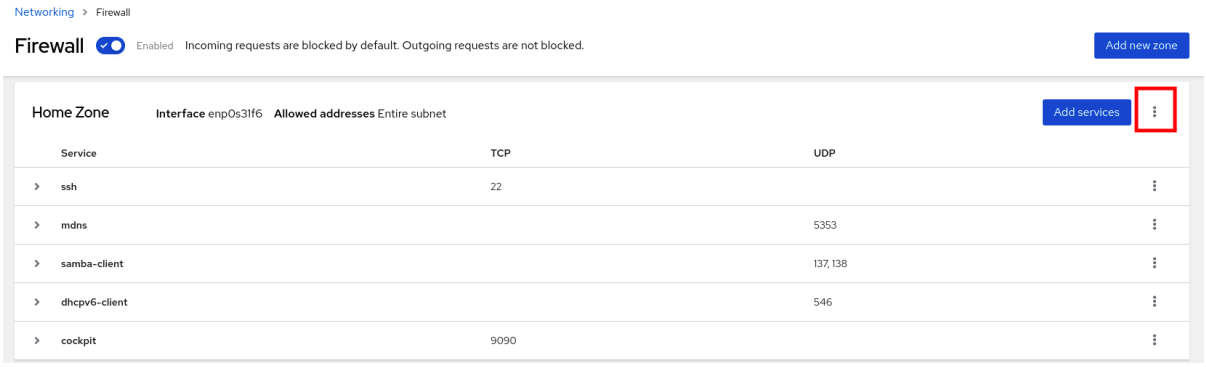
2. 네트워킹을 클릭합니다.

3. 규칙 및 영역 편집 버튼을 클릭합니다.



규칙 및 영역 편집 버튼이 표시되지 않으면 관리자 권한을 사용하여 웹 콘솔에 로그인합니다.

4. 제거할 영역의 옵션 아이콘을 클릭합니다.



5. 삭제를 클릭합니다.

이제 영역이 비활성화되어 있으며 인터페이스에 영역에 구성된 열린 서비스와 포트가 포함되지 않습니다.

14장. 생성된 ANSIBLE 플레이북 적용

SELinux 관련 문제를 해결할 때 웹 콘솔에서 쉘 스크립트 또는 **Ansible** 플레이북을 생성한 다음 더 많은 시스템을 내보내고 적용할 수 있습니다.

사전 요구 사항

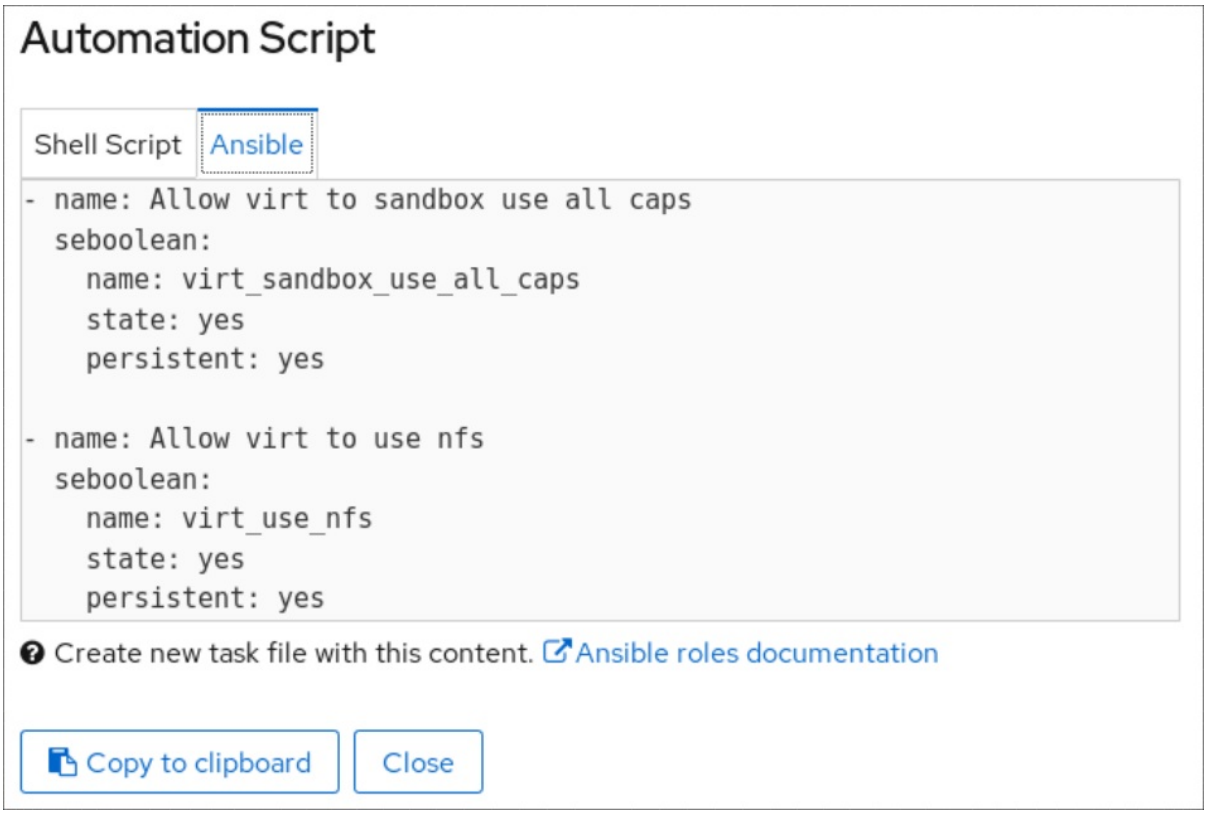
- 웹 콘솔 인터페이스를 설치하고 액세스할 수 있어야 합니다.

  자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. **SELinux** 를 클릭합니다.
2. 오른쪽 상단에서 **"Automation script"**를 클릭합니다.

   생성된 스크립트가 있는 창이 열립니다. 쉘 스크립트와 **Ansible** 플레이북 생성 옵션 탭을 탐색할 수 있습니다.



3. **Copy to clipboard** 버튼을 클릭하여 스크립트 또는 플레이북을 선택하고 적용합니다.

결과적으로 더 많은 시스템에 적용할 수 있는 자동화 스크립트가 있습니다.

추가 리소스

- **SELinux** 관련 문제 해결
- 여러 시스템에 동일한 **SELinux** 구성 배포
- **ansible-playbook** 명령에 대한 자세한 내용은 **ansible-playbook(1)** 도움말 페이지를 참조하십시오.

15장. 웹 콘솔을 사용하여 파티션 관리

웹 콘솔을 사용하여 **RHEL 9**에서 파일 시스템을 관리하는 방법을 알아봅니다.

사용 가능한 파일 시스템에 대한 자세한 내용은 사용 가능한 파일 시스템 개요 를 참조하십시오.

15.1. 웹 콘솔에서 파일 시스템으로 포맷된 파티션 표시

웹 콘솔의 **Storage** 섹션에는 **Filesystems** 테이블에 사용 가능한 모든 파일 시스템이 표시됩니다.

이 섹션에서는 웹 콘솔에 표시된 파일 시스템으로 포맷된 파티션 목록으로 이동합니다.

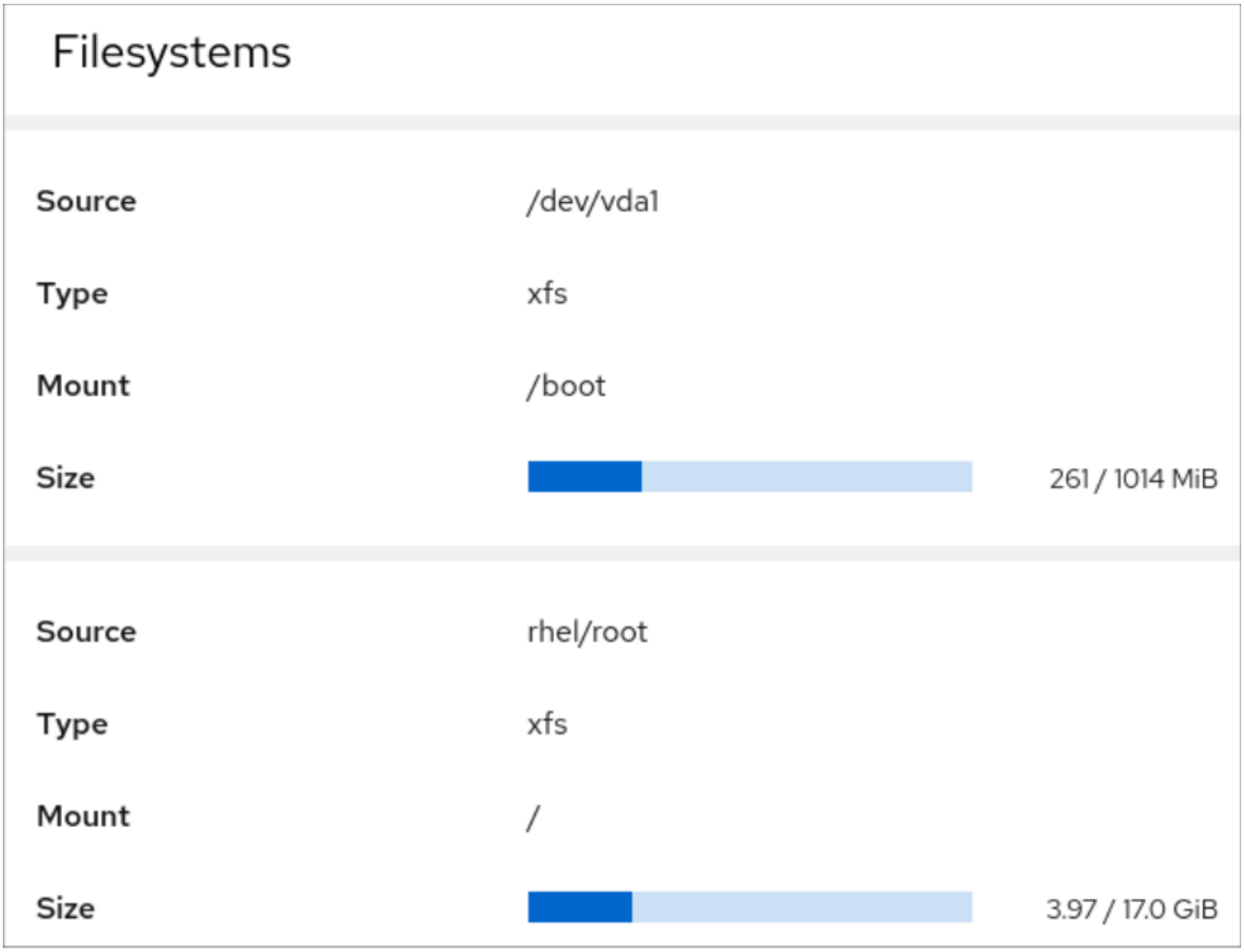
사전 요구 사항

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 스토리지 탭을 클릭합니다.

파일 시스템 테이블에서 파일 시스템, 이름, 크기, 각 파티션에서 사용 가능한 공간 수로 포맷된 사용 가능한 모든 파티션을 확인할 수 있습니다.



15.2. 웹 콘솔에서 파티션 생성

새 파티션을 생성하려면 다음을 수행합니다.

- 기존 파티션 테이블 사용
- 파티션 만들기

사전 요구 사항

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

- **Storage** 탭의 기타 장치 테이블에 표시되는 시스템에 연결된 포맷되지 않은 볼륨입니다.

절차

1. **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 스토리지 탭을 클릭합니다.
3. 기타 장치 테이블에서 파티션을 생성할 볼륨을 클릭합니다.
4. **Content (콘텐츠)** 섹션에서 **Create Partition** 단추를 클릭합니다.
5. 파티션 만들기 대화 상자에서 새 파티션의 크기를 선택합니다.
6. **Erase** 드롭다운 메뉴에서 다음을 선택합니다.
   - 기존 데이터를 덮어 쓰지 마십시오. **RHEL** 웹 콘솔은 디스크 헤더만 다시 작성합니다. 이 옵션의 장점은 포맷 속도입니다.
   - 기존 데이터를 **0**으로 덮어 쓰기 **-RHEL** 웹 콘솔은 전체 디스크를 **0**으로 다시 작성합니다. 이 옵션은 프로그램이 전체 디스크를 통과해야하기 때문에 속도가 느려지지만 더 안전합니다. 디스크에 데이터가 포함되어 있고 덮어써야 하는 경우 이 옵션을 사용합니다.
7. 유형 드롭다운 메뉴에서 파일 시스템을 선택합니다.
   - **XFS** 파일 시스템은 대규모 논리 볼륨을 지원하고, 중단 없이 물리적 드라이브를 온라인으로 전환하며, 기존 파일 시스템을 확장합니다. 다른 강력한 기본 설정이 없는 경우 이 파일 시스템을 선택한 상태로 두십시오.
   - **ext4** 파일 시스템은 다음을 지원합니다.

- 논리 볼륨
- 시스템 중단 없이 온라인으로 물리적 드라이브 전환
- 파일 시스템 증가
- 파일 시스템 축소

추가 옵션은 **LUKS(Linux Unified Key Setup)**에서 수행한 파티션 암호화를 사용하도록 설정하는 것입니다. 이 경우 암호를 사용하여 볼륨을 암호화할 수 있습니다.

8. 이름 필드에 논리 볼륨 이름을 입력합니다.

9. **Mounting(** 마운트 **)** 드롭다운 메뉴에서 **Custom (**사용자 지정**)**을 선택합니다.

   Default 옵션을 사용하면 다음 부팅 시 파일 시스템이 마운트되지 않습니다.

10. **Mount Point** 필드에 마운트 경로를 추가합니다.

11. 부팅 시 마운트를 선택합니다.

12. 파티션 만들기 버튼을 클릭합니다.

    포맷은 볼륨 크기와 선택한 포맷 옵션에 따라 몇 분이 걸릴 수 있습니다.

포맷이 성공적으로 완료되면 **Filesystem** 탭에서 포맷된 논리 볼륨의 세부 정보를 확인할 수 있습니다.

검증 단계

- 파티션이 성공적으로 추가되었는지 확인하려면 **Storage (**스토리지**)** 탭으로 전환하고 **Filesystems** 테이블을 확인합니다.

15.3. 웹 콘솔에서 파티션 삭제

다음 절차에서는 웹 콘솔 인터페이스에서 파티션을 삭제하는 방법을 알려줍니다.

사전 요구 사항

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- 파티션의 파일 시스템을 마운트 해제합니다.

  파티션 마운트 및 마운트 해제에 대한 자세한 내용은 웹 콘솔에서 파일 시스템 마운트 및 마운트 해제를참조하십시오.

절차

1. **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 스토리지 탭을 클릭합니다.
3. **Filesystems** 테이블에서 파티션을 삭제할 볼륨을 선택합니다.
4. 콘텐츠 섹션에서 삭제할 파티션을 클릭합니다.
5. 파티션이 축소되어 삭제 버튼을 클릭할 수 있습니다.

   파티션을 마운트 및 사용해서는 안 됩니다.

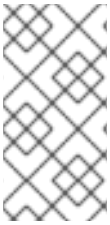
검증 단계

- 파티션이 성공적으로 제거되었는지 확인하려면 **Storage** (스토리지) 탭으로 전환하고

Content (콘텐츠) 테이블을 확인합니다.

15.4. 웹 콘솔에서 파일 시스템 마운트 및 마운트 해제

RHEL 시스템에서 파티션을 사용하려면 파일 시스템을 파티션에 장치로 마운트해야 합니다.



참고

또한 파일 시스템을 마운트 해제할 수 있으며 **RHEL** 시스템은 사용을 중지합니다. 파일 시스템을 마운트 해제하면 장치를 삭제, 제거 또는 다시 포맷할 수 있습니다.

사전 요구 사항

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- 파일 시스템을 마운트 해제하려면 시스템이 파티션에 저장된 파일, 서비스 또는 애플리케이션을 사용하지 않는지 확인합니다.

절차

1. **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 스토리지 탭을 클릭합니다.
3. **Filesystems** 테이블에서 파티션을 삭제할 볼륨을 선택합니다.
4. 콘텐츠 섹션에서 마운트 또는 마운트 해제할 파일 시스템이 있는 파티션을 클릭합니다.
5. 마운트 또는 마운트 해제 버튼을 클릭합니다.

이때 작업에 따라 파일 시스템이 마운트되거나 마운트 해제되었습니다.

16장. 웹 콘솔에서 NFS 마운트 관리

RHEL 9 웹 콘솔을 사용하면 **NFS(Network File System)** 프로토콜을 사용하여 원격 디렉터리를 마운트할 수 있습니다.

NFS를 사용하면 네트워크에 있는 원격 디렉터리에 연결하고 마운트할 수 있으며 디렉터리가 실제 드라이브에 있는 것처럼 파일을 사용할 수 있습니다.

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다.

  자세한 내용은 웹 콘솔 설치를 참조하십시오.

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- **NFS** 서버 이름 또는 **IP** 주소
- 원격 서버의 디렉터리 경로입니다.

16.1. 웹 콘솔에서 NFS 마운트 연결

NFS를 사용하여 원격 디렉터리를 파일 시스템에 연결합니다.

사전 요구 사항

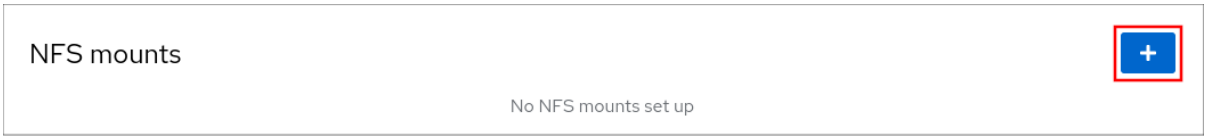
- **NFS** 서버 이름 또는 **IP** 주소
- 원격 서버의 디렉터리 경로입니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 스토리지 를 클릭합니다.

3. **NFS** 마운트 섹션에서 **+** 를 클릭합니다.



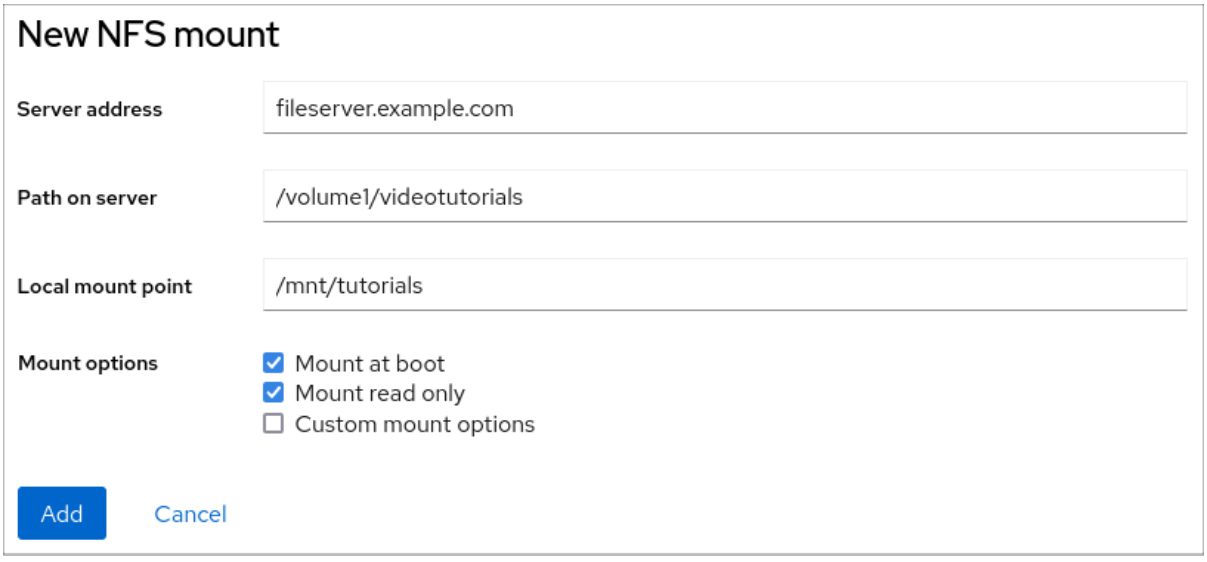
4. 새 **NFS** 마운트 대화 상자에서 원격 서버의 서버 또는 **IP** 주소를 입력합니다.

5. 서버 경로 필드에 마운트하려는 디렉터리의 경로를 입력합니다.

6. 로컬 마운트 지점 필드에 로컬 시스템에서 디렉터리를 찾을 경로를 입력합니다.

7. 부팅 시 마운트를 선택합니다. 이렇게 하면 로컬 시스템을 다시 시작한 후에도 디렉터리에 연결할 수 있습니다.

8. 필요한 경우 콘텐츠를 변경하지 않으려면 마운트 읽기 를 선택합니다.



9. 추가를 클릭합니다.

검증 단계

- 마운트된 디렉터리를 열고 콘텐츠에 액세스할 수 있는지 확인합니다.

연결 문제를 해결하려면 사용자 지정 마운트 옵션을 사용하여 조정할 수 있습니다.

16.2. 웹 콘솔에서 NFS 마운트 옵션 사용자 정의

기존 **NFS** 마운트를 편집하고 사용자 지정 마운트 옵션을 추가합니다.

사용자 지정 마운트 옵션은 시간 제한 변경 또는 인증 구성과 같은 **NFS** 마운트의 연결 문제 해결 또는 매개 변수를 변경하는 데 도움이 될 수 있습니다.

사전 요구 사항

- **NFS** 마운트가 추가되었습니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 스토리지 를 클릭합니다.
3. 조정할 **NFS** 마운트를 클릭합니다.
4. 원격 디렉터리가 마운트된 경우 **Unmount** 를 클릭합니다.

사용자 지정 마운트 옵션 구성 중에 디렉터리를 마운트해서는 안 됩니다. 그렇지 않으면 웹 콘솔에서 구성을 저장하지 않으므로 오류가 발생합니다.

1. 편집 을 클릭합니다.

1. **NFS** 마운트 대화 상자에서 사용자 지정 마운트 옵션을 선택합니다.

2. 마운트 옵션을 쉼표로 구분하여 입력합니다. 예를 들어 다음과 같습니다.

- **nfsvers=4 this - NFS** 프로토콜 버전 번호
- **SELinux** 요청 시간이 초과된 후 복구 유형
- **NFS** 서버의 **sec=krb5** 해결 파일은 **Kerberos** 인증으로 보호할 수 있습니다. **NFS** 클라이언트와 서버는 모두 **Kerberos** 인증을 지원해야 합니다.

NFS 마운트 옵션의 전체 목록은 명령줄에 **man nfs** 를 입력합니다.

1. 적용을 클릭합니다.

2. 마운트 를 클릭합니다.

검증 단계

- 마운트된 디렉터리를 열고 콘텐츠에 액세스할 수 있는지 확인합니다.

17장. 웹 콘솔에서 REDUNDANT ARRAYS OF INDEPENDENT DISKS 관리

분산 디스크(RAID)의 중복 배열은 더 많은 디스크를 하나의 스토리지로 정렬하는 방법을 나타냅니다. RAID는 디스크 장애로부터 디스크에 저장된 데이터를 보호합니다.

RAID는 다음 데이터 배포 전략을 사용합니다.

- mirroringContentSources-이/가 서로 다른 두 위치에 복사됩니다. 하나의 디스크에 오류가 발생하면 복사본이 있고 데이터가 손실되지 않습니다.
- 스트래핑 - - - - - 문제 해결은 디스크 사이에 균등하게 분산됩니다.

보호 수준은 RAID 수준에 따라 다릅니다.

RHEL 웹 콘솔은 다음과 같은 RAID 수준을 지원합니다.

- RAID 0 (Stripe)
- RAID 1 (Mirror)
- RAID 4 (파리티 패리티)
- RAID 5 (Distributed 패리티)
- RAID 6 (때의 분산 패리티)
- RAID 10(미러 미러)

RAID에서 디스크를 사용하려면 다음이 필요합니다.

- **RAID**를 생성합니다.
- 파일 시스템으로 포맷합니다.
- 서버에 **RAID**를 마운트합니다.

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되어 액세스할 수 있습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- **cockpit-storaged** 패키지가 시스템에 설치됩니다.

17.1. 웹 콘솔에서 RAID 생성

RHEL 9 웹 콘솔에서 **RAID**를 구성합니다.

사전 요구 사항

- 시스템에 연결된 물리적 디스크입니다. 각 **RAID** 수준에는 다른 양의 디스크가 필요합니다.

절차

1. **RHEL 9** 웹 콘솔을 엽니다.
2. 스토리지 를 클릭합니다.
3. 장치 테이블에서 메뉴 아이콘을 클릭합니다.
4. **RAID** 장치 생성을 클릭합니다.

5. **RAID** 장치 생성 대화 상자에서 새 **RAID**의 이름을 입력합니다.

6. **RAID** 수준 드롭다운 목록에서 사용하려는 **RAID** 수준을 선택합니다.

7. **Chunk Size** 드롭다운 목록에서 사전 정의된 값을 그대로 둡니다.

   Chunk Size 값은 데이터 기록에 대한 각 블록의 크기를 지정합니다. 청크 크기가 **512KiB**인 경우 시스템은 첫 번째 **512KiB**를 첫 번째 디스크에 쓰고 두 번째 **512KiB**는 두 번째 디스크에 기록되고 세 번째 청크는 세 번째 디스크에 기록됩니다. **RAID**에 디스크 **3**개가 있는 경우 네 번째 **512KiB**가 첫 번째 디스크에 다시 기록됩니다.

8. **RAID**에 사용할 디스크를 선택합니다.

9. 생성을 클릭합니다.

검증 단계

- 스토리지 섹션으로 이동하여 **RAID** 장치 상자에서 새 **RAID**를 확인하고 포맷을 할 수 있는지 확인합니다.

웹 콘솔에서 새 **RAID**를 포맷하고 마운트하는 방법은 다음과 같습니다.

RAID 포맷

파티션 테이블에 파티션 생성

RAID 상단에 볼륨 그룹 생성

17.2. 웹 콘솔에서 RAID 포맷

RHEL 9 웹 인터페이스에서 생성된 새 소프트웨어 **RAID** 장치를 포맷합니다.

사전 요구 사항

- 물리적 디스크는 **RHEL 9**에서 연결되고 표시됩니다.
- **RAID**가 생성되었습니다.
- **RAID**에 사용할 파일 시스템을 고려합니다.
- 파티션 테이블 생성을 고려하십시오.

절차

1. **RHEL 9** 웹 콘솔을 엽니다.
2. 스토리지 를 클릭합니다.
3. **RAID** 장치 상자에서 클릭하여 포맷할 **RAID**를 선택합니다.
4. **RAID** 세부 정보 화면에서 콘텐츠 부분까지 아래로 스크롤합니다.
5. 새로 생성된 **RAID**를 클릭합니다.
6. **Format** 버튼을 클릭합니다.
7. **Erase** 드롭다운 목록에서 다음을 선택합니다.
   - 기존 데이터를 덮어 쓰지 마십시오. **RHEL** 웹 콘솔은 디스크 헤더만 다시 작성합니다. 이 옵션의 장점은 포맷 속도입니다.
   - 기존 데이터를 **0**으로 덮어 쓰기 **-RHEL** 웹 콘솔은 전체 디스크를 **0**으로 다시 작성합니다. 이 옵션은 프로그램이 전체 디스크를 통과해야 하므로 속도가 느립니다. **RAID**에 데이터가 포

함되어 있고 데이터를 다시 작성해야 하는 경우 이 옵션을 사용합니다.

8. 유형 드롭다운 목록에서 다른 강력한 기본 설정이 없는 경우 **XFS** 파일 시스템을 선택합니다.

9. 파일 시스템의 이름을 입력합니다.

10. 마운트 드롭다운 목록에서 사용자 지정을 선택합니다.

    Default 옵션을 사용하면 다음 부팅 시 파일 시스템이 마운트되지 않습니다.

11. **Mount Point** 필드에 마운트 경로를 추가합니다.

12. 부팅 시 마운트를 선택합니다.

13. **Format** 버튼을 클릭합니다.

    사용 된 포맷 옵션 및 **RAID** 크기에 따라 포맷하는 데 몇 분이 걸릴 수 있습니다.

    성공적으로 완료되면 파일 시스템 탭에서 포맷된 **RAID**의 세부 정보를 확인할 수 있습니다.

14. **RAID**를 사용하려면 마운트 를 클릭합니다.

이 시점에서 시스템은 마운트된 **RAID** 및 포맷된 **RAID**를 사용합니다.

17.3. RAID에서 파티션 테이블 생성에 웹 콘솔 사용

RHEL 9 인터페이스에서 생성된 새 소프트웨어 **RAID** 장치에서 파티션 테이블로 **RAID**를 포맷합니다.

RAID는 다른 스토리지 장치로 포맷해야 합니다. 두 가지 옵션이 있습니다.

- 파티션없이 **RAID** 장치 포맷
- 파티션이 포함된 파티션 테이블 만들기

사전 요구 사항

- 물리 디스크는 에서 연결되고 볼 수 있습니다.
- **RAID**가 생성되었습니다.
- **RAID**에 사용되는 파일 시스템을 고려합니다.
- 파티션 테이블 생성을 고려하십시오.

절차

1. **RHEL 9** 콘솔을 엽니다.
2. 스토리지 를 클릭합니다.
3. **RAID** 장치 상자에서 편집할 **RAID**를 선택합니다.
4. **RAID** 세부 정보 화면에서 콘텐츠 부분까지 아래로 스크롤합니다.
5. 새로 생성된 **RAID**를 클릭합니다.
6. 파티션 테이블 만들기 버튼을 클릭합니다.
7. **Erase** 드롭다운 목록에서 다음을 선택합니다.
   -

기존 데이터를 덮어 쓰지 마십시오. **RHEL** 웹 콘솔은 디스크 헤더만 다시 작성합니다. 이 옵션의 장점은 포맷 속도입니다.

- 기존 데이터를 **0**으로 덮어 쓰기 **-RHEL** 웹 콘솔은 전체 **RAID**를 **0**으로 다시 작성합니다. 이 옵션은 프로그램이 전체 **RAID**를 통과해야 하기 때문에 느립니다. **RAID**에 데이터가 포함되어 있고 데이터를 다시 작성해야 하는 경우 이 옵션을 사용합니다.

8. 파티션 드롭다운 목록에서 다음을 선택합니다.

- 최신 시스템 및 하드 디스크 **> 2TB (GPT)**와 호환되며, **4**개 이상의 파티션이 있는 대규모 **RAID**에 대해 권장되는 파티션 테이블입니다.

- 모든 시스템 및 장치 **(MBR)**와 호환 **: Master Boot Record**는 최대 **2TB**의 디스크에서 작동합니다. 또한 **MBR**은 **4**개의 기본 파티션 최대를 지원합니다.

9. **Format** 을 클릭합니다.

이때 파티션 테이블이 생성되어 파티션을 생성할 수 있습니다.

파티션을 만들려면 **RAID**에서 파티션을 생성하는 데 웹 콘솔 사용을 참조하십시오.

17.4. RAID에 파티션을 만들기 위해 웹 콘솔 사용

기존 파티션 테이블에 파티션을 만듭니다.

사전 요구 사항

- 파티션 테이블이 생성됩니다. 자세한 내용은 **Using the web console for creating a partition table on RAID**를 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔을 엽니다.

2. 스토리지 를 클릭합니다.

3. **RAID** 장치 상자에서 편집할 **RAID**를 클릭합니다.

4. **RAID** 세부 정보 화면에서 콘텐츠 부분까지 아래로 스크롤합니다.

5. 새로 생성된 **RAID**를 클릭합니다.

6. 파티션 만들기를 클릭합니다.

7. 파티션 만들기 대화 상자에서 첫 번째 파티션의 크기를 설정합니다.

8. **Erase** 드롭다운 목록에서 다음을 선택합니다.

   - 기존 데이터를 덮어 쓰지 마십시오. **RHEL** 웹 콘솔은 디스크 헤더만 다시 작성합니다. 이 옵션의 장점은 포맷 속도입니다.

   - 기존 데이터를 **0**으로 덮어 쓰기 **-RHEL** 웹 콘솔은 전체 **RAID**를 **0**으로 다시 작성합니다. 이 옵션은 프로그램이 전체 **RAID**를 통과해야 하기 때문에 느립니다. **RAID**에 데이터가 포함되어 있고 데이터를 다시 작성해야 하는 경우 이 옵션을 사용합니다.

9. 유형 드롭다운 목록에서 다른 강력한 기본 설정이 없는 경우 **XFS** 파일 시스템을 선택합니다.

10. 파일 시스템의 이름을 입력합니다. 이름에는 공백을 사용하지 마십시오.

11. 마운트 드롭다운 목록에서 사용자 지정을 선택합니다.

    Default 옵션을 사용하면 다음 부팅 시 파일 시스템이 마운트되지 않습니다.

12. **Mount Point** 필드에 마운트 경로를 추가합니다.

13. 부팅 시 마운트를 선택합니다.

14. 파티션 만들기를 클릭합니다.

사용 된 포맷 옵션 및 **RAID** 크기에 따라 포맷하는 데 몇 분이 걸릴 수 있습니다.

성공적으로 완료되면 다른 파티션을 계속 만들 수 있습니다.

이 시점에서 시스템은 마운트된 **RAID** 및 포맷된 **RAID**를 사용합니다.

17.5. RAID 상단에 볼륨 그룹 생성에 웹 콘솔 사용

소프트웨어 **RAID**에서 볼륨 그룹을 구축합니다.

사전 요구 사항

- 포맷 및 마운트되지 않은 **RAID** 장치.

절차

1. **RHEL 9** 웹 콘솔을 엽니다.

2. 스토리지 를 클릭합니다.

3. 볼륨 그룹 상자에서 **+** 아이콘을 클릭합니다.

4. 볼륨 그룹 만들기 대화 상자에서 새 볼륨 그룹의 이름을 입력합니다.

5. 디스크 목록에서 **RAID** 장치를 선택합니다.

   목록에 **RAID**가 표시되지 않으면 시스템에서 **RAID**를 마운트 해제합니다. **RAID** 장치는

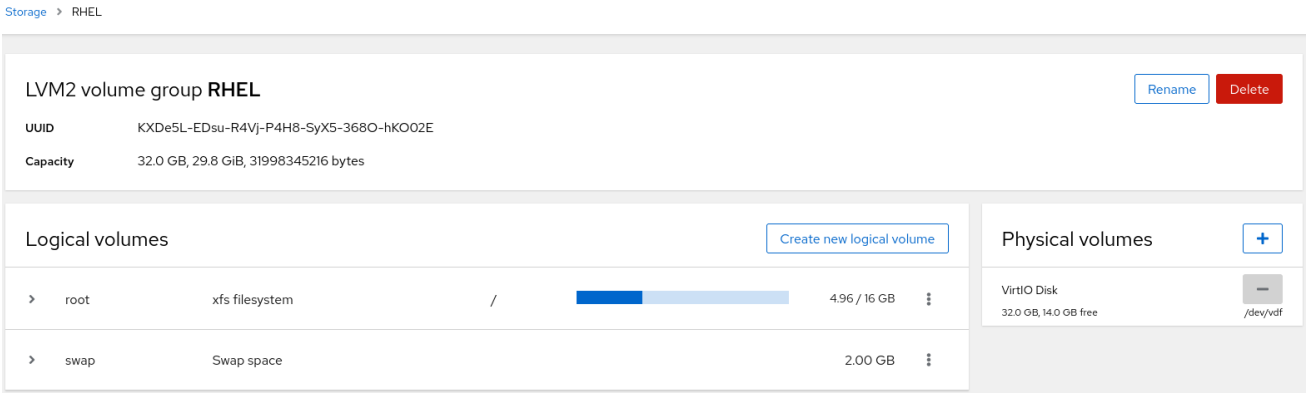
RHEL 9 시스템에서 사용할 수 없습니다.

6. 생성을 클릭합니다.

새 볼륨 그룹이 생성되었으며 논리 볼륨을 계속 생성할 수 있습니다.

18장. LVM 논리 볼륨 구성에 웹 콘솔 사용

Red Hat Enterprise Linux 9는 **LVM** 논리 볼륨 관리자를 지원합니다. **Red Hat Enterprise Linux 9**를 설치하면 설치 중에 자동으로 **LVM**에 설치됩니다.



스크린샷은 설치 중에 자동으로 생성된 두 개의 논리 볼륨이 있는 **RHEL 9** 시스템을 새로 설치하는 웹 콘솔 보기를 보여줍니다.

논리 볼륨에 대한 자세한 내용은 다음 섹션을 따르십시오.

- 논리 볼륨 관리자란 무엇이며 언제 사용해야 합니까?
- 볼륨 그룹은 무엇이며 이를 만드는 방법
- 논리 볼륨이란 무엇이며 이를 만드는 방법
- 논리 볼륨 포맷 방법
- 논리 볼륨의 크기 조정 방법

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다.

  자세한 내용은 웹 콘솔 설치 및 활성화를 참조하십시오.

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.

- 물리적 드라이브, **RAID** 장치 또는 논리 볼륨을 생성할 수 있는 다른 유형의 블록 장치입니다.

18.1. 웹 콘솔의 논리 볼륨 관리자

RHEL 9 웹 콘솔은 **LVM** 볼륨 그룹과 논리 볼륨을 생성할 수 있는 그래픽 인터페이스를 제공합니다.

볼륨 그룹은 물리 및 논리 볼륨 간의 계층을 생성합니다. 논리 볼륨 자체에 영향을 주지 않고 물리 볼륨을 추가하거나 제거할 수 있습니다. 볼륨 그룹은 그룹에 포함된 모든 물리적 드라이브의 용량으로 구성된 용량이 있는 하나의 드라이브로 나타납니다.

물리적 드라이브를 웹 콘솔의 볼륨 그룹에 결합할 수 있습니다.

논리 볼륨은 단일 물리 드라이브로 작동하며 시스템의 볼륨 그룹 위에 구축됩니다.

논리 볼륨의 주요 장점은 다음과 같습니다.

- 물리적 드라이브에 사용된 파티션 시스템보다 유연성이 향상됩니다.
- 더 많은 물리적 드라이브를 하나의 볼륨에 연결할 수 있습니다.
- 다시 시작하지 않고 온라인으로 볼륨의 용량을 늘리거나 줄일 수 있습니다.
- 스냅샷을 생성하는 기능.

추가 리소스

- 논리 볼륨 구성 및 관리

18.2. 웹 콘솔에서 볼륨 그룹 생성

하나 이상의 물리 드라이브 또는 기타 스토리지 장치에서 볼륨 그룹을 생성합니다.

논리 볼륨은 볼륨 그룹에서 생성됩니다. 각 볼륨 그룹에는 여러 논리 볼륨이 포함될 수 있습니다.

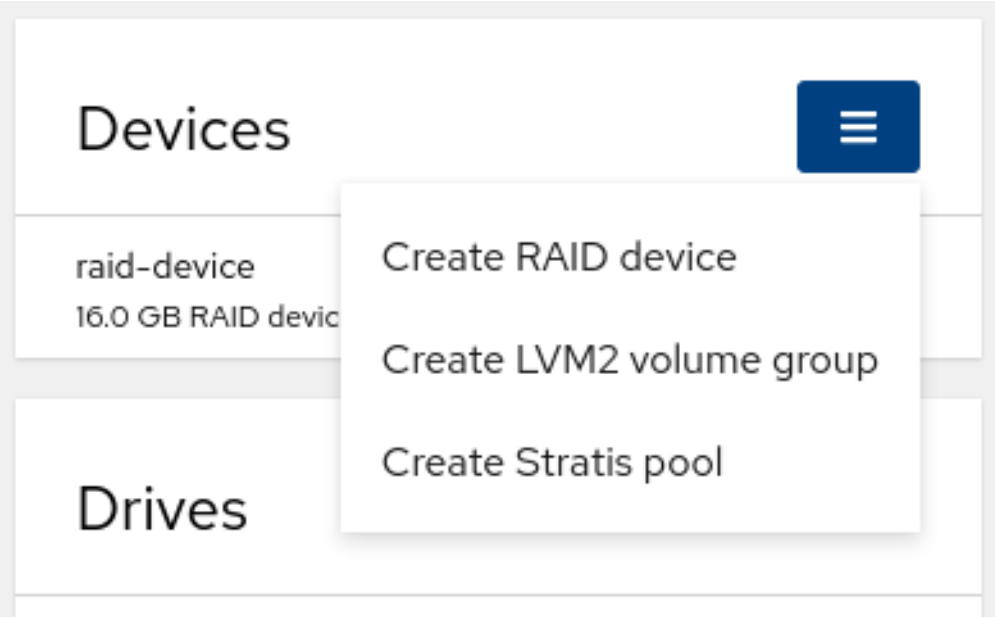
자세한 내용은 **LVM** 볼륨 그룹 관리를 참조하십시오.

사전 요구 사항

- 물리 드라이브 또는 볼륨 그룹을 생성할 다른 스토리지 장치 유형.

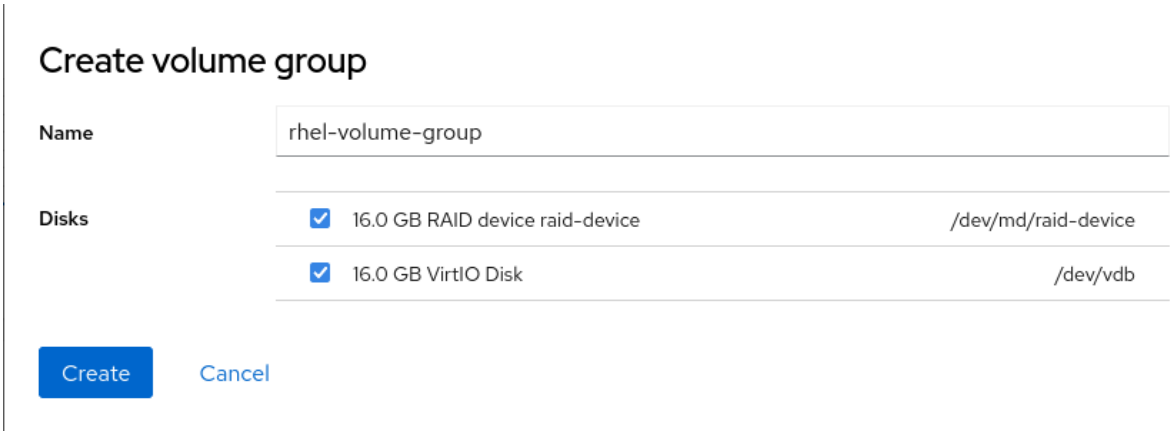
절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.
2. 스토리지 를 클릭합니다.
3. 장치 섹션의 드롭다운 메뉴에서 **Create LVM2** 볼륨 그룹을 선택합니다.



4. 이름 필드에 공백이 없는 그룹의 이름을 입력합니다.

5. 결합할 드라이브를 선택하여 볼륨 그룹을 만듭니다.



예상대로 장치를 볼 수 없는 상황이 발생할 수 있습니다. **RHEL** 웹 콘솔은 사용되지 않는 블록 장치만 표시합니다. 사용된 장치는 예를 들면 다음과 같습니다.

- 파일 시스템으로 포맷된 장치
- 다른 볼륨 그룹의 물리 볼륨
- 물리 볼륨은 다른 소프트웨어 **RAID** 장치의 멤버입니다.

장치가 표시되지 않으면 비어 있거나 사용되지 않도록 포맷하십시오.

6. 생성을 클릭합니다.

웹 콘솔은 장치 섹션에 볼륨 그룹을 추가합니다. 그룹을 클릭하면 해당 볼륨 그룹에서 할당된 논리 볼륨을 만들 수 있습니다.

18.3. 웹 콘솔에서 논리 볼륨 생성

논리 볼륨은 물리적 드라이브 역할을 합니다. **RHEL 9** 웹 콘솔을 사용하여 볼륨 그룹에 **LVM** 논리 볼륨을 생성할 수 있습니다.

사전 요구 사항

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 볼륨 그룹이 생성되었습니다. 자세한 내용은 웹 콘솔에서 볼륨 그룹 생성을 참조하십시오.

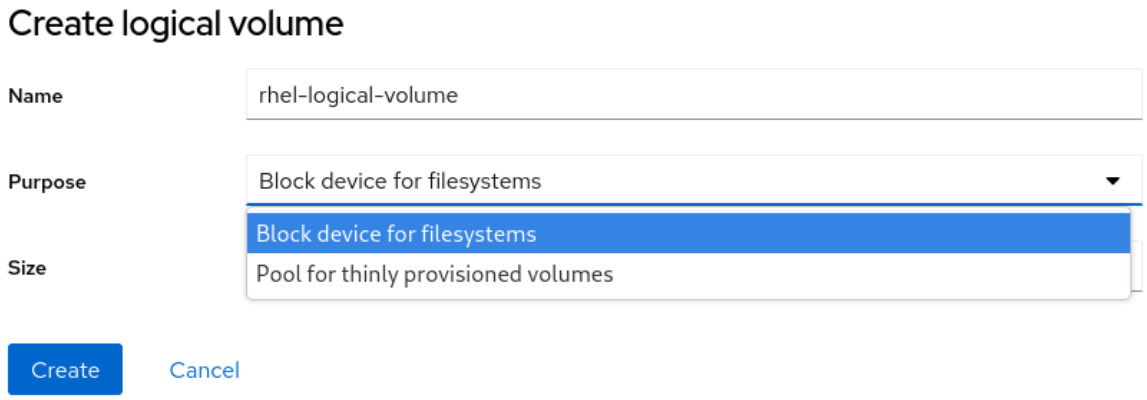
절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.
2. 스토리지 를 클릭합니다.
3. 장치 섹션에서 논리 볼륨을 생성할 볼륨 그룹을 클릭합니다.
4. 논리 볼륨 섹션에서 새 논리 볼륨 만들기 를 클릭합니다.
5. 이름 필드에 공백 없이 새 논리 볼륨의 이름을 입력합니다.

6.

Purpose (용도) 드롭다운 메뉴에서 파일 시스템에 대한 블록 장치를 선택합니다.

이 구성을 사용하면 볼륨 그룹에 포함된 모든 드라이브의 용량 합계와 동일한 최대 볼륨 크기를 사용하여 논리 볼륨을 생성할 수 있습니다.

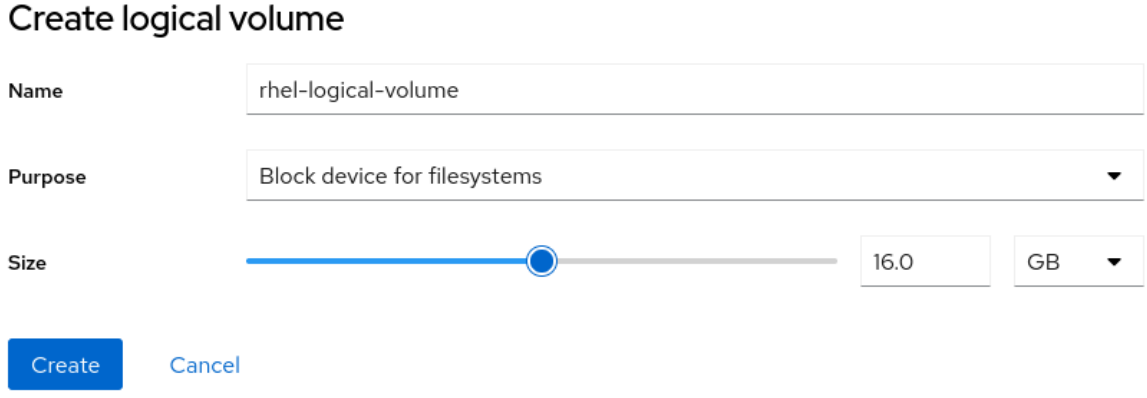


7.

논리 볼륨의 크기를 정의합니다. 다음을 고려하십시오.

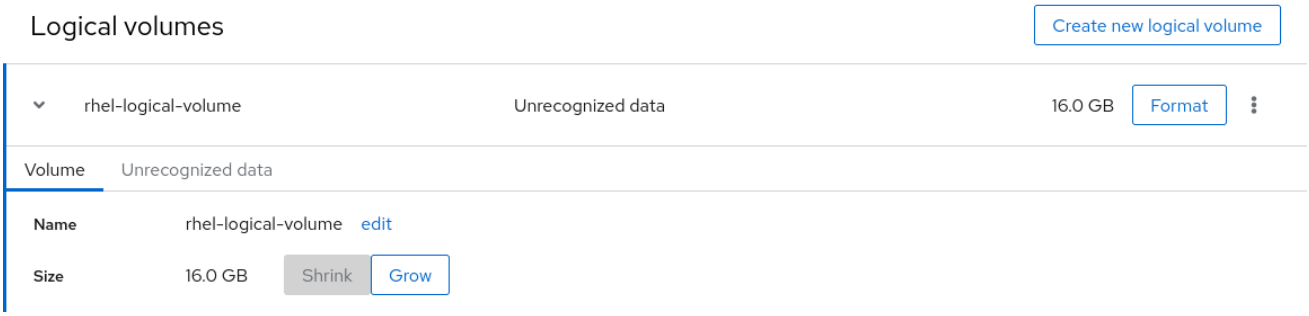
- 이 논리 볼륨을 사용하는 시스템에 필요한 공간은 얼마입니까.
- 생성하려는 논리 볼륨 수입니다.

전체 공간을 사용할 필요는 없습니다. 필요한 경우 나중에 논리 볼륨을 늘릴 수 있습니다.



8. 생성을 클릭합니다.

설정을 확인하려면 논리 볼륨을 클릭하고 세부 정보를 확인합니다.



이 단계에서는 논리 볼륨이 생성되었으며 포맷 프로세스를 사용하여 파일 시스템을 생성하고 마운트해야 합니다.

18.4. 웹 콘솔에서 논리 볼륨 포맷

논리 볼륨은 물리적 드라이브 역할을 합니다. 이를 사용하려면 파일 시스템으로 포맷해야 합니다.

주의

논리 볼륨을 포맷하면 볼륨의 모든 데이터가 지워집니다.

선택한 파일 시스템에 따라 논리 볼륨에 사용할 수 있는 구성 매개변수가 결정됩니다. 예를 들어 일부 **XFS** 파일 시스템은 볼륨 축소를 지원하지 않습니다. 자세한 내용은 웹 콘솔에서 논리 볼륨 스케일링을 참조하십시오.

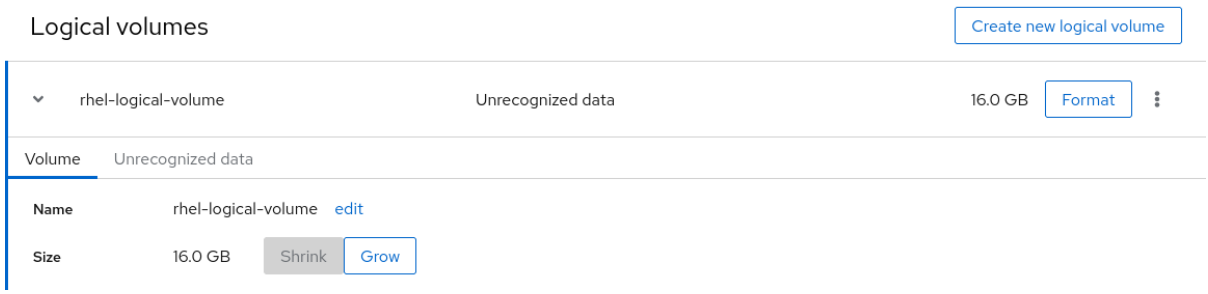
다음 단계에서는 논리 볼륨을 포맷하는 절차를 설명합니다.

사전 요구 사항

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 생성된 논리 볼륨. 자세한 내용은 웹 콘솔에서 논리 볼륨 생성을 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.
2. 스토리지 를 클릭합니다.
3. 장치 섹션에서 논리 볼륨이 배치된 볼륨 그룹을 클릭합니다.
4. 논리 볼륨 섹션에서 포맷 을 클릭합니다.



5. 이름 필드에 파일 시스템의 이름을 입력합니다.
6. 유형 드롭다운 메뉴에서 파일 시스템을 선택합니다.
   - **XFS** 파일 시스템은 대규모 논리 볼륨을 지원하고, 중단 없이 물리적 드라이브를 온라인으로 전환하며, 기존 파일 시스템을 확장합니다. 다른 강력한 기본 설정이 없는 경우 이 파일

시스템을 선택한 상태로 두십시오.

XFS는 **XFS** 파일 시스템으로 포맷된 볼륨의 크기 감소를 지원하지 않습니다.

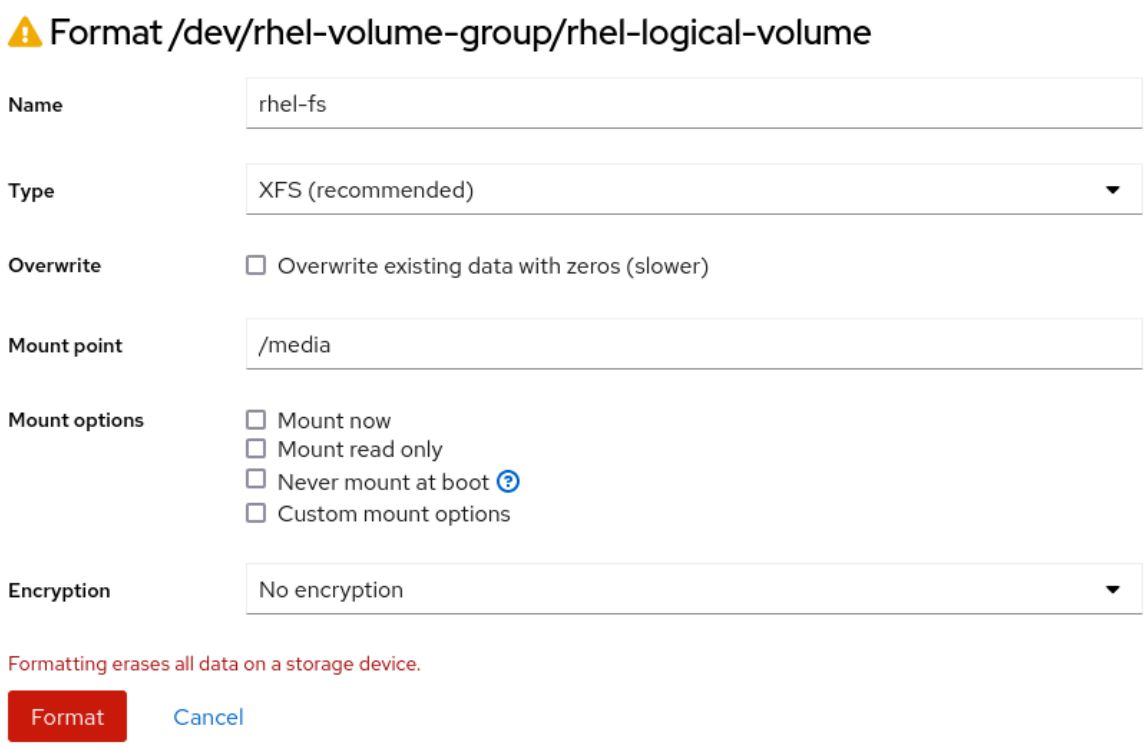
- **ext4** 파일 시스템은 다음을 지원합니다.
  - 논리 볼륨
  - 시스템 중단 없이 온라인으로 물리적 드라이브 전환
  - 파일 시스템 증가
  - 파일 시스템 축소

LUKS(Linux Unified Key Setup) 암호화를 사용하여 버전을 선택할 수 있으므로 암호를 사용하여 볼륨을 암호화할 수 있습니다.

7. **Overwrite** 옵션을 선택합니다.

- 기존 데이터를 덮어 쓰지 마십시오. **RHEL** 웹 콘솔은 디스크 헤더만 다시 작성합니다. 이 옵션의 장점은 포맷 속도입니다.
- 기존 데이터를 **0**으로 덮어 쓰기 **-RHEL** 웹 콘솔은 전체 디스크를 **0**으로 다시 작성합니다. 이 옵션은 프로그램이 전체 디스크를 통과해야 하므로 속도가 느립니다. 디스크에 데이터가 포함되어 있고 덮어써야 하는 경우 이 옵션을 사용합니다.

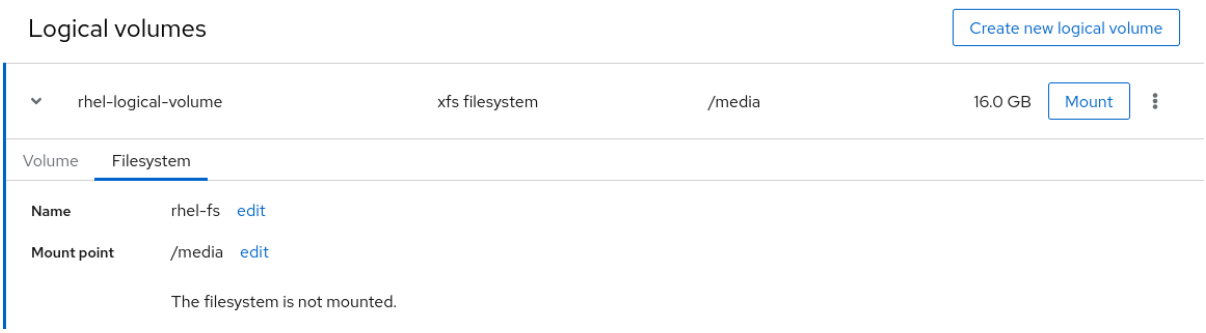
8. **Mount Point** 필드에 마운트 경로를 추가합니다.



9. **Format** 을 클릭합니다.

포맷은 볼륨 크기와 선택한 포맷 옵션에 따라 몇 분이 걸릴 수 있습니다.

포맷이 성공적으로 완료되면 **Filesystem** 탭에서 포맷된 논리 볼륨의 세부 정보를 확인할 수 있습니다.



10. 논리 볼륨을 사용하려면 마운트 를 클릭합니다.

이때 시스템은 마운트 및 포맷된 논리 볼륨을 사용할 수 있습니다.

18.5. 웹 콘솔에서 논리 볼륨 크기 조정

RHEL 9 웹 콘솔에서 논리 볼륨을 확장하거나 줄이는 방법을 알아봅니다.

논리 볼륨의 크기를 조정할 수 있는지 여부는 사용 중인 파일 시스템에 따라 다릅니다. 대부분의 파일 시스템을 사용하면 온라인으로 볼륨을 확장(재중 중단 없이)할 수 있습니다.

논리 볼륨에 축소를 지원하는 파일 시스템이 포함된 경우 논리 볼륨의 크기를 줄일 수도 있습니다. 예를 들어 **ext3**/**ext4** 파일 시스템에서 사용할 수 있어야 합니다.

주의

GFS2 또는 **XFS** 파일 시스템이 포함된 볼륨을 줄일 수 없습니다.

사전 요구 사항

- 논리 볼륨 크기 조정을 지원하는 파일 시스템이 포함된 기존 논리 볼륨입니다.

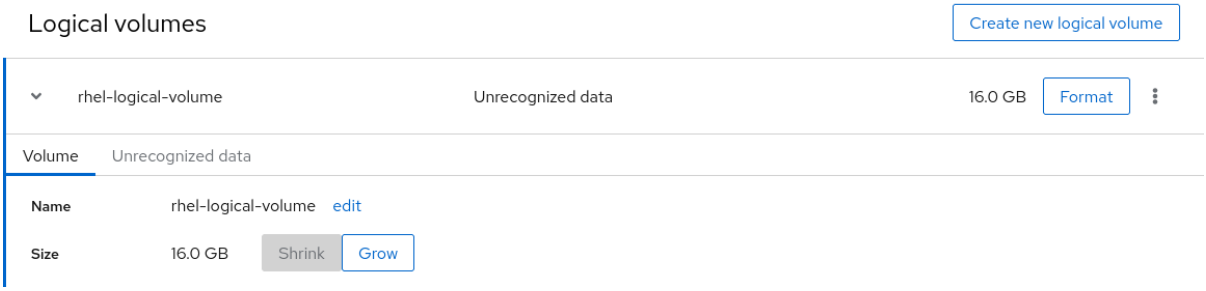
절차

다음 단계에서는 볼륨을 오프라인으로 사용하지 않고 논리 볼륨을 확장하는 절차를 제공합니다.

1. **RHEL** 웹 콘솔에 로그인합니다.
2. 스토리지 를 클릭합니다.
3. 장치 섹션에서 논리 볼륨이 배치된 볼륨 그룹을 클릭합니다.

4. 논리 볼륨 섹션에서 논리 볼륨을 클릭합니다.

5. **Volume** 탭에서 **Grow** 를 클릭합니다.



6. **Grow** 논리 볼륨 대화 상자에서 볼륨 크기를 조정합니다.

7. **Grow** 를 클릭합니다.

LVM은 시스템 중단 없이 논리 볼륨을 확장합니다.

18.6. 추가 리소스

- 논리 볼륨 구성 및 관리

19장. 씬 논리 볼륨 구성에 웹 콘솔 사용

씬 프로비저닝된 논리 볼륨을 사용하면 지정된 애플리케이션 또는 서버에 공간을 더 많이 할당할 수 있습니다. 논리 볼륨에 실제로 포함된 공간보다 많은 공간을 할당할 수 있습니다.

자세한 내용은 씬 프로비저닝된 스냅샷 볼륨 생성을 참조하십시오.

다음 섹션에서는 다음을 설명합니다.

- 씬 프로비저닝된 논리 볼륨의 풀 생성.
- 씬 논리 볼륨 생성.
- 씬 논리 볼륨 포맷.

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다.

  자세한 내용은 웹 콘솔 설치를 참조하십시오.

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 물리 드라이브 또는 볼륨 그룹을 생성할 다른 스토리지 장치 유형.

19.1. 웹 콘솔에서 씬 논리 볼륨용 풀 생성

씬 프로비저닝된 볼륨에 사용할 풀을 만듭니다.

사전 요구 사항

- 볼륨 그룹이 생성되었습니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.

2. 스토리지 를 클릭합니다.

3. 씬 볼륨을 생성할 볼륨 그룹을 클릭합니다.

4. 새 논리 볼륨 만들기를 클릭합니다.

5. 이름 필드에 공백 없이 씬 볼륨의 새 풀의 이름을 입력합니다.

6. **Purpose (**용도**)** 드롭다운 메뉴에서 씬 프로비저닝된 볼륨에 **Pool(**풀**)**을 선택합니다. 이 구성을 사용하면 **thin** 볼륨을 만들 수 있습니다.

7. 씬 볼륨 풀의 크기를 정의합니다. 다음을 고려하십시오.

   - 이 풀에는 몇 개의 씬 볼륨이 필요합니까**?**
   - 각 씬 볼륨의 예상 크기는 무엇입니까**?**

   전체 공간을 사용할 필요는 없습니다. 필요한 경우 나중에 풀을 늘릴 수 있습니다.

8. 생성을 클릭합니다.

   씬 볼륨의 풀이 생성되고 씬 볼륨을 추가할 수 있습니다.

19.2. 웹 콘솔에서 씬 논리 볼륨 생성

풀에 **thin** 논리 볼륨을 생성합니다. 풀에는 여러 씬 볼륨이 포함될 수 있으며 씬 볼륨은 씬 볼륨 자체의 풀만큼 클 수 있습니다.

중요

씬 볼륨을 사용하려면 논리 볼륨의 실제 사용 가능한 물리 공간을 정기적으로 검사해야 합니다.

사전 요구 사항

- 생성된 **thin** 볼륨의 풀입니다.

  자세한 내용은 웹 콘솔에서 **thin** 논리 볼륨을 위한 풀 생성을 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.
2. 스토리지 를 클릭합니다.
3. 씬 볼륨을 생성할 볼륨 그룹을 클릭합니다.
4. 원하는 풀을 클릭합니다.
5. **Create Thin Volume** 을 클릭합니다.
6. **Create Thin Volume** 대화 상자에서 공백 없이 **thin** 볼륨의 이름을 입력합니다.
7. **thin** 볼륨의 크기를 정의합니다.
8. 생성을 클릭합니다.

이 단계에서는 **thin** 논리 볼륨이 생성되었으므로 포맷해야 합니다.

19.3. 웹 콘솔에서 논리 볼륨 포맷

논리 볼륨은 물리적 드라이브 역할을 합니다. 이를 사용하려면 파일 시스템으로 포맷해야 합니다.

주의

논리 볼륨을 포맷하면 볼륨의 모든 데이터가 지워집니다.

선택한 파일 시스템에 따라 논리 볼륨에 사용할 수 있는 구성 매개변수가 결정됩니다. 예를 들어 일부 **XFS** 파일 시스템은 볼륨 축소를 지원하지 않습니다. 자세한 내용은 웹 콘솔에서 논리 볼륨 스케일링을 참조하십시오.

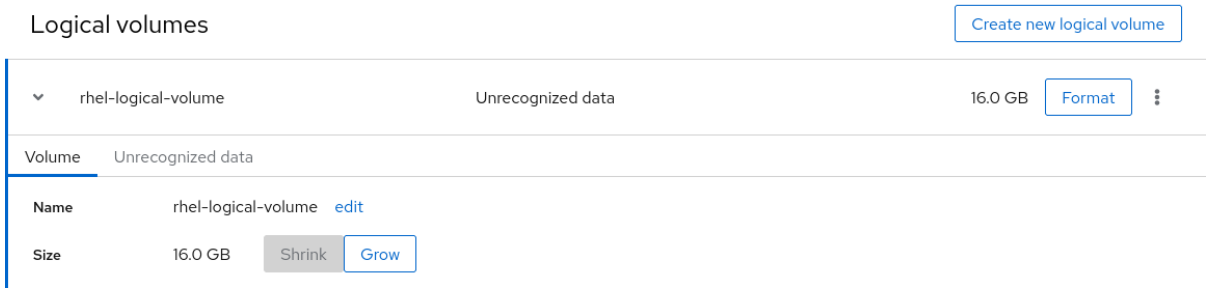
다음 단계에서는 논리 볼륨을 포맷하는 절차를 설명합니다.

사전 요구 사항

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 생성된 논리 볼륨. 자세한 내용은 웹 콘솔에서 논리 볼륨 생성을 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.
2. 스토리지 를 클릭합니다.
3. 장치 섹션에서 논리 볼륨이 배치된 볼륨 그룹을 클릭합니다.
4. 논리 볼륨 섹션에서 포맷 을 클릭합니다.



5. 이름 필드에 파일 시스템의 이름을 입력합니다.

6. 유형 드롭다운 메뉴에서 파일 시스템을 선택합니다.

- **XFS** 파일 시스템은 대규모 논리 볼륨을 지원하고, 중단 없이 물리적 드라이브를 온라인으로 전환하며, 기존 파일 시스템을 확장합니다. 다른 강력한 기본 설정이 없는 경우 이 파일 시스템을 선택한 상태로 두십시오.

  XFS는 **XFS** 파일 시스템으로 포맷된 볼륨의 크기 감소를 지원하지 않습니다.

- **ext4** 파일 시스템은 다음을 지원합니다.
  - 논리 볼륨
  - 시스템 중단 없이 온라인으로 물리적 드라이브 전환
  - 파일 시스템 증가
  - 파일 시스템 축소

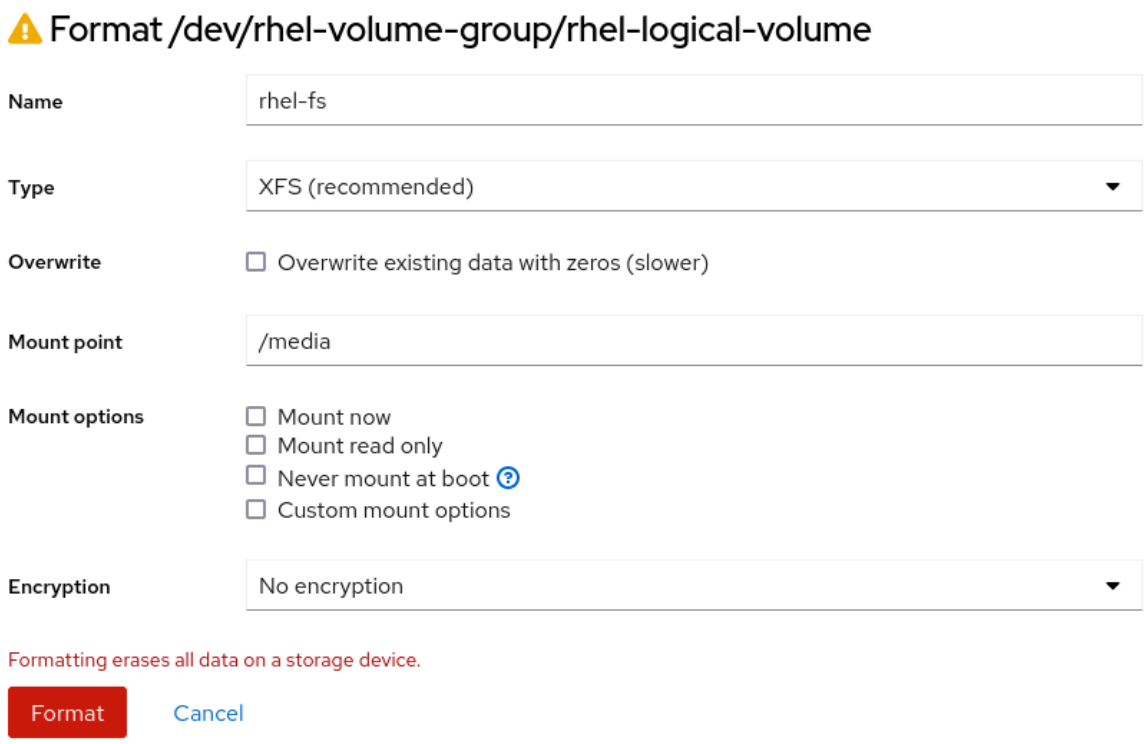
LUKS(Linux Unified Key Setup) 암호화를 사용하여 버전을 선택할 수 있으므로 암호를 사용하여 볼륨을 암호화할 수 있습니다.

7. **Overwrite** 옵션을 선택합니다.

- 기존 데이터를 덮어 쓰지 마십시오. **RHEL** 웹 콘솔은 디스크 헤더만 다시 작성합니다. 이 옵션의 장점은 포맷 속도입니다.

- 기존 데이터를 **0**으로 덮어 쓰기 **-RHEL** 웹 콘솔은 전체 디스크를 **0**으로 다시 작성합니다. 이 옵션은 프로그램이 전체 디스크를 통과해야 하므로 속도가 느립니다. 디스크에 데이터가 포함되어 있고 덮어써야 하는 경우 이 옵션을 사용합니다.

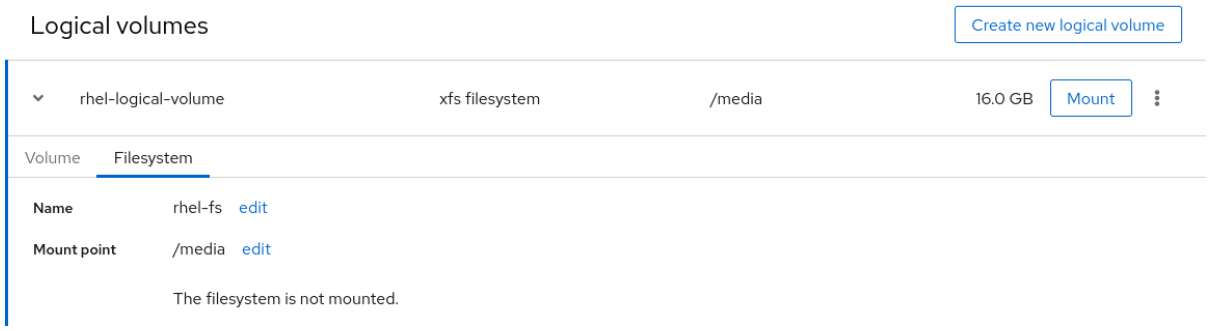
8. **Mount Point** 필드에 마운트 경로를 추가합니다.



9. **Format** 을 클릭합니다.

포맷은 볼륨 크기와 선택한 포맷 옵션에 따라 몇 분이 걸릴 수 있습니다.

포맷이 성공적으로 완료되면 **Filesystem** 탭에서 포맷된 논리 볼륨의 세부 정보를 확인할 수 있습니다.



10. 논리 볼륨을 사용하려면 마운트 를 클릭합니다.

이때 시스템은 마운트 및 포맷된 논리 볼륨을 사용할 수 있습니다.

20장. 볼륨 그룹에서 물리적 드라이브 변경에 대한 웹 콘솔 사용

RHEL 9 웹 콘솔을 사용하여 볼륨 그룹의 드라이브를 변경합니다.

물리적 드라이브의 변경은 다음 절차로 구성됩니다.

- 논리 볼륨에서 물리적 드라이브 추가.
- 논리 볼륨에서 물리적 드라이브 제거.

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다.

  자세한 내용은 웹 콘솔 설치를 참조하십시오.
- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 이전 또는 손상된 상태를 교체하기 위한 새로운 물리적 드라이브.
- 물리적 드라이브는 볼륨 그룹으로 구성되어 있어야 합니다.

20.1. 웹 콘솔의 볼륨 그룹에 물리적 드라이브 추가

RHEL 9 웹 콘솔을 사용하면 새 물리 드라이브 또는 기타 유형의 볼륨을 기존 논리 볼륨에 추가할 수 있습니다.

사전 요구 사항

- 볼륨 그룹을 생성해야 합니다.
- 컴퓨터에 연결된 새 드라이브입니다.

절차

1. **RHEL 9** 콘솔에 로그인합니다.
2. 스토리지 를 클릭합니다.
3. 볼륨 그룹 상자에서 물리 볼륨을 추가할 볼륨 그룹을 클릭합니다.
4. 물리 볼륨 상자에서 **+** 버튼을 클릭합니다.
5. 디스크 추가 대화 상자에서 기본 드라이브를 선택하고 추가 를 클릭합니다.

결과적으로 **RHEL 9** 웹 콘솔은 물리 볼륨을 추가합니다.

검증 단계

- 섹션의 물리 볼륨을 확인하고 논리 볼륨이 드라이브에 즉시 쓰기를 시작할 수 있습니다.

20.2. 웹 콘솔의 볼륨 그룹에서 물리적 드라이브 제거

논리 볼륨에 여러 개의 물리적 드라이브가 포함된 경우 온라인으로 물리적 드라이브 중 하나를 제거할 수 있습니다.

시스템은 제거 과정에서 다른 드라이브로 제거되도록 드라이브의 모든 데이터를 자동으로 이동합니다. 다소 시간이 걸릴 수 있습니다.

웹 콘솔은 또한 실제 드라이브를 제거하기에 충분한 공간이 있는지 확인합니다.

사전 요구 사항

- 물리 드라이브가 두 개 이상 연결된 볼륨 그룹입니다.

절차

다음 단계에서는 **RHEL RHEL** 웹 콘솔에서 중단하지 않고 볼륨 그룹에서 드라이브를 제거하는 방법을 설명합니다.

1. **RHEL 9** 웹 콘솔에 로그인합니다.
2. 스토리지 를 클릭합니다.
3. 논리 볼륨이 있는 볼륨 그룹을 클릭합니다.
4. 물리 볼륨 섹션에서 선호하는 볼륨을 찾습니다.
5. **-** 아이콘을 클릭합니다.

   RHEL 9 웹 콘솔은 논리 볼륨에 디스크를 제거하기에 충분한 여유 공간이 있는지 확인합니다. 그렇지 않으면 디스크를 제거할 수 없으며 다른 디스크를 먼저 추가해야 합니다. 자세한 내용은 웹 콘솔의 논리 볼륨에 물리적 드라이브 추가를 참조하십시오.

결과적으로 **RHEL 9** 웹 콘솔은 생성된 논리 볼륨에서 물리 볼륨을 제거해도 중단되지 않습니다.

21장. 가상 데이터 최적화 도구 볼륨 관리에 웹 콘솔 사용

RHEL 9 웹 콘솔을 사용하여 VDO(가상 데이터 최적화 도구)를 구성합니다.

다음을 수행하는 방법을 배웁니다.

- VDO 볼륨 생성
- VDO 볼륨 형식
- VDO 볼륨 확장

사전 요구 사항

- RHEL 9 웹 콘솔이 설치되어 액세스할 수 있습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- cockpit-storaged 패키지가 시스템에 설치됩니다.

21.1. 웹 콘솔의 VDO 볼륨

Red Hat Enterprise Linux 9는 VDO(Virtual Data Optimizer)를 지원합니다.

VDO는 다음을 결합하는 블록 가상화 기술입니다.

압축

자세한 내용은 VDO에서 압축 활성화 또는 비활성화를 참조하십시오.

중복 제거

자세한 내용은 VDO에서 압축 활성화 또는 비활성화를 참조하십시오.

씬 프로비저닝

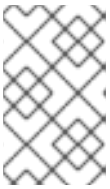
자세한 내용은 씬 프로비저닝된 볼륨(타사 볼륨) 생성 및 관리를 참조하십시오.

이러한 기술 사용 **VDO:**

- 스토리지 공간 인라인 저장
- 파일 압축
- 중복 제거
- 물리적 또는 논리적 저장소에서 제공하는 것보다 많은 가상 공간을 할당할 수 있습니다.
- 스토리지를 확장하여 가상 스토리지를 확장할 수 있습니다.

VDO는 다양한 유형의 스토리지 위에 생성할 수 있습니다. **RHEL 9** 웹 콘솔에서는 다음과 같이 **VDO**를 구성할 수 있습니다.

- **LVM**

  참고

  씬 프로비저닝 볼륨 상단에 **VDO**를 구성할 수 없습니다.

- 물리 볼륨
- 소프트웨어 **RAID**

스토리지 스택의 **VDO** 배치에 대한 자세한 내용은 시스템 요구 사항을 참조하십시오.

추가 리소스

- **VDO**에 대한 자세한 내용은 스토리지 분할 및 압축을 참조하십시오.

21.2. 웹 콘솔에서 VDO 볼륨 생성

RHEL 웹 콘솔에서 **VDO** 볼륨을 생성합니다.

사전 요구 사항

- **VDO**를 생성할 물리적 드라이브, **LVM** 또는 **RAID**입니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 스토리지 를 클릭합니다.

3. **VDO** 장치 상자에서 **+** 아이콘을 클릭합니다.

4. 이름 필드에 공백이 없는 **VDO** 볼륨의 이름을 입력합니다.

5. 사용할 드라이브를 선택합니다.

6. 논리 크기 표시줄에서 **VDO** 볼륨의 크기를 설정합니다. **10**배 이상 확장할 수 있지만 **VDO** 볼륨을 만드는 목적으로 고려해야 합니다.

   - 활성 **VM** 또는 컨테이너 스토리지의 경우 볼륨의 물리 크기 **10**배인 논리 크기를 사용합니다.

   - 오브젝트 스토리지의 경우 볼륨의 물리 크기를 세 배인 논리 크기를 사용합니다.

자세한 내용은 **Deploying VDO** 을 참조하십시오.

7. 인덱스 메모리 모음에서 **VDO** 볼륨에 메모리를 할당합니다.

   VDO 시스템 요구 사항에 대한 자세한 내용은 시스템 요구 사항을 참조하십시오.

8. 압축 옵션을 선택합니다. 이 옵션은 다양한 파일 형식을 효율적으로 줄일 수 있습니다.

   자세한 내용은 **VDO**에서 압축 활성화 또는 비활성화를 참조하십시오.

9. **D training plication** 옵션을 선택합니다.

   이 옵션을 사용하면 중복 블록의 여러 복사본을 제거하여 스토리지 리소스 사용을 줄일 수 있습니다. 자세한 내용은 **VDO**에서 압축 활성화 또는 비활성화를 참조하십시오.

10. **[**선택 사항**] 512**바이트 블록 크기가 필요한 애플리케이션에 **VDO** 볼륨을 사용하려면 **Use 512** 바이트 에뮬레이션 을 선택합니다. 이렇게 하면 **VDO** 볼륨의 성능이 저하되지만 거의 필요하지 않습니다. 의심의 여지가있는 경우, 그것을 남겨 두십시오.

11. 생성을 클릭합니다.

검증 단계

- **Storage (**스토리지**)** 섹션에서 새 **VDO** 볼륨이 표시되는지 확인합니다. 그러면 파일 시스템으로 포맷할 수 있습니다.

21.3. 웹 콘솔에서 **VDO** 볼륨 포맷

VDO 볼륨은 물리적 드라이브 역할을 합니다. 이를 사용하려면 파일 시스템으로 포맷해야 합니다.

주의

VDO 형식에서는 볼륨의 모든 데이터가 지워집니다.

다음 단계에서는 **VDO** 볼륨을 포맷하는 절차를 설명합니다.

사전 요구 사항

- **VDO** 볼륨이 생성됩니다. 자세한 내용은 웹 콘솔에서 **VDO** 볼륨 생성을 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 스토리지 를 클릭합니다.
3. **VDO** 볼륨을 클릭합니다.
4. 인식되지 않는 데이터 탭을 클릭합니다.
5. **Format** 을 클릭합니다.
6. **Erase** 드롭다운 메뉴에서 다음을 선택합니다.

기존 데이터를 덮어쓰지 마십시오.

RHEL 웹 콘솔은 디스크 헤더만 다시 작성합니다. 이 옵션의 장점은 서식 지정 속도입니다.

기존 데이터를 **0**으로 덮어쓰기

RHEL 웹 콘솔은 전체 디스크를 **0**으로 다시 작성합니다. 이 옵션은 프로그램이 전체 디

스크를 통과해야 하므로 속도가 느립니다. 디스크에 데이터가 포함되어 다시 작성해야 하는 경우 이 옵션을 사용합니다.

7. 유형 드롭다운 메뉴에서 파일 시스템을 선택합니다.

- **XFS** 파일 시스템은 대규모 논리 볼륨을 지원하고, 중단 없이 물리적 드라이브를 온라인으로 전환하며, 확장 가능합니다. 다른 강력한 기본 설정이 없는 경우 이 파일 시스템을 선택한 상태로 두십시오.

  XFS는 볼륨 축소를 지원하지 않습니다. 따라서 **XFS**로 포맷된 볼륨을 줄일 수 없습니다.

- **ext4** 파일 시스템은 논리 볼륨을 지원하여 중단, 확장 및 축소 없이 물리적 드라이브를 온라인으로 전환합니다.

LUKS(Linux Unified Key Setup) 암호화를 사용하여 버전을 선택할 수 있으므로 암호를 사용하여 볼륨을 암호화할 수 있습니다.

8. 이름 필드에 논리 볼륨 이름을 입력합니다.

9. **Mounting(** 마운트 **)** 드롭다운 메뉴에서 **Custom (**사용자 지정**)**을 선택합니다.

   Default 옵션을 사용하면 다음 부팅 시 파일 시스템이 마운트되지 않습니다.

10. **Mount Point** 필드에 마운트 경로를 추가합니다.

11. 부팅 시 마운트를 선택합니다.

12. **Format** 을 클릭합니다.

    사용 된 포맷 옵션 및 볼륨 크기에 따라 포맷하는 데 몇 분이 걸릴 수 있습니다.

    성공적으로 완료되면 **Filesystem** 탭에서 포맷된 **VDO** 볼륨의 세부 정보를 볼 수 있습니다.

13. **VDO** 볼륨을 사용하려면 마운트 를 클릭합니다.

이 시점에서 시스템은 마운트된 **VDO** 볼륨을 사용합니다.

21.4. 웹 콘솔에서 VDO 볼륨 확장

RHEL 9 웹 콘솔에서 **VDO** 볼륨을 확장합니다.

사전 요구 사항

- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- **VDO** 볼륨이 생성되었습니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 스토리지 를 클릭합니다.
3. **VDO** 장치 상자에서 **VDO** 볼륨을 클릭합니다.
4. **VDO** 볼륨 세부 정보에서 **Grow** 버튼을 클릭합니다.
5. **VDO** 대화 상자의 **Grow** 논리 크기에서 **VDO** 볼륨의 논리 크기를 확장합니다.

1. **Grow** 를 클릭합니다.

검증 단계

- 새 크기에 대한 **VDO** 볼륨 세부 정보를 확인하여 변경 사항이 성공했는지 확인합니다.

22장. RHEL 웹 콘솔에서 LUKS 암호를 사용하여 데이터 잠금

웹 콘솔의 스토리지 탭에서 **LUKS(Linux Unified Key Setup)** 버전 **2** 형식을 사용하여 암호화된 장치를 생성, 잠금, 잠금, 크기 조정 및 구성할 수 있습니다.

이 새로운 **LUKS** 버전은 다음과 같습니다.

- 보다 유연한 정책 잠금 해제
- 더 강력한 암호화
- 향후 변경 사항과의 호환성 개선

사전 요구 사항

- **RHEL 9** 웹 콘솔이 설치되었습니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- **cockpit-storaged** 패키지가 시스템에 설치됩니다.

22.1. LUKS 디스크 암호화

Linux Unified Key Setup-on-disk-format(LUKS)을 사용하면 블록 장치를 암호화할 수 있으며 암호화된 장치 관리를 간소화하는 툴 세트를 제공합니다. **LUKS**를 사용하면 여러 사용자 키가 파티션의 대량 암호화에 사용되는 마스터 키의 암호를 해독할 수 있습니다.

RHEL은 **LUKS**를 사용하여 블록 장치 암호화를 수행합니다. 기본적으로 블록 장치를 암호화하는 옵션은 설치 중에 확인되지 않습니다. 디스크를 암호화하기 위해 옵션을 선택하면 컴퓨터를 부팅할 때마다 시스템에서 암호를 입력하라는 메시지를 표시합니다. 이 암호는 파티션을 해독하는 대량 암호화 키를 "잠금 해제합니다". 기본 파티션 테이블을 수정하려면 암호화할 파티션을 선택할 수 있습니다. 이는 파티션 테이블 설정에 설정되어 있습니다.

LUKS의 기능

- **LUKS**는 전체 블록 장치를 암호화하므로 이동식 스토리지 미디어 또는 랩탑 디스크 드라이브와 같은 모바일 장치의 콘텐츠를 보호하기에 적합합니다.

- 암호화된 블록 장치의 기본 내용은 임의하므로 스왑 장치를 암호화하는 데 유용합니다. 이는 데이터 저장을 위해 특별히 포맷된 블록 장치를 사용하는 특정 데이터베이스에서도 유용할 수 있습니다.

- **LUKS**는 기존 장치 매퍼 커널 하위 시스템을 사용합니다.

- **LUKS**는 사전 공격으로부터 보호하는 암호 강화를 제공합니다.

- **LUKS** 장치에는 여러 개의 키 슬롯이 포함되어 있어 사용자가 백업 키 또는 암호를 추가할 수 있습니다.

LUKS가 수행할 수 *없*는 작업

- **LUKS**와 같은 디스크 암호화 솔루션은 시스템이 꺼져 있을 때만 데이터를 보호합니다. 시스템이 켜져 있고 **LUKS**가 디스크의 암호를 해독하면 해당 디스크의 파일은 일반적으로 액세스할 수 있는 모든 사용자가 사용할 수 있습니다.

- **LUKS**는 많은 사용자가 동일한 장치에 고유한 액세스 키를 보유해야 하는 시나리오에 적합하지 않습니다. **LUKS1** 형식은 **8**개의 키 슬롯을 제공하며, **LUKS2**는 최대 **32**개의 키 슬롯을 제공합니다.

- **LUKS**는 파일 수준 암호화가 필요한 애플리케이션에 적합하지 않습니다.

암호화

LUKS에 사용되는 기본 암호는 **aes-xts-plain64** 입니다. **LUKS**의 기본 키 크기는 **512**비트입니다. **Anaconda (XTS** 모드**)**가 있는 **LUKS**의 기본 키 크기는 **512**비트입니다. 사용 가능한 암호는 다음과 같습니다.

- **AES -** 고급 암호화 표준

- **Twofish(128**비트 블록 암호**)**

- **serpent**

추가 리소스

- **LUKS** 프로젝트 홈 페이지
- **LUKS On-Disk** 형식 사양
- **FIPS PUB 197**

22.2. 웹 콘솔에서 LUKS 암호 구성

시스템의 기존 논리 볼륨에 암호화를 추가하려면 볼륨 포맷을 통해서만 수행할 수 있습니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- **cockpit-storaged** 패키지가 시스템에 설치됩니다.
- 암호화 없이 기존 논리 볼륨을 사용할 수 있습니다.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 스토리지 를 클릭합니다.
3. 포맷할 스토리지 장치를 선택합니다.
4. 메뉴 아이콘을 클릭하고 형식 옵션을 선택합니다.

5. 암호화 데이터 상자를 선택하여 스토리지 장치에서 암호화를 활성화합니다.

6. 새 암호를 설정하고 확인합니다.

7. **[**선택 사항**]** 추가 암호화 옵션 수정

8. 포맷 설정을 완료합니다.

9. **Format** 을 클릭합니다.

22.3. 웹 콘솔에서 LUKS 암호 변경

웹 콘솔에서 암호화된 디스크 또는 파티션에서 **LUKS** 암호를 변경합니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.
- **cockpit-storaged** 패키지가 시스템에 설치됩니다.

절차

1. 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. **Storage**를 클릭합니다.

3. 드라이브 테이블에서 암호화된 데이터가 있는 디스크를 선택합니다.

4. **Content** 에서 암호화된 파티션을 선택합니다.

5. 암호화를 클릭합니다.

6. 키 테이블에서 펜 아이콘을 클릭합니다.

7. 암호 변경 대화 상자 창에서 다음을 수행합니다.

   a. 현재 암호를 입력합니다.

   b. 새 암호를 입력합니다.

   c. 새 암호를 확인합니다.

8. 저장을클릭합니다.

23장. 웹 콘솔에서 소프트웨어 업데이트 관리

RHEL 9 웹 콘솔에서 소프트웨어 업데이트를 관리하는 방법과 이를 자동화하는 방법을 알아봅니다.

웹 콘솔의 소프트웨어 업데이트 모듈은 **dnf** 유틸리티를 기반으로 합니다. **dnf** 를 사용하여 소프트웨어를 업데이트하는 방법에 대한 자세한 내용은 패키지 업데이트 섹션을 참조하십시오.

23.1. 웹 콘솔에서 수동 소프트웨어 업데이트 관리

이 섹션에서는 웹 콘솔을 사용하여 소프트웨어를 수동으로 업데이트하는 방법을 설명합니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 소프트웨어 업데이트를 클릭합니다.

   마지막 검사가 **24**시간 전에 발생한 경우 사용 가능한 업데이트 목록이 자동으로 새로 고침됩니다. 새로 고침을 트리거하려면 **Check for Updates** 버튼을 클릭합니다.

3. 업데이트 적용.

   a. 사용 가능한 업데이트를 모두 설치하려면 **Install all updates** 버튼을 클릭합니다.

   b. 보안 업데이트를 사용할 수 있는 경우 보안 업데이트 설치 버튼을 클릭하여 별도로 설치할 수 있습니다. 업데이트가 실행되는 동안 업데이트 로그를 볼 수 있습니다.

4. 시스템이 업데이트를 적용한 후에는 시스템을 다시 시작하는 것이 좋습니다.

   업데이트 시 개별적으로 재시작하지 않으려는 새로운 커널 또는 시스템 서비스가 포함되어 있는 경우 특히 이 문제를 해결하는 것이 좋습니다.

5. **Ignore** 를 클릭하여 다시 시작을 취소하거나 지금 다시 시작을 클릭하여 시스템을 다시 시작합니다.

   시스템을 다시 시작한 후 웹 콘솔에 로그인하고 소프트웨어 업데이트 페이지로 이동하여 업데이트가 성공했는지 확인합니다.

23.2. 웹 콘솔에서 자동 소프트웨어 업데이트 관리

웹 콘솔에서는 모든 업데이트 또는 보안 업데이트를 적용하고 자동 업데이트 시간을 관리하도록 선택할 수 있습니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 소프트웨어 업데이트를 클릭합니다.

3. **Settings** (설정) 표에서 **Edit** (편집) 버튼을 클릭합니다.

4. 자동 업데이트 유형 중 하나를 선택합니다. 보안 업데이트에서만 또는 모든 업데이트에서 선택할 수 있습니다.

5. 자동 업데이트의 날짜를 수정하려면 매일 드롭다운 메뉴를 클릭하고 특정 날짜를 선택합니다.

6. 자동 업데이트 시간을 수정하려면 **6:00** 필드를 클릭하고 특정 시간을 선택하거나 입력합니다.

7. 자동 소프트웨어 업데이트를 비활성화하려면 **No updates** 유형을 선택합니다.

23.3. 웹 콘솔에 소프트웨어 업데이트를 적용한 후 온디맨드 재시작 관리

지능형 다시 시작 기능은 소프트웨어 업데이트를 적용한 후 전체 시스템을 재부팅해야 하는지 또는 특정 서비스만 다시 시작하기에 충분한 경우 사용자에게 알립니다.

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다. 자세한 내용은 웹 콘솔 설치를 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

2. 소프트웨어 업데이트를 클릭합니다.

3. 시스템 업데이트를 적용합니다.

4. 업데이트가 완료되면 **Reboot system…**을 클릭합니다., **restart services…**, 또는 **Ignore**

5. 무시하려면 다음 중 하나를 수행하여 다시 시작 또는 재부팅 메뉴로 돌아갈 수 있습니다.

   a. 재부팅:

      i. **Software Updates** (소프트웨어 업데이트) 페이지의 **Status** (상태) 필드에서 **Reboot system** (시스템 재부팅) 버튼을 클릭합니다.

      ii. (선택 사항) 로그인한 사용자에게 메시지를 작성합니다.

iii. **Delay** 드롭다운 메뉴에서 지연을 선택합니다.

iv. **Reboot (**재부팅**)**를 클릭합니다.

b. 서비스 다시 시작**:**

i. **Restart services…**을 클릭합니다**.** 버튼을 클릭하여 **Software Updates** 페이지의 상태 필드에 있습니다**.**

다시 시작해야 하는 모든 서비스 목록이 표시됩니다**.**

ii. 서비스 재시작 을 클릭합니다**.**

선택한 상황에 따라 시스템이 재부팅되거나 서비스가 다시 시작됩니다**.**

23.4. 웹 콘솔에서 커널 실시간 패치에 패치 적용

웹 콘솔을 사용하면 **kpatch** 프레임워크를 사용하여 재부팅하지 않고도 커널 보안 패치를 적용할 수 있습니다**.** 다음 절차에서는 기본 유형의 패치를 설정하는 방법을 보여줍니다**.**

사전 요구 사항

- 웹 콘솔을 설치하고 액세스할 수 있어야 합니다**.** 자세한 내용은 웹 콘솔 설치를 참조하십시오**.**

절차

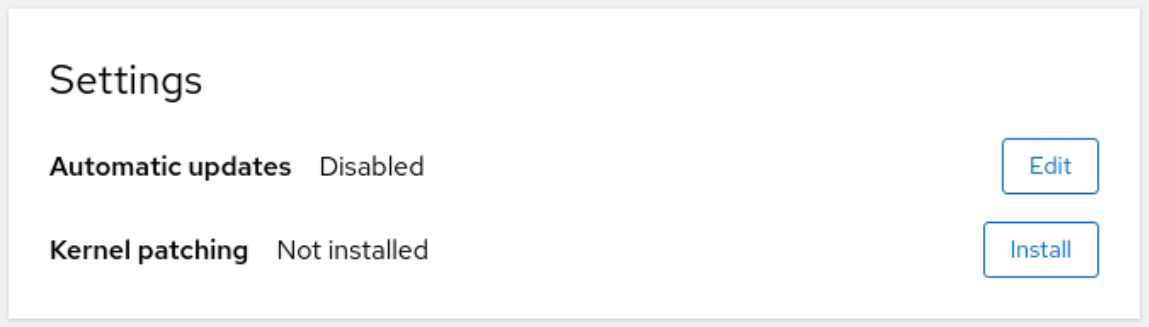
1. 관리 권한으로 웹 콘솔에 로그인합니다**.** 자세한 내용은 웹 콘솔에 로그인을 참조하십시오**.**

2. 소프트웨어 업데이트를 클릭합니다**.**

3. 커널 패치 설정 상태를 확인합니다**.**

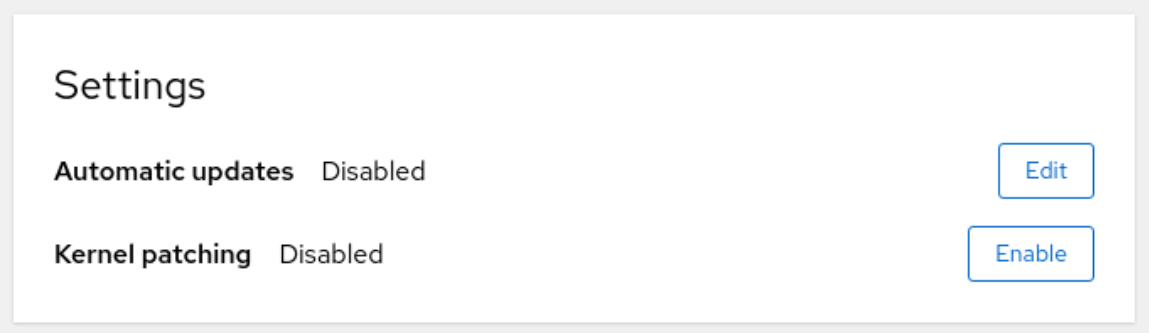
a.

패치가 설치되어 있지 않으면 설치를 클릭합니다.



b.

커널 패치를 활성화하려면 활성화를 클릭합니다.

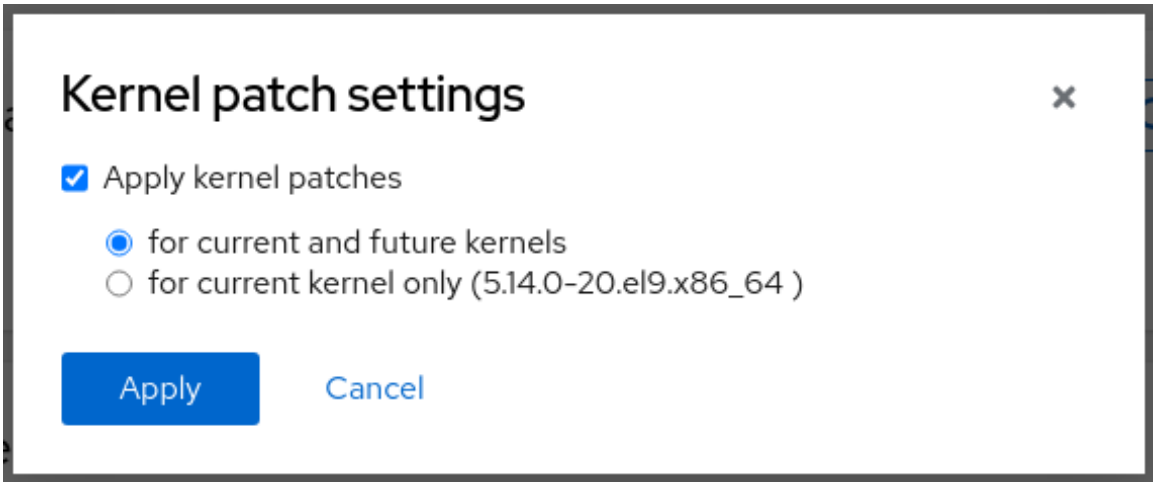


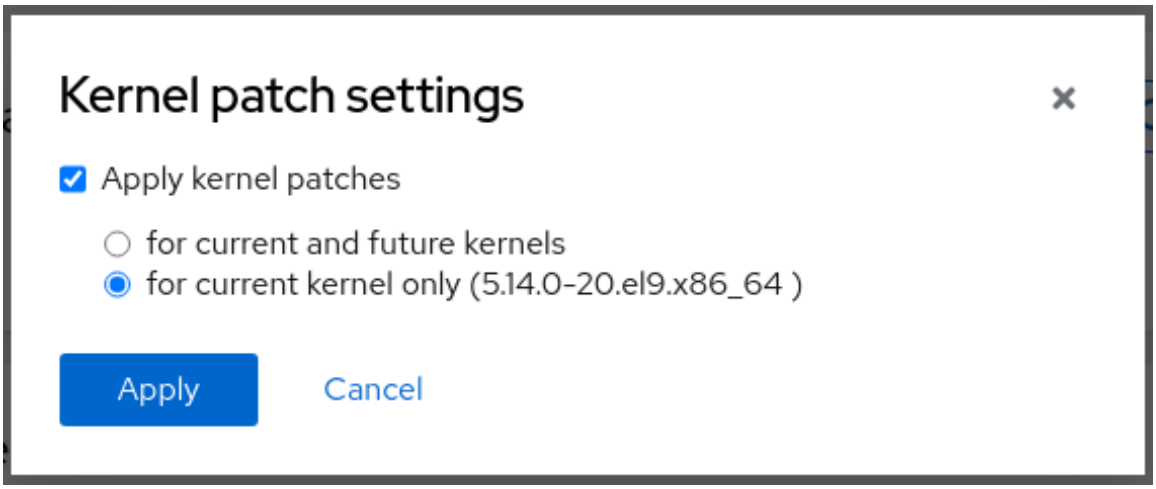
c.

커널 패치 적용을 위한 확인란을 선택합니다.

d.

현재 커널 및 향후 커널 또는 현재 커널에만 패치를 적용할지 여부를 선택합니다. 향후 커널에 패치를 적용하기로 선택한 경우 향후 커널 릴리스에 대한 패치도 적용됩니다.

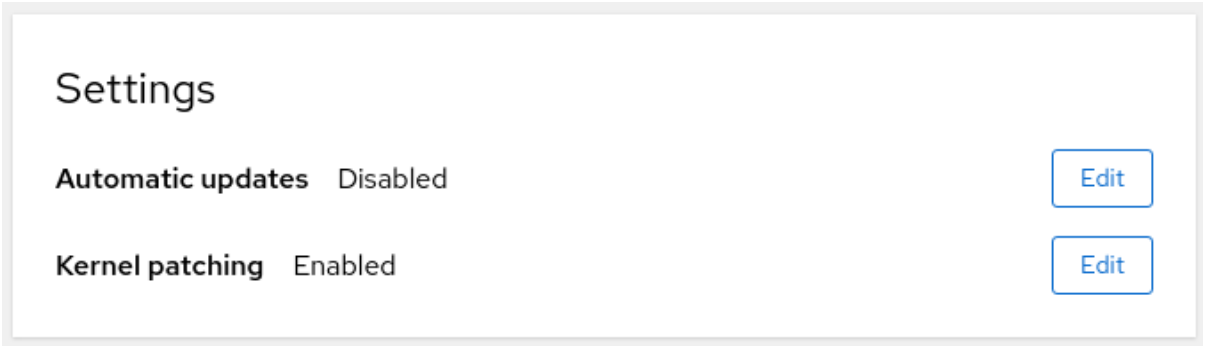




e. 적용을 클릭합니다.

검증

- 소프트웨어 업데이트 섹션의 설정 표에서 커널 패치가 활성화되어 있는지 확인합니다.



추가 리소스

- 커널 라이브 패치로 패치 적용

24장. 웹 콘솔에서 서브스크립션 관리

웹 콘솔에서 **Red Hat Enterprise Linux 9**에 대한 서브스크립션을 관리합니다.

Red Hat Enterprise Linux에 대한 서브스크립션을 받으려면 **Red Hat** 고객 포털 또는 활성화 키의 계정이 있어야 합니다.

이 장의 내용은 다음과 같습니다.

- **RHEL 9** 웹 콘솔의 서브스크립션 관리
- 웹 콘솔에서 **Red Hat** 사용자 이름 및 암호를 사용하여 시스템에 대한 서브스크립션 등록.
- 활성화 키로 서브스크립션을 등록합니다.

사전 요구 사항

- 구입한 서브스크립션.
- 웹 콘솔이 **Red Hat** 고객 포털과 통신해야 하므로 서브스크립션이 적용되는 시스템은 인터넷에 연결되어 있어야 합니다.

24.1. 웹 콘솔에서 서브스크립션 관리

RHEL 9 웹 콘솔은 로컬 시스템에 설치된 **Red Hat Subscription Manager**를 사용하기 위한 인터페이스를 제공합니다.

서브스크립션 관리자는 **Red Hat Customer Portal**에 연결하고 사용 가능한 모든 것을 확인합니다.

- 활성 서브스크립션

- 만료된 서브스크립션
- 서브스크립션 갱신

서브스크립션을 갱신하거나 **Red Hat** 고객 포털에서 다른 서브스크립션을 받으려면 서브스크립션 관리자 데이터를 수동으로 업데이트할 필요가 없습니다. 서브스크립션 관리자는 **Red Hat Customer Portal**과 데이터를 자동으로 동기화합니다.

24.2. 웹 콘솔에서 인증 정보를 사용하여 서브스크립션 등록

다음 단계를 사용하여 **RHEL** 웹 콘솔을 사용하여 계정 자격 증명으로 새로 설치된 **Red Hat Enterprise Linux**를 등록합니다.

사전 요구 사항

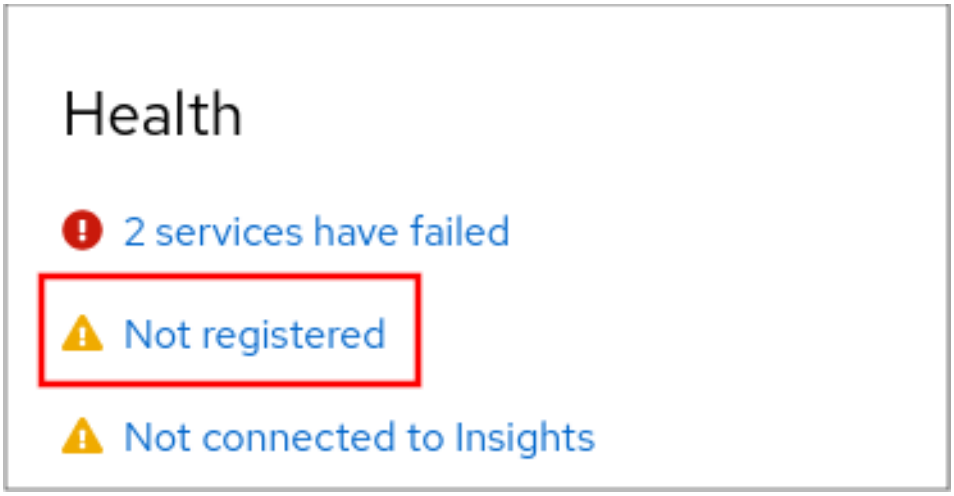
- **Red Hat** 고객 포털에서 유효한 사용자 계정.

  Red Hat 로그인 생성 페이지를 참조하십시오.

- **RHEL** 시스템에 대한 활성 서브스크립션입니다.

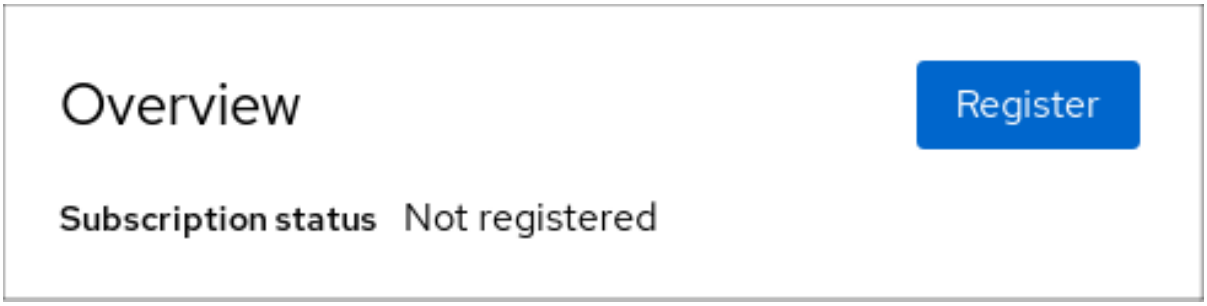
절차

1. **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.
2. 개요 페이지의 **Health filed**에서 **Not registered** 경고를 클릭하거나 메인 메뉴에서 **Subscriptions (**서브스크립션**)**를 클릭하여 서브스크립션 정보를 페이지로 이동합니다.

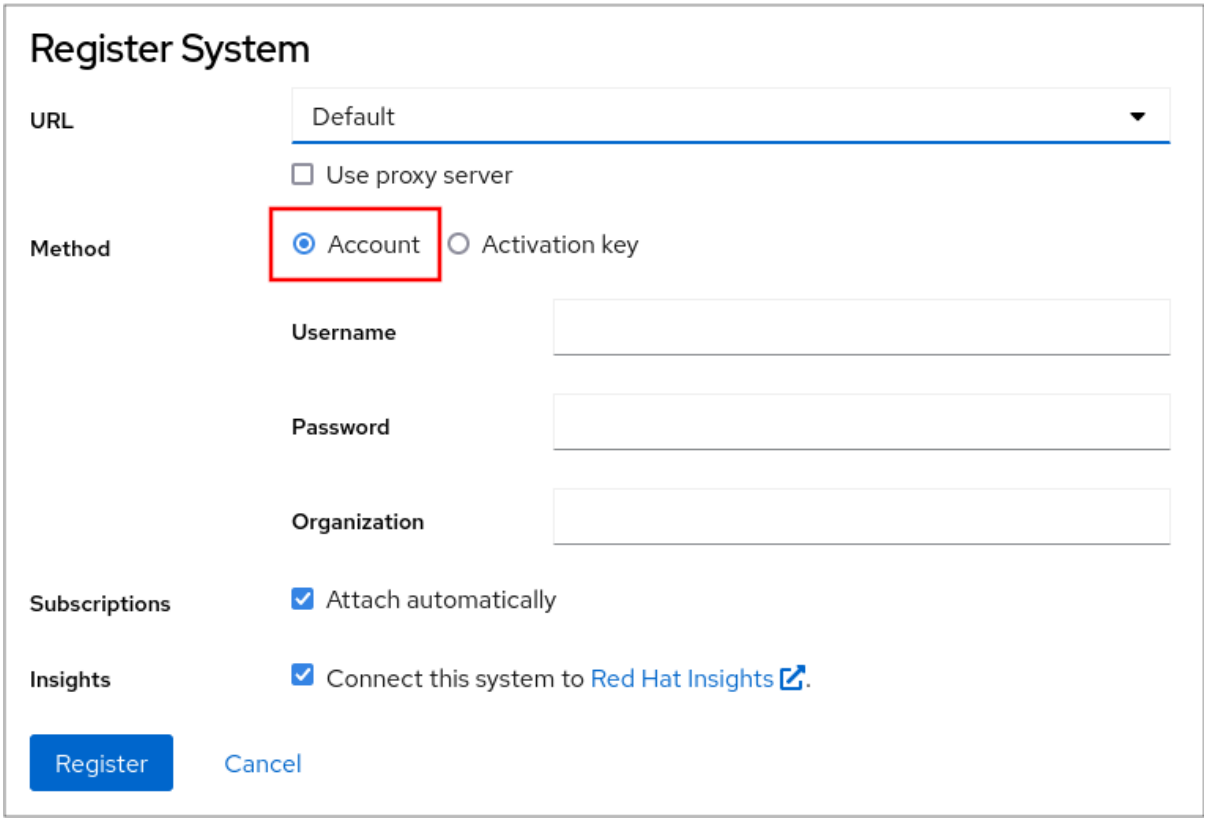


.

3. **Overview filed**에서 **Register** 를 클릭합니다**.**



4. 시스템 등록 대화 상자에서 계정 자격 증명을 사용하여 등록할 항목을 선택합니다**.In the Register system dialog box, select that you want to register using your account credentials.**



5. 사용자 이름을 입력합니다.

6. 암호를 입력합니다.

7. 필요한 경우 조직의 이름 또는 **ID**를 입력합니다.

Red Hat 고객 포털에서 두 개 이상의 조직에 속해 있는 경우 조직 이름 또는 조직 **ID**를 추가해야 합니다. 조직 **ID**를 얻으려면 **Red Hat** 담당자로 이동합니다.

- 시스템을 **Red Hat Insights**에 연결하지 않으려면 **Insights** 확인란을 선택 취소합니다.

8. **Register** 버튼을 클릭합니다.

이 시점에서 **Red Hat Enterprise Linux** 시스템이 성공적으로 등록되었습니다.

24.3. 웹 콘솔에서 활성화 키로 서브스크립션 등록

다음 단계를 사용하여 **RHEL** 웹 콘솔을 사용하여 새로 설치된 **Red Hat Enterprise Linux**를 활성화 키로 등록합니다.

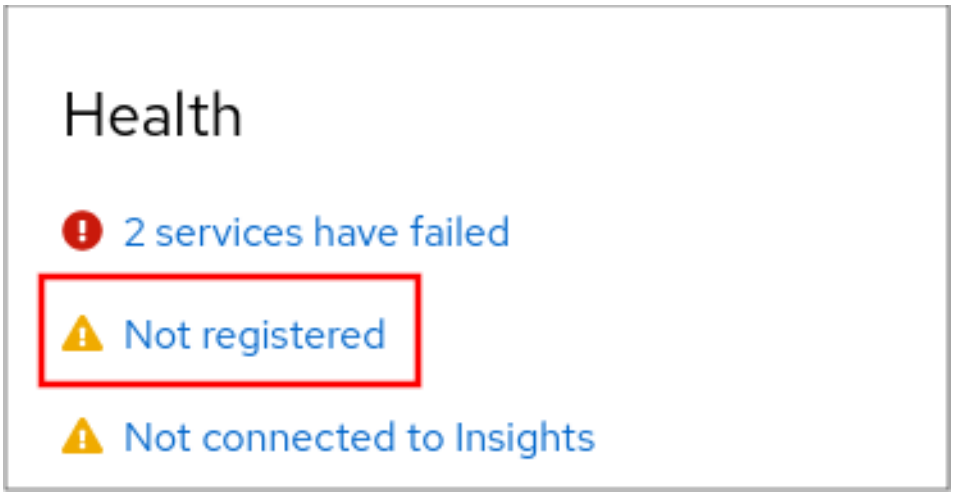
사전 요구 사항

- 포털에 사용자 계정이 없는 경우 공급 업체가 활성화 키를 제공합니다.

절차

1. **RHEL** 웹 콘솔에 로그인합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

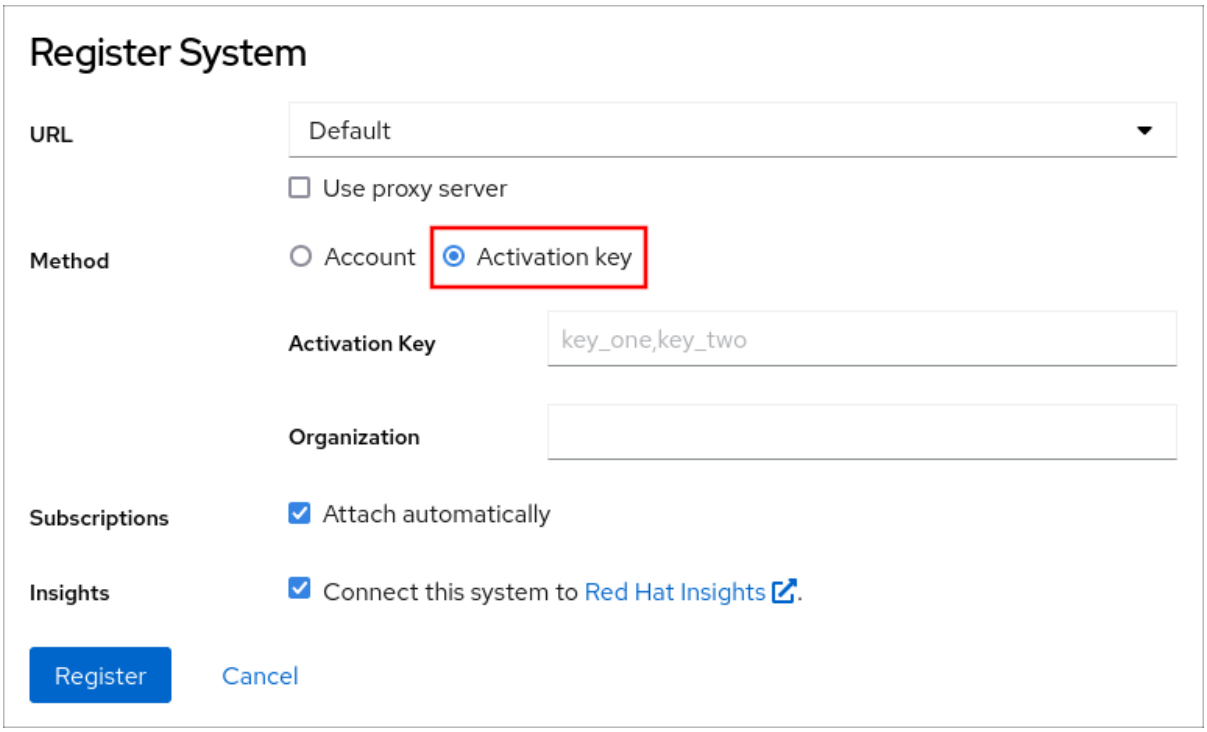
2. 개요 페이지의 **Health filed**에서 **Not registered** 경고를 클릭하거나 메인 메뉴에서 **Subscriptions (**서브스크립션)를 클릭하여 서브스크립션 정보를 페이지로 이동합니다.



.

3. **Overview filed**에서 **Register** 를 클릭합니다.

4. 시스템 등록 대화 상자에서 활성화 키를 사용하여 등록할지 선택합니다.



5. 키 또는 키를 입력합니다.

6. 조직의 이름 또는 **ID**를 입력합니다.

   조직 **ID**를 가져오려면 **Red Hat** 담당자로 이동합니다.

   - 시스템을 **Red Hat Insights**에 연결하지 않으려면 **Insights** 확인란을 선택 취소합니다.

7. **Register** 버튼을 클릭합니다.

이 시점에서 **Red Hat Enterprise Linux** 시스템이 성공적으로 등록되었습니다.

25장. 웹 콘솔에서 KDUMP 구성

RHEL 9 웹 콘솔에서 **kdump** 설정을 설정 및 테스트합니다.

웹 콘솔은 **RHEL 9**의 기본 설치의 일부이며 부팅 시 **kdump** 서비스를 활성화하거나 비활성화합니다. 또한 웹 콘솔을 사용하면 **kdump** 에 예약된 메모리를 설정하거나 압축되지 않았거나 압축된 형식으로 ***vmcore* saving** 위치를 선택할 수 있습니다.

25.1. 웹 콘솔에서 KDUMP 메모리 사용량 및 대상 위치 구성

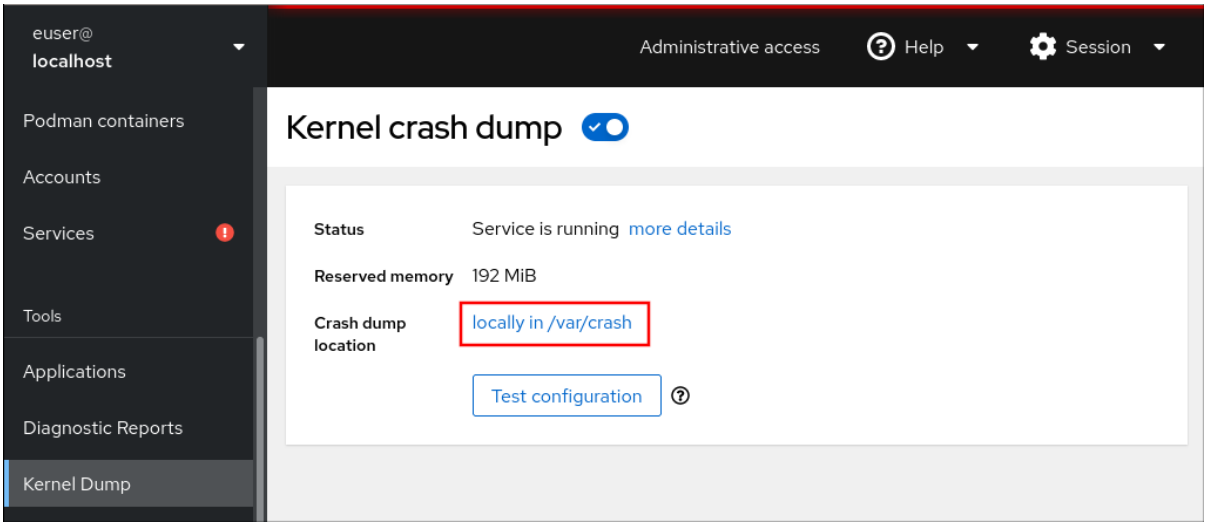
아래 절차에서는 **RHEL** 웹 콘솔 인터페이스의 **Kernel Dump** 탭을 사용하여 **kdump** 커널용으로 예약된 메모리 양을 구성하는 방법을 보여줍니다. 이 절차에서는 **vmcore dump** 파일의 대상 위치와 구성을 테스트하는 방법도 설명합니다.

절차

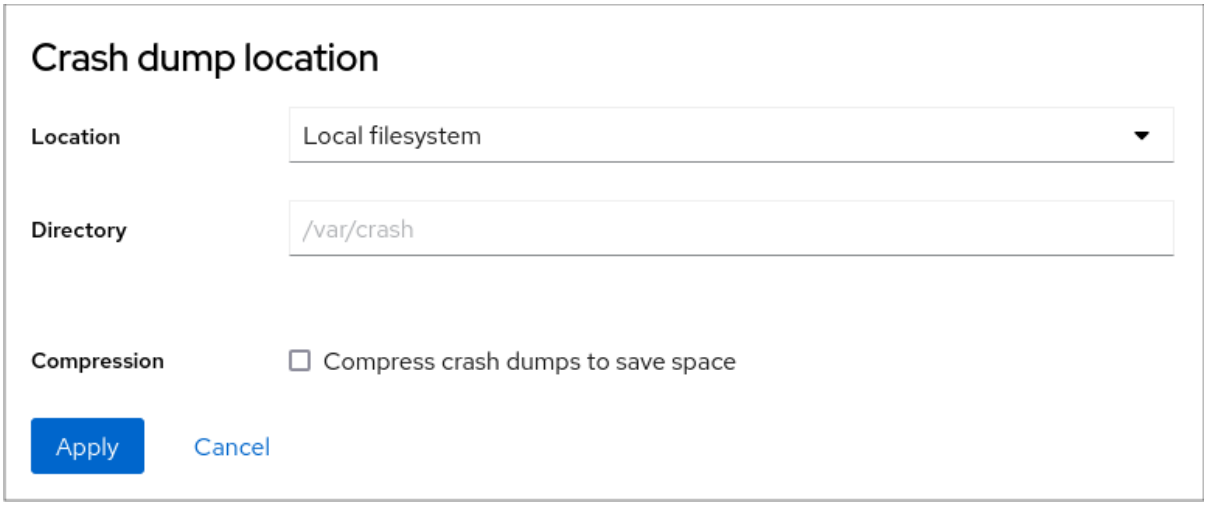
1. 커널 덤프 탭을 열고 **kdump** 서비스를 시작합니다.

2. 명령줄을 사용하여 **kdump** 메모리 사용량을 구성합니다.

3. **Crash dump location** 옵션 옆에 있는 링크를 클릭합니다.



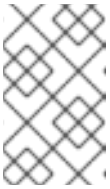
4. 드롭다운에서 로컬 파일 시스템 옵션을 선택하고 덤프를 저장할 디렉터리를 지정합니다.



- 또는 드롭다운에서 **Remote over SSH** 옵션을 선택하여 **SSH** 프로토콜을 사용하여 **vmcore**를 원격 시스템으로 보냅니다.

  원격 시스템 주소,**ssh** 키 위치 및 대상 디렉터리로 **Server, ssh** 키 및 디렉터리 필드를 입력합니다.

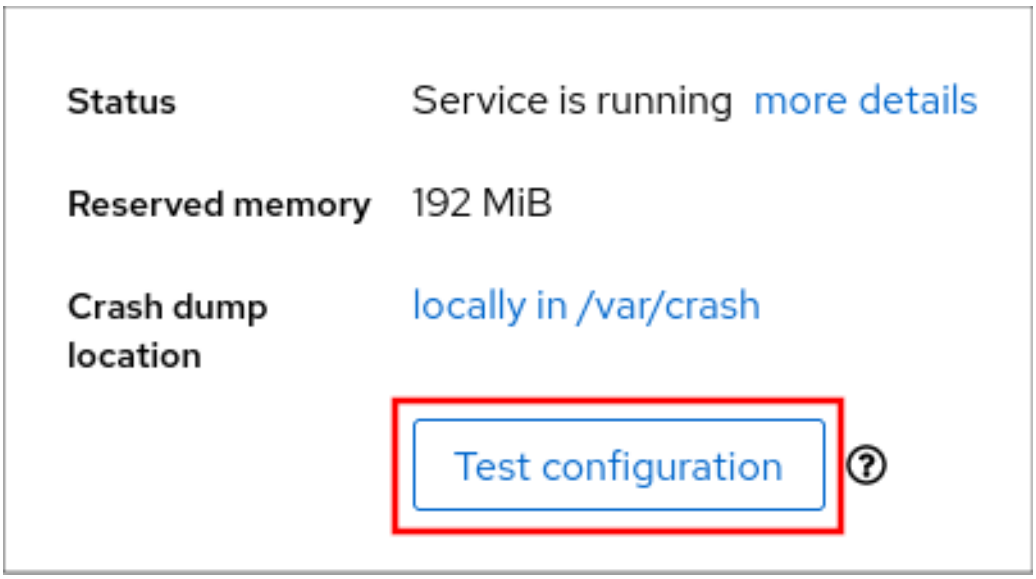
- 또 다른 선택 사항은 드롭다운에서 **NFS**를 통한 원격 옵션을 선택하고 **Mount** 필드를 작성하여 **NFS** 프로토콜을 사용하여 **vmcore**를 원격 시스템으로 보내는 것입니다.



참고

압축 확인란을 선택하여 **vmcore** 파일의 크기를 줄입니다.

5. 커널을 중단시켜 구성을 테스트합니다.



a. 테스트 구성 을 클릭합니다.

b. **Test kdump** 설정 필드에서 **Crash** 시스템을 클릭합니다.

주의

이 단계는 커널 실행을 방해하고 시스템 충돌 및 데이터 손실을 초래합니다.

추가 리소스

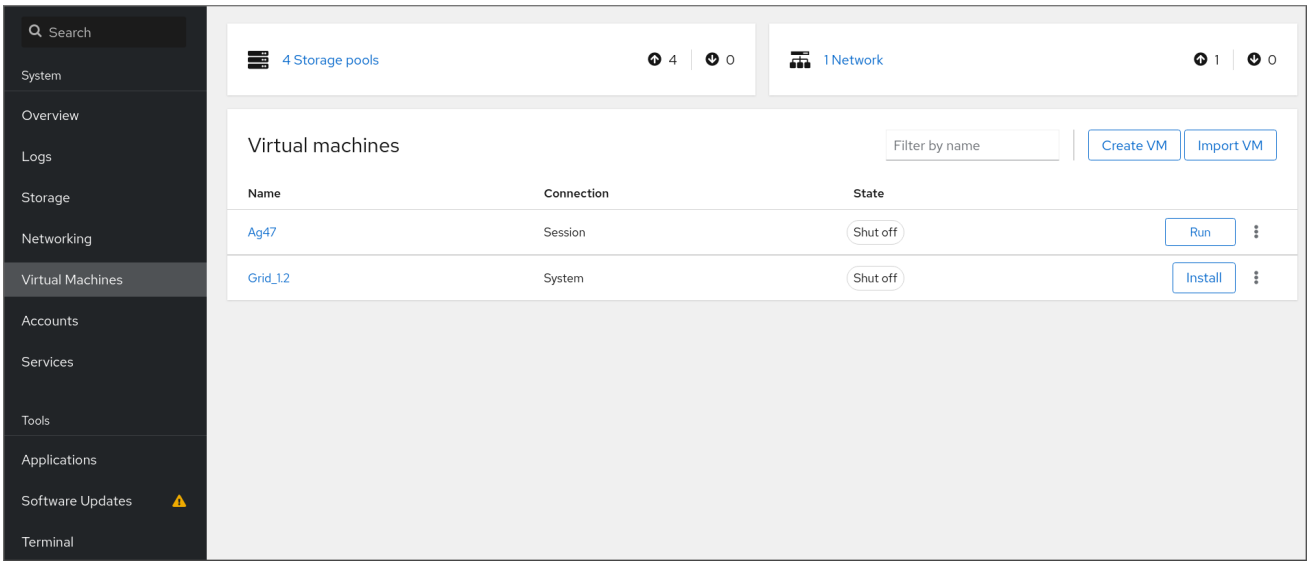
- 지원되는 **kdump** 대상
- **OpenSSH**로 두 시스템 간의 보안 통신 사용

25.2. 추가 리소스

- **RHEL** 웹 콘솔을 사용하여 시작하기

26장. 웹 콘솔에서 가상 머신 관리

RHEL 9 호스트의 그래픽 인터페이스에서 가상 머신을 관리하려면 **RHEL 9** 웹 콘솔에서 가상 머신 창을 사용할 수 있습니다.



26.1. 웹 콘솔을 사용한 가상 머신 관리 개요

RHEL 9 웹 콘솔은 시스템 관리를 위한 웹 기반 인터페이스입니다. 웹 콘솔은 호스트 시스템에서 **VM(**가상 머신**)**에 대한 그래픽 보기를 제공하므로 이러한 **VM**을 생성, 액세스 및 구성할 수 있습니다.

웹 콘솔을 사용하여 **RHEL 9**에서 **VM**을 관리하려면 먼저 가상화 를 위한 웹 콘솔 플러그인 을 설치해야 합니다.

다음 단계

- 웹 콘솔에서 **VM** 관리 활성화에 대한 지침은 가상 머신 관리를 위한 웹 콘솔 설정을 참조하십시오.

26.2. 가상 머신 관리를 위해 웹 콘솔 설정

RHEL 9 웹 콘솔을 사용하여 **VM(**가상 머신**)**을 관리하기 전에 호스트에 웹 콘솔 가상 머신 플러그인을 설치해야 합니다.

사전 요구 사항

- 웹 콘솔이 시스템에 설치되어 활성화되어 있는지 확인합니다.

```
# systemctl status cockpit.socket
cockpit.socket - Cockpit Web Service Socket
Loaded: loaded (/usr/lib/systemd/system/cockpit.socket
[...]
```

이 명령에서 **Unit cockpit.socket**을 반환할 수 없는 경우 웹 콘솔 설치 문서를 따라 웹 콘솔을 활성화합니다.

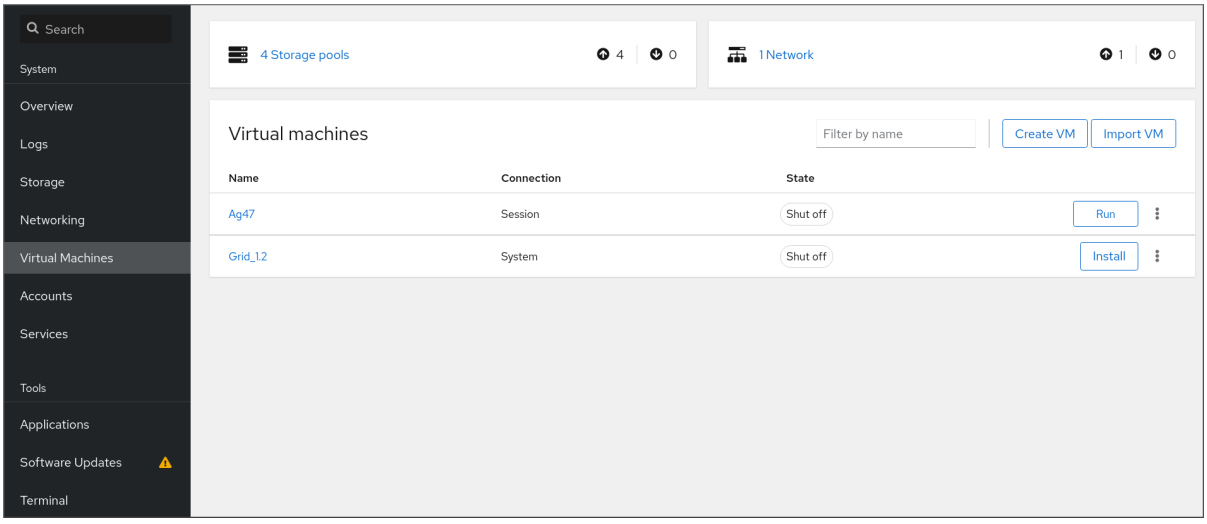
절차

- **cockpit-machines** 플러그인을 설치합니다.

```
# dnf install cockpit-machines
```

검증

1. 예를 들어 브라우저에 **https://localhost:9090** 주소를 입력하여 웹 콘솔에 액세스합니다.
2. 로그인합니다.
3. 설치에 성공하면 **Virtual Machines** (가상 머신)가 웹 콘솔 사이드 메뉴에 표시됩니다.



추가 리소스

- RHEL 9 웹 콘솔을 사용하여 시스템 관리

26.3. 웹 콘솔을 사용하여 가상 머신 이름 변경

VM(가상 머신)을 생성한 후 충돌을 피하도록 **VM**의 이름을 바꾸거나 사용 사례에 따라 새로운 고유 이름을 할당할 수 있습니다. **RHEL** 웹 콘솔을 사용하여 **VM**의 이름을 변경할 수 있습니다.

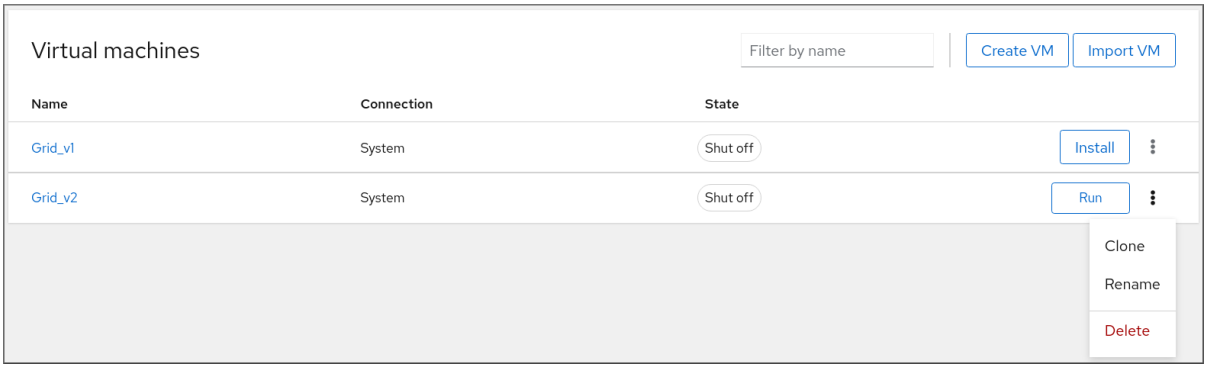
사전 요구 사항

- 웹 콘솔 **VM** 플러그인이 시스템에 설치되어 있습니다.
- **VM**이 종료되었는지 확인합니다.

절차

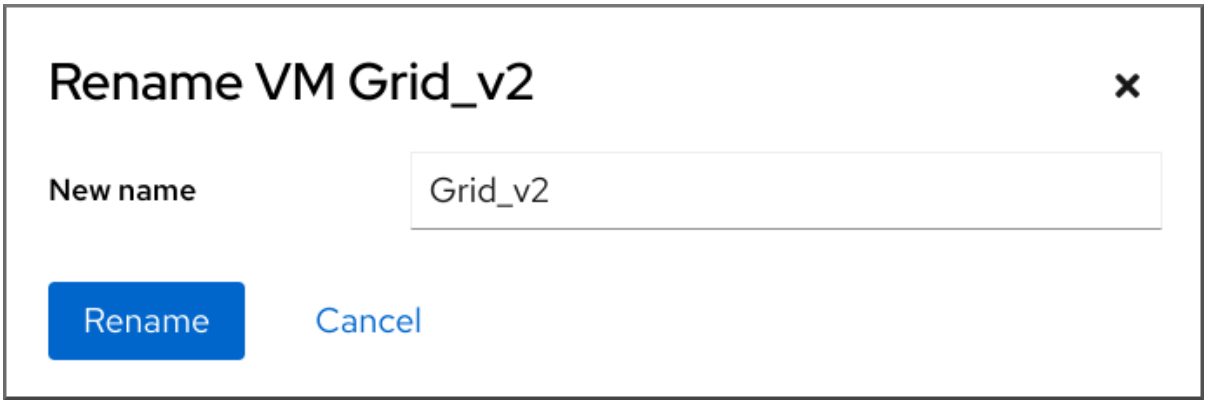
1. **Virtual Machines** (가상 머신) 인터페이스에서 이름을 변경할 **VM**의 메뉴 버튼을 클릭합니다.

   다양한 **VM** 작업에 대한 제어가 있는 드롭다운 메뉴가 나타납니다.



2. **Rename** 을 클릭합니다.

   Rename a VM 대화 상자가 나타납니다.



3. **New name (**새 이름**)** 필드에 **VM**의 이름을 입력합니다**.**

4. **Rename** 을 클릭합니다**.**

검증

- 새 **VM** 이름이 **Virtual Machines** 인터페이스에 표시되어야 합니다**.**

26.4. 웹 콘솔에서 사용할 수 있는 가상 머신 관리 기능

RHEL 9 웹 콘솔을 사용하여 시스템에서 가상 머신**(VM)**을 관리하기 위해 다음 작업을 수행할 수 있습니다**.**

표 **26.1. RHEL 9** 웹 콘솔에서 수행할 수 있는 **VM** 작업

Task	자세한 내용은 다음을 참조하십시오.
VM을 생성하고 게스트 운영 체제로 설치	웹 콘솔을 사용하여 가상 머신 생성 및 게스트 운영 체제 설치
VM을 삭제합니다.	웹 콘솔을 사용하여 가상 머신 삭제
VM을 시작, 종료, 재시작	웹 콘솔 을 사용하여 가상 머신 시작 및 웹 콘솔을 사용하여 가상 머신 종료 및 재시작
다양한 콘솔을 사용하여 VM에 연결하고 상호 작용	웹 콘솔을 사용하여 가상 머신과 상호 작용
VM에 대한 다양한 정보 보기	웹 콘솔을 사용하여 가상 머신 정보 보기
VM에 할당된 호스트 메모리 조정	웹 콘솔을 사용하여 가상 머신 메모리 추가 및 제거
VM의 네트워크 연결 관리	가상 머신 네트워크 인터페이스 관리에 웹 콘솔 사용

Task	자세한 내용은 다음을 참조하십시오.
호스트에서 사용 가능한 VM 스토리지를 관리하고 가상 디스크를 VM에 연결합니다.	가상 머신 스토리지 관리
VM의 가상 CPU 설정 구성	웹 콘솔을 사용하여 가상 CPU 관리
VM 실시간 마이그레이션	웹 콘솔을 사용하여 가상 머신 실시간 마이그레이션
VM 이름 변경	웹 콘솔을 사용하여 가상 머신 이름 변경
호스트와 VM 간에 파일 공유	virtiofs를 사용하여 호스트와 가상 머신 간 파일을 공유하도록 웹 콘솔을 사용하여 파일 공유
호스트 장치 관리	웹 콘솔을 사용하여 가상 장치 관리

27장. 웹 콘솔에서 원격 시스템 관리

원격 시스템에 연결하고 **RHEL 9** 웹 콘솔에서 관리합니다.

다음 장에서는 다음을 설명합니다.

- 연결된 시스템의 최적 토폴로지입니다.
- 원격 시스템을 추가 및 제거하는 방법.
- 원격 시스템 인증에 **SSH** 키를 사용하는 이유 및 방법.

사전 요구 사항

- 원격 시스템에서 **SSH** 서비스를 엽니다.

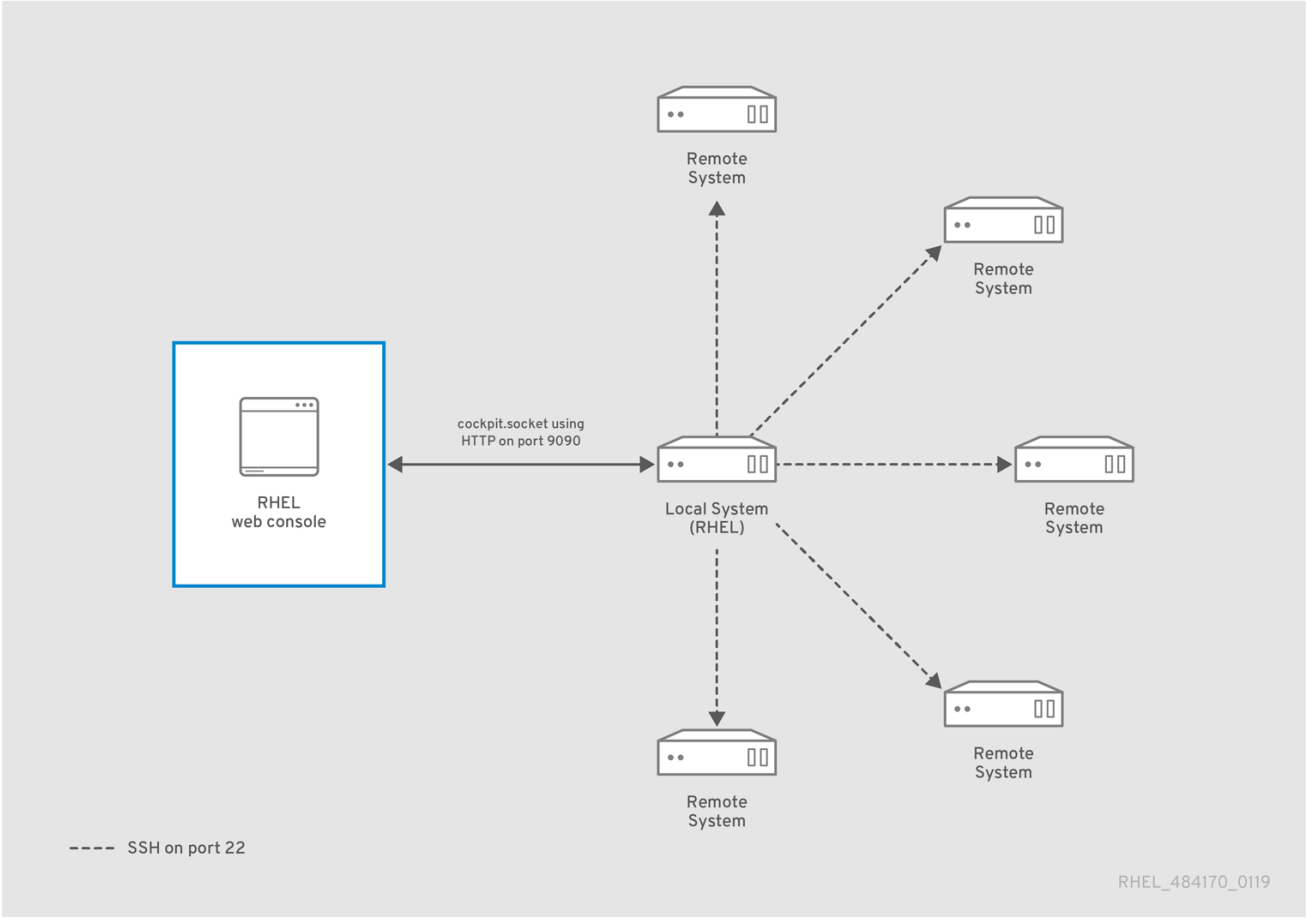
27.1. 웹 콘솔의 원격 시스템 관리자

RHEL 9 웹 콘솔을 사용하여 네트워크에서 원격 시스템을 관리하려면 연결된 서버의 토폴로지를 고려해야 합니다.

최적의 보안을 위해 **Red Hat**은 다음과 같은 연결 설정을 권장합니다.

- 웹 콘솔과 함께 **bastion** 호스트로 하나의 시스템을 사용합니다. **bastion** 호스트는 열려 있는 **HTTPS** 포트가 있는 시스템입니다.
- 다른 모든 시스템은 **SSH**를 통해 통신합니다.

bastion 호스트에서 실행되는 웹 인터페이스를 사용하면 기본 구성에서 포트 **22**를 사용하여 **SSH** 프로토콜을 통해 다른 모든 시스템에 연결할 수 있습니다.



27.2. 웹 콘솔에 원격 호스트 추가

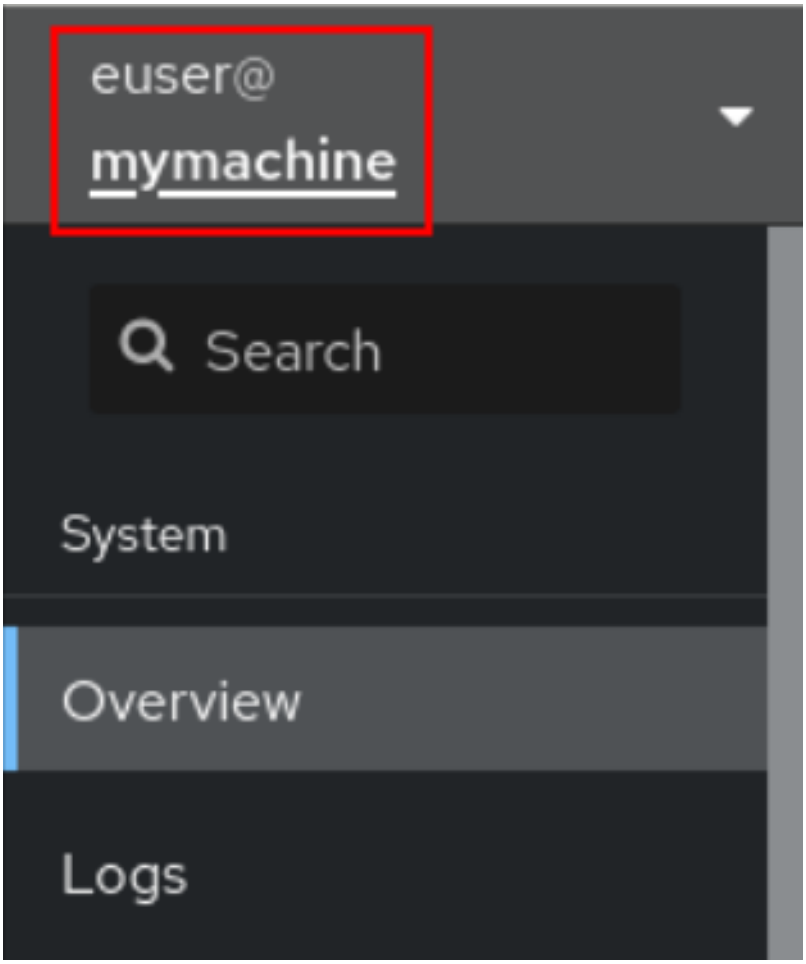
이 섹션에서는 다른 시스템을 사용자 이름 및 암호로 연결하는 데 도움이 됩니다.

사전 요구 사항

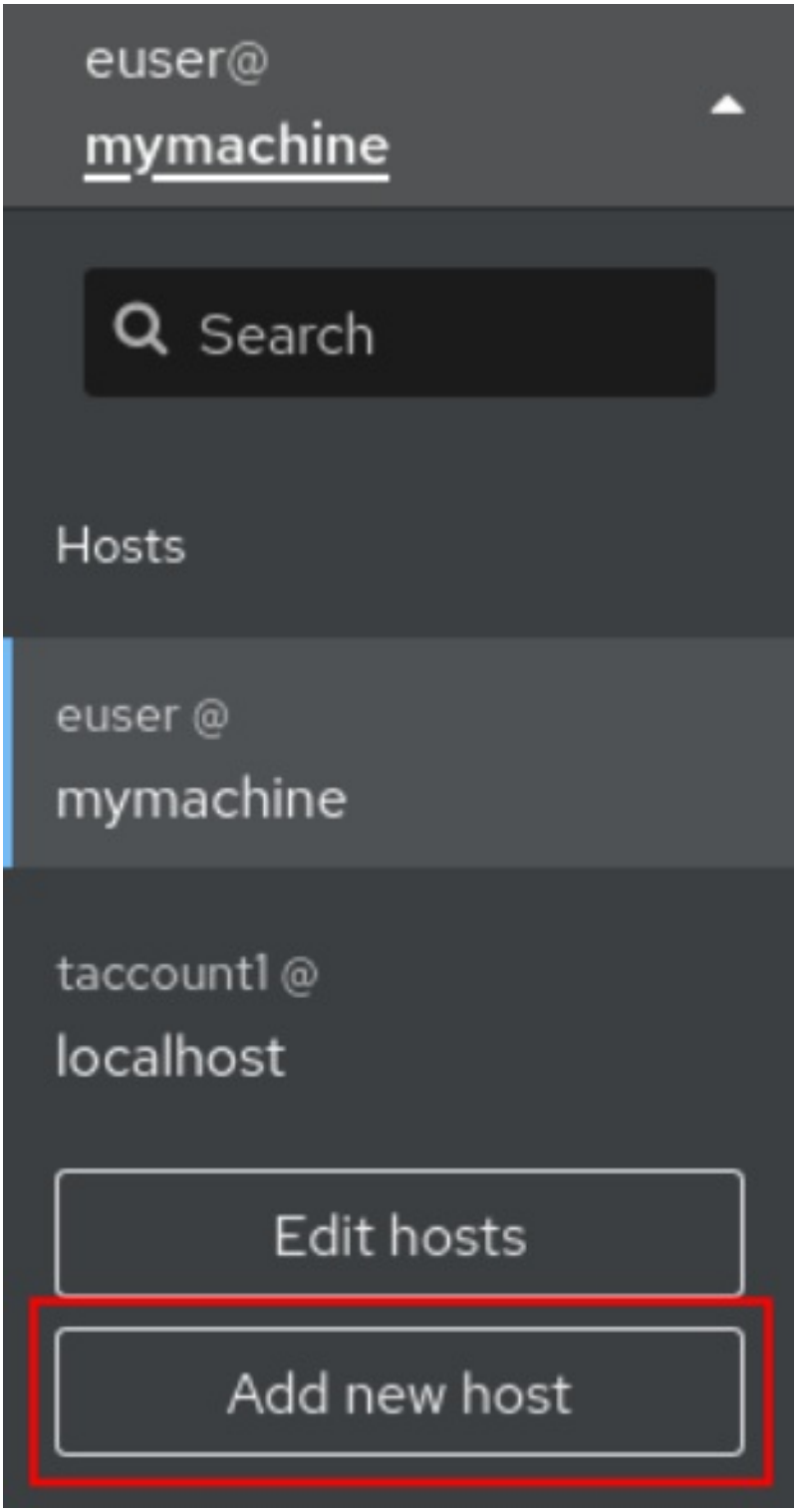
- 관리 권한이 있는 웹 콘솔에 로그인해야 합니다. 자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에서 개요 페이지의 왼쪽 상단에 있는 **username@hostname** 을 클릭합니다.



2. 드롭다운 메뉴에서 **Add new host (**새 호스트 추가**)** 버튼을 클릭합니다**.**



3. 새 호스트 추가 대화 상자에서 추가할 호스트를 지정합니다.

4. (선택 사항) 연결할 계정의 사용자 이름을 추가합니다.

원격 시스템의 모든 사용자 계정을 사용할 수 있습니다. 그러나 관리 권한이 없는 사용자 계정의 자격 증명을 사용하는 경우 관리 작업을 수행할 수 없습니다.

로컬 시스템에 대해 와 동일한 인증 정보를 사용하는 경우 웹 콘솔은 로그인할 때마다 원격 시스템을 자동으로 인증합니다. 그러나 더 많은 머신에서 동일한 자격 증명을 사용하면 보안 위험이 발생할 수 있습니다.

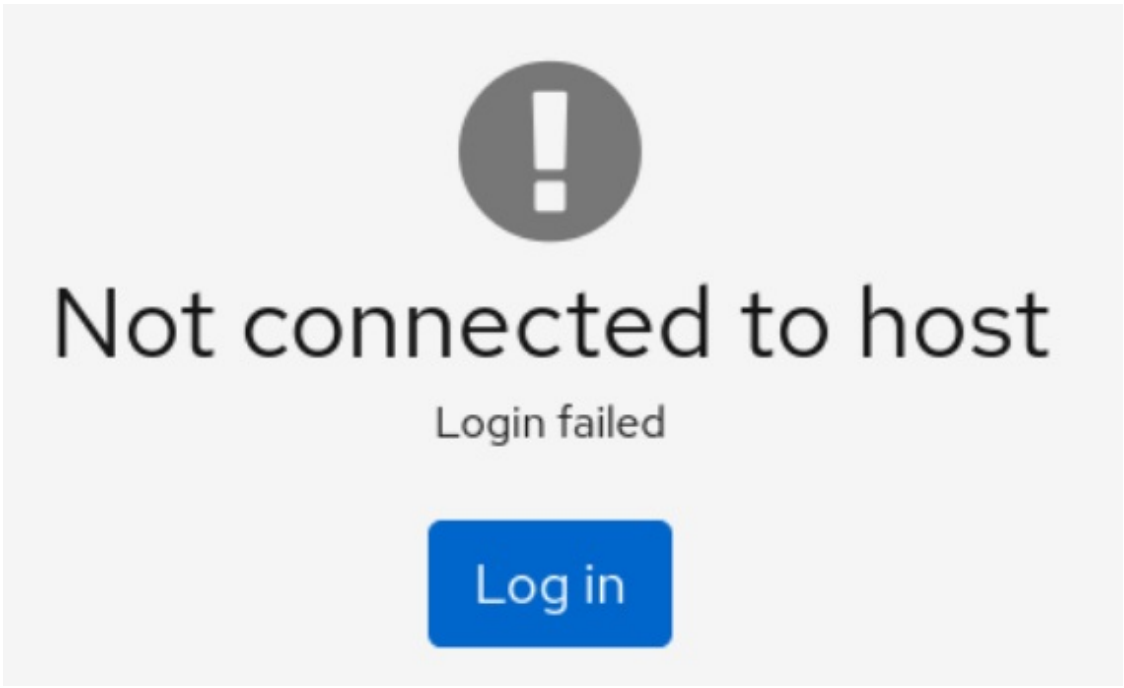
5. (선택 사항) 색상 필드를 클릭하여 시스템의 색상을 변경합니다.

6. 추가를 클릭합니다.

새 호스트가 **username@hostname** 드롭다운 메뉴의 호스트 목록에 나타납니다.

참고

웹 콘솔은 원격 시스템에 로그인하는 데 사용한 암호를 저장하지 않으므로 각 시스템을 다시 시작한 후 다시 로그인해야 합니다. 다음에 로그인하면 연결이 끊긴 원격 시스템의 기본 화면에 있는 **Log in** 버튼을 클릭하여 로그인 대화 상자를 엽니다.



27.3. 웹 콘솔에서 원격 호스트 제거

이 섹션에서는 웹 콘솔에서 다른 시스템을 제거하는 방법을 안내합니다.

사전 요구 사항

- 원격 시스템이 추가되었습니다.

  자세한 내용은 웹 콘솔에 원격 호스트 추가를 참조하십시오.

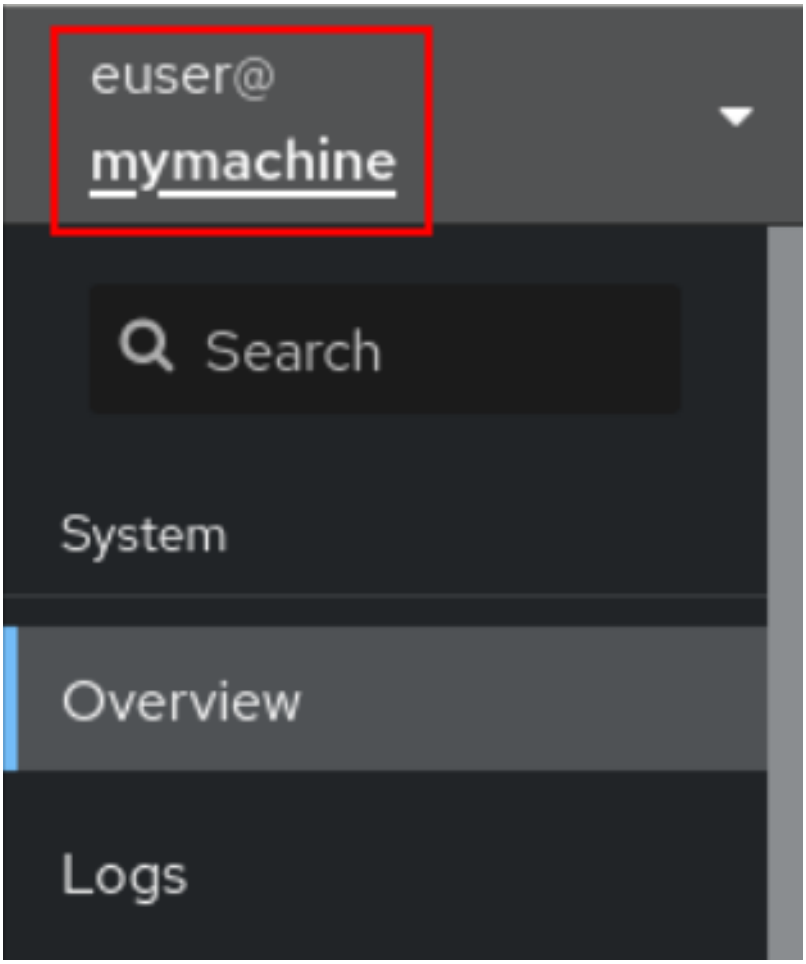
- 관리자 권한을 사용하여 웹 콘솔에 로그인해야 합니다.

  자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

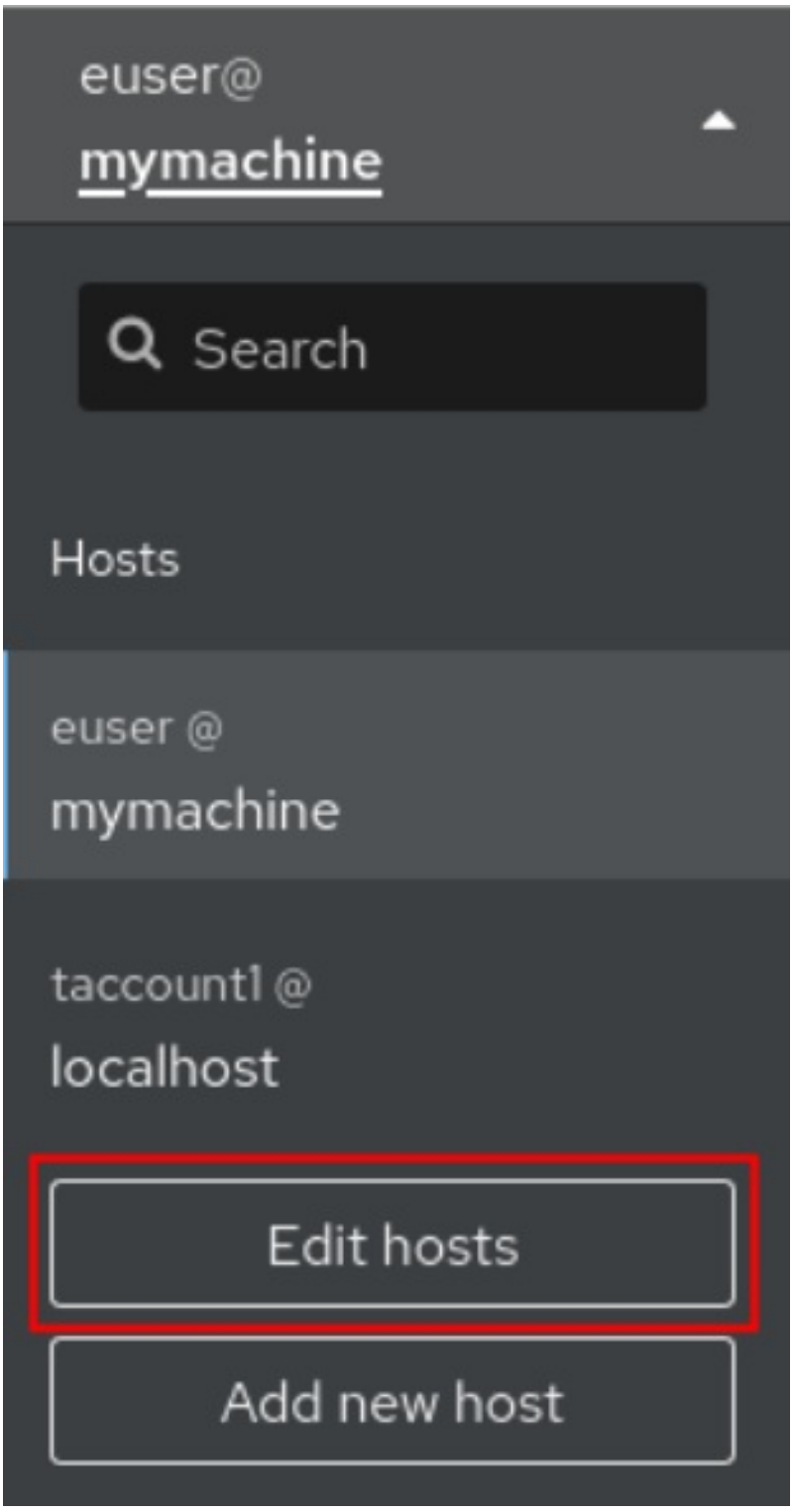
절차

1. **RHEL {ProddductNumber}** 웹 콘솔에 로그인합니다.

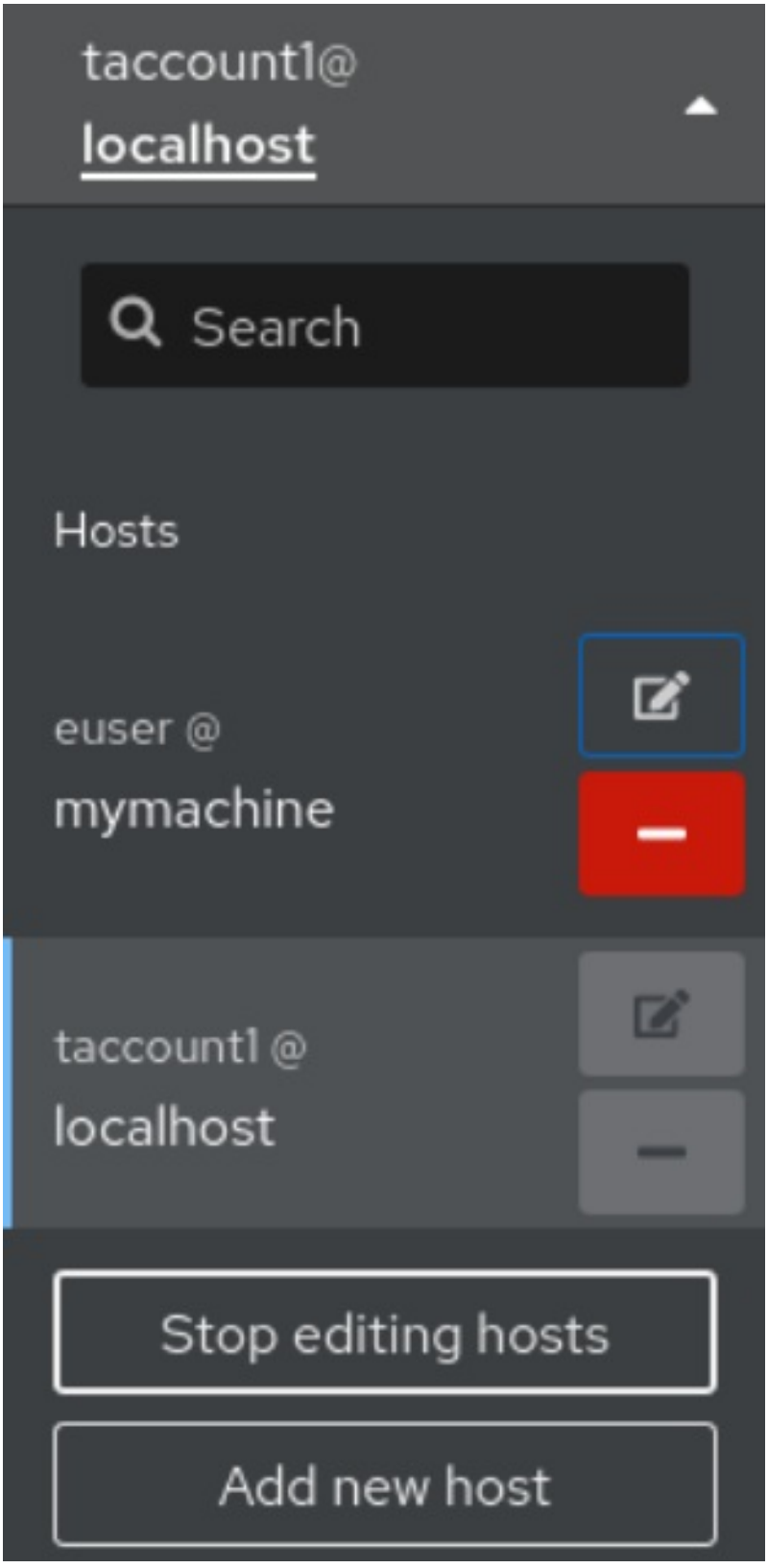
2. 개요 페이지의 왼쪽 상단에서 **username@hostname** 을 클릭합니다.



3. **Edit Server** 아이콘을 클릭합니다.



4. 웹 콘솔에서 호스트를 제거하려면 호스트 이름 옆에 있는 빨간색 빼기 기호 버튼을 클릭합니다. 현재 연결된 호스트는 제거할 수 없습니다.



결과적으로 서버는 웹 콘솔에서 제거됩니다.

27.4. 새 호스트에 대한 SSH 로그인 활성화

새 호스트를 추가하면 **ssh** 키를 사용하여 로그인할 수도 있습니다. 시스템에 **ssh** 키가 이미 있는 경우 웹 콘솔에서 기존 키를 사용합니다. 그렇지 않으면 웹 콘솔에서 키를 만들 수 있습니다.

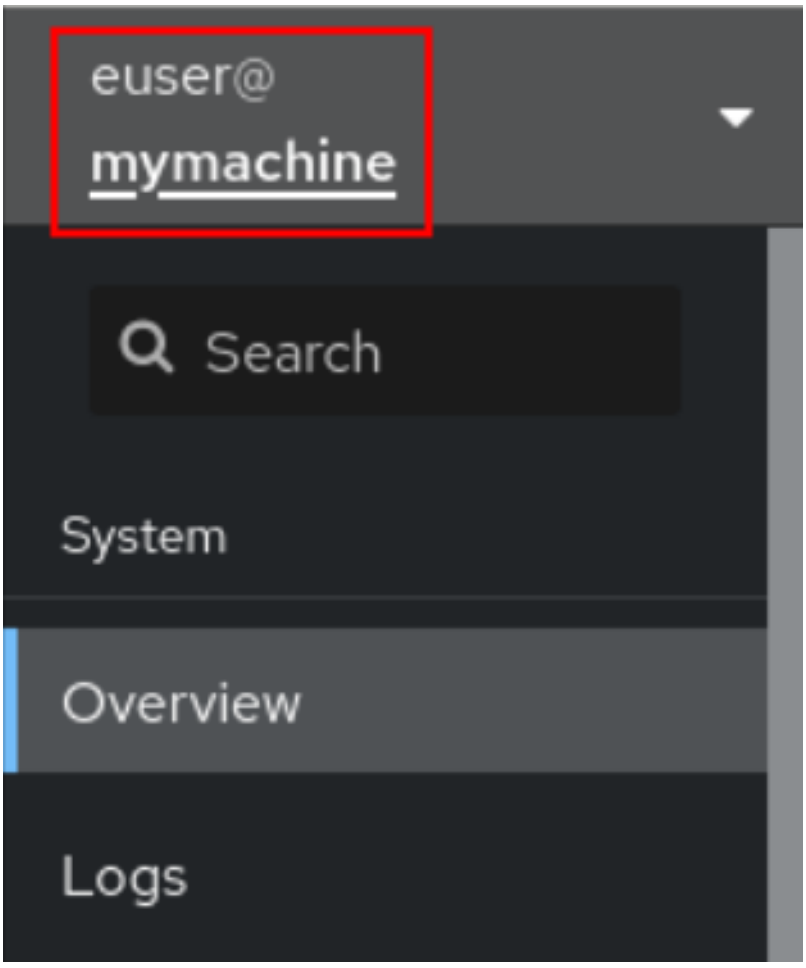
사전 요구 사항

- 관리 권한이 있는 웹 콘솔에 로그인해야 합니다.

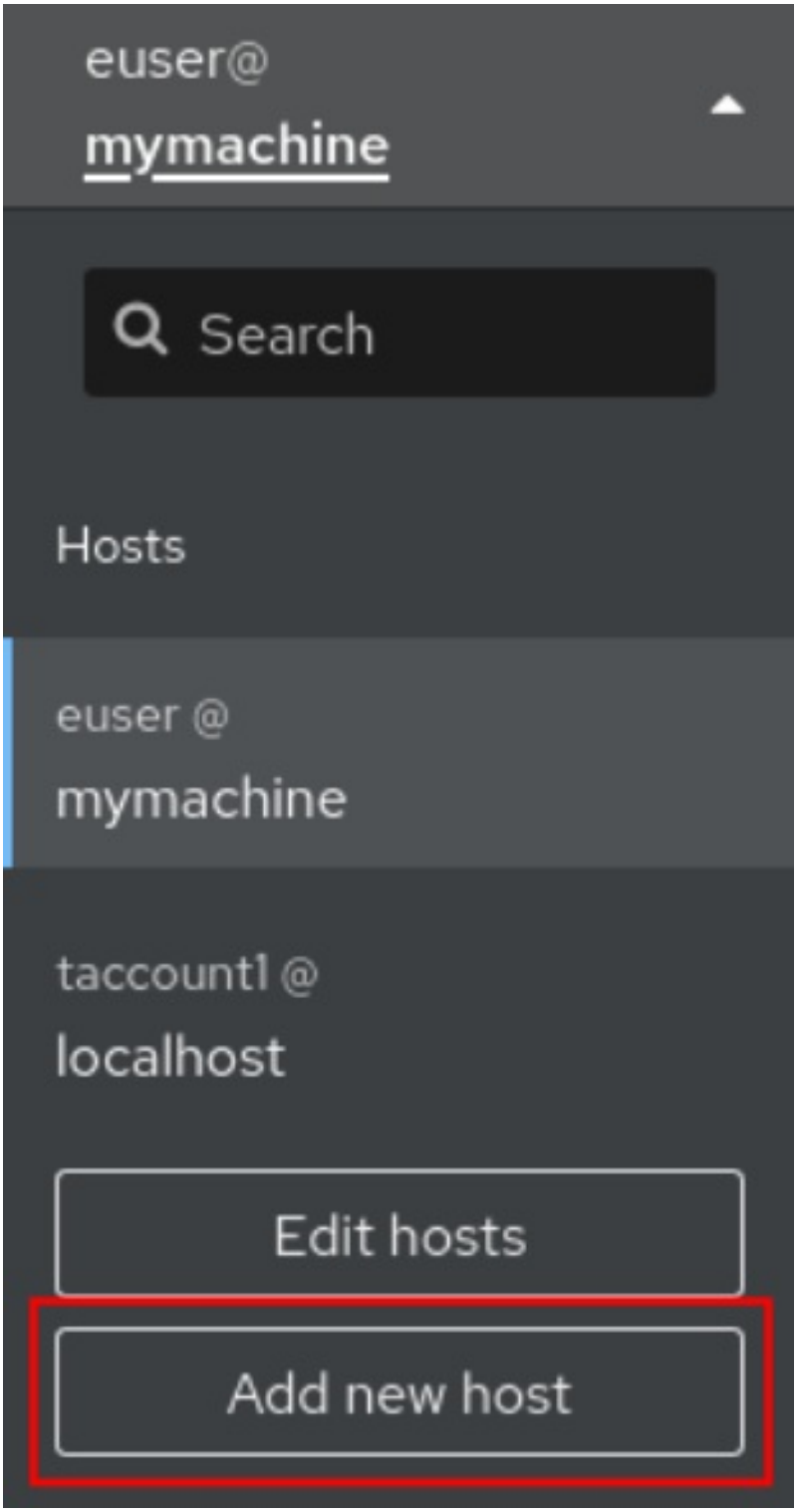
  자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

절차

1. **RHEL 9** 웹 콘솔에서 개요 페이지의 왼쪽 상단에 있는 **username@hostname** 을 클릭합니다.



2. 드롭다운 메뉴에서 **Add new host (**새 호스트 추가**)** 버튼을 클릭합니다.



3. 새 호스트 추가 대화 상자에서 추가할 호스트를 지정합니다.

4. 연결할 계정의 사용자 이름을 추가합니다.

원격 시스템의 모든 사용자 계정을 사용할 수 있습니다. 그러나 관리 권한이 없는 사용자 계정의 자격 증명을 사용하는 경우 관리 작업을 수행할 수 없습니다.

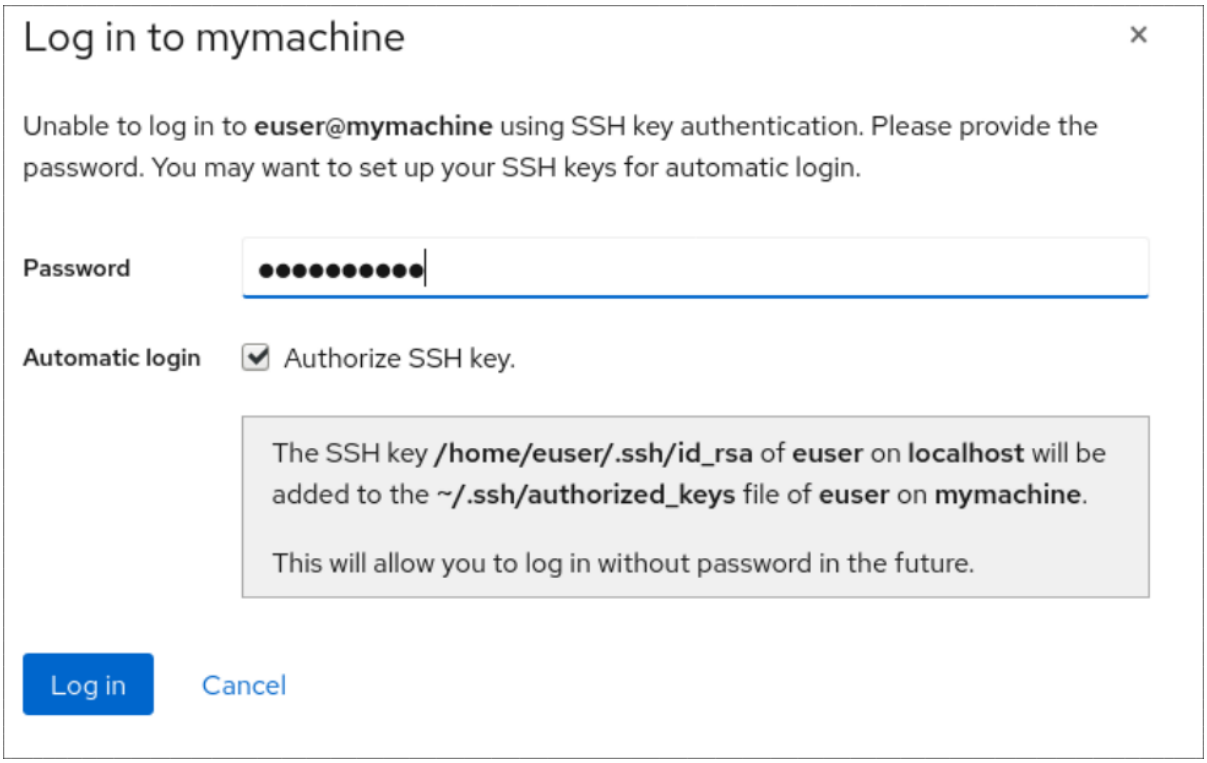
5. (선택 사항) 색상 필드를 클릭하여 시스템의 색상을 변경합니다.

6. 추가를 클릭합니다.

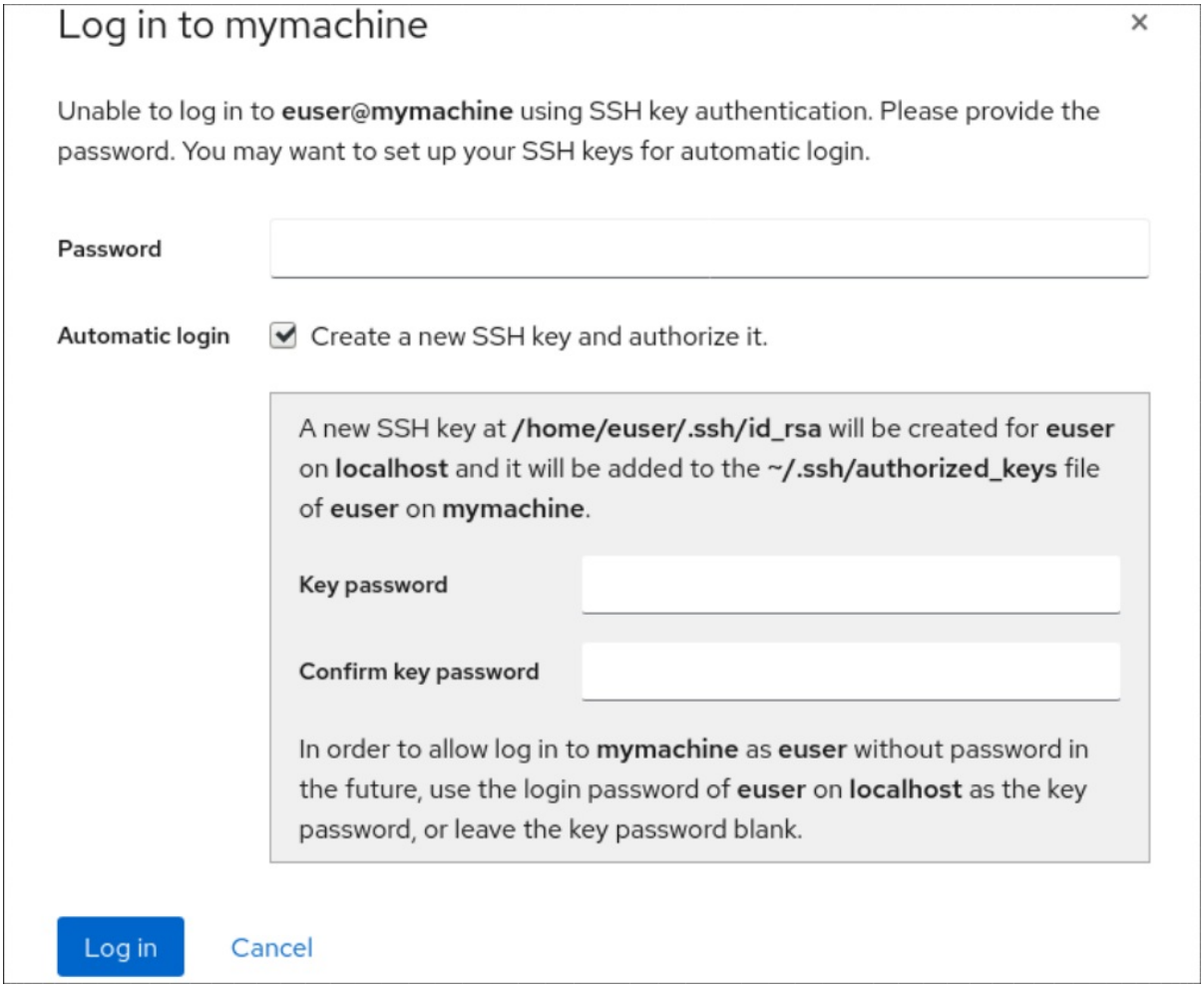
   암호를 묻는 새 대화 상자가 나타납니다.

7. 사용자 계정 암호를 입력합니다.

8. **ssh** 키가 이미 있는 경우 권한 부여 키를 확인합니다.



9. **Create a new SSH key**를 선택하고 **SSH** 키가 없는 경우 권한을 부여합니다. 웹 콘솔에서 이를 만듭니다.



a. **SSH** 키의 암호를 추가합니다.

b. 암호를 확인합니다.

10. **Log in**을 클릭합니다.

새 호스트가 **username@hostname** 드롭다운 메뉴의 호스트 목록에 나타납니다.

검증 단계

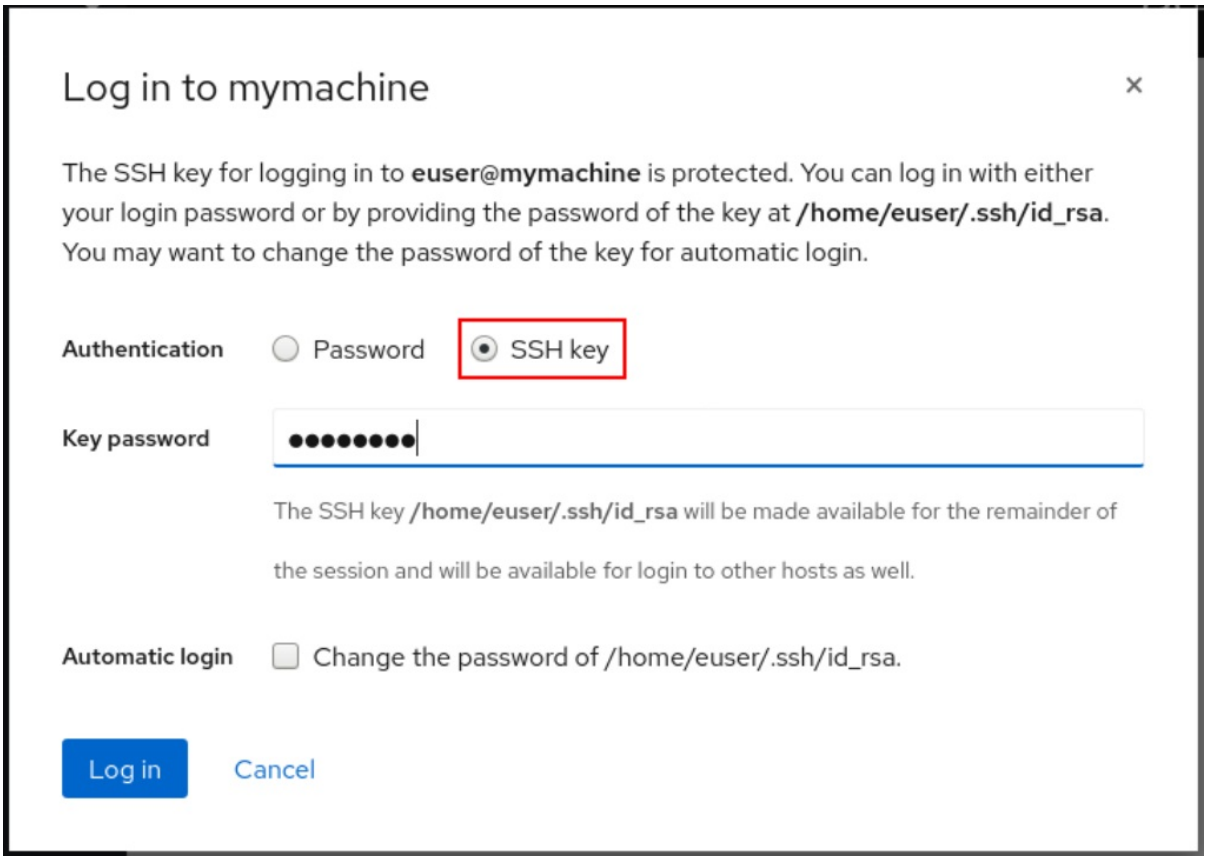
1. 로그아웃합니다.

2. 다시 로그인합니다.

3.

Not connected to host screen(호스트에 연결되어 있지 않음) 화면에서 **Log in** (로그인)을 클릭합니다.

4. 인증 옵션으로 **SSH** 키 를 선택합니다.



5. 키 암호를 입력합니다.

6. 로그인을 클릭합니다.

추가 리소스

- **OpenSSH**로 두 시스템 간의 보안 통신 사용

28장. IDM 도메인에서 RHEL 9 웹 콘솔에 대한 SINGLE SIGN-ON 구성

RHEL 9 웹 콘솔에서 **IdM(Identity Management)**에서 제공하는 **SSO(Single Sign-On)** 인증을 사용하는 방법을 알아봅니다.

제품 상세 정보:

- **IdM** 도메인 관리자는 **RHEL 9** 웹 콘솔을 사용하여 로컬 시스템을 관리할 수 있습니다.
- **IdM** 도메인의 **Kerberos** 티켓이 있는 사용자는 웹 콘솔에 액세스하기 위해 로그인 인증 정보를 제공하지 않아도 됩니다.
- **IdM** 도메인에 알려진 모든 호스트는 **RHEL 9** 웹 콘솔의 로컬 인스턴스에서 **SSH**를 통해 액세스할 수 있습니다.
- 인증서 구성은 필요하지 않습니다. 콘솔의 웹 서버는 **IdM** 인증 기관에서 발급하고 브라우저에서 승인한 인증서로 자동 전환합니다.

이 장에서는 **RHEL** 웹 콘솔에 로그인하기 위해 **SSO**를 구성하는 다음 단계를 설명합니다.

1. **RHEL 9** 웹 콘솔을 사용하여 **IdM** 도메인에 시스템을 추가합니다.

   자세한 내용은 웹 콘솔을 사용하여 **RHEL 9** 시스템을 **IdM** 도메인에 가입하십시오.

2. 인증에 **Kerberos**를 사용하려면 시스템에서 **Kerberos** 티켓을 가져와야 합니다.

   자세한 내용은 **Kerberos** 인증을 사용하여 웹 콘솔에 로깅 을 참조하십시오.

3. **IdM** 서버의 관리자가 모든 호스트에서 모든 명령을 실행할 수 있도록 허용합니다.

   자세한 내용은 **IdM** 서버의 도메인 관리자에게 관리자 **sudo** 액세스 활성화를참조하십시오.

사전 요구 사항

- **RHEL 9** 시스템에 설치된 **RHEL** 웹 콘솔.

  자세한 내용은 웹 콘솔 설치를 참조하십시오.

- **RHEL** 웹 콘솔이 있는 시스템에 **IdM** 클라이언트가 설치되어 있어야 합니다.

  자세한 내용은 **IdM** 클라이언트 설치를 참조하십시오.

28.1. 웹 콘솔을 사용하여 RHEL 9 시스템을 IDM 도메인에 가입

웹 콘솔을 사용하여 **Red Hat Enterprise Linux 9** 시스템을 **IdM(Identity Management)** 도메인에 연결할 수 있습니다.

사전 요구 사항

- **IdM** 도메인이 실행 중이며 가입하려는 클라이언트에서 연결할 수 있습니다.
- **IdM** 도메인 관리자 인증 정보가 있습니다.

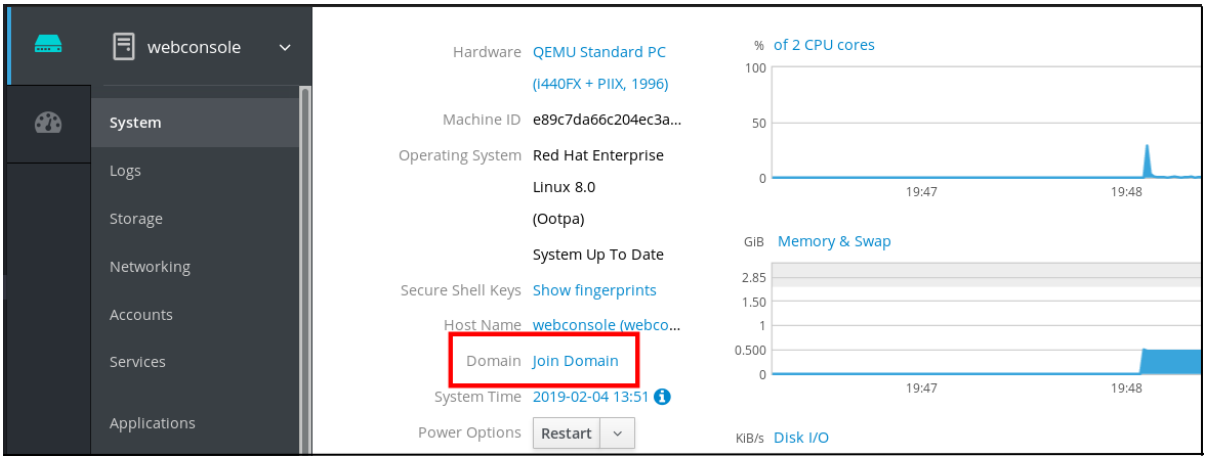
절차

1. **RHEL** 웹 콘솔에 로그인합니다.

   자세한 내용은 웹 콘솔에 로그인을 참조하십시오.

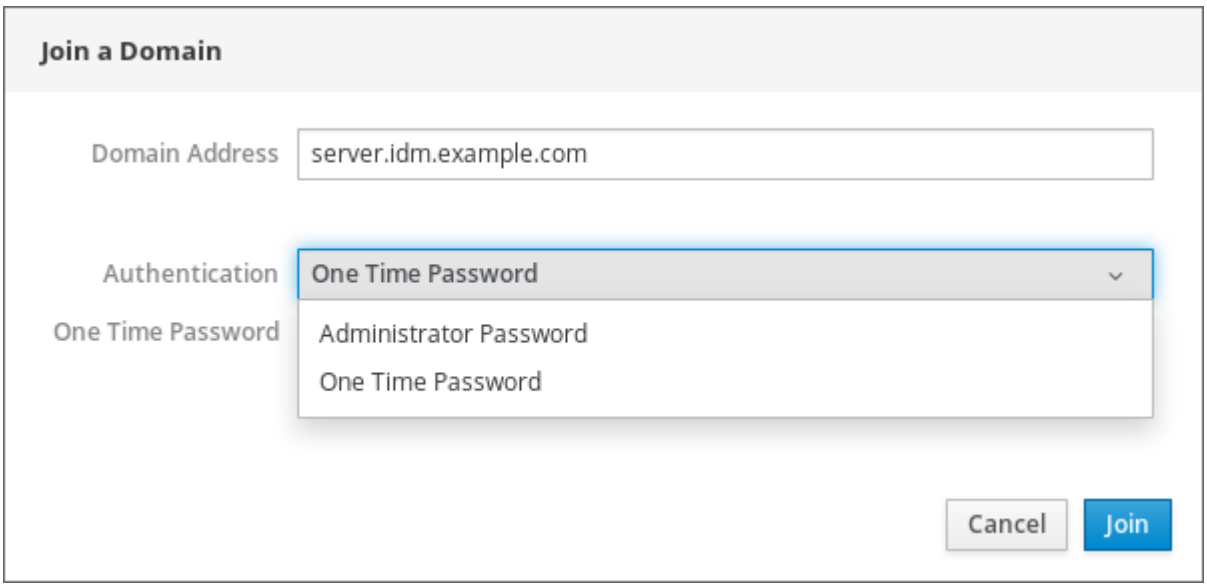
2. 시스템 탭을 엽니다.

3. **Join Domain** 을 클릭합니다.



4. **Domain(** 도메인**)** 대화 상자에 **Domain Address (**도메인 주소**)** 필드에 **IdM** 서버의 호스트 이름을 입력합니다**.**

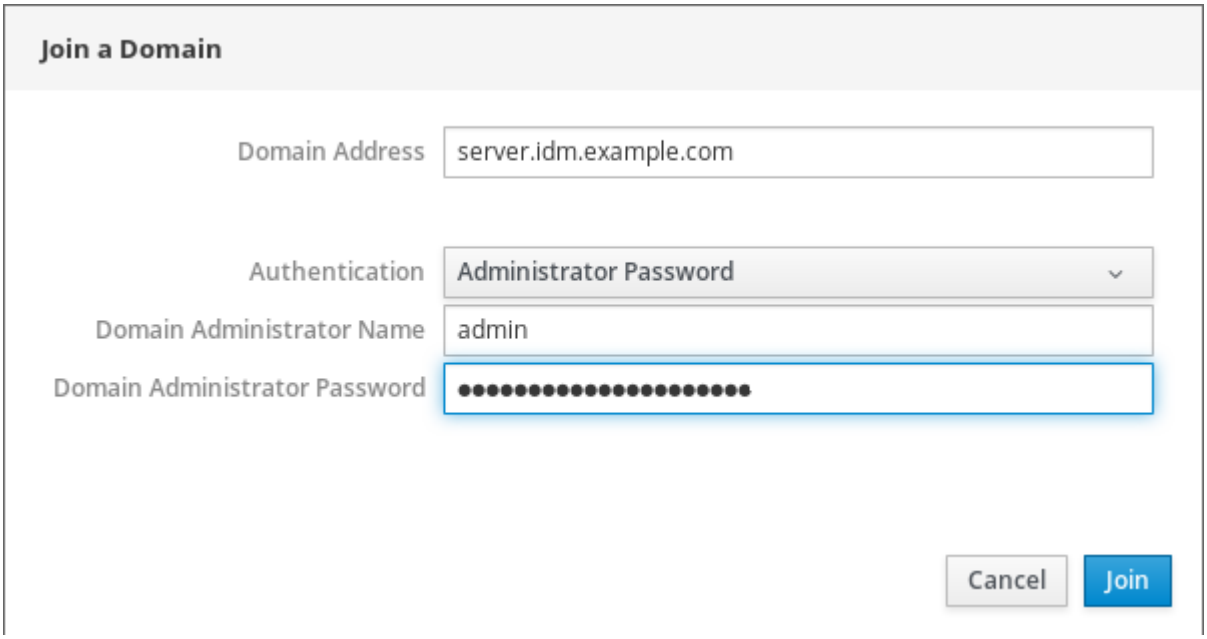
5. 인증 드롭다운 목록에서 암호를 사용할지 아니면 인증에 일회성 암호를 사용할지 선택합니다**.**



6. **Domain Administrator Name** 필드에 **IdM** 관리 계정의 사용자 이름을 입력합니다**.**

7. 암호 필드에서 인증 드롭다운 목록에서 선택한 내용에 따라 암호 또는 일회성 암호를 추가합니다**.**

8. 참여를 클릭합니다.



검증 단계

1. **RHEL 9** 웹 콘솔에 오류가 표시되지 않으면 시스템이 **IdM** 도메인에 가입되어 시스템 화면에 도메인 이름을 확인할 수 있습니다.

2. 사용자가 도메인의 멤버인지 확인하려면 터미널 페이지를 클릭하고 **id** 명령을 입력합니다.

```
$ id
euid=548800004(example_user) gid=548800004(example_user)
groups=548800004(example_user)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

추가 리소스

- 계획 **ID** 관리
- **ID** 관리 설치
- **IdM** 사용자, 그룹, 호스트 및 액세스 제어 규칙 관리

28.2. KERBEROS 인증을 사용하여 웹 콘솔에 로그인

다음 절차에서는 **Kerberos** 인증을 사용하도록 **RHEL 9** 시스템을 설정하는 방법에 대한 단계를 설명합니다.

중요

SSO를 사용하면 일반적으로 웹 콘솔에 관리 권한이 없습니다. 이 작업은 암호 없는 **sudo**를 구성한 경우에만 작동합니다. 웹 콘솔에서는 대화식으로 **sudo** 암호를 요청하지 않습니다.

사전 요구 사항

- 회사 환경에서 실행 중이고 연결할 수 있는 **IdM** 도메인.

  자세한 내용은 웹 콘솔을 사용하여 **RHEL 9** 시스템을 **IdM** 도메인에 가입을참조하십시오.

- **RHEL** 웹 콘솔을 사용하여 연결 및 관리하려는 원격 시스템에서 **cockpit.socket** 서비스를 활성화합니다.

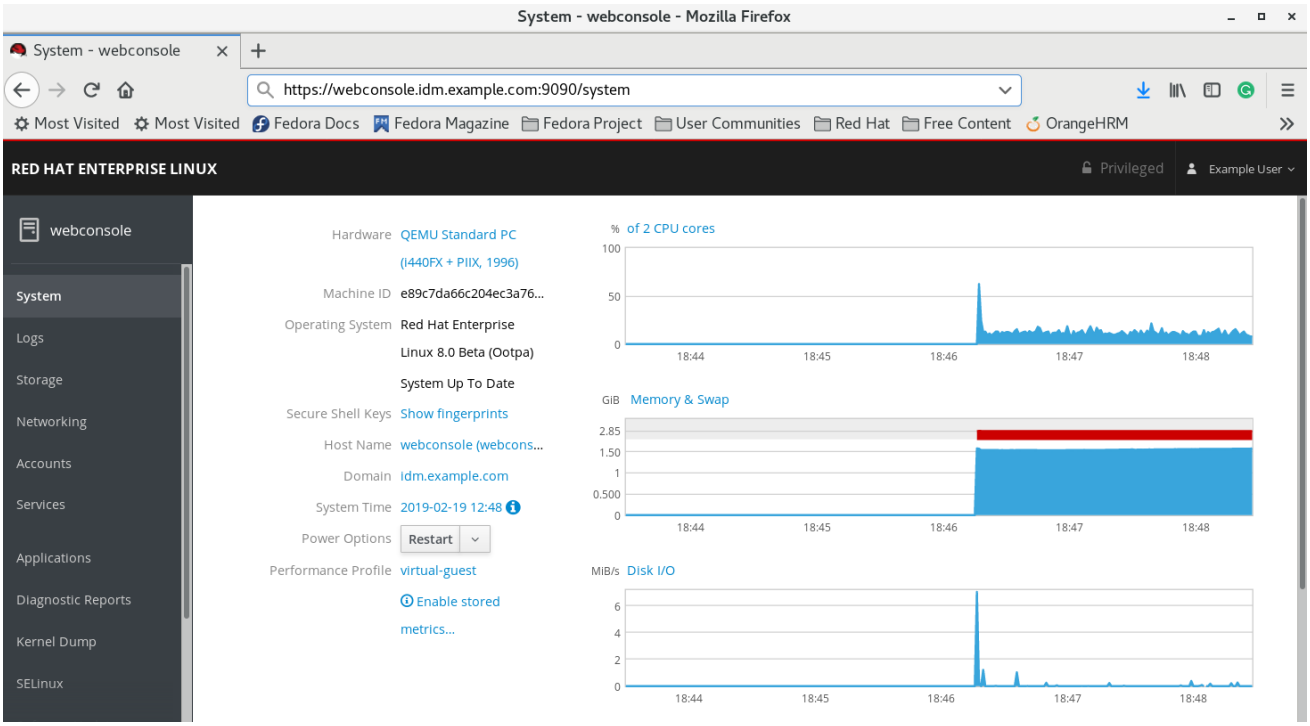
  자세한 내용은웹 콘솔 설치 링크를 참조하십시오.

- **SSSD** 클라이언트에서 관리하는 **Kerberos** 티켓을 사용하지 않는 경우 **kinit** 유틸리티를 사용하여 수동으로 티켓을 요청하십시오.

절차

https://dns_name:9090 주소를 사용하여 **RHEL** 웹 콘솔에 로그인합니다.

이 시점에서 **RHEL** 웹 콘솔에 성공적으로 연결되어 구성을 시작할 수 있습니다.



28.3. IDM 서버의 도메인 관리자에게 관리자 SUDO 액세스 활성화

다음 절차에서는 도메인 관리자가 **IdM(Identity Management)** 도메인의 모든 호스트에서 모든 명령을 실행할 수 있도록 하는 방법에 대한 단계를 설명합니다.

이 작업을 수행하려면 **IdM** 서버 설치 중에 자동으로 생성된 **admins** 사용자 그룹에 대한 **sudo** 액세스를 활성화합니다.

admins 그룹에 추가된 모든 사용자는 그룹에서 **ipa-advise** 스크립트를 실행하는 경우 **sudo** 액세스 권한을 갖습니다.

사전 요구 사항

- 서버에서 **IdM 4.7.1** 이상을 실행합니다.

절차

1. **IdM** 서버에 연결합니다.
2. **ipa-advise** 스크립트를 실행합니다.

```
$ ipa-advise enable-admins-sudo | sh -ex
```

콘솔에 오류가 표시되지 않으면 **admins** 그룹에는 **IdM** 도메인의 모든 시스템에 대한 관리자 권한이 있습니다**.**

29장. 중앙 집중식 관리 사용자를 위한 웹 콘솔을 사용하여 스마트 카드 인증 구성

다음을 통해 중앙에서 관리하는 사용자를 위해 **RHEL** 웹 콘솔에서 스마트 카드 인증을 구성합니다.

- **IdM (Identity Management)**
- **Identity Management**와 교차 포리스트 신뢰에 연결된 **Active Directory**

사전 요구 사항

- 스마트 카드 인증을 사용할 시스템은 **Active Directory** 또는 **Identity Management** 도메인의 멤버여야 합니다.
- 스마트 카드 인증에 사용되는 인증서는 **ID** 관리 또는 **Active Directory**의 특정 사용자와 연결되어 있어야 합니다.

  ID 관리에서 인증서와 인증서를 연결하는 방법에 대한 자세한 내용은 **IdM** 웹 **UI**의 사용자 항목에 인증서 추가 또는 **IdM CLI**의 사용자 항목에 인증서를 추가하는 것을 참조하십시오.

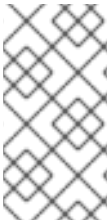
29.1. 중앙 집중식 관리형 사용자를 위한 스마트 카드 인증

스마트 카드는 카드에 저장된 인증서를 사용하여 개인 인증을 제공할 수 있는 물리적 장치입니다. 개인 인증은 사용자 암호와 동일한 방식으로 스마트 카드를 사용할 수 있음을 의미합니다.

스마트 카드에 사용자 자격 증명을 개인 키와 인증서 형식으로 저장할 수 있습니다. 특수 소프트웨어 및 하드웨어는 액세스하는 데 사용됩니다. 스마트 카드를 리더 또는 **USB** 소켓에 삽입하고 암호를 제공하는 대신 스마트 카드에 대해**kubelet** 코드를 제공합니다.

IdM(Identity Management)은 다음을 사용하여 스마트 카드 인증을 지원합니다.

- **IdM** 인증 기관에서 발급한 사용자 인증서입니다.
- **ADCS(Active Directory Certificate Service)** 인증 기관에서 발급한 사용자 인증서입니다.



참고

스마트 카드 인증 사용을 시작하려면 하드웨어 요구 사항을 참조하십시오. **RHEL8+**의 스마트 카드 지원.

29.2. 스마트 카드를 관리하고 사용하는 툴 설치

스마트 카드를 구성하려면 인증서를 생성하고 스마트 카드에 저장할 수 있는 툴이 필요합니다.

다음을 수행해야 합니다.

- 인증서를 관리하는 데 도움이 되는 **gnutls-utils** 패키지를 설치합니다.
- 스마트 카드로 작업할 라이브러리 및 유틸리티 집합을 제공하는 **opensc** 패키지를 설치합니다.
- 스마트 카드 리더와 통신하는 **pcscd** 서비스를 시작합니다.

절차

1. **opensc** 및 **gnutls-utils** 패키지를 설치합니다.

```
# dnf -y install opensc gnutls-utils
```

2. **pcscd** 서비스를 시작합니다.

```
# systemctl start pcscd
```

pcscd 서비스가 실행 중인지 확인합니다.

29.3. 스마트 카드에 인증서 저장

이 섹션에서는 다음을 구성하는 데 도움이 되는 **pkcs15-init** 툴을 사용한 스마트 카드 구성에 대해 설명합니다.

- 스마트 카드 삭제
- 새로운**ECDHEs** 및 선택적**kubelet Unblocking Keys** 설정 **(PUKs)**
- 스마트 카드에 새 슬롯 생성
- 인증서**,** 개인 키 및 공개 키를 슬롯에 저장
- 스마트 카드 설정 잠금 **(**일부 스마트 카드에는 이러한 유형의 종료가 필요합니다**)**

사전 요구 사항

- **pkcs15-init** 툴이 포함된 **opensc** 패키지가 설치되어 있습니다**.**

  자세한 내용은 스마트 카드 관리 및 사용에 대한 툴 설치를 참조하십시오**.**
- 카드가 리더에 삽입되어 컴퓨터에 연결되어 있습니다**.**
- 스마트 카드에 저장할 개인 키**,** 공개 키 및 인증서가 있습니다**.** 이 프로세스에서는 개인 키 **,** 공개 키 및 인증서에 사용되는 이름입니다**.**
- 현재 스마트 카드 사용자 **BOOM** 및 **Security officerECDHE(SO-PIN)**

절차

1. 스마트 카드를 지우고 **BOOM**으로 자신을 인증합니다**.**

```
$ 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]:
```

   카드가 삭제되었습니다**.**

2.

스마트 카드를 초기화하고, 사용자**kubelet** 및 **PUK**를 설정하고, 보안 부서 및 **PUK**를 설정합니다.

```
$ 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
```

pcks15-init 툴은 스마트 카드에 새 슬롯을 생성합니다.

3.

슬롯의 라벨 및 인증 **ID**를 설정합니다.

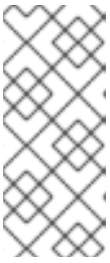
```
$ pkcs15-init --store-pin --label testuser \
   --auth-id 01 --so-pin 65498714 --pin 963214 --puk 321478
Using reader with a card: Reader name
```

레이블은 사람이 읽을 수 있는 값(이 경우)으로 설정됩니다. **auth-id** 는 두 개의 **16**진수 값이어야 합니다. 이 경우 **01** 로 설정됩니다.

4.

스마트 카드의 새 슬롯에 개인 키를 저장하고 레이블을 지정합니다.

```
$ pkcs15-init --store-private-key testuser.key --label testuser_key \
   --auth-id 01 --id 01 --pin 963214
Using reader with a card: Reader name
```



참고

id에 지정하는 값은 개인 키 및 인증서를 저장할 때 동일해야 합니다. **--id** 에 대한 값을 지정하지 않으면 툴에 의해 더 복잡한 값을 계산하므로 자체 값을 더 쉽게 정의할 수 있습니다.

5.

스마트 카드의 새 슬롯에 인증서를 저장하고 레이블을 지정합니다.

```
$ 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.

(선택 사항) 스마트 카드의 새 슬롯에 공개 키를 저장하고 레이블을 지정합니다.

```
$ pkcs15-init --store-public-key testuserpublic.key
   --label testuserpublic_key --auth-id 01 --id 01 --pin 963214
Using reader with a card: Reader name
```

참고

공개 키가 개인 키 및/또는 인증서에 해당하는 경우 해당 개인 키 및/또는 인증서와 동일한 **ID**를 지정해야 합니다.

7. (선택 사항) 일부 스마트 카드는 설정을 잠그는 방식으로 카드를 종료해야 합니다.

```
$ pkcs15-init -F
```

이 단계에서 스마트 카드에는 새로 생성된 슬롯에 인증서, 개인 키 및 공개 키가 포함됩니다. 또한 사용자**kubelet** 및 **PUK** 및 보안 부서, **PUK** 및 **PUK**를 생성했습니다.

29.4. 웹 콘솔에 대한 스마트 카드 인증 활성화

웹 콘솔에서 스마트 카드 인증을 사용하려면 **cockpit.conf** 파일에서 스마트 카드 인증을 활성화합니다.

또한 동일한 파일에서 암호 인증을 비활성화할 수 있습니다.

사전 요구 사항

- **RHEL** 웹 콘솔이 설치되었습니다.

절차

1. 관리자 권한으로 **RHEL** 웹 콘솔에 로그인합니다.
2. 터미널을 클릭합니다.
3. **/etc/cockpit/cockpit.conf** 에서 **ClientCertAuthentication** 을 **yes** 로 설정합니다.

```
[WebService]
ClientCertAuthentication = yes
```

4. 선택적으로 다음을 사용하여 **cockpit.conf**에서 암호 기반 인증을 비활성화합니다.

```
[Basic]
action = none
```

이 구성에서는 암호 인증을 비활성화하고 항상 스마트 카드를 사용해야 합니다.

5. 웹 콘솔을 다시 시작하여 **cockpit.service** 에서 변경 사항을 수락하는지 확인합니다.

```
# systemctl restart cockpit
```

29.5. 스마트 카드를 사용하여 웹 콘솔에 로그인

스마트 카드를 사용하여 웹 콘솔에 로그인할 수 있습니다.

사전 요구 사항

- **Active Directory** 또는 **Identity Management** 도메인에서 생성된 사용자 계정에 연결된 스마트 카드에 저장된 유효한 인증서입니다.
- 스마트 카드의 잠금을 해제하는 **line**입니다.
- 스마트 카드가 리더에 입력되었습니다.

절차

1. 웹 브라우저를 열고 주소 표시줄에 웹 콘솔의 주소를 추가합니다.

   브라우저가 스마트 카드에 저장된 인증서를 보호하도록 요청하는 경우.

2. 암호 필요 대화 상자에서**ECDSA**를 입력하고 확인을 클릭합니다.

3. 사용자 식별 요청 대화 상자에서 스마트 카드에 저장된 인증서를 선택합니다.

4. **Remember this decision** 를 선택합니다.

   다음 번에는 시스템이 이 창을 열지 않습니다.

5. **OK**를 클릭합니다.

이제 연결되고 웹 콘솔에 해당 콘텐츠가 표시됩니다.

29.6. 스마트 카드 사용자에게 암호가 없는 SUDO 활성화

인증서를 사용하여 웹 콘솔에 로그인하면 관리 모드(**sudo**를 통해 루트 권한)로 전환해야 할 수 있습니다. 사용자 계정에 암호가 있는 경우 **sudo** 에 인증할 수 있습니다.

또는 **Red Hat Identity Management**를 사용하는 경우 초기 웹 콘솔 인증서 인증을 **sudo, SSH** 또는 기타 서비스에 대한 인증에 신뢰할 수 있는 것으로 선언할 수 있습니다. 이를 위해 웹 콘솔은 사용자 세션에 **S4U2Proxy Kerberos** 티켓을 자동으로 생성합니다.

사전 요구 사항

- **IdM (Identity Management)**
- **Identity Management**를 사용하여 가장 안전한 신뢰로 연결된 **Active Directory**
- 웹 콘솔에 로그인하도록 스마트 카드가 설정됩니다. 자세한 내용은 웹 콘솔을 사용하여 스마트 카드 인증 구성을 참조하십시오.

절차

1. 티켓에서 액세스할 수 있는 호스트를 나열하도록 제약 조건 위임 규칙을 설정합니다.

   예 **29.1.** 제약 조건 위임 규칙 설정

웹 콘솔 세션은 **host.example.com** 을 실행하며 **sudo** 를 사용하여 자체 호스트에 액세스할 수 있는 신뢰할 수 있어야 합니다. 또한 두 번째 신뢰할 수 있는 호스트 **remote.example.com** 을 추가하고 있습니다.

- 다음 위임을 생성합니다.
  - 다음 명령을 실행하여 특정 규칙이 액세스할 수 있는 대상 머신 목록을 추가합니다.

```
# 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
```

  - 웹 콘솔 세션**(HTTP/principal)**이 해당 호스트 목록에 액세스할 수 있도록 하려면 다음 명령을 실행합니다.

```
# 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. 해당 서비스에서 **GSS** 인증을 활성화합니다.

a. **sudo**의 경우 **/etc/sssd/sssd.conf** 파일에서 **pam_sss_gss** 모듈을 활성화합니다.

i. **root**로 도메인의 항목을 **/etc/sssd/sssd.conf** 구성 파일에 추가합니다.

```
[domain/example.com]
pam_gssapi_services = sudo, sudo-i
```

ii. 첫 번째 줄의 **/etc/pam.d/sudo** 파일에서 모듈을 활성화합니다.

```
auth sufficient pam_sss_gss.so
```

b. **SSH**의 경우 **/etc/ssh/sshd_config** 파일의 **GSSAPIAuthentication** 옵션을 **yes** 로 업데이트합니다.

주의

위임된 **S4U** 티켓은 웹 콘솔에서 연결할 때 원격 **SSH** 호스트에 전달되지 않습니다. 티켓을 사용하여 원격 호스트에서 **sudo**에 인증해도 작동하지 않습니다.

검증

1. 스마트 카드를 사용하여 웹 콘솔에 로그인합니다.
2. 제한된 액세스 버튼을 클릭합니다.
3. 스마트 카드를 사용하여 인증합니다.

OR

1. **SSH**를 사용하여 다른 호스트에 연결을 시도합니다.

29.7. DOS 공격을 방지하기 위해 사용자 세션 및 메모리 제한

인증서 인증은 다른 사용자를 가장하려는 공격자와 **cockpit-ws** 웹 서버의 인스턴스를 분리하고 격리하여 보호됩니다. 그러나 이로 인해 잠재적인 서비스 거부 **(DoS)** 공격이 발생합니다. 원격 공격자는 많은 수의 인증서를 생성하고 각각 다른 인증서를 사용하여 **cockpit-ws** 에 많은 수의 **HTTPS** 요청을 보낼 수 있습니다.

이 **DoS**를 방지하기 위해 이러한 웹 서버 인스턴스의 총 리소스는 제한됩니다. 기본적으로 연결 수 및 메모리 사용량에 대한 제한은 **200** 스레드와 **75% (**소프트**) / 90% (**하드**)** 메모리 제한으로 설정됩니다.

다음 절차에서는 연결 및 메모리 수를 제한하여 리소스 보호에 대해 설명합니다.

절차

1. 터미널에서 **system-cockpithttps.slice** 구성 파일을 엽니다.

```
# systemctl edit system-cockpithttps.slice
```

2. **TasksMax** 를 ***100*** 으로 제한하고 **CPUQuota** 를 ***30%*** 로 제한합니다.

```
[Slice]
# change existing value
TasksMax=100
# add new restriction
CPUQuota=30%
```

3. 변경 사항을 적용하려면 시스템을 다시 시작하십시오.

```
# systemctl daemon-reload
# systemctl stop cockpit
```

이제 새로운 메모리 및 사용자 세션 제한이 **DoS** 공격으로부터 **cockpit-ws** 웹 서버를 보호합니다.