SUSE Manager 4.3

설치 및 업그레이드 가이드

Contents

설치 및 업그레이드 가이드 개요

업데이트 날짜: 2025-09-24

이 가이드는 SUSE Manager 서버 및 프록시 설치 및 업그레이드에 대한 지침을 제공합니다. 다음과 같은 섹션으로 구성되었습니다.

- 요구사항: 시작하기 전 필요한 하드웨어, 소프트웨어 및 네트워크 요구사항을 설명합니다.
- 설치: SUSE Manager 구성 요소의 설치 프로세스를 설명합니다.
- 설정: 설치 후 SUSE Manager 환경에서 사용하기 위해 필요한 초기 단계를 설명합니다.
- 업그레이드: 기본 데이터베이스를 포함하여 SUSE Manager 구성 요소의 업그레이드에 대해 설명합니다.

공용 클라우드 인스턴스를 사용하여 SUSE Manager를 설치할 수 있습니다. 공용 클라우드에서 SUSE Manager 사용에 대한 자세한 내용은 **Specialized-guides › Public-cloud-guide**를 참조하십시오. 클라이언트 업그레이드에 대한 자세한 내용은 **Client-configuration › Client-upgrades**를 참조하십시오.

Chapter 1. Enable LTS

Long Term Support (LTS) extends the lifecycle of SUSE Manager. It is available as an extension for SUSE Manager Server, Proxy, and Retail Branch Server. For more information about Long Term Service Pack Support (LTSS) in general, refer to https://www.suse.com/products/long-term-service-pack-support/.

To enable the LTS extensions, perform the following steps.

Procedure: Enabling SUSE Manager Server LTS

1. **root** 로 로그인합니다.
2. Make sure your system is registered with a subscription that is eligible for LTS. If the system is not yet registered, run:

```
SUSEConnect -e <EMAIL_ADDRESS> -r <SUSE_MANAGER_CODE> \
  -p SUSE-Manager-Server/<productnumber>/<architecture>
```

3. Make sure the LTS extension is available for your system:

```
SUSEConnect --list-extensions | grep -i LTS
```

   Output:

```
SUSE Manager Server LTS 4.3 x86_64
 Activate with: SUSEConnect -p suse-manager-server-lts/4.3/x86_64 -r
<ADDITIONAL_REGCODE>
```

4. Activate LTS with:

```
SUSEConnect -p suse-manager-server-lts/4.3/x86_64 -r <ADDITIONAL_REGCODE>
```

To enable SUSE Manager Proxy LTS 4.3 x86_64 or SUSE Manager Retail Branch Server LTS 4.3 x86_64 proceed accordingly.

Chapter 2. 일반 요구사항

설치를 시작하기 전, 다음이 준비되었는지 확인해야 합니다.

- 현재 SUSE Customer Center 조직 인증서
- 설치 미디어에 액세스
- 환경의 하드웨어 및 네트워크 요구사항 충족 여부
- 환경에 필요한 모든 필수 SSL 인증서

이 섹션은 이러한 각 요구사항에 대한 자세한 정보를 제공합니다.

지원되는 클라이언트 및 기능의 전체 목록은 **Client-configuration › Supported-features**을 참조하십시오.

SUSE Manager 4.3은 호스트 운영 체제로 SLES 15 SP4를 기반으로 합니다. SUSE Manager에서는 2년의 유지보수 라이프싸이클이 제공됩니다. 자세한 내용은 https://www.suse.com/lifecycle/에서 확인할 수 있습니다.

15의 장기 서비스 팩 지원(LTSS)은 SUSE Manager에 추가할 수 없습니다. SLES for SAP를 SUSE Manager에 대한 토대로 사용하여 기본 운영 체제의 라이프싸이클을 연장할 수 없습니다.

2.1. SUSE Customer Center 인증서 가져오기

SUSE Customer Center를 통해 계정을 생성한 후 SUSE Linux Enterprise Server 및 SUSE Manager를 설치합니다.

절차: SCC 조직 인증서 가져오기

1. 웹 브라우저에서 https://scc.suse.com/login으로 이동합니다.
2. SCC 계정에 로그인하거나 프롬프트를 따라 새 계정을 생성합니다.
3. 아직 수행하지 않은 경우, **[조직에 연결]**을 클릭한 후 조직을 입력하거나 검색합니다.
4. **[내 조직 관리]**를 클릭한 후 조직 이름을 클릭하여 목록에서 조직을 선택합니다.
5. **[조직]** 탭을 클릭한 후 **[조직 인증서]** 탭을 선택합니다.
6. SUSE Manager 설정 중에 사용할 로그인 정보를 기록합니다.

조직의 설정에 따라, **[서브스크립션 활성화]** 메뉴를 사용하여 서브스크립션을 활성화해야 할 수 있습니다.

SCC 사용에 대한 자세한 내용은 https://scc.suse.com/docs/help에서 참조하십시오.

2.2. Unified Installer

SUSE Manager 서버 및 프록시는 SUSE Linux Enterprise Unified Installer을 사용하여 설치됩니다.

예를 들어 "SUSE Manager Lifecycle Management+" 구독에서 SUSE Manager에 대한 유효한 등록 코드만 필요합니다. 자세한 내용은 https://www.suse.com/products/terms_and_conditions.pdf에서 SUSE 규정

및 조건을 참조하십시오. SLES 15 SP4에 대한 별도의 코드는 필요하지 않습니다.

아직 완료하지 않은 경우 https://download.suse.com에서 SUSE Linux Enterprise Unified Installer을 다운로드합니다.

SUSE Linux Enterprise 15 SP4(으)로의 직접 링크이며, SUSE Manager(https://www.suse.com/download/suse-manager)를 설치하는 데 필요합니다.

IBM Z 등의 최신 버전 또는 다른 아키텍처는 각 항목을 선택하십시오. Unified Installer을 사용하면 SLES, SLES for SAP Applications 또는 SUSE Manager 등 여러 SLE 기반 기본 제품을 설치할 수 있습니다.

2.3. SUSE Manager Web UI에서 지원되는 브라우저

Web UI를 사용하여 SUSE Manager 환경을 관리하려면, 최신 웹 브라우저를 사용 중인지 확인해야 합니다.

SUSE Manager 지원 웹 브라우저:

- SUSE Linux Enterprise Server와 함께 제공되는 최신 Firefox 브라우저
- 모든 운영 체제의 최신 Chrome 브라우저
- Windows와 함께 제공되는 최신 Edge 브라우저

Windows Internet Explorer는 지원되지 않습니다. SUSE Manager Web UI는 Windows Internet Explorer에서 올바르게 렌더링되지 않습니다.

2.4. SSL 인증서

SUSE Manager에서는 SSL 인증서를 사용하여 클라이언트가 올바른 서버에 등록되었는지 확인합니다. 기본적으로 SUSE Manager에서는 자체 서명 인증서가 사용됩니다. 타사 CA가 서명한 인증서인 경우 SUSE Manager 설치로 인증서를 임포트할 수 있습니다.

- 자체 서명 인증서에 대한 자세한 내용은 **Administration › Ssl-certs-selfsigned**를 참조하십시오.
- 임포트한 인증서에 대한 자세한 내용은 **Administration › Ssl-certs-imported**에서 참조하십시오.

2.5. 하드웨어 요구사항

이 표는 x86-64 및 ppc64le 아키텍처의 SUSE Manager 서버 및 프록시에 대한 하드웨어와 소프트웨어 요구사항이 정리되어 있습니다.

IBM Z 하드웨어 요구사항은 **Installation-and-upgrade › Install-ibmz**를 참조하십시오.

SUSE Manager for Retail 하드웨어 요구사항은 **Retail › Retail-requirements**을 참조하십시오.

2.5.1. 서버 하드웨어 요구사항

SUSE Manager 서버는 **/var/spacewalk/** 디렉토리에 패키지를 저장합니다. 이 디렉토리의 공간이 부족하면 리포지토리를 동기화할 수 없습니다. **/var/spacewalk/** 디렉토리에 필요한 공간은 미러링할 클라이언트 및 리포지토리에 따라 예상할 수 있습니다.

파일 시스템 및 파티셔닝 세부 정보에 대한 자세한 내용은 installation-and-upgrade:hardware-requirements.pdf에서 확인할 수 있습니다.

표 1. x86-64 아키텍처에 대한 서버 하드웨어 요구사항

하드웨어	세부 정보	권장
CPU	-	최소 4개의 전용 64비트 CPU 코어 (x86-64)
램	테스트 또는 기반 설치	최소 16 GB
	운영 서버	최소 32 GB
디스크 공간	/ (루트 디렉토리)	최소 40 GB
	/var/lib/pgsql	최소 50 GB
	/var/spacewalk	필수 최소 스토리지: 100 GB(구현된 검사에서 확인됨) * 각 SUSE 제품 및 Package Hub당 50 GB 각 Red Hat 제품당 360 GB
	/var/cache	최소 10 GB. SUSE 제품당 100 MB, Red Hat 또는 기타 제품당 1 GB를 추가합니다. 서버가 ISS Master인 경우 용량을 두 배로 늘립니다.
	스왑 공간	3 GB

표 2. IBM POWER8 또는 POWER9 아키텍처에 대한 서버 하드웨어 요구사항

하드웨어	세부 정보	권장
CPU		최소 4개의 전용 코어
RAM	테스트 또는 기반 설치	최소 16 GB
	운영 서버	최소 32 GB
디스크 공간	/ (루트 디렉토리)	최소 100 GB
	/var/lib/pgsql	최소 50 GB
	/var/spacewalk	필수 최소 스토리지: 100 GB(구현된 검사에서 확인됨) * 각 SUSE 제품 및 Package Hub당 50 GB 각 Red Hat 제품당 360 GB

하드웨어	세부 정보	권장
	/var/cache	최소 10 GB. SUSE 제품당 100 MB, Red Hat 또는 기타 제품당 1 GB를 추가합니다. 서버가 ISS Master인 경우 용량을 두 배로 늘립니다.
	스왑 공간	3 GB

SUSE Manager 성능은 하드웨어 리소스, 네트워크 대역폭, 클라이언트와 서버 간 대기 시간 등에 따라 달라집니다.

사용 중인 환경과 다양한 배포에 따라 적절한 수의 프록시가 배치된 SUSE Manager 서버의 최적 성능을 달성하려면 단일 서버당 10,000개의 클라이언트를 초과하지 않는 것이 좋습니다. 클라이언트가 10,000개를 초과하는 경우 허브 설정으로 이동하여 컨설팅을 포함하는 것이 매우 권장됩니다. 미세 조정 및 적절한 수의 프록시가 포함된 경우에도 클라이언트의 수가 그렇게 많으면 성능 문제가 발생할 수 있습니다.

대규모 클라이언트 관리에 대한 자세한 내용은 **Specialized-guides › Large-deployments**에서 확인할 수 있습니다.

2.5.2. 프록시 하드웨어 요구사항

표 3. 프록시 하드웨어 요구사항

하드웨어	세부 정보	권장
CPU		최소 2개의 전용 64비트 CPU 코어
RAM	테스트 서버	최소 2GB
	프로덕션 서버	최소 8GB
디스크 공간	/(루트 디렉토리)	최소 40GB
	/srv	최소 100GB
	/var/cache(Squid)	최소 100GB

SUSE Manager 프록시는 **/var/cache/** 디렉토리에 패키지를 캐시합니다. **/var/cache/**의 공간이 부족한 경우 프록시는 사용되지 않는 오래된 패키지를 제거한 후 새 패키지로 교체합니다.

이 동작의 결과:

- 프록시에서 **/var/cache/**디렉토리에 더 많은 공간이 확보되고 프록시와 SUSE Manager 서버 간의 트래픽이 감소합니다.
- 프록시에서 **/var/cache/**디렉토리의 크기와 SUSE Manager 서버에서 **/var/spacewalk/**의 크기를 동일하게 설정하면, 최초 동기화 후 대규모 트래픽이 발생하는 것을 방지할 수 있습니다.
- SUSE Manager 서버의 **/var/cache/** 디렉토리는 프록시에 비해 작을 수 있습니다. 크기 예상에 대한 설명은 서버 하드웨어 요구사항 섹션을 참조하십시오.

In general, SUSE recommends to adjust the value for the cache directory to about 60 % of available free space. Users can set the **cache_dir** option in the **squid.conf** manually.

For more information, see specialized-guides:large-deployments/tuning.pdf.

2.5.3. 저장소 장치 및 권한

SUSE Manager용 리포지토리와 데이터베이스는 별도의 저장소 장치에 저장하는 것이 좋습니다. 이를 통해 데이터 손실을 방지할 수 있습니다.

YaST SUSE Manager 설정 절차를 실행하기 전에 저장소 장치를 설정해야 합니다.

Cobbler 또는 PostgreSQL 저장소의 경우 NFS를 사용하지 말고, SELinux 환경의 경우에도 NFS를 사용하지 마십시오. 이러한 경우는 지원되지 않습니다.

SUSE Manager에 필요한 3가지 다른 볼륨:

- 데이터베이스 볼륨: **/var/lib/pgsql**
- 채널 볼륨: **/var/spacewalk**
- 캐시: **/var/cache**

모든 볼륨의 파일 시스템 형식으로는 XFS를 사용하는 것이 좋습니다. 또한, 온프레미스 설치의 경우 논리적 볼륨 관리(LVM)를 사용하여 디스크를 관리할 수 있습니다. 리포지토리 저장소의 디스크 크기는 SUSE Manager를 사용하여 관리한 배포 및 채널의 수에 따라 다릅니다. 필요한 예상 크기에 대한 설명은 이 섹션의 테이블을 참조하십시오.

SUSE Manager 서버에서 이 명령을 사용하여 사용할 수 있는 모든 저장소 장치를 찾습니다.

```
hwinfo --disk | grep -E "장치 파일:"
```

lsblk 명령을 사용하여 각 장치의 이름 및 크기를 확인합니다.

장치 이름과 함께 **suma-storage** 명령을 사용하여 외부 디스크를 데이터베이스 및 리포지토리의 위치로 설정합니다.

```
suma-storage <channel_devicename> [<database_devicename>]
```

외부 저장소 볼륨은 **/manager_storage** 및 **/pgsql_storage**에 마운트된 XFS 파티션으로 설정됩니다.

채널 데이터 및 데이터베이스 모두에서 동일한 저장소 장치를 사용할 수 있습니다. 채널 리포지토리가 증가하여 저장소가 가득 차 데이터베이스 무결성이 손상될 수 있으므로 이 방법은 권장되지 않습니다. 별도의 저장소 장치를 사용하면 성능도 향상할 수 있습니다. 1개의 저장소 장치를 사용하려면 단일 장치 이름 파라미터와 함께 **suma-storage**를 실행합니다.

프록시를 설치하는 경우에는 **suma-storage** 명령에서 단일 장치 이름 파라미터만 사용할 수 있고 외부 저장소 위치가 Squid 캐시로 설정됩니다.

SUSE Manager 서버 및 프록시에 대한 디스크 파티션을 생성할 때는 권한을 올바르게 설정했는지 확인하십시오.

/var/lib/pgsql의 경우:

- 소유자: 읽기, 쓰기, 실행
- 그룹: 읽기, 실행
- 사용자: 없음

/var/spacewalk의 경우:

- 소유자: 읽기, 쓰기, 실행
- 그룹: 읽기, 쓰기, 실행
- 사용자: 읽기, 실행

다음 명령으로 권한 확인:

```
ls -l /var/lib/pgsql /var/spacewalk
```

출력은 다음과 같아야 합니다.

```
drwxr-x--- 1 postgres postgres /var/lib/pgsql
drwxrwxr-x 1 wwwrun   www      /var/spacewalk
```

필요한 경우, 다음 명령으로 권한 변경:

```
chmod 750 /var/lib/pgsql
chmod 775 /var/spacewalk
```

그리고 다음으로 소유자 변경:

```
chown postgres:postgres /var/lib/pgsql
chown wwwrun:www /var/spacewalk
```

2.6. 네트워크 요구사항

이 섹션에서는 SUSE Manager의 네트워크 및 포트 요구사항에 대한 자세한 설명을 제공합니다.

FQDN(정규화된 도메인 이름)

SUSE Manager 서버는 FQDN이 올바르게 확인되어야 합니다. FQDN을 확인할 수 없는 경우 여러 다른 구성 요소에서 심각한 문제가 발생할 수 있습니다.

호스트 이름 및 DNS의 구성에 대한 자세한 내용은 https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-network.html#sec-network-yast-change-host를 참조하십시오.

호스트 이름 및 IP 주소

클라이언트가 SUSE Manager 도메인 이름을 올바르게 확인하도록 하려면, 서버 및 클라이언트 머신 모두 작동하는 DNS 서버에 연결되어야 합니다. 또한, 역방향 조회도 올바르게 구성되었는지 확인해야 합니다.

DNS 서버 설정에 대한 자세한 내용은 https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-dns.html을 참조하십시오.

SUSE Linux Enterprise 미디어에서 설치 시 프록시 사용

내부 네트워크에 위치하고 SUSE Customer Center에 액세스할 수 없는 경우, 설치 중에 프록시를 설정 및 사용할 수 있습니다.

SUSE Linux Enterprise 설치 중에 SUSE Customer Center에 액세스하기 위해 프록시를 구성하는 것에 대한 자세한 내용은 https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-boot-parameters.html#sec-boot-parameters-advanced-proxy를 참조하십시오.

SUSE Manager의 호스트 이름에는 대문자가 포함되지 않아야 합니다. 그러지 않으면 _jabberd_에서 오류가 발생하게 됩니다. SUSE Manager의 호스트 이름은 신중하게 선택해야 합니다. 서버 이름을 변경할 수 있지만 변경을 계획한 후 진행하는 것이 중요합니다. 서버의 호스트 이름을 변경하면 서버에 연결된 모든 클라이언트가 변경 사항을 인식해야 합니다.

프로덕션 환경에서 SUSE Manager 서버와 클라이언트는 항상 방화벽을 사용해야 합니다. 전체 필수 포트 목록은 **Installation-and-upgrade › Ports**를 참조하십시오.

연결이 끊긴 설정 및 포트 구성에 대한 자세한 내용은 **Administration › Disconnected-setup**을 참조하십시오.

2.6.1. HTTP 또는 HTTPS OSI 레벨 7 프록시 후방 배포

Some environment enforce internet access through a HTTP or HTTPS proxy. This could be a Squid server or similar. To allow the SUSE Manager Server internet access in such configuration, you need to configure the following.

절차: HTTP 또는 HTTPS OSI 레벨 7 프록시 구성

1. 운영 체제 인터넷 액세스의 경우, 필요에 따라 **/etc/sysconfig/proxy**를 수정합니다.

```
PROXY_ENABLED="no"
HTTP_PROXY=""
HTTPS_PROXY=""
NO_PROXY="localhost, 127.0.0.1"
```

2. For Java application internet access, modify **/etc/rhn/rhn.conf** according to your needs. For example, set:

```
# Use proxy FQDN, or FQDN:port
server.satellite.http_proxy =
server.satellite.http_proxy_username =
server.satellite.http_proxy_password =
# no_proxy is a comma seperated list
server.satellite.no_proxy =
```

3. Restart spacewalk services to enforce the new configuration:

```
spacewalk-services restart
```

2.6.2. 필수 네트워크 포트

이 섹션에서는 SUSE Manager에서의 다양한 통신을 위해 사용되는 전체 포트 목록이 제공됩니다.

이러한 모든 포트를 열 필요는 없습니다. 사용 중인 서비스에 필요한 포트만 열면 됩니다.

외부 인바운드 서버 포트

무단 액세스로부터 서버를 보호하려면 SUSE Manager 서버에서 외부 인바운드 포트를 열어 방화벽을 구성해야 합니다.

이러한 포트를 열면 외부 네트워크 트래픽이 SUSE Manager 서버에 액세스할 수 있습니다.

표 4. SUSE Manager 서버의 외부 포트 요구사항

포트 번호	프로토콜	사용 대상	참고
22			ssh-push 및 ssh-push-tunnel 통신 방법에서 필요합니다.
67	TCP/UDP	DHCP	클라이언트가 서버의 IP 주소를 요청할 때만 필요합니다.
69	TCP/UDP	TFTP	자동 클라이언트 설치를 위해 서버가 PXE로 사용될 때 필요합니다.
80	TCP	HTTP	일부 부트스트랩 리포지토리 및 자동 설치에서 일시적으로 필요합니다. 80 포트는 Web UI를 제공하기 위해 사용되지 않습니다.
443	TCP	HTTPS	Web UI, 클라이언트, 서버 및 프록시(**tftpsync**) 요청입니다.
4505	TCP	salt	클라이언트로부터의 통신 요청을 수락하기 위해 필요합니다. 클라이언트가 연결을 시작하며, Salt 마스터로부터 명령을 수신하기 위해 열려 있는 상태를 유지합니다.

포트 번호	프로토콜	사용 대상	참고
4506	TCP	salt	클라이언트로부터의 통신 요청을 수락하기 위해 필요합니다. 클라이언트가 연결을 시작하며, Salt 마스터로 결과를 다시 보고하기 위해 열려 있는 상태를 유지합니다.
5222	TCP	osad	OSAD 동작을 클라이언트로 푸시하기 위해 필요합니다.
5269	TCP	jabberd	프록시와 동작을 서로 푸시하기 위해 필요합니다.
25151	TCP	Cobbler	

외부 아웃바운드 서버 포트

액세스할 수 있는 서버를 제한하려면 SUSE Manager 서버에서 외부 아웃바운드 포트를 열어 방화벽을 구성해야 합니다.

이러한 포트를 열면 SUSE Manager 서버로부터의 네트워크 트래픽이 외부 서비스와 통신할 수 있습니다.

표 5. SUSE Manager 서버의 외부 포트 요구사항

포트 번호	프로토콜	사용 대상	참고
80	TCP	HTTP	SUSE Customer Center를 위해 필요합니다. 80 포트는 Web UI를 제공하기 위해 사용되지 않습니다.
443	TCP	HTTPS	SUSE Customer Center를 위해 필요합니다.
5269	TCP	jabberd	프록시와 동작을 서로 푸시하기 위해 필요합니다.

내부 서버 포트

내부 포트는 SUSE Manager 서버에 의해 내부적으로 사용됩니다. 내부 포트는 **localhost**에서만 액세스할 수 있습니다.

대부분의 경우에는 이러한 포트를 조정할 필요가 없습니다.

표 6. SUSE Manager 서버의 내부 포트 요구사항

포트 번호	참고
2828	Satellite-search API, Tomcat 및 Taskomatic의 RHN 애플리케이션에서 사용됩니다.

포트 번호	참고
2829	Taskomatic API, Tomcat의 RHN 애플리케이션에서 사용됩니다.
8005	Tomcat 종료 포트입니다.
8009	Tomcat-Apache HTTPD(AJP)입니다.
8080	Tomcat-Apache HTTPD(HTTP)입니다.
9080	Salt-API, Tomcat 및 Taskomatic의 RHN 애플리케이션에서 사용됩니다.
25151	Cobbler의 XMLRPC API
32000	Taskomatic 및 satellite-search에서 실행되는 Java 가상 머신(JVM)으로의 TCP 연결을 위한 포트입니다.

32768 이상 포트는 사용 후 삭제 포트로 사용됩니다. 이러한 포트는 대부분 TCP 연결을 수신하기 위해 사용됩니다. TCP 연결 요청이 수신되면, 발신자가 이러한 사용 후 삭제 포트 번호 중 하나를 선택하여 대상 포트로 사용합니다.

다음 명령을 사용하여 임시 포트인 포트를 찾을 수 있습니다.

```
cat /proc/sys/net/ipv4/ip_local_port_range
```

외부 인바운드 프록시 포트

무단 액세스로부터 프록시를 보호하려면 SUSE Manager 프록시에서 외부 인바운드 포트를 열어 방화벽을 구성해야 합니다.

이러한 포트를 열면 외부 네트워크 트래픽이 SUSE Manager 프록시에 액세스할 수 있습니다.

표 7. SUSE Manager 프록시의 외부 포트 요구사항

포트 번호	프로토콜	사용 대상	참고
22			ssh-push 및 ssh-push-tunnel 통신 방법에서 필요합니다. 프록시에 연결된 클라이언트가 서버에서 체크인을 시작하며 클라이언트를 통해 호핑을 수행합니다.
67	TCP/UDP	DHCP	클라이언트가 서버의 IP 주소를 요청할 때만 필요합니다.
69	TCP/UDP	TFTP	자동 클라이언트 설치를 위해 서버가 PXE로 사용될 때 필요합니다.

포트 번호	프로토콜	사용 대상	참고
443	TCP	HTTPS	Web UI, 클라이언트, 서버 및 프록시(**tftpsync**) 요청입니다.
4505	TCP	salt	클라이언트로부터의 통신 요청을 수락하기 위해 필요합니다. 클라이언트가 연결을 시작하며, Salt 마스터로부터 명령을 수신하기 위해 열려 있는 상태를 유지합니다.
4506	TCP	salt	클라이언트로부터의 통신 요청을 수락하기 위해 필요합니다. 클라이언트가 연결을 시작하며, Salt 마스터로 결과를 다시 보고하기 위해 열려 있는 상태를 유지합니다.
5222	TCP		OSAD 동작을 클라이언트로 푸시하기 위해 필요합니다.
5269	TCP		서버와 동작을 서로 푸시하기 위해 필요합니다.

외부 아웃바운드 프록시 포트

액세스할 수 있는 프록시를 제한하려면 SUSE Manager 프록시에서 외부 아웃바운드 포트를 열어 방화벽을 구성해야 합니다.

이러한 포트를 열면 SUSE Manager 프록시로부터의 네트워크 트래픽이 외부 서비스와 통신할 수 있습니다.

표 8. SUSE Manager 프록시의 외부 포트 요구사항

Port number	Protocol	Used By	Notes
80			Used to reach the server.
443	TCP	HTTPS	Required for SUSE Customer Center.
4505	TCP	salt	Required to connect to Salt master either directly or via proxy.
4506	TCP	salt	Required to connect to Salt master either directly or via proxy.

Port number	Protocol	Used By	Notes
5269	TCP		Required to push actions to and from the server.

외부 클라이언트 포트

SUSE Manager 서버와 클라이언트 사이에서 방화벽을 구성하려면 외부 클라이언트 포트가 열려 있어야 합니다.

대부분의 경우에는 이러한 포트를 조정할 필요가 없습니다.

표 9. SUSE Manager 클라이언트의 외부 포트 요구사항

Port number	Direction	Protocol	Notes
22	Inbound	SSH	Required for ssh-push and ssh-push-tunnel contact methods.
80	Outbound		Used to reach the server or proxy.
443	Outbound		Used to reach the server or proxy.
4505	Outbound	TCP	Required to connect to Salt master either directly or via proxy.
4506	Outbound	TCP	Required to connect to Salt master either directly or via proxy.
5222	Outbound	TCP	Required to push OSAD actions to the server or proxy.
9090	Outbound	TCP	Required for Prometheus user interface.
9093	Outbound	TCP	Required for Prometheus alert manager.
9100	Outbound	TCP	Required for Prometheus node exporter.
9117	Outbound	TCP	Required for Prometheus Apache exporter.

Port number	Direction	Protocol	Notes
9187	Outbound	TCP	Required for Prometheus PostgreSQL.

필수 URL

SUSE Manager에서 클라이언트를 등록하고 업데이트를 수행하기 위해 액세스할 수 있어야 하는 URL이 몇 개 있습니다. 대부분의 경우에는 해당 URL에 대한 액세스를 허용하는 것으로 충분합니다.

- **scc.suse.com**
- **updates.suse.com**
- **installer-updates.suse.com**

SUSE 이외의 클라이언트를 사용하는 경우에는 해당 운영 체제용 특정 패키지를 제공하는 다른 서버에 대한 액세스도 허용해야 할 수 있습니다. 예를 들어, Ubuntu 클라이언트가 있는 경우 Ubuntu 서버에 액세스할 수 있어야 합니다.

SUSE 이외의 클라이언트에 대한 방화벽 액세스 문제 해결과 관련한 자세한 내용은 **Administration › Troubleshooting**에서 확인할 수 있습니다.

2.7. PostgreSQL 요구사항

PostgreSQL 데이터베이스만 지원됩니다. 원격 PostgreSQL 데이터베이스 또는 원격 파일 시스템(예: NFS)을 PostgreSQL 데이터베이스와 함께 사용하는 기능은 지원되지 않습니다. 즉, PostgreSQL은 SUSE Manager에 대해 사용 가능한 가장 빠른 저장소 장치에 있어야 합니다.

추가 배경 정보:

잠재적인 성능 문제로 인해 PostgreSQL 데이터베이스를 SUSE Manager에서 원격으로 실행하는 것은 일반적으로 권장하지 않습니다. 대부분의 경우 작동하고 안정적이지만 문제가 발생하면 항상 데이터가 손실될 위험이 있습니다.

그러한 경우 SUSE에서 지원을 제공하지 못할 수 있습니다.

2.8. 지원되는 클라이언트 시스템

다음 테이블에는 기존 및 Salt 클라이언트에 지원되는 운영 체제가 나열됩니다.

이 테이블에서 ✔는 운영 체제를 실행하는 클라이언트가 SUSE에서 지원됨을 의미하며 ✖는 지원되지 않음을 나타냅니다. ?이(가) 표시된 필드는 고려 중임을 나타내며 나중에 지원되거나 그렇지 않을 수도 있습니다.

SUSE 운영 체제의 경우, 버전 및 SP 레벨이 일반 지원(일반 또는 LTSS)에 속해야 SUSE Manager에서 지원될 수 있습니다. 지원되는 제품 버전에 대한 자세한 내용은 다음을 참조하십시오.

https://www.suse.com/lifecycle

Red Hat Enterprise Linux, CentOS 및 Oracle Linux 등 SUSE 외 운영 체제의 경우 사용

> 가능한 최신 버전만 일반 지원이 제공됩니다.
>
> Older minor releases might still work, but will only be supported on a limited and reasonable-effort basis. If issues arise on an outdated minor release, users will be asked to upgrade to the latest available minor version before further support is provided.

표 10. 지원되는 클라이언트 시스템

운영 체제	아키텍처	기존 클라이언트	Salt 클라이언트
SUSE Linux Enterprise 15, 12	x86-64, ppc64le, IBM Z, aarch64	✔	✔
SUSE Linux Enterprise Server for SAP 15, 12	x86-64, ppc64le	✔	✔
SLE Micro	x86-64, aarch64, s390x	✖	✔
SL Micro	x86-64, aarch64, s390x	✖	✔
openSUSE Leap 15	x86-64, aarch64	✔	✔
SUSE Liberty Linux 9, 8, 7	x86-64	✖	✔
AlmaLinux 9, 8	x86-64, aarch64	✖	✔
Amazon Linux 2	x86-64, aarch64	✖	✔
CentOS 8, 7	x86-64, aarch64	✖	✔
Debian 12, 11	x86-64	✖	✔
Oracle Linux 9, 8, 7	x86-64, aarch64	✖	✔
Red Hat Enterprise Linux 9, 8, 7	x86-64	✖	✔
Rocky Linux 9, 8	x86-64, aarch64	✖	✔
Ubuntu 24.04, 22.04, 20.04	amd64	✖	✔

배포의 수명이 만료하면 3개월의 유예 기간이 시작되며 지원은 중단한 것으로 간주됩니다. 이 기간이 경과하면 해당 제품은 지원하지 않는 것으로 간주됩니다. 모든 지원은 최선의 노력으로 제공합니다.

수명 종료에 대한 자세한 설명은 https://endoflife.software/operating-systems를 참조하십시오.

> Salt SSH는 **/var/tmp**를 사용하여 Salt Bundle을 배포하고 번들된 Python으로 클라이언트에서 Salt 명령을 실행합니다. 그러므로 **noexec** 옵션으로 **/var/tmp**를 마운트하지 않아야 합니다. 부트스트랩 프로세스는 Salt SSH를 사용하여 클라이언트에 도달하므로 **/var/tmp**가 **noexec** 옵션으로 마운트된 클라이언트를 Web UI로 부트스트랩할 수 없습니다.

클라이언트 하드웨어를 설정할 때, SUSE Manager에 대한 다음 추가 사항과 함께 운영 체제 및 클라이언트에서 수행할

워크로드에 충분한 공간이 있는지 확인해야 합니다.

표 11. 클라이언트 추가 하드웨어 요구사항

하드웨어	필요한 하드웨어 크기
RAM	512MB
디스크 공간:	200MB

2.9. 공용 클라우드 요구사항

이 섹션에서는 공용 클라우드 인프라에 SUSE Manager를 설치하기 위한 요구사항을 제공합니다. Amazon EC2, Google Compute Engine, Microsoft Azure에서 이러한 지침을 테스트했지만 약간의 차이는 있지만 다른 공급자에서도 작동해야 합니다.

시작하기 전 고려해야 할 사항은 다음과 같습니다.

- SUSE Manager 설정 절차는 정방향 확인 된 역방향 DNS 조회를 수행합니다. 설정 절차를 완료하고 SUSE Manager이 예상대로 작동하려면 이 작업이 성공해야 합니다. SUSE Manager를 설정하기 전에 호스트 이름 및 IP 구성을 수행하는 것이 중요합니다.
- SUSE Manager 서버 및 프록시 인스턴스는 DNS 항목을 관리할 수 있는 네트워크 구성에서 실행해야 하지만 인터넷에서 전체적으로 액세스할 수 없습니다.
- 이 네트워크 구성에서는 DNS 확인이 제공되어야 합니다. **hostname -f**에서 FQDN(정규화된 도메인 이름)을 반환해야 합니다.
- DNS 확인은 클라이언트 연결에도 중요합니다.
- DNS는 선택한 클라우드 프레임워크와 독립적입니다. 자세한 지침은 클라우드 공급자의 설명서를 참조하십시오.
- 외부 가상 디스크에서 소프트웨어 리포지토리, 서버 데이터베이스 및 프록시 squid 캐시를 찾는 것이 좋습니다. 이를 수행하면 인스턴스가 예기치 않게 종료되는 경우 데이터 손실을 방지할 수 있습니다. 이 섹션에는 외부 가상 디스크를 설정하기 위한 지침이 포함되어 있습니다.

기존 클라이언트를 부트스트랩하려면 클라이언트에 로그인한 상태에서 서버의 호스트 이름을 확인할 수 있는지 확인하십시오. 서버의 FQDN을 클라이언트의 **/etc/hosts** 로컬 확인 파일에 추가해야 할 수도 있습니다. 서버의 로컬 IP 주소가 포함된 **hostname -f** 명령을 사용하여 확인할 수 있습니다.

2.9.1. 네트워크 요구사항

공용 클라우드에서 SUSE Manager를 사용하는 경우 제한 네트워크를 사용해야 합니다. 방화벽이 올바르게 설정된 VPC 개인 서브넷을 사용하는 것이 좋습니다. 지정된 IP 범위의 시스템만 인스턴스에 액세스할 수 있습니다.

퍼블릭 클라우드에서 SUSE Manager을 실행하면 강력한 보안 조치를 구현할 수 있습니다. 인스턴스에 대한 액세스 제한, 필터링, 모니터링 및 감사 기능은 필수 기능입니다. SUSE는 적절한 경계 보안이 부족한 전역 액세스 SUSE Manager 인스턴스를 사용하지 않을 것을 강력하게 권장됩니다.

SUSE Manager Web UI에 액세스하려면, 네트워크 액세스 제어를 구성할 때 HTTPS를 허용하십시오. 이렇게 하면

SUSE Manager Web UI에 액세스할 수 있습니다.

EC2 및 Azure에서 새 보안 그룹을 만들고 HTTPS에 대한 인바운드 및 아웃바운드 규칙을 추가합니다. GCE에서 **방화벽** 섹션 아래의 **HTTPS 트래픽 허용** 상자를 선택합니다.

2.9.2. 스토리지 볼륨 준비

SUSE Manager용 리포지토리와 데이터베이스는 루트 볼륨에 대한 별도의 저장소 장치에 저장하는 것이 좋습니다. 이렇게 하면 데이터 손실을 방지할 수 있습니다. 공용 클라우드 설치에서는 LVM(논리적 볼륨 관리)을 사용하지 마십시오.

YaST SUSE Manager 설정 절차를 실행하기 전에 저장소 장치를 설정해야 합니다.

리포지토리 저장소를 위한 디스크 크기는 SUSE Manager로 관리할 배포 및 채널 수에 따라 다릅니다. 가상 디스크를 연결하면 인스턴스에 Unix 장치 노드로 표시됩니다. 장치 노드의 이름은 공급자 및 선택한 인스턴스 유형에 따라 다릅니다.

SUSE Manager 서버의 루트 볼륨이 100GB 이상인지 확인합니다. 500GB 이상의 추가 저장소 디스크를 추가하고 가능하면 SSD 저장소를 선택하십시오. SUSE Manager 서버의 클라우드 이미지는 인스턴스가 시작될 때 스크립트를 사용하여 별도의 볼륨을 할당합니다.

인스턴스를 시작할 때 SUSE Manager 서버에 로그인하고 이 명령을 사용하여 사용 가능한 모든 저장소 장치를 찾을 수 있습니다.

```
hwinfo --disk | grep -E "장치 파일:"
```

선택해야 할 장치가 확실하지 않은 경우 **lsblk** 명령을 사용하여 각 장치의 이름과 크기를 확인하십시오. 찾고 있는 가상 디스크의 크기와 일치하는 이름을 선택하십시오.

suma-storage 명령어로 외부 디스크를 설정할 수 있습니다. 그러면 **/manager_storage**에 마운트된 XFS 파티션이 생성되고 이를 데이터베이스 및 리포지토리의 위치로 사용합니다.

```
/usr/bin/suma-storage <devicename>
```

권장 최소 크기 등 저장소 볼륨 및 파티션에 대한 자세한 내용은 **Installation-and-upgrade › Hardware-requirements**에서 참조하십시오.

Chapter 3. 설치

이 섹션은 SUSE Manager 구성 요소의 설치 프로세스를 설명합니다.

공용 클라우드 인스턴스를 사용하여 SUSE Manager를 설치할 수 있습니다. 공용 클라우드에서 SUSE Manager 사용에 대한 자세한 내용은 **Specialized-guides › Public-cloud-guide**을 참조하십시오.

3.1. SUSE Manager 서버

3.1.1. SUSE Manager 4.3 서버 설치

SUSE Manager은(는) SUSE Linux Enterprise 제품군 내의 SUSE 제품입니다. 이 섹션에서는 SUSE Linux Enterprise 설치 미디어에서 SUSE Manager 서버를 설치하는 방법을 설명합니다. 예를 들어 "SUSE Manager Lifecycle Management+" 구독에서 이 주제에서는 SUSE Customer Center에 대한 유효한 조직 자격 증명이 이미 있고 SUSE Manager에 대한 등록 코드를 획득했다고 가정합니다.

SUSE Customer Center를 사용한 등록, SUSE Customer Center에서 조직 인증서 검색 또는 설치 미디어 가져오기에 대한 자세한 내용은**Installation-and-upgrade › General-requirements**에서 참조하십시오.

SUSE Manager를 설치하기 전, **Installation-and-upgrade › Hardware-requirements**에서 요구사항을 확인하여 물리적 또는 가상 머신에 충분한 여유 공간과 RAM이 있는지 확인하십시오.

- SUSE Manager를 설치하는 권장 방법은 Unified Installer이 있는 SUSE Linux Enterprise 설치 미디어를 사용하는 것입니다.
- SUSE Manager 이미지를 사용할 수 있는 공용 클라우드에 SUSE Manager을 설치하는 경우 해당 이미지를 사용합니다. 자세한 내용은 **Specialized-guides › Public-cloud-guide**에서 확인할 수 있습니다.
- SUSE Manager 이미지를 사용할 수 없는 공용 클라우드에 SUSE Manager을 설치하는 경우 SUSE Linux Enterprise Server 15 SP4에서 시작하여 기본 제품을 SUSE Manager 4.3(으)로 변경합니다. 자세한 내용은 **Installation-and-upgrade › Install-vm**에서 확인할 수 있습니다.

SUSE Manager 설치 중

절차: DVD 이미지를 사용하여 SUSE Manager 서버 설치

1. Unified Installer을 사용하여 시스템을 부팅합니다. 부팅에 실패하면, BIOS에서 부팅 순서를 조정해야 합니다.
2. 메시지가 표시되면, **설치**를 선택합니다.
3. **언어, 키보드 및 제품 선택** 화면에서 **SUSE Manager Server**를 확인하고 **[다음]**을 클릭합니다.
4. 최종 사용자 라이선스 계약을 읽고 동의한 후 **[다음]**을 클릭합니다.
5. **등록** 화면에서 **scc.suse.com을 통해 시스템 등록** 확인란을 선택하고 SUSE Customer Center 인증서를 입력한 후 **[다음]**을 클릭합니다.
6. **확장 및 모듈** 화면에서 필요한 추가 확장 또는 모듈을 선택한 후 **[다음]**을 클릭합니다. 필수 모듈은 미리 선택되어 있으며 비활성화할 수 없습니다.

7. 선택 사항: **추가 기능 제품** 화면에서 필요한 추가 또는 추가 기능 제품을 선택하고 **[다음]**을 클릭합니다. SUSE Manager에서 다른 워크로드를 실행하지 않는 것이 좋습니다. 하드웨어 벤더가 제공한 드라이버 리포지토리 등 반드시 필요한 추가 기능만 사용하십시오.
8. **시스템 역할** 화면에서 **SUSE Manager Server** 확인란을 선택한 후 **[다음]**을 클릭합니다.
9. **추천하는 파티션 구성** 화면에서 기본값을 수락하거나 **[안내에 따른 설정]** 또는 **[고급 파티션 도구]** 옵션을 사용하여 파티션 구성 모델을 사용자 정의한 후 **[다음]**을 클릭합니다.
10. **시계 및 시간대** 화면에 지역과 시간대를 입력한 후 **[다음]**을 클릭합니다.
11. **로컬 사용자** 화면에서 새 사용자를 생성한 후 **[다음]**을 클릭합니다.
12. **시스템 관리자 루트** 화면에서 루트 사용자를 생성한 후 **[다음]**을 클릭합니다.
13. **설치 설정** 화면에서 설정을 검토합니다.
14. **설치 설정** 화면에서 **[설치]**를 클릭합니다.

기본 SUSE Manager 서버 설치에서는 그래픽 데스크톱 환경이 활성화되지 않습니다. SUSE Manager 서버에서 그래픽 인터페이스 로컬을 사용하여 YaST와 같은 설정 도구를 실행하려면 **소프트웨어**를 클릭하고 **X Window 시스템** 패턴을 선택합니다.

설치 절차가 완료되면 명령 프롬프트에서 **SUSEConnect --status-text** 명령을 사용하여 모든 필수 모듈이 설치되었는지 확인할 수 있습니다. SUSE Manager 서버에 필요한 모듈은 다음과 같습니다.

- SUSE Linux Enterprise Server Basesystem 모듈
- Python 3 모듈
- Server Applications 모듈
- Web and Scripting 모듈
- SUSE Manager Server 모듈

SUSE Manager 서버의 설치가 완료되면 사용할 수 있도록 설정해야 합니다. 자세한 내용은 **Installation-and-upgrade › Server-setup**에서 참조하십시오.

3.1.2. SUSE Manager VM 이미지를 사용하여 가상 머신 환경에 SUSE Manager 설치

이 장에서는 커널 가상 머신(KVM) 또는 VMware 이미지를 배포하는 절차에 대해 설명합니다.

SUSE Manager 4.3의 이미지는 형식이 다양합니다. 이미지는 SUSE Linux Enterprise Server 15 SP4을(를) 기본 운영 체제로 사용하고 빌드 시점의 SUSE Manager 소프트웨어를 최신 버전으로 유지합니다. https://download.suse.com/ 에서 사용자 환경에 적합한 SUSE Manager 이미지를 다운로드하십시오.

Ignition 등의 툴을 사용하여 **root** 암호를 설정하는 것은 선택 사항입니다. **Ignition**에 대한 자세한 내용은 **Installation-and-upgrade › Install-ignition**에서 확인할 수 있습니다.

가상 머신 관리자 설정

이 섹션에서는 SUSE Manager에 필요한 KVM(커널 가상 머신) 설정에 대해 설명합니다. 가상 머신 관리자(virt-manager)와 통합된 KVM을 이 설치를 위한 샌드박스로 사용할 수 있습니다.

다음 테이블에는 최소 요구사항이 제공됩니다. 이러한 설정은 클라이언트가 1개인 서버와 같이 빠른 테스트 설치에 적합합니다. 프로덕션 환경을 사용하려면 **Installation-and-upgrade › Hardware-requirements**에서 제공되는 요구사항을 확인합니다.

가상 머신 설정 개요	
설치 방법	기존 디스크 이미지 임포트
OS:	SUSE Linux Enterprise 15 SP4
메모리:	16GB
CPU:	4
가상 디스크:	
VirtIO 디스크 1	SUSE-Manager-Server.x86_64-4.3.10-KVM.qcow2
VirtIO 디스크 2	**/var/spacewalk**용 101GB
VirtIO 디스크 3	**/var/lib/pgsql**용 50GB
VirtIO 디스크 4	스왑용 4GB
이름:	suse-manager-test-setup
네트워크:	Bridge br0

SUSE Linux Enterprise 가상화에 대한 자세한 내용은 https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-virtualization.html에서 확인할 수 있습니다.

SUSE Manager 가상 머신 생성 - KVM

SUSE Manager 저장소 파티션에 필요한 추가 가상 디스크 3개와 함께 가상 머신을 생성합니다.

절차: virt-manager를 사용한 VM 및 추가 파티션 생성

1. **virt-manager**에서 **File › 새 가상 머신**을 엽니다.
2. **새 가상 머신 만들기** 대화 상자에서 **기존 디스크 이미지 가져오기**를 선택한 다음 **[전달]**로 확인합니다.
3. 다운로드한 SUSE Manager KVM 이미지의 파일 이름을 입력하고 운영체제로 **SUSE Linux Enterprise 15 SP4**를 설정합니다. **[전달]**을 사용하여 확인합니다.
4. RAM 및 CPU 수(RAM 16GB 및 CPU 4개 이상)를 구성합니다. **[전달]**로 확인합니다.
5. VM의 이름을 설정하고 **구성을 사용자 정의한 후 설치** 확인란을 선택합니다.
6. **네트워크 선택** 드롭다운 메뉴에서 구성된 브리지 장치를 선택합니다.
7. **[완료]**를 사용하여 확인합니다.
8. 개요 대시보드의 왼쪽 탐색 모음 하단에서 **[하드웨어 추가]**를 클릭하여 다음 사양의 추가 가상 디스크를 생성합니다. 이러한 디스크는 절차: SUSE Manager 실행 준비에서 파티셔닝 및 탑재됩니다.

저장소 크기 값은 절대적으로 최솟값이며 소규모 테스트 또는 데모 설치용으로만 적합합니다.

> 특히 **/var/spacewalk/**에서는 빠르게 추가 공간이 필요하게 됩니다. 또한, Kiwi 이미지가 저장되는 **/srv**에 대한 별도의 파티션도 생성하는 것이 좋습니다.

VirtIO 저장소 디스크	이름	크기
VirtIO 디스크 2	spacewalk	500GB
VirtIO 디스크 3	pgsql	100GB
VirtIO 디스크 4	스왑	4GB

9. **[설치 시작]**을 클릭하여 SUSE Manager 이미지에서 새 VM을 부팅합니다.
10. JeOS Firstboot 화면에서 **[시작]** 버튼을 선택하여 계속 진행하고, 다음 구성 옵션(키보드 레이아웃, 라이선스 계약, 시간대, 루트 암호)을 확인합니다.
11. 설치가 완료되면 루트로 로그인합니다.
12. installation-and-upgrade:install-vm.pdf에 따라 진행합니다.

SUSE Manager 가상 머신 생성 -VMware

이 섹션에서는 VMware 구성에서 VMware 환경 내에서 SUSE Manager 스토리지 파티션에 필수적인 추가 가상 디스크 생성을 중심으로 설명합니다.

절차: VMware 가상 머신 생성

1. SUSE Manager 서버 **.vmdk** 파일을 다운로드합니다. 그런 다음 사본을 VMware 스토리지로 전송합니다.
2. Make a copy of uploaded **.vmdk** file using VMware web interface. This will convert provided **.vmdk** file to the format suitable for vSphere hypervisor. Use this new copy as a base image for the virtual machine.
3. 게스트 OS 제품군 **Linux** 및 게스트 OS 버전 SUSE Linux Enterprise 15(64비트)를 기반으로 새 가상 시스템을 생성하고 이름을 지정합니다.
4. 500GB(또는 이상)의 추가적인 **Hard Disk 2**를 추가합니다.
5. RAM 및 CPU 수(RAM 16GB 및 CPU 4개 이상)를 구성합니다.
6. 필요에 따라 네트워크 어댑터를 설정합니다.
7. VM을 켭니다.
8. JeOS Firstboot 화면에서 시작을 선택하여 계속 진행하고, 다음 구성 대화 상자(키보드 레이아웃, 라이선스 계약, 시간대, 루트 암호)를 확인합니다.
9. 설치가 완료되면 루트 권한으로 로그인합니다.
10. installation-and-upgrade:install-vm.pdf에 따라 진행합니다.

SUSE Manager용 가상 머신 준비

시작하기 전에 SUSE Customer Center(https://scc.suse.com)에서 SUSE Manager 등록 코드를 받으십시오.

절차: SUSE Manager 실행 준비

1. **root** 로 로그인합니다.
2. SCC를 사용하여 SUSE Manager를 등록합니다. 예를 들어, **<productnumber>**을(를) **4.3**(으)로 바꾸고 **<architecture>**를 **x86_64**로 바꿉니다.

```
SUSEConnect -e <EMAIL_ADDRESS> -r <SUSE_MANAGER_CODE> \
  -p SUSE-Manager-Server/<productnumber>/<architecture>
```

3. 확장 프로그램 목록 명령을 실행하여 승인된 확장 프로그램의 유효성을 검사합니다.

```
SUSEConnect --list-extensions
```

4. SUSE Manager 리포지토리 추가:

```
SUSEConnect -p sle-module-basesystem/15.4/x86_64
SUSEConnect -p sle-module-server-applications/15.4/x86_64
SUSEConnect -p sle-module-web-scripting/15.4/x86_64
SUSEConnect -p sle-module-suse-manager-server/<productnumber>/x86_64
```

5. SUSE Manager 저장소를 준비합니다. **suma-storage** 명령은 이전에 생성한 외부 저장소를 SUSE Manager에 사용할 수 있도록 자동으로 준비하고 구성합니다. 다음 명령에서 첫 번째 파라미터는 SUSE Manager 데이터를 위한 장치이고, 두 번째 파라미터는 데이터베이스를 위한 장치입니다.

```
suma-storage /dev/vdb /dev/vdc
```

6. 이제 SUSE Manager를 위한 가상 머신을 설정할 준비가 되었습니다.

SUSE Manager 설정을 진행하려면, **Installation-and-upgrade › Server-setup**을 참조하십시오.

3.1.3. IBM Z에 설치

이 섹션은 IBM Z 메인프레임을 운영하는 z/VM 시스템 프로그래머를 대상으로 제공됩니다. 그리고 독자가 IBM Z 작동 프로토콜에 대한 z/VM 시스템 프로그래머 교육을 받은 것으로 간주하고 기존 메인프레임 시스템에 SUSE Manager를 설치하는 단계를 설명합니다. 이 섹션에서는 IBM Z에서 사용할 수 있는 다양한 하드웨어 구성 프로파일을 다루지 않지만, IBM Z에 SUSE Manager 서버를 배포하기 위해 필요한 절차 및 요구사항에 대한 기본적인 개요를 제공합니다.

이 섹션에서는 SUSE Linux Enterprise 설치 미디어를 사용한 SUSE Manager 서버 설치 방법을 설명합니다. SUSE Customer Center를 사용하여 SUSE Manager 제품을 등록하고 등록 코드를 가져온 상태여야 합니다.

SUSE Customer Center를 사용한 등록, SUSE Customer Center에서 조직 인증서 검색 또는 설치 미디어 가져오기에 대한 자세한 내용은**Installation-and-upgrade › General-requirements**에서 참조하십시오.

시스템 요구사항

시작하기 전, 환경이 기본 시스템 요구사항을 충족하는지 확인하십시오.

호환 IBM Z 시스템:

- IBM zEnterprise EC12

- IBM zEnterprise EC12
- IBM zEnterprise BC12
- IBM z13
- LinuxOne Rockhopper
- LinuxOne Emperor

표 12. 하드웨어 요구사항

하드웨어	권장
CPU	최소 4개의 전용 64비트 CPU 코어
RAM:	테스트 서버: 최소 16GB RAM 및 2GB 스왑 공간
	기본 설치: 최소 16GB
	프로덕션 서버: 최소 32GB
디스크 공간:	루트 파티션: 최소 100GB
	/var/lib/pgsql: 최소 50GB
	/var/spacewalk: SUSE 제품당 최소 50GB 및 Red Hat 제품당 360GB

메모리는 사용할 수 있는 RAM VDISK 전체에서 분할되고 환경에 적합하도록 스왑되어야 합니다. 프로덕션 시스템에서 실제 메모리 대 VDISK의 비율을 설치 중인 클라이언트의 수에 따라 평가해야 합니다.

데이터베이스 저장소를 위한 추가 디스크가 필요합니다. 이는 **HYPERPAV**와 함께 사용하는 것이 바람직한 **zFCP** 또는 **DASD** 장치여야 합니다. 데이터베이스 저장소 디스크에는 다음이 있어야 합니다.

- **/var/lib/pgsql**의 경우 최소 50GB
- **/var/spacewalk**에서 각 SUSE 제품의 경우 최소 50GB
- **/var/spacewalk**에서 각 Red Hat 제품의 경우 최소 360GB

SUSE Manager에 디스크 저장소가 충분한지 확인한 후 **yast2 susemanager_setup**을 실행해야 합니다. 기본적으로 기본 데이터베이스 및 패치 디렉토리 등 SUSE Manager 파일 시스템은 루트 디렉토리에 위치합니다. 설치가 완료되면 조정할 수 있지만, 조정 사항을 지정하고 면밀하게 모니터링하는 것이 중요합니다. 저장소 관리 및 디스크 공간 회수에 대한 내용은 SUSE Manager 관리 가이드의 문제 해결 섹션을 참조하십시오.

SUSE Manager에서 디스크 공간이 부족한 경우 데이터베이스 및 파일 구조에 심각한 영향을 미칠 수 있습니다. 전체 복구는 이전 백업을 사용하거나 SUSE Manager를 새로 설치하여 수행할 수 있습니다. SUSE 기술 서비스는 디스크 공간 부족이 발생한 시스템에는 지원을 제공할 수 없습니다.

네트워크 요구사항:

- OSA Express Ethernet(고속 및 기가비트 이더넷 포함)

- HiperSockets 또는 Guest LAN
- 10GBE, VSWITCH
- RDMA over Converged Ethernet(RoCE)

포함되지만 더 이상 지원되지 않는 인터페이스:

- CTC 또는 가상 CTC
- IUCV용 IP 네트워크 인터페이스

설치 후 변경이 어렵기 때문에 시작하기 전 SUSE Manager를 실행할 z/VM에 고정 IP 주소 및 호스트 이름이 있어야 합니다. 호스트 이름은 8자 미만이고 대문자가 포함되지 않아야 합니다.

IBM Z에 SUSE Manager 설치

이 섹션은 SUSE Linux Enterprise 제품군의 제품으로 SUSE Manager를 설치하는 방법을 설명합니다. IBM Z 하드웨어에서의 제품 배포에 대한 일반 정보는 https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-zseries.html을 참조하십시오.

절차: DVD 이미지를 사용하여 SUSE Manager 서버 설치

1. Unified Installer을 사용하여 시스템을 부팅합니다. 부팅에 실패하면, BIOS에서 부팅 순서를 조정해야 합니다.
2. 메시지가 표시되면, **설치**를 선택합니다.

그리고 **Installation-and-upgrade › Install-server-unified**의 설명을 따릅니다.

SUSE Manager의 설치를 완료하려면 **Installation-and-upgrade › Server-setup**을 참조하십시오.

3.1.4. 공용 클라우드에 설치

공용 클라우드는 BYOS(Bring Your Own Subscription) 모델에서 SUSE Manager를 제공합니다. 즉, SUSE Manager가 사전 설치되어 있으므로 설치 단계를 수행할 필요가 없습니다.

그러나 SUSE Manager를 사용하려면 몇 가지 추가 설정 단계를 수행해야 합니다. 공용 클라우드 설정 지침은 **Installation-and-upgrade › Pubcloud-setup**을 참조하십시오.

3.1.5. 부팅 이미지 구성 툴

SUSE Manager VM 이미지는 JeOS firstboot 구성 대화 상자를 사용하여 준비됩니다. **Ignition** 같은 부팅 이미지 구성 툴을 사용하는 것은 이제 선택 사항입니다.

Ignition을 사용한 SUSE Manager 기본 구성

Ignition은 처음 부팅할 때 사용자의 사양에 따라 시스템을 구성할 수 있는 프로비저닝 도구입니다. 시스템이 처음 부팅되면 **Ignition**이 initramfs의 일부로 로드되고 특정 디렉토리(USB 플래시 디스크 또는 URL 제공 가능) 내에서 구성 파일을 검색합니다.

Ignition은 JSON 형식의 구성 파일을 사용합니다. 파일 이름은 **config.ign**입니다.

config.ign은 Ignition에 대한 해결 방법을 제공하는 JSON 구성 파일입니다. 이 파일을 JSON으로 수동으로 만들거나 Fuel Ignition 도구를 사용하여 기본 해결 방법 세트를 생성할 수 있습니다. Fuel Ignition 도구는 전체 옵션 세트를 제공하지 않으므로 파일을 수동으로 수정해야 할 수도 있습니다. 자세한 내용은 https://ignite.opensuse.org/에서 확인할 수 있습니다.

설치할 때 구성 파일 **config.ign**은 **ignition**으로 레이블이 지정된 구성 미디어의 **ignition** 하위 디렉토리에 있어야 합니다. 디렉토리 구조는 다음과 같아야 합니다.

```
<root directory>
 └──── ignition
     └──── config.ign
```

QEMU/KVM 가상 머신을 구성하려면 **config.ign** 파일의 경로를 qemu 명령의 특성으로 제공합니다. 예:

```
-fw_cfg name=opt/com.coreos/config,file=PATH_TO_config.ign
```

config.ign 파일에는 객체, 문자열, 정수, 부울, 객체 목록의 다양한 데이터 형식이 포함되어 있습니다. 전체 사양은 https://coreos.github.io/ignition/configuration-v3_3/에서 확인할 수 있습니다.

Ignition을 사용하여 루트 비밀번호 설정

SUSE Manager VM 이미지가 루트 또는 다른 사용자 계정을 설정하지 않습니다. 처음 부팅할 때 사용자 또는 **root** 인증을 설정해야 합니다. **passwd** 특성을 사용하여 사용자를 추가할 수 있습니다. 시스템에 로그인하려면 루트를 생성하고 루트의 비밀번호를 설정하거나 **Ignition** 구성에 SSH 키를 추가합니다. 예를 들어, **openssl** 명령을 사용하여 루트 비밀번호를 해시해야 합니다.

```
openssl passwd -6
```

이 명령은 사용자가 선택한 비밀번호의 해시를 생성합니다. 이 해시를 **passwordHash** 특성의 값으로 사용합니다.

사용자 특성에는 **name** 특성이 하나 이상 포함되어야 합니다. **ssh_authorized_keys**는 사용자의 ssh 키 목록입니다.

다음 내용으로 **root/ignition/config.ign** 파일을 생성합니다

```
{
  "ignition": {
    "version": "3.2.0"
  },
  "passwd": {
    "users": [
      {
        "name": "root",
        "passwordHash": "$2a$10$qV298UV11u9lCFDjpHpCUe1cErBiVR.G3shukxs3.2PAO1xhJWs0K"
      }
    ]
  }
}
```

다음 명령을 사용하여 **Ignition** ISO 파일을 준비합니다.

```
mkisofs -full-iso9660-filenames -o suma_ignition.iso -V ignition root
```

만든 **suma_ignition.iso** 파일을 처음 부팅할 때 가상 머신에 볼륨으로 연결합니다. 이 특정 예제에서는 **루트** 비밀번호를 **linux**로 설정합니다. 이 예제의 비밀번호 해시를 본인의 비밀번호 해시로 바꿉니다.

Ignition에 대한 자세한 내용은 https://documentation.suse.com/sle-micro/5.4/single-html/SLE-Micro-deployment/#cha-images-ignition에서 확인할 수 있습니다.

3.2. SUSE Manager 프록시

3.2.1. SUSE Manager 4.3 프록시 설치

SUSE Manager 프록시는 SUSE Linux Enterprise 제품군 내의 SUSE 제품입니다. 이 섹션에서는 SUSE Linux Enterprise 설치 미디어에서 SUSE Manager 프록시를 설치하는 방법을 설명합니다. 예를 들어 "SUSE Manager Lifecycle Management+" 구독에서 SUSE Manager 프록시에 대한 등록 코드를 이미 받았다고 가정합니다.

SUSE Customer Center를 사용한 등록, SUSE Customer Center에서 조직 인증서 검색 또는 설치 미디어 가져오기에 대한 자세한 내용은**Installation-and-upgrade › General-requirements**에서 참조하십시오.

가상 머신에 SUSE Manager 프록시를 설치하려면, **Installation-and-upgrade › Hardware-requirements**의 요구사항을 확인하여 가상 머신의 디스크 공간 및 RAM이 충분한지 확인합니다.

SUSE Manager 프록시는 내부 서버에서 소프트웨어 패키지를 캐시하는 SUSE Manager 구성 요소입니다. 프록시는 또한 SUSE의 패치 업데이트 또는 타사 조직에서 생성한 사용자 지정 RPM을 캐시합니다. 프록시를 사용하면 클라이언트 시스템이 업데이트를 위해 프록시에 연결하고 SUSE Manager 서버가 더 이상 모든 클라이언트 요청을 처리할 필요가 없기 때문에 대역폭을 보다 효과적으로 사용할 수 있습니다. SUSE Manager Proxy는 Traditional 및 Salt 클라이언트를 모두 제공할 수 있습니다. 프록시는 투명한 사용자 지정 패키지 배포도 지원합니다.

SUSE Manager 프록시는 다음과 같은 기능을 제공하는 오픈 소스(GPLv2) 솔루션입니다.

- Squid 프록시 내에서 소프트웨어 패키지를 캐시합니다.
- 클라이언트 시스템은 SUSE Manager Proxy를 SUSE Manager 서버 인스턴스로 간주합니다.
- SUSE Manager Proxy는 SUSE Manager 서버를 통해 클라이언트 시스템으로 등록됩니다.

SUSE Manager Proxy의 기본 목적은 대역폭 요구사항을 줄이고 응답 시간을 가속화하여 SUSE Manager의 성능을 향상하는 것입니다.

절차: Unified Installer을 사용한 SUSE Manager 프록시 설치

1. 설치 이미지에서 Unified Installer을 부팅하려면 BIOS에서 부팅 순서를 조정해야 할 수 있습니다.
2. 메시지가 표시되면, **설치**를 선택합니다.
3. **언어, 키보드 및 제품 선택** 화면에서 **SUSE Manager Proxy** 확인란을 선택한 후 **[다음]**을 클릭합니다.
4. 최종 사용자 라이선스 계약을 읽고 동의한 후 **[다음]**을 클릭합니다.
5. **등록** 화면에서 **scc.suse.com을 통해 시스템 등록** 확인란을 선택하고 SUSE Customer Center 인증서를 입력한

후 [**다음**]을 클릭합니다.

6. **사용 가능한 확장 및 모듈** 화면에서 필요한 확장 또는 모듈을 선택한 후 [**다음**]을 클릭합니다. **Basesystem**, **SUSE Manager Proxy** 및 **Server Applications**는 SUSE Manager 프록시를 설치하기 위해 사전에 선택되며 필수입니다. 옵션: 다음 **제품에 추가** 화면에서 필요한 추가 또는 추가 제품을 선택하고 [**다음**]을 클릭합니다.
7. **시스템 역할** 화면에서 **SUSE Manager Proxy** 확인란을 선택한 후 [**다음**]을 클릭합니다.
8. **추천하는 파티션 구성** 화면에서 기본값을 수락하거나 [**안내에 따른 설정**] 또는 [**고급 파티션 도구**] 옵션을 사용하여 파티션 구성 모델을 사용자 정의한 후 [**다음**]을 클릭합니다.
9. **시계 및 시간대** 화면에 지역과 시간대를 입력한 후 [**다음**]을 클릭합니다.
10. **로컬 사용자** 화면에서 새 사용자를 생성한 후 [**다음**]을 클릭합니다.
11. **설치 설정** 화면에서 설정을 검토한 후 [**설치**]를 클릭합니다.

설치 절차가 완료되면 모든 필수 모듈이 설치되었는지 확인할 수 있습니다. 명령 프롬프트에 다음을 입력:

```
SUSEConnect --status-text
```

SUSE Manager 프록시에 필요한 모듈은 다음과 같습니다.

- SUSE Linux Enterprise Server Basesystem 모듈
- Server Applications 모듈
- SUSE Manager Proxy 모듈

설치된 SUSE Manager 프록시를 클라이언트로 등록: **Installation-and-upgrade › Proxy-registration**을 진행합니다.

3.2.2. 패키지에서 SUSE Manager 프록시 설치

패키지에서 SUSE Manager 프록시를 설치하려면 SUSE Linux Enterprise Server 미디어를 설치하여 시작해야 합니다. 이 섹션에서는 SUSE Manager 프록시의 기본으로 SUSE Linux Enterprise Server를 설치하기 위해 필요한 KVM 설정에 대해 설명합니다. 이 섹션에서는 KVM 및 가상 머신 관리자를 설치용 샌드박스로 사용합니다.

SLES KVM 요구사항

이러한 설정을 사용하여 **virt-manager**(**<version>**을 실제 버전 문자열로 바꿈) 명령으로 새 가상 머신을 생성합니다.

표 13. SLES KVM 설정

설치 방법:	**로컬 설치 미디어(ISO 이미지 또는 CDROM)**
OS:	Linux
버전:	**SLE-<version>-Server-x86_64-GM-DVD1.iso**
메모리:	테스트 서버 최고 2GB
	프로덕션 서버 최소 8GB

설치 방법:	로컬 설치 미디어(ISO 이미지 또는 CDROM)
CPU:	2
저장소 형식:	ISO 3GB
디스크 공간:	분할된 230GB
	/ (루트) 최소 24GB
	(가상 디스크 1) **/srv** 최소 100GB
	(가상 디스크 2) **/var/cache** (Squid) 최소 100GB
이름:	example-proxy
네트워크	Bridge br0

SLES KVM 설정

이 섹션에서는 KVM 및 **virt-manager** 명령을 통해 전체 설치 미디어를 사용한 SUSE Manager 프록시의 설치에 대해 설명합니다. 시작하기 전, SUSE Customer Center를 사용하여 계정을 생성하고 SUSE Linux Enterprise Server 설치 미디어를 다운로드해야 합니다.

절차: SLES 설치 준비

1. Virtual Machine Manager 도구(**virt-manager**)에서 **File › 새 가상 머신**을 클릭합니다.
2. **[로컬 설치 미디어(ISO 이미지 또는 CDROM)]**를 클릭합니다.
3. **새 가상 머신 생성** 대화 상자에서 **[찾아보기]**를 클릭한 후 SCC 계정에서 다운로드한 전체 SLES 이미지를 찾습니다.
4. RAM이 2GB 이상이고 CPU가 2개 이상으로 머신을 구성해야 합니다.

설치를 위한 최소 230GB의 저장소가 있는 저장 장치를 생성합니다. SLES를 설치하는 동안 이 디스크의 파티션을 다음과 같이 구성해야 합니다.

+

디스크 공간 요구사항
/srv/를 위한 100GB XFS 파티션(또는 전용 가상 디스크)
/var/cache/를 위한 100GB XFS 파티션(또는 전용 가상 디스크)

+

나머지 저장소 공간은 루트 파티션을 위해 운영 체제에서 사용됩니다.

1. **[완료]**를 클릭하여 설치 설정을 저장하고 설치를 시작합니다.

SUSE Linux Enterprise Server 설치에 대한 자세한 내용은 다음을 참조하십시오.

https://documentation.suse.com/sles/15-SP4/html/SLES-all/article-installation.html

SUSE Manager Proxy용 SLES 변경

절차: SUSE Manager 프록시를 설치하기 위해 SLES 변경

1. **root** 로 로그인합니다.
2. **sles-release** 패키지의 설치를 제거합니다.

```
rpm -e --nodeps sles-release
```

3. SCC를 사용하여 SUSE Manager 프록시를 등록합니다(예: **<productversion>**을 **4.3**(으)로 바꾸고 **<architecture>**를 **x86_64**로 바꿈).

```
SUSEConnect -e <EMAIL_ADDRESS> -r <SUSE_MANAGER_PROXY_CODE> \
-p SUSE-Manager-Proxy/<productversion>/<architecture>
```

4. SUSE Manager 리포지토리 추가:

```
SUSEConnect -p sle-module-basesystem/15.4/x86_64
SUSEConnect -p sle-module-server-applications/15.4/x86_64
SUSEConnect -p sle-module-suse-manager-proxy/4.3/x86_64
```

   권장 패키지 설치를 허용했는지 확인합니다. **/etc/zypp/zypp.conf**에서 설정을 확인하십시오.

```
solver.onlyRequires = false
```

5. SUSE Manager 프록시 패턴을 설치합니다.

```
zypper in -t pattern suma_proxy
```

6. 재부팅합니다.

설치된 SUSE Manager 프록시를 클라이언트로 등록: **Installation-and-upgrade › Proxy-registration**을 진행합니다.

3.2.3. SUSE Manager 프록시 KVM 이미지를 사용하여 가상 머신 환경에 SUSE Manager 프록시 설치

가상 머신 관리자 설정

이 장에서는 SUSE Manager 프록시에 필요한 KVM(커널 가상 머신) 설정에 대해 설명합니다. 가상 머신 관리자(virt-manager)와 통합된 KVM을 이 설치를 위한 샌드박스로 사용할 수 있습니다.

SUSE Manager 4.3 프록시에 대한 VM 이미지는 다양한 형식이 있습니다. 여기에는 SUSE Linux Enterprise Server 15 SP4을(를) 기본 운영 체제로 하고 빌드 시점의 SUSE Manager 프록시 소프트웨어를 최신 상태로 유지합니다. https://download.suse.com/에서 사용자 환경에 적합한 SUSE Manager 프록시 이미지를 다운로드하십시오.

다음 테이블에는 최소 요구사항이 제공됩니다. 이러한 설정은 클라이언트가 1개인 서버와 같이 빠른 테스트 설치에 적합합니다. 프로덕션 환경을 사용하려면 **Installation-and-upgrade ›**

Hardware-requirements에서 제공되는 요구사항을 확인합니다.

가상 머신 설정 개요	
설치 방법	기존 디스크 이미지 임포트
OS:	SUSE Linux Enterprise 15 SP4
메모리:	8GB
CPU:	2
가상 디스크:	
VirtIO 디스크 1	SUSE-Manager-Proxy.x86_64-4.3.13-KVM.qcow2
VirtIO 디스크 2	**/var/cache/**용 100GB
VirtIO 디스크 3	**/srv/**용 101GB
이름:	suse-manager-proxy-setup
네트워크	Bridge br0

SUSE Linux Enterprise 가상화에 대한 자세한 내용은 https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-virtualization.html에서 확인할 수 있습니다.

SUSE Manager 프록시 가상 머신 설치

SUSE Manager 프록시 스토리지 파티션에 필요한 추가 가상 디스크를 사용하여 가상 머신을 생성합니다.

절차: virt-manager를 사용한 VM 및 추가 파티션 만들기

1. **virt-manager**에서 **File › 새 가상 머신**을 엽니다.
2. **새 가상 머신 만들기** 대화 상자에서 **기존 디스크 이미지 가져오기**를 선택한 다음 **[전달]**로 확인합니다.
3. 다운로드한 SUSE Manager 프록시 KVM 이미지의 파일 이름을 입력하고 운영체제로 **SUSE Linux Enterprise 15 SP4**를 설정합니다. **[전달]**을 사용하여 확인합니다.
4. RAM 및 CPU 수(RAM 8GB 및 CPU 2개 이상)를 구성합니다. **[전달]**로 확인합니다.
5. VM의 이름을 설정하고 **구성을 사용자 정의한 후 설치** 확인란을 선택합니다.
6. **네트워크 선택** 드롭다운 메뉴에서 구성된 브리지 장치를 선택합니다.
7. **[완료]**를 사용하여 확인합니다.
8. 개요 대시보드의 왼쪽 탐색 모음 하단에 있는 **[하드웨어 추가]**를 클릭하여 가상 디스크를 추가로 만듭니다. 이러한 디스크는 나중에 파티셔닝되고 탑재됩니다.

저장소 크기 값은 절대적으로 최솟값이며 소규모 테스트 또는 데모 설치용으로만 적합합니다. 또한 Retail Branchservers 서버의 이미지가 저장되는 **/srv/tftpboot/**에 별도의 파티션을 생성하는 것도 고려하십시오.

VirtIO 저장소 디스크	이름	크기
VirtIO 디스크 2	squidcache	101 GB
VirtIO 디스크 3	tftpboot	100 GB

9. 왼쪽 탐색 모음의 위에서 **[설치 시작]**을 클릭하여 SUSE Manager 프록시 이미지에서 새 VM을 부팅합니다. **JeOS Firstboot** 시작 옵션이 표시될 때까지 기다립니다.

JeOS 처음 부팅 설정 실행

1. 확인하여 **JeOS 처음 부팅** 설정을 시작합니다.
2. **en_US**와 같은 시스템 로캘을 선택합니다.
3. **us**와 같은 키보드 레이아웃을 선택합니다.
4. 최종 사용자 라이선스 계약을 확인합니다.
5. **UTC**와 같은 표준 시간대를 선택합니다.
6. 루트 암호를 입력하고 확인합니다. 루트 암호는 안전하게 보관해야 합니다.
7. 로그인 프롬프트가 표시될 때까지 기다립니다.

SUSE Manager 프록시용 가상 머신 준비

시작하기 전에 SUSE Customer Center - https://scc.suse.com에서 이 이미지의 등록 코드를 받습니다.

절차: SUSE Manager 프록시 실행 준비

1. **root** 로 로그인합니다.
2. SCC를 사용한 SUSE Manager 프록시 등록:

```
SUSEConnect -e <EMAIL_ADDRESS> -r <SUSE_MANAGER_PROXY_CODE>
```

3. SUSE Manager 프록시 스토리지를 준비합니다. **suma-storage** 명령은 프록시와 함께 사용할 수 있도록 이전에 만든 외부 스토리지를 자동으로 준비 및 구성합니다. 다음 명령에서 첫 번째 파라미터는 **suma-storage**가 처리할 수 있는 SUSE Manager 프록시 Squid 캐시용 장치입니다.

```
suma-storage /dev/vdb
```

4. 이제 SUSE Manager 프록시용 가상 머신을 설정할 준비가 되었습니다.

설치된 SUSE Manager 프록시를 클라이언트로 등록: **Installation-and-upgrade › Proxy-registration**을 진행합니다.

3.2.4. SUSE Manager 프록시 VMware 이미지를 사용하여 가상 머신 환경에 SUSE Manager 프록시 설치

가상 머신 설정

SUSE Manager 4.3 프록시에 대한 VM 이미지는 다양한 형식이 있습니다. 여기에는 SUSE Linux Enterprise Server 15 SP4을(를) 기본 운영 체제로 하고 빌드 시점의 SUSE Manager 프록시 소프트웨어를 최신 상태로 유지합니다. https://download.suse.com/에서 사용자 환경에 적합한 SUSE Manager 프록시 이미지를 다운로드하십시오.

다음 테이블에는 최소 요구사항이 제공됩니다. 이러한 설정은 클라이언트가 1개인 서버와 같이 빠른 테스트 설치에 적합합니다. 프로덕션 환경을 사용하려면 **Installation-and-upgrade › Hardware-requirements**에서 제공되는 요구사항을 확인합니다.

가상 머신 설정 개요	
설치 방법	기존 디스크 이미지 임포트
OS:	SUSE Linux Enterprise 15 SP4
메모리:	8GB
CPU:	2
가상 디스크:	
VirtIO 디스크 1	SUSE-Manager-Proxy.x86_64-4.3.13-VMWare.vmdk
VirtIO 디스크 2	**/var/cache/**용 100GB
VirtIO 디스크 3	**/srv/**용 101GB
이름:	suse-manager-proxy-setup
네트워크	Bridge br0

SUSE Linux Enterprise 가상화에 대한 자세한 내용은 https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-virtualization.html에서 확인할 수 있습니다.

SUSE Manager 가상 머신 생성 -VMware

이 섹션에서는 VMware 구성에서 VMware 환경 내에서 SUSE Manager 스토리지 파티션에 필수적인 추가 가상 디스크 생성을 중심으로 설명합니다.

절차: VMware 가상 머신 생성

1. SUSE Manager 서버 **.vmdk** 파일을 다운로드합니다. 그런 다음 사본을 VMware 스토리지로 전송합니다.
2. Make a copy of uploaded **.vmdk** file using VMware web interface. This will convert provided **.vmdk** file to the format suitable for vSphere hypervisor. Use this new copy as a base image for the virtual machine.
3. 게스트 OS 제품군 **Linux** 및 게스트 OS 버전 SUSE Linux Enterprise 15(64비트)를 기반으로 새 가상 시스템을 생성하고 이름을 지정합니다.
4. 500GB(또는 이상)의 추가적인 **Hard Disk 2**를 추가합니다.
5. RAM 및 CPU 개수를 구성합니다(RAM 8GB 이상, CPU 2개 이상).

6. 필요에 따라 네트워크 어댑터를 설정합니다.
7. VM을 켭니다.
8. JeOS Firstboot 화면에서 시작을 선택하여 계속 진행하고, 다음 구성 대화 상자(키보드 레이아웃, 라이선스 계약, 시간대, 루트 암호)를 확인합니다.
9. 설치가 완료되면 루트 권한으로 로그인합니다.
10. SCC를 사용한 SUSE Manager 프록시 등록, SUSE Manager 프록시 스토리지 준비 및 추가 단계를 위해서는 installation-and-upgrade:install-proxy-vm.pdf에 따라 진행합니다.

3.2.5. 컨테이너화된 SUSE Manager 프록시를 설치합니다.

소개

SUSE Manager 프록시 컨테이너는 SUSE Linux Enterprise Server 15 SP3 이상 버전에서만 지원됩니다.

컨테이너를 SUSE Manager 프록시의 기반으로 사용하려면, 먼저 SUSE Manager 서버에 Salt 클라이언트로 등록해야 합니다. 또한 **Containers Module**을 컨테이너 호스트에서 사용할 수 있어야 합니다.

컨테이너 호스트를 기존 클라이언트로 연결하면 필수 패키지를 사용할 수 없기 때문에 작동하지 않습니다.

SUSE Manager 서버에 Salt 클라이언트를 등록하는 방법에 대한 자세한 내용은 **Client-configuration › Registration-overview**에서 확인할 수 있습니다.

컨테이너 호스트 요구사항

SUSE Manager 서버의 도메인 이름을 클라이언트에서 확인할 수 있는지 확인합니다.

- 컨테이너 프록시와 클라이언트 머신 모두 DNS 서버에 연결되어 있어야 합니다.
- 역방향 조회가 작동해야 합니다.

표 14. 프록시 컨테이너 호스트 하드웨어 요구사항

하드웨어	세부 정보	권장
CPU		최소 2개의 전용 64비트 CPU 코어
RAM	테스트 서버	최소 2GB
	프로덕션 서버	최소 8GB
디스크 공간		최소 100GB

표 15. 프록시 컨테이너 호스트 소프트웨어 요구사항

소프트웨어	세부 사항	설명
연결 방법	Salt	호스트는 Salt 클라이언트로 구성되어야 합니다.

호스트 시스템에 Container Services 설치

SUSE Manager Proxy 컨테이너는 **podman** 및 **systemd**를 사용하여 모든 프록시 컨테이너를 실행 및 관리합니다.

첫 번째 단계는 **uyuni-proxy-systemd-services** 패키지에서 제공하는 컨테이너 제어 파일을 설치하는 것입니다.

절차: SUSE Manager 프록시에 대한 컨테이너 서비스 설치

SUSE Manager의 컨테이너 호스트에 **Containers Module** 소프트웨어 채널을 할당합니다. 시스템에 소프트웨어 채널을 할당하는 방법에 대한 자세한 내용은 **Administration › Channel-management**에서 확인할 수 있습니다.

1. 컨테이너 호스트에서 **root**로 로그인합니다.
2. 수동으로 SUSE Manager 프록시 서비스 패키지 설치:

```
zypper install uyuni-proxy-systemd-services
```

패키지 **uyuni-proxy-systemd-service**는 다음 채널에서 제공됩니다.

- SLE-Manager-Tools_15
- SLE Micro의 경우 SLE-Manager-Tools-For-Micro_5

SUSE Manager 프록시 구성 사용자 정의

SUSE Manager 프록시 컨테이너는 장기 저장을 위해 일부 볼륨을 마운트해야 합니다. 이러한 볼륨은 **podman**에 의해 자동으로 생성되며, **podman volume ls** 명령을 사용하여 나열할 수 있습니다. 기본적으로 **podman**은 볼륨의 파일을 **/var/lib/containers/storage/volumes**에 저장합니다. 볼륨의 이름은 다음과 같습니다.

- **uyuni-proxy-squid-cache**
- **uyuni-proxy-rhn-cache**
- **uyuni-proxy-tftpboot**

기본 볼륨 설정을 무효화하려면 **podman volume create** 명령을 사용하여 포드를 처음 시작하기 전에 볼륨을 생성합니다.

podman 컨테이너 포드에 전달된 사용자 정의 인자를 **/etc/sysconfig/uyuni-proxy-systemd-services.config**에 추가할 수 있습니다.

```
EXTRA_POD_ARGS=''
```

이 파일에서 컨테이너 이미지에 사용할 태그를 수정할 수 있습니다.

```
TAG=latest
```

uyuni-proxy-systemd-services.config 파일, 특히 **TAG** 설정을 변경하는 것은 위험하며 시스템이 작동하지 않을 수 있습니다.

서비스에 사용자 정의 컨테이너 이미지 사용

기본적으로 SUSE Manager 프록시 제품군은 각 서비스에서 동일한 이미지 버전 및 레지스트리 경로를 사용하도록 설정됩니다. 그러나 특정 서비스에 대한 기본값을 무시할 수 있습니다. 패키지와 함께 번들로 제공되는 **uyuni-proxy** CLI는 다음 매개변수를 사용하여 **update image**를 실행합니다.

- 서비스 이름에 **-s**
- 버전 태그에 **-t**
- 레지스트리 경로에 **-r**

예를 들어, 다음과 같이 사용합니다.

```
uyuni-proxy update image -s httpd -t 0.1.0 -r registry.opensuse.org/uyuni
```

이 명령은 **registry.opensuse.org/uyuni**가 레지스트리이고 **0.1.0**이 버전 태그인 httpd 서비스의 구성 파일을 재시작하기 전에 조정합니다.

값을 기본값으로 재설정하려면 프록시 재설정 명령을 실행하고 서비스에 **-s** 파라미터를 지정합니다.

```
uyuni-proxy reset -s httpd
```

이 명령은 **httpd** 서비스의 구성을 전역 기본값으로 재설정한 후 다시 로드합니다.

자세한 내용은 **uyuni-proxy --help**에서 확인할 수 있습니다.

컨테이너 호스트 방화벽에서 제공되는 서비스에 대한 네트워크 액세스 허용

SUSE Manager Proxy 컨테이너는 노드 포트 서비스로 작동합니다. 즉, 프록시 컨테이너 포드가 컨테이너 호스트 네트워크 TCP 및 UDP 포트 공간을 공유합니다. 이러한 이유로 컨테이너 호스트 방화벽은 SUSE Manager Proxy 컨테이너에서 사용하는 포트에서 유입되는 트래픽을 수락하도록 구성해야 합니다. 해당 포트:

- 69/UDP - TFTP
- 80/TCP - HTTP
- 443/TCP - HTTPS
- 4505/TCP - Salt
- 4506/TCP - Salt
- 8022/TCP - SSH

Installation-and-upgrade › Proxy-container-setup의 설치된 SUSE Manager 프록시를 컨테이너로 설정을 진행합니다.

3.2.6. k3s에 컨테이너화된 SUSE Manager 프록시 설치

k3s 설치

컨테이너 호스트 시스템에 로드 밸런서 및 traefik 라우터를 제외하고 **k3s**를 설치합니다(**<K3S_HOST_FQDN>**을 k3s

호스트의 FQDN으로 바꿈).

```
curl -sfL https://get.k3s.io | INSTALL_K3S_EXEC="--disable=traefik --disable=servicelb
--tls-san=<K3S_HOST_FQDN>" sh -
```

클러스터 액세스 구성

helm은 대상 kubernetes 클러스터에 연결하기 위한 구성 파일이 필요합니다.

클러스터 서버 시스템에서 다음 명령을 실행하여 **kubeconfig-k3s.yaml** 구성 파일을 생성합니다. **kubeconfig-k3s.yaml** 파일은 선택적으로 작업 시스템으로 전송할 수 있습니다.

```
kubectl config view --flatten=true | sed 's/127.0.0.1/<K3S_HOST_FQDN>/' >kubeconfig-
k3s.yaml
```

helm을 호출하기 전 다음을 실행:

```
export KUBECONFIG=/path/to/kubeconfig-k3s.yaml
```

helm 설치

helm을 설치하려면 컨테이너 모듈이 필요합니다.

설치하려면 다음을 실행:

```
helm의 zypper
```

metalLB 설치

MetalLB는 SUSE Manager 프록시 포드 서비스를 외부로 노출하는 로드 밸런서입니다. 설치하려면 다음을 실행:

```
helm repo add metallb https://metallb.github.io/metallb
helm install --create-namespace -n metallb metallb metallb/metallb
```

MetalLB는 사용할 가상 IP 주소 범위를 알기 위한 구성이 필요합니다. 이 예에서 가상 IP 주소는 **192.168.122.240**~**192.168.122.250**이지만, 호스트가 SUSE Manager 프록시만 노출하는 경우 해당 범위는 단일 주소로 감소할 수 있습니다. 이러한 주소는 서버 네트워크의 하위 집합이어야 합니다.

다음 설정과 배포된 네트워크에 적합한 IP 주소 범위를 갖는 **metallb-config.yaml** 구성 파일을 생성합니다.

```
apiVersion: metallb.io/v1beta1
kind: IPAddressPool
metadata:
  name: l2-pool
  namespace: metallb
spec:
  addresses:
  - 192.168.122.240-192.168.122.250
---
apiVersion: metallb.io/v1beta1
```

```
kind: L2Advertisement
metadata:
  name: l2
  namespace: metallb
spec:
  ipAddressPools:
  - l2-pool
```

다음을 실행하여 이 구성 적용:

```
kubectl apply -f metallb-config.yaml
```

SUSE Manager 프록시 helm 차트 배포

MetalLB가 SUSE Manager 프록시 서비스에 사용할 IP 주소를 강제 적용하는 구성 파일을 생성합니다. 이 IP 주소는 프록시 구성을 생성할 때 프록시 FQDN이 입력한 주소여야 합니다. 또한, 프록시에 연결하려면 SUSE Manager 서버 및 클라이언트 시스템 모두에서 해당 주소를 확인할 수 있어야 합니다.

이 예에서는 **192.168.122.241**을 사용합니다.

다음과 같은 내용을 갖는 **custom-values.yaml** 파일을 생성합니다. **MetalLB** IP 주소 범위에 1개의 주소만 포함된 경우 마지막 줄을 제거할 수 있습니다.

```
services:
  annotations:
    metallb.universe.tf/allow-shared-ip: key-to-share-ip
    metallb.universe.tf/loadBalancerIPs: 192.168.122.241
```

metallb.universe.tf/allow-shared-ip 파라미터는 변경할 필요가 없습니다. **metallb.universe.tf/loadBalancerIPs** 파라미터를 네트워크 설정에 적합하도록 조정해야 합니다.

SUSE Manager 프록시 포드에서 사용할 볼륨의 스토리지를 구성하려면 다음 클레임에 대한 영구 볼륨을 정의합니다. 자세한 내용은 https://kubernetes.io/docs/concepts/storage/persistent-volumes/(kubernetes) 또는 https://rancher.com/docs/k3s/latest/en/storage/(k3s) 문서를 참조하십시오. 영구 볼륨 클레임의 이름은 다음과 같습니다.

- **squid-cache-pv-claim**
- **/package-cache-pv-claim**
- **/tftp-boot-pv-claim**

Installation-and-upgrade › Proxy-container-setup의 설명과 같이 SUSE Manager 프록시에 대한 구성을 생성합니다. 구성 **tar.gz** 파일을 복사 및 추출한 후 helm 차트를 배포합니다.

```
tar xf /path/to/config.tar.gz
helm install uyuni-proxy oci://registry.suse.com/suse/manager/4.3/proxy -f config.yaml -f
httpd.yaml -f ssh.yaml -f custom-values.yaml
```

Chapter 4. 설정

이 섹션에서는 설치 후 SUSE Manager 환경에서 사용하기 위해 필요한 초기 단계를 설명합니다.

4.1. SUSE Manager 서버

4.1.1. SUSE Manager 서버 설정

이 섹션에서는 다음 절차를 사용한 SUSE Manager 서버 설정에 대해 설명합니다.

- YaST를 사용한 SUSE Manager 설정 시작
- SUSE Manager Web UI를 사용하여 기본 관리 계정 생성
- 기본 조직의 이름 지정 및 로그인 인증서 추가
- SUSE Customer Center에서 SUSE Linux Enterprise 제품 채널 동기화

SUSE Manager는 SUSE Linux Enterprise 제품군의 일부이므로 SUSE Linux Enterprise Server에서 제공하는 소프트웨어와 호환됩니다.

SUSE Manager은(는) 복잡한 시스템이므로 타사 소프트웨어를 설치하는 것은 허용되지 않습니다. 타사 벤더가 제공하는 모니터링 소프트웨어를 설치하는 것은 SSL, 암호화 소프트웨어 및 유사한 도구 등의 기본 라이브러리를 바꾸지 않는 경우에만 허용됩니다. 제품 지원의 일환으로 SUSE는 타사 소프트웨어를 제거(및 관련 구성 변경)한 후 클린 시스템에서 문제를 재현하도록 요청할 권리를 보유합니다.

SUSE Manager 서버를 재귀 등록하지 마십시오. SUSE Manager 서버는 개별 관리하거나 별도의 다른 SUSE Manager 서버를 사용하여 관리해야 합니다. 여러 서버 사용에 대한 자세한 내용은 **Specialized-guides › Large-deployments**에서 참조하십시오.

YaST를 사용한 SUSE Manager 설정

이 섹션에서는 YaST를 사용한 SUSE Manager 설정 단계를 설명합니다.

절차: SUSE Manager 설정

1. SUSE Manager 서버에서 명령줄에 **yast2 susemanager_setup** 명령을 입력하여 설정을 시작합니다.
2. 소개 화면에서 **SUSE Manager 설정 › SUSE Manager를 처음부터 설정**을 선택한 후 **[다음]**을 클릭하여 계속 진행합니다.
3. 상태 알림을 수신할 전자 메일 주소를 입력하고 **[다음]**을 클릭하여 계속 진행합니다. 일부 경우 SUSE Manager은(는) 대량의 알림 이메일을 전송할 수 있습니다. 필요한 경우, 설정 후 Web UI에서 이메일 알림을 비활성화할 수 있습니다. 이메일 알림 비활성화에 대한 자세한 내용은 **Reference › Users**을 참조하십시오.
4. 인증서 정보 및 비밀번호를 입력합니다. 사용자 정의 SSL 인증서를 사용하려면 먼저 이 정보를 설정해야 합니다. SSL 인증서에 대한 자세한 내용은 **Administration › Ssl-certs**를 참조하십시오.
5. **[다음]**을 클릭하여 계속합니다.
6. **SUSE Manager 설정 › 데이터베이스 설정** 화면에서 데이터베이스 사용자 및 비밀번호를 입력하고 **[다음]**을 클릭하여 계속 진행합니다.

7. **[다음]**을 클릭하여 계속합니다.
8. 메시지가 표시되면 **[예]**를 클릭하여 설정을 실행하고 완료될 때까지 기다립니다.
9. **[다음]**을 클릭하여 계속합니다. SUSE Manager Web UI의 주소를 메모해 둡니다.
10. **[완료]**를 클릭하여 SUSE Manager의 설정을 완료합니다.

인증서 비밀번호를 생성할 때 길이가 7자 이상인지 확인하십시오. 공백, 작은따옴표 또는 큰따옴표(' 또는 "), 느낌표(!) 또는 달러 기호($)를 포함할 수 없습니다. 항상 비밀번호를 저장하십시오. 이 비밀번호가 없으면 SUSE Manager 프록시를 설정할 수 없습니다.

기본 관리 계정 변경

이 섹션에서는 SUSE Manager에서 조직의 기본 관리 계정을 생성하는 단계를 설명합니다.

기본 관리 계정은 SUSE Manager에서 최상위 권한 계정 이므로 계정 액세스 정보를 안전한 곳에 보관해야 합니다.

보안을 위해 기본 관리자가 조직 및 개별 그룹을 관리하기 위한 저수준 관리 계정 을 생성하는 것이 좋습니다.

최신 브라우저 버전에서는 사용자가 HSTS를 사용하도록 설정한 경우 SUSE Manager 서버 FQDN에 대한 웹 액세스를 차단할 수 있습니다.

HTTP를 통해 **pub** 디렉토리에서 CA 인증서를 설치하고 브라우저로 가져오면 서버에 액세스할 수 있습니다.

1. On the server, go to **http://<server>.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT**.
2. 인증서 파일을 가져오십시오. 브라우저 설정(Firefox의 경우)에서 메뉴:개인 정보 및 보안[인증서 > 인증서 보기]를 열고 파일을 가져오십시오.

절차: 기본 관리 계정 설정

1. 설정 완료 후 제공되는 주소를 브라우저에 입력합니다. 이 주소를 사용하여 SUSE Manager Web UI를 열 수 있습니다.
2. Web UI에서 **조직 생성 › 조직 이름** 필드로 이동하여 조직 이름을 입력합니다.
3. **조직 생성 › 원하는 로그인** 및 **조직 생성 › 원하는 비밀번호** 필드에 사용자 이름 및 비밀번호를 입력합니다.
4. 시스템 알림을 위한 전자 메일 등 계정 정보 필드를 입력합니다.
5. **[조직 생성]**을 클릭하여 관리 계정의 생성을 완료합니다.

이제 SUSE Manager **홈 › 개요** 페이지가 표시됩니다.

SUSE Customer Center에서 제품 동기화

SUSE Customer Center(SCC)는 지원되는 모든 엔터프라이즈 클라이언트 시스템을 위한 패키지, 소프트웨어 및 업데이트가 포함된 리포지토리 컬렉션을 유지합니다. 이러한 리포지토리는 배포, 릴리스 및 아키텍처별 소프트웨어를 제공하는 각 채널로 구성됩니다. SCC를 사용하여 동기화한 후 클라이언트에 업데이트가 수신되고 그룹으로 구성한 후

특정 제품 소프트웨어 채널로 할당될 수 있습니다.

이 섹션에서는 Web UI에서 SCC를 사용한 동기화 및 첫 번째 클라이언트 채널 추가에 대해 설명합니다.

소프트웨어 저장소를 SCC와 동기화하기 전에 SUSE Manager에 조직 자격 증명을 입력해야 합니다. 이전 버전에서는 미러 자격 증명이 대신 사용되었습니다. 조직 자격 증명을 통해 SUSE 제품 다운로드에 액세스할 수 있습니다. https://scc.suse.com/organizations에서 조직 자격 증명을 찾을 수 있습니다.

SUSE Manager Web UI에 조직 인증서를 입력합니다.

절차: 조직 인증서 입력

1. SUSE Manager Web UI에서 **관리 › 설정 마법사**를 선택합니다.
2. **설정 마법사** 페이지에서 **[조직 인증서]** 탭을 선택합니다.
3. **[새 인증서 추가]**를 클릭합니다.
4. 대화 상자에 **사용자 이름** 및 **암호**를 입력하고 **[저장]**을 눌러 확인합니다.

체크 표시 아이콘으로 인증서가 확인되면 절차: SUSE Customer Center를 사용한 동기화를 진행합니다.

절차: SUSE Customer Center를 사용한 동기화

1. Web UI에서 **관리 › 설정 마법사**로 이동합니다.
2. **설정 마법사** 페이지에서 **[SUSE 제품]** 탭을 선택합니다. 이전에 SUSE Customer Center에 등록한 경우 제품 목록이 테이블을 채웁니다. 이 작업에는 몇 분 정도 걸릴 수 있습니다. 오른쪽**SUSE 고객 센터에서 제품 카탈로그 새로 고침** 섹션에서 작업 진행 상황을 모니터링 할 수 있습니다. 제품 표에는 아키텍처, 채널 및 상태 정보가 나열됩니다.
3. 표시되는 제품의 목록을 필터링하려면 **Filter by product description** 또는 **Filter by architecture**를 사용하십시오. SUSE Linux Enterprise 클라이언트가 **x86_64** 아키텍처 기반인 경우 페이지의 스크롤을 내려 이 채널에 대한 확인란을 선택합니다.
   - 각 채널의 왼쪽에 있는 확인란을 선택하여 채널을 SUSE Manager에 추가합니다. 설명의 왼쪽에 있는 화살표 기호를 클릭하여 제품을 펼치고 사용할 수 있는 모듈을 나열합니다.
   - **[제품 추가]**를 클릭하여 제품의 동기화를 시작합니다.

채널을 추가하면 SUSE Manager가 동기화할 채널을 예약합니다. SUSE Manager가 SUSE Customer Center에 위치한 SUSE 레포지토리에서 서버의 로컬 **/var/spacewalk/** 디렉토리로 채널 소프트웨어 소스를 복사하므로 이 작업에는 시간이 오래 걸릴 수 있습니다.

일부 환경에서는 커널에서 제공되는 Transparent Huge Pages 로 인해 PostgreSQL 워크로드의 속도가 크게 느려질 수 있습니다.

Transparant Huge Pages 를 비활성화하려면 **transparent_hugepage** 커널 파라미터를 **안 함**으로 설정합니다. 변경은 **/etc/default/grub**에서 수행되고 **GRUB_CMDLINE_LINUX_DEFAULT** 라인에 추가되어야 하며, 그러한 예는 다음과 같습니다.

```
GRUB_CMDLINE_LINUX_DEFAULT="resume=/dev/sda1 splash=silent quiet
showopts elevator=none transparent_hugepage=never"
```

> 새 구성을 작성하려면 **grub2-mkconfig -o /boot/grub2/grub.cfg** 명령을 실행합니다.

/var/log/rhn/reposync 디렉토리의 채널 로그 파일을 검토하여 채널 동기화 진행 상황을 실시간으로 모니터링합니다.

```
tail -f /var/log/rhn/reposync/<CHANNEL_NAME>.log
```

채널 동기화 프로세스가 완료되면 클라이언트를 등록할 수 있습니다. 자세한 지침은 **Client-configuration › Registration-overview**을 참조하십시오.

4.1.2. 설치 마법사

SUSE Manager의 설치를 완료하면 설정 마법사를 사용하여 마지막 몇 단계를 완료할 수 있습니다. 설정 마법사를 사용하면 HTTP 프록시, 조직 인증서 및 SUSE 제품을 구성할 수 있습니다.

설정 마법사는 SUSE Manager Web UI에 처음으로 로그인하면 기본적으로 표시됩니다. **관리 › 설정 마법사**로 이동하여 설정 마법사에 직접 액세스할 수도 있습니다.

HTTP 프록시 구성

SUSE Manager는 프록시를 사용하여 SUSE Customer Center(SCC) 또는 기타 원격 서버에 연결할 수 있습니다. 프록시를 구성하려면 **HTTP 프록시**로 이동합니다.

프록시의 호스트 이름을 입력합니다. **<hostname>:<port>** 구문을 사용합니다. 예: **<example.com>:8080**.

필드를 지워 프록시의 사용을 비활성화할 수 있습니다.

> SUSE Manager 프록시의 사용자 이름 또는 암호를 선택할 때 **@** 또는 **:** 문자가 포함되지 않아야 합니다. 이러한 문자는 예약되어 있습니다.

조직 인증서 구성

SUSE Customer Center 계정은 조직의 관리 계정과 연결됩니다. SUSE Customer Center 액세스는 조직 내의 다른 사용자와 공유될 수 있습니다. **조직 인증서** 탭으로 이동하여 조직 내의 사용자에게 SUSE Customer Center 계정에 액세스할 수 있는 권한을 부여합니다.

[새 인증서 추가]를 클릭하고 액세스 권한을 부여할 사용자의 사용자 이름 및 암호를 입력한 후 **[저장]**을 클릭합니다. 액세스 권한을 부여한 사용자를 위한 새 인증서 카드가 표시됩니다. 카드에서 이 버튼을 사용하여 액세스를 수정하거나 철회합니다.

- 인증서 유효성 검사 상태를 확인합니다(녹색 체크 표시 또는 빨간색 엑스자 아이콘). SCC로 인증서를 다시 확인하려면 아이콘을 클릭합니다.
- 서버 간 동기화를 위한 기본 인증서를 설정합니다(노란색 별 모양 아이콘).
- 특정 인증서에 연결된 서브스크립션이 나열됩니다(목록 아이콘).
- 인증서를 편집합니다(연필 아이콘).
- 인증서를 삭제합니다(휴지통 아이콘).

제품 구성

SUSE 서브스크립션을 통해 다양한 제품에 액세스할 수 있습니다. **제품** 탭으로 이동하여 사용할 수 있는 제품을 찾아보고 SUSE Customer Center를 통해 SUSE Manager와(과) 동기화합니다.

필터를 사용하면 설명 또는 아키텍처를 기준으로 제품을 검색할 수 있습니다.

목록은 구독이 있는 제품을 맨 위에 표시하는 제품 이름을 기준으로 구성됩니다. 무료로 사용 가능한 제품이 목록 끝에 나타납니다. 각 제품에 대하여 사용될 수 있는 아키텍처를 살펴볼 수 있습니다. 제품 이름 옆의 화살표를 클릭하여 연결된 채널 및 확장을 확인합니다. **[채널]** 아이콘을 클릭하여 각 제품과 연결된 전체 채널 목록을 확인합니다.

SUSE Linux Enterprise 15 이상 기반 제품의 경우 필수 패키지와만 동기화하거나 권장 제품도 포함하도록 선택할 수 있습니다. 모든 제품을 동기화하려면 **[권장에 포함]** 스위치를 켜고 필수 제품만 동기화하려면 이 스위치를 끕니다.

개별 제품을 선택하거나 선택을 취소하여 동기화할 제품을 세부적으로 설정할 수 있습니다.

선택을 완료하면 **[제품 추가]**를 클릭한 후 **[새로 고침]**을 클릭하여 동기화를 예약합니다.

각 제품에 대한 동기화 진행률이 제품 이름 옆의 진행률 표시줄에 표시됩니다. 선택한 제품에 따라 동기화에는 최대 몇 시간이 걸릴 수 있습니다. 동기화가 완료되면 새 제품을 SUSE Manager에서 사용할 수 있습니다.

동기화에 실패한 경우, 타사 GPG 키 또는 회사 방화벽이 다운로드 서버에 대한 액세스를 차단하기 때문일 수 있습니다. 오류에 대한 알림 세부사항을 확인하십시오. 제품 동기화 문제 해결에 대한 자세한 내용은 **Administration › Troubleshooting**에서 확인할 수 있습니다.

4.1.3. 웹 인터페이스 설정

SUSE Manager Web UI를 사용하려면 브라우저에서 SUSE Manager URL로 이동합니다. SUSE Manager 관리 계정을 사용하여 Web UI에 로그인합니다.

Web UI를 사용하는 중에 ⓘ 아이콘을 클릭하면 해당 섹션의 문서에 액세스할 수 있습니다.

Web UI에 처음으로 로그인하고 설정 마법사를 완료하여 사용자 기본 설정을 설정합니다. **관리 › 설정 마법사**로 이동하여 설정 마법사에 언제라도 액세스할 수도 있습니다.

초기 설정이 완료된 후 로그인하면 **홈 › 개요** 섹션으로 이동됩니다. 이 섹션에는 시스템 관련 중요 정보를 제공하는 요약 창이 포함되어 있습니다.

작업 창은 가장 일반적인 Web UI 작업에 대한 바로 가기를 제공합니다.

비활성 시스템 창은 SUSE Manager 서버로의 체크인이 중지된 모든 클라이언트를 보여줍니다. 이러한 클라이언트를 확인해야 합니다.

가장 중요한 시스템 창은 소프트웨어 업데이트가 필요한 모든 클라이언트를 보여줍니다. 목록에서 클라이언트 이름을 클릭하면 해당 클라이언트의 **시스템 › 시스템 정보** 섹션으로 이동합니다. 이 페이지에서 필수 업데이트를 적용할 수 있습니다.

최근 스케줄된 작업 창은 가장 최근 실행된 작업 및 상태를 보여줍니다. 세부 사항을 확인하려면 작업의 레이블을 클릭합니다.

보안 관련 패치 창은 클라이언트에 적용해야 하는 사용 가능한 모든 보안 패치를 보여줍니다. 클라이언트를 안전하게 유지하려면 최대한 빨리 보안 패치를 적용하는 것이 매우 중요합니다.

시스템 그룹 창은 생성된 모든 시스템 그룹 및 그러한 그룹의 클라이언트가 완전하게 업데이트되었는지를 보여줍니다.

최근 등록된 시스템 창은 최근 30일 이내에 등록한 모든 클라이언트를 보여줍니다. 목록에서 클라이언트 이름을 클릭하면 해당 클라이언트의 **시스템 › 시스템 정보** 섹션으로 이동합니다.

웹 인터페이스 탐색

SUSE Manager Web UI에서는 탐색을 지원하는 일부 표준 요소가 사용됩니다. Web UI를 사용하는 ⓘ 아이콘을 클릭하면 해당 섹션의 문서에 액세스할 수 있습니다.

상단 탐색줄

상단 탐색줄을 사용하면 시스템 전체의 기능에 액세스할 수 있습니다.

알림

알림 종 아이콘은 원 안에 읽지 않은 알림 메시지 수를 표시합니다. 알림 아이콘을 클릭하여 **홈 › 알림 메시지**로 이동합니다.

검색

검색 돋보기 아이콘을 클릭하여 검색 상자를 엽니다. 시스템(클라이언트), 패키지, 패치 또는 문서를 검색할 수 있습니다. **[검색]**을 클릭하여 관련 **고급 검색** 페이지로 이동해 검색 결과를 확인합니다.

선택한 시스템

선택한 시스템 아이콘은 현재 선택한 시스템의 수를 원 안에 표시합니다. 선택한 시스템 아이콘을 클릭하여 **시스템 › 시스템 세트 관리자 › 개요**로 이동합니다. 지우개 아이콘을 클릭하여 모든 시스템의 선택을 취소합니다. 시스템 세트 관리자에 대한 자세한 내용은 **Client-configuration › System-set-manager**에서 확인할 수 있습니다.

사용자 계정

사용자 계정 아이콘은 현재 로그인한 사용자의 이름과 함께 표시됩니다. 사용자 계정 아이콘을 클릭하여 **홈 › 사용자 계정 › 내 계정**으로 이동합니다.

조직

조직 아이콘은 현재 황성 조직의 이름과 함께 표시됩니다. 조직 아이콘을 클릭하여 **홈 › 내 조직 › 구성**으로 이동합니다.

기본 설정

톱니바퀴 아이콘을 클릭하여 **홈 › 기본 설정**으로 이동합니다.

로그아웃

종료 아이콘을 클릭하여 현재 사용자를 로그아웃하고 로그인 화면으로 돌아갑니다.

배포를 추가하거나 채널을 새로 동기화하거나 SUSE Manager 서버에 시스템을 등록하는 경우 색인이 생성되고 검색 결과에 표시되는 데 몇 분 정도 걸릴 수 있습니다. 검색 색인을 강제로 다시 작성해야 하는 경우 명령 프롬프트에서 다음 명령을 사용하십시오.

```
rhn-search cleanindex
```

왼쪽 탐색줄

왼쪽 탐색줄은 SUSE Manager Web UI의 기본 메뉴입니다.

확장

아이콘이나 메뉴 항목의 아래쪽 화살표를 클릭하면 실제로 페이지를 로드하지 않고 메뉴 트리에서 이 부분을 확장합니다.

축소

메뉴 시스템의 열린 부분을 접으려면 메뉴 항목의 위쪽 화살표를 클릭합니다.

자동 로드

메뉴 항목의 이름을 클릭하면 해당 메뉴 항목의 첫 번째 사용 가능한 페이지가 자동으로 로드되어 표시됩니다.

검색

검색 문자열을 **검색 페이지** 필드에 입력하여 메뉴 트리의 항목을 검색합니다. 사용할 수 있는 메뉴 항목은 사용자의 역할에 따라 다릅니다.

SUSE Manager 관리자만 다음 섹션에 액세스할 수 있습니다.

- **이미지**
- **사용자**
- **관리**

테이블

여러 섹션은 테이블로 정보를 제공합니다. 테이블 오른쪽 위와 아래에 위치한 뒤로 및 다음 화살표를 클릭하여 대부분의 테이블을 탐색할 수 있습니다. **홈 › 내 기본 설정**으로 이동하여 각 페이지에 표시되는 기본 항목 수를 변경합니다.

테이블 상단의 검색 창을 사용하면 대부분의 테이블에서 내용을 필터링할 수 있습니다. 정렬할 열 헤더를 클릭하여 테이블 항목을 정렬합니다. 반대로 정렬하려면 열 헤더를 다시 클릭합니다.

패치 경고 아이콘

패치는 패치 유형에 따라 세 가지 주요 아이콘으로 표시됩니다. 아이콘은 심각도에 따라 녹색, 노란색 또는 빨간색으로 표시됩니다.

	방패 아이콘은 보안 경고입니다.
	빨간색 방패는 가장 높은 우선 순위의 보안 경고입니다.
	곤충 아이콘은 버그 수정 알림입니다.
·	사각형 아이콘은 개선 사항 알림입니다.

추가적인 정보를 제공하기 위해 몇 개의 추가 아이콘이 사용됩니다.

	원형 화살표 아이콘은 패치를 적용하려면 재부팅이 필요하다는 것을 나타냅니다.
	보관 상자 아이콘은 패치가 패키지 관리에 영향을 준다는 것을 나타냅니다.

인터페이스 사용자 정의

기본적으로 SUSE Manager Web UI에서는 설치한 제품에 적절한 테마를 사용합니다. 테마를 변경하여 Uyuni 또는 SUSE Manager 색상을 반영할 수 있습니다. SUSE Manager 테마에서도 어두운 옵션을 사용할 수 있습니다. Web UI를 사용하여 테마를 변경하려면, **홈 › My 기본 설정**으로 이동하여 **스타일 테마** 섹션을 찾습니다.

기본 테마 변경에 대한 내용은 **Administration › Users**을 참조하십시오.

요청 시간 초과 값

Web UI를 사용 중이므로 SUSE Manager 서버로 요청을 보냅니다. 경우에 따라 이러한 요청은 시간이 오래 걸리거나 완전히 실패할 수 있습니다. 기본적으로 요청은 30초 후에 시간이 초과되고 요청을 다시 전송하기 위한 링크와 함께 Web UI에 메시지가 표시됩니다.

web.spa.timeout 매개 변수를 조정하여 **etc/rhn/rhn.conf** 구성 파일에서 기본 시간 초과 값을 구성할 수 있습니다. 이 매개 변수를 변경한 후 tomcat 서비스를 다시 시작하십시오. 인터넷 연결 속도가 느리거나 한 번에 여러 클라이언트에서 정기적으로 작업을 수행하는 경우 이 설정을 더 높은 숫자로 변경하면 유용할 수 있습니다.

4.1.4. 공용 클라우드 설정

클라우드 작업에서 **registercloudguest**로 SUSE Manager 서버를 등록하거나 **SUSEConnect**로 SUSE Customer Center가 제공하는 권한을 통해 업데이트를 받을 수 있는 권한을 등록해야 로그인할 수 있습니다. 자세한 내용은 **Specialized-guides › Public-cloud-guide**에서 확인할 수 있습니다.

YaST SUSE Manager 설정 절차를 실행하기 전에 저장소 장치를 설정해야 합니다. 자세한 내용은 **Installation-and-upgrade › Pubcloud-requirements**에서 참조하십시오.

클라우드 공급자의 지침에 따라 SSH를 통해 인스턴스에 연결한 후 다음 명령을 실행하여 설정을 시작합니다.

```
yast susemanager_setup
```

메시지를 따르고 설정이 완료될 때까지 기다리십시오.

YaST를 사용하여 SUSE Manager를 설정하는 방법에 대한 자세한 지침은 **Installation-and-upgrade › Server-setup**에서 참조하십시오.

공용 클라우드 모듈 활성화

공용 클라우드 인스턴스에서 SUSE Manager를 사용하려면 공용 클라우드 모듈을 활성화해야 합니다.

절차: 공용 클라우드 모듈 활성화

1. SUSE Manager 서버에서 YaST 관리 도구를 열고 **소프트웨어 › 소프트웨어 리포지토리**로 이동합니다.
2. **[추가]**를 클릭한 후 **등록 서버에서 확장 및 모듈**을 선택합니다.
3. **사용 가능한 확장** 필드에서 **Public Cloud 모듈**을 선택합니다.

명령줄을 사용하려면 다음 명령으로 모듈을 추가할 수 있습니다.

```
SUSEConnect -p sle-module-public-cloud/15.4/x86_64
```

설치 절차가 완료되면 모든 필수 모듈이 설치되었는지 확인할 수 있습니다. 명령 프롬프트에 다음을 입력:

```
SUSEConnect --status-text
```

공용 클라우드의 SUSE Manager 서버에 필요한 모듈은 다음과 같습니다.

- SUSE Linux Enterprise Server Basesystem 모듈
- Python 3 모듈
- Server Applications 모듈
- Web and Scripting 모듈
- SUSE Manager Server 모듈
- Public Cloud 모듈

Web UI에서 설정을 완료합니다.

다음과 같은 주소를 사용하여 웹 브라우저에서 SUSE Manager Web UI를 엽니다.

```
https://<public_IP>
```

관리자 계정으로 SUSE Manager Web UI에 로그인합니다. 사용자 이름과 비밀번호는 공급자에 따라 다릅니다.

표 16. 기본 관리자 계정 상세 정보

공급자	기본 사용자 이름Username	Default Password
Amazon EC2	**admin**	**<instance-ID>**
Google Compute Engine	**admin**	**<instance-ID>**
Microsoft Azure	**admin**	**<instance-name>-suma**

인스턴스 이름 또는 ID는 공용 클라우드 인스턴스 웹 콘솔 또는 명령 프롬프트에서 검색할 수 있습니다.

Amazon EC2:

```
ec2metadata --instance-id
```

Google Compute Engine:

```
gcemetadata --query instance --id
```

Microsoft Azure:

```
azuremetadata --compute --name
```

관리자 계정에 처음으로 로그인하면 자동으로 생성된 조직 이름이 제공됩니다. menu : Admin[조직]으로 이동하여 조직 이름을 편집하여 변경합니다.

관리자 계정에 처음으로 로그인하는 경우 기본 비밀번호를 변경하여 계정을 보호하십시오.

SUSE Manager 서버 설정과 관련한 자세한 내용은 **Installation-and-upgrade › Server-setup**에서 참조하십시오.

제품 추가 및 리포지토리 동기화 시작

SUSE Manager Web UI를 사용하여 필수 소프트웨어 제품을 추가하고 리포지토리 동기화를 예약하십시오. 이를 수행하기 위한 최상의 방법은 **Admin › 설정 마법사**로 이동하고 프롬프트를 따르는 것입니다.

설정 마법사에 대한 자세한 내용은 **Installation-and-upgrade › Setup-wizard**에서 참조하십시오.

Ubuntu 또는 Red Hat Enterprise Linux 클라이언트를 등록하려면 사용자 정의 리포지토리 및 채널을 설정해야 합니다. 자세한 정보는 **Client-configuration › Registration-overview**의 관련 섹션을 참조하십시오.

채널을 동기화하려면 **Software › 관리 › 채널**로 이동하십시오. 생성한 각 채널을 클릭하고 **Repositories › 동기화** 탭으로 이동한 다음 **[지금 동기화]**를 클릭합니다. 이 화면에서 동기화를 예약할 수도 있습니다.

클라이언트를 부트스트랩하기 전, 해당 제품에 대해 선택한 모든 채널이 동기화되었는지 확인하십시오.

클라이언트를 부트스트랩하기 전, 해당 제품에 대해 선택한 모든 채널이 동기화되었는지 확인하십시오.

SUSE Manager 서버의 설정이 완료되면 클라이언트를 등록할 수 있습니다. 공용 클라우드에 클라이언트를 등록하는 방법에 대한 자세한 내용은 **Client-configuration › Clients-pubcloud**을 참조하십시오.

4.1.5. PAYG 인스턴스 연결

3곳의 주요 공용 클라우드 공급자(AWS, GCP 및 Azure)에서, SUSE:

- SLES, SLES for SAP 등을 위한 맞춤형 PAYG 제품 이미지를 제공합니다.
- PAYG(으)로 제공되는 제품을 위한 영역별 RMT 서버 미러링 리포지토리를 운영합니다.

이 설명서에서는 기존 PAYG 인스턴스를 SUSE Manager 서버에 연결하는 방법을 설명하고 인스턴스에서 인증서 모음과 관련한 기본적인 정보를 제공합니다. 연결은 SUSE Manager 서버가 클라우드 RMT 호스트에 연결할 수 있도록 인증 데이터를 추출하기 위해 수행됩니다. 그런 다음 SUSE Manager 서버는 SUSE Customer Center 조직 인증서로 아직 사용할 수 없는 RMT 호스트의 제품에 액세스할 수 있습니다.

PAYG 기능 사용 전 확인 사항:

- 원하는 리포지토리에 액세스할 수 있도록 올바른 SUSE 제품 이미지(예: SLES, SLES for SAP 또는 SLE HPC)에서 PAYG 인스턴스가 시작됩니다.
- SUSE Manager 서버는 직접 또는 배스천을 통해 PAYG 인스턴스(이상적으로는 동일한 영역에 위치)에 연결됩니다.
- 기본 SUSE Customer Center 계정이 필요합니다. **Admin › 설정 마법사 › 조직 자격 증명**에 유효한 SUSE Customer Center 자격 증명을 입력합니다. 이 계정은 PAYG 인스턴스에 관계없이 부스트래핑을 위한 SUSE Manager 클라이언트 도구에 액세스하는 데 필요합니다.
- PAYG 인스턴스를 SUSE Manager로 부트스트랩하면 SUSE Manager는 PAYG 리포지토리를 비활성화한 다음, RMT 서버에서 데이터를 미러링한 리포지토리를 추가합니다. 최종 결과는 SUSE Manager 서버 자체를 통해 RMT 서버에서 동일한 리포지토리를 획득하는 PAYG 인스턴스가 됩니다. 물론 리포지토리는 여전히 주로 SCC에서 설정할 수 있습니다.

PAYG 인스턴스 연결

절차: 새 PAYG 인스턴스 연결

1. SUSE Manager Web UI에서 **관리 › 설치 마법사 › PAYG**으로 이동하고 **[PAYG 추가]**를 클릭합니다.
2. 페이지 섹션 **PAYG 연결 설명**으로 시작하십시오.
3. **설명** 필드에 설명을 추가합니다.
4. **인스턴스 SSH 연결 데이터** 페이지 섹션으로 이동합니다.
5. **호스트** 필드에 SUSE Manager에서 연결할 인스턴스 DNS 또는 IP 주소를 입력합니다.
6. **SSH 포트** 필드에 포트 번호를 입력하거나 기본값 22를 사용합니다.
7. **사용자** 필드에 클라우드에 지정된 대로 사용자 이름을 입력합니다.
8. **암호** 필드에 암호를 입력합니다.
9. **SSH 개인 키** 필드에 인스턴스 키를 입력합니다.
10. **SSH 개인 키 암호 문구** 필드에 키 암호 문구를 입력합니다.

인증 키는 항상 PEM 형식이어야 합니다.

인스턴스에 직접 연결하지 않고 SSH 배스천을 통해 연결하는 경우 절차: SSH 배스천 연결 데이터 추가를 진행합니다.

그 외의 경우, [proc-finishing-rhui-connecting]를 진행합니다.

절차: SSH 배스천 연결 데이터 추가

1. **SSH 배스천 연결 데이터** 페이지 섹션으로 이동합니다.
2. **호스트** 필드에 배스천 호스트 이름을 입력합니다.
3. **SSH 포트** 필드에 배스천 포트 번호를 입력합니다.
4. **사용자** 필드에 배스천 사용자 이름을 입력합니다.

5. **암호** 필드에 배스천 암호를 입력합니다.
6. **SSH 개인 키** 필드에 배스천 키를 입력합니다.
7. **SSH 개인 키 암호 문구** 필드에 배스천 키 암호 문구를 입력합니다.

절차: PAYG 연결 종료 명령으로 설정 프로세스를 완료하십시오.

절차: PAYG 연결 종료

1. 새로운 PAYG 연결 데이터 추가를 완료하려면 **[만들기]**를 클릭하십시오.
2. PAYG 연결 데이터 **세부 정보** 페이지로 돌아갑니다. 업데이트된 연결 상태는 **정보** 상단 섹션에 표시됩니다.
3. 연결 상태는 **관리자 > 설정 마법사 > Pay-as-you-go** 화면에도 표시됩니다.
4. 인스턴스에 대한 인증 데이터가 올바르면, **상태** 열에 "자격 증명이 업데이트됨" 메시지가 표시됩니다.

언제든 잘못된 데이터를 입력하면 새로 생성된 인스턴스가 **관리자 > 설정 마법사 > PAYG**에 표시되고 **상태** 열에 오류 메시지가 표시됩니다.

서버에서 인증 데이터를 사용할 수 있게 되면 사용 가능한 제품 목록이 업데이트됩니다.

사용 가능한 제품은 PAYG 인스턴스에 설치된 것과 동일한 제품군 및 아키텍처의 모든 버전입니다. 예를 들어, 인스턴스에 SUSE Linux Enterprise Server 15 SP1 제품이 설치되어 있으면 SUSE Linux Enterprise Server 15 SP2, SUSE Linux Enterprise Server 15 SP3, SUSE Linux Enterprise Server 15 SP4, SUSE Linux Enterprise Server 15가 **관리자 > 설정 마법사 > 제품**에 자동으로 표시됩니다.

제품이 사용 가능한 것으로 표시되면 사용자는 제품 이름 옆의 확인란을 선택하고 **[제품 추가]**를 클릭하여 SUSE Manager에 제품을 추가할 수 있습니다.

성공 메시지가 표시되면 **소프트웨어 > 채널 목록 > 전체**로 이동하여 Web UI에서 새로 추가된 채널을 확인할 수 있습니다.

각 채널의 동기화 진행 상황을 모니터링하려면 SUSE Manager 서버의 **/var/log/rhn/reposync** 디렉토리에서 로그 파일을 확인하십시오.

제품이 PAYG 인스턴스와 SUSE Customer Center 구독 중 하나에서 모두 제공되는 경우 제품 목록에 한 번만 나타납니다.

해당 제품에 속한 채널이 동기화되면 데이터는 Pay-As-You-Go 인스턴스가 아닌 SCC 구독에서 계속 가져올 수 있습니다.

인스턴스 연결 데이터 삭제

다음 절차는 인스턴스의 SSH 연결 데이터를 삭제하는 방법을 설명합니다.

절차: 인스턴스에 대한 연결 데이터 삭제

1. **관리자 > 설정 마법사 > PAYG**를 여십시오.
2. 기존 인스턴스 목록에서 인스턴스를 검색하십시오.
3. 인스턴스 세부 정보를 클릭하십시오.

4. **[삭제]** 버튼을 선택하고 선택 항목을 확인하십시오.
5. 인스턴스 목록으로 되돌아갑니다. 방금 삭제한 항목은 더 이상 표시되지 않습니다.

인스턴스 자격 증명 수집 상태

SUSE Manager 서버는 인스턴스에서 수집한 자격 증명을 사용하여 RMT 서버에 연결하고 reposync를 사용하여 패키지를 다운로드합니다. 이러한 자격 증명은 정의된 SSH 연결 데이터를 사용하여 taskomatic에 의해 10분마다 새로 고쳐집니다. RMT 서버에 대한 연결은 PAYG 인스턴스에서 수집된 마지막으로 알려진 인증 자격 증명을 항상 사용합니다.

수집된 PAYG 인스턴스 인증서의 상태는 **Status** 열 또는 인스턴스 세부 정보 페이지에 표시됩니다. 인스턴스에 연결할 수 없으면 인증서 업데이트 프로세스가 실패합니다.

인스턴스에 연결할 수 없는 경우, 자격 증명 업데이트 프로세스가 실패하고 두 번째 새로 고침 실패 후 자격 증명이 무효화됩니다. 자격 증명이 유효하지 않으면 채널 동기화가 실패합니다. 이를 방지하려면 연결된 인스턴스를 계속 실행하십시오.

SSH 연결 데이터가 명시적으로 삭제된 경우를 제외하고, PAYG 인스턴스는 SUSE Manager 서버에 연결된 상태를 유지합니다. 인스턴스에 대한 SSH 연결 데이터를 삭제하려면 절차: 인스턴스에 대한 연결 데이터 삭제 명령을 사용하십시오.

항상 SUSE Manager 서버에서 PAYG 인스턴스에 액세스할 수 있는 것은 아닙니다.

- 인스턴스가 존재하지만 중지된 경우에는 마지막으로 알려진 자격 증명을 사용하여 인스턴스에 연결을 시도합니다. 자격 증명 유효 기간은 클라우드 공급자에 따라 다릅니다.
- 인스턴스가 더 이상 존재하지 않지만 여전히 SUMA에 등록되어 있으면, 해당 인증서는 더 이상 유효하지 않으며 인증이 실패합니다. 오류 메시지는 상태 열에 표시됩니다.

오류 메시지는 인스턴스를 사용할 수 없다는 것만을 나타냅니다. 인스턴스 상태에 대한 자세한 진단은 클라우드 공급자에서 수행해야 합니다.

PAYG 인스턴스에서 다음 작업 또는 변경 사항이 발생하면 자격 증명이 작동하지 않게 됩니다. * zypper 자격 증명 파일 제거 * 가져온 인증서 제거 * **/etc/hosts**에서 클라우드 관련 항목 제거

PAYG 시스템을 클라이언트로 등록

자격 증명을 수집하는 PAYG 인스턴스를 Salt 클라이언트로 등록할 수 있습니다. 인스턴스에는 유효한 클라우드 연결이 등록되어 있어야 하며, 그렇지 않으면 채널에 액세스할 수 없습니다. 사용자가 클라우드 패키지를 제거하면 자격 증명 수집이 작동하지 않을 수 있습니다.

우선 PAYG 인스턴스를 설정하여 인증 데이터를 수집합니다. 그러면 채널을 동기화할 수 있습니다.

나머지 프로세스는 비퍼블릭 클라우드 클라이언트에서와 동일하며 채널 동기화, 자동 부트스트랩 스크립트 생성, 활성화 키 생성 및 등록 시작으로 구성됩니다.

클라이언트 등록에 대한 자세한 내용은 **Client-configuration › Registration-overview**에서 확인할 수 있습니다.

문제 해결

자격 증명 확인

- 스크립트가 자격 증명 수집에 실패하면 로그 및 Web UI에 적절한 오류 메시지가 표시되어야 합니다.
- 자격 증명이 작동하지 않으면 **reposync**에 적절한 오류가 표시되어야 합니다.

registercloudguest 설치

- 공용 클라우드 업데이트 인프라에 대한 **registercloudguest** 연결을 새로 고치거나 변경해도 자격 증명을 사용하는 데 방해가 되지 않아야 합니다.
- 클라우드 게스트 명령에 새 클라우드 연결이 등록되어 있지 않은 경우 **registercloudguest --clean**을 실행하면 문제가 발생할 수 있습니다.

4.2. SUSE Manager 프록시

4.2.1. SUSE Manager 프록시 등록

SUSE Manager 프록시 시스템은 Unified Installer으로 설치되며 부트스트랩 스크립트 또는 GUI를 사용하여 SUSE Manager에 등록된 Salt 또는 기존 클라이언트입니다.

프록시 설치에 대한 자세한 내용은 **Installation-and-upgrade › Install-proxy-unified**에서 참조하십시오.

기존 프록시를 Salt 프록시로 마이그레이션할 수 없습니다. 기존 프록시를 Salt 프록시로 변경하려면 프록시를 재설치해야 합니다. 프록시 재설치에 대한 자세한 내용은 **Installation-and-upgrade › Proxy-setup**에서 참조하십시오.

Salt 클라이언트가 성공적으로 부트스트랩된 후에는 SUSE Manager Proxy로 구성되어야 합니다.

이 절차는 활성화 키를 사용한 소프트웨어 채널 설정 및 설치된 프록시를 SUSE Manager 클라이언트로 등록하는 방법에 대해 설명합니다.

활성화 키를 생성하는 동안 올바른 하위 채널을 선택할 수 있으려면 4.3 프록시 4.3 채널과 모든 권장 및 필수 SUSE Linux Enterprise 15 SP4 채널을 완전히 다운로드했는지 확인합니다.

절차: 프록시 등록

1. **SLE-Product-SUSE-Manager-Proxy-4.3-Pool** 기본 채널을 기반으로 활성화 키를 생성합니다. 활성화 키에 대한 자세한 내용은 **Client-configuration › Activation-keys**을 참조하십시오.

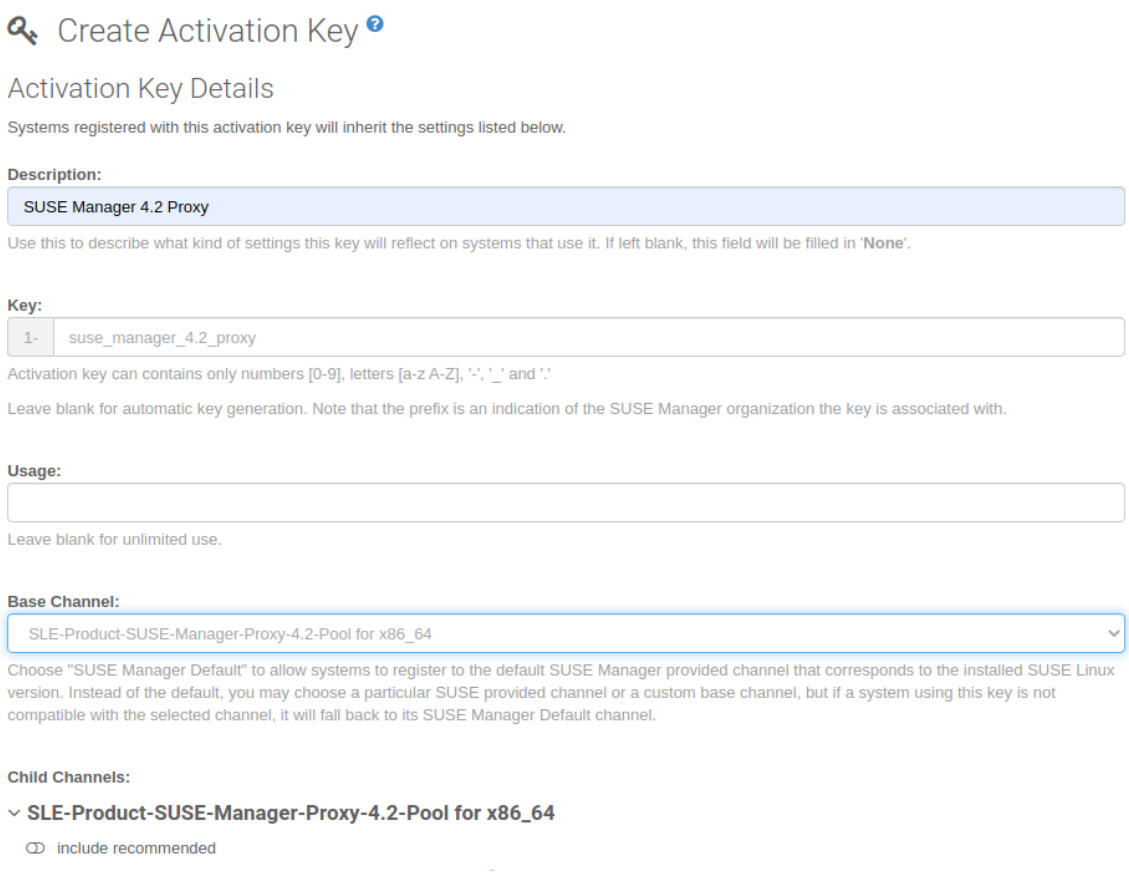


그림 1. 프록시 활성화 키

2. **하위 채널** 목록에서 **권장에 포함** 아이콘을 클릭하여 권장 채널을 선택합니다.
   - SLE-Module-Basesystem15-SP4-Pool
   - SLE-Module-Basesystem15-SP4-Updates
   - SLE-Module-Server-Applications15-SP4-Pool
   - SLE-Module-Server-Applications15-SP4-Updates
   - SLE-Module-SUSE-Manager-Proxy-4.3-Pool
   - SLE-Module-SUSE-Manager-Proxy-4.3-Updates

   SLE-Product-SUSE-Manager-Proxy-4.3-Updates 채널은 필수입니다.

   > 활성화 키를 생성하는 동안 올바른 하위 채널을 선택할 수 있으려면 4.3 프록시 4.3 채널과 모든 권장 및 필수 SUSE Linux Enterprise 15 SP4 채널을 완전히 다운로드했는지 확인합니다.

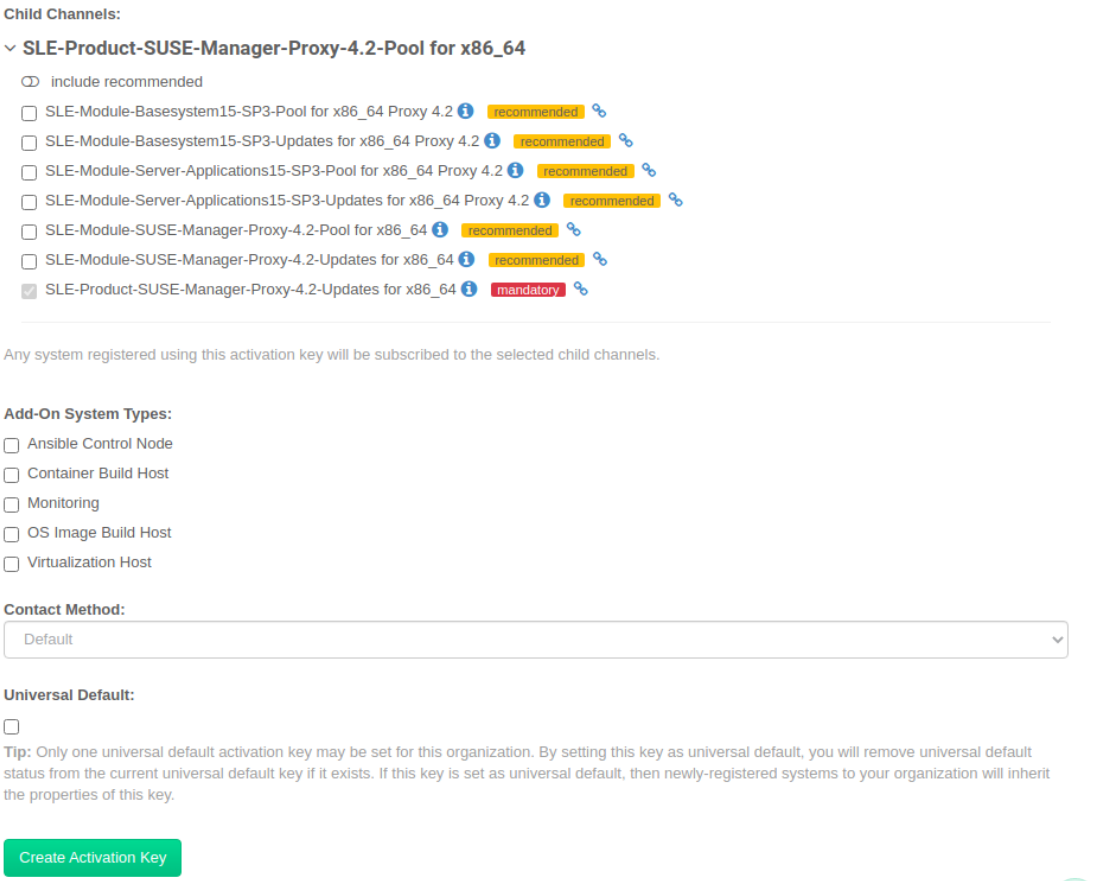


그림 2. 기본 및 하위 프록시 채널

3. 프록시를 부트스트랩하려면 부트스트랩 스크립트를 사용하십시오. 부트스트랩 스크립트에 대한 자세한 내용은 **Client-configuration › Registration-bootstrap**에서 참조하십시오.

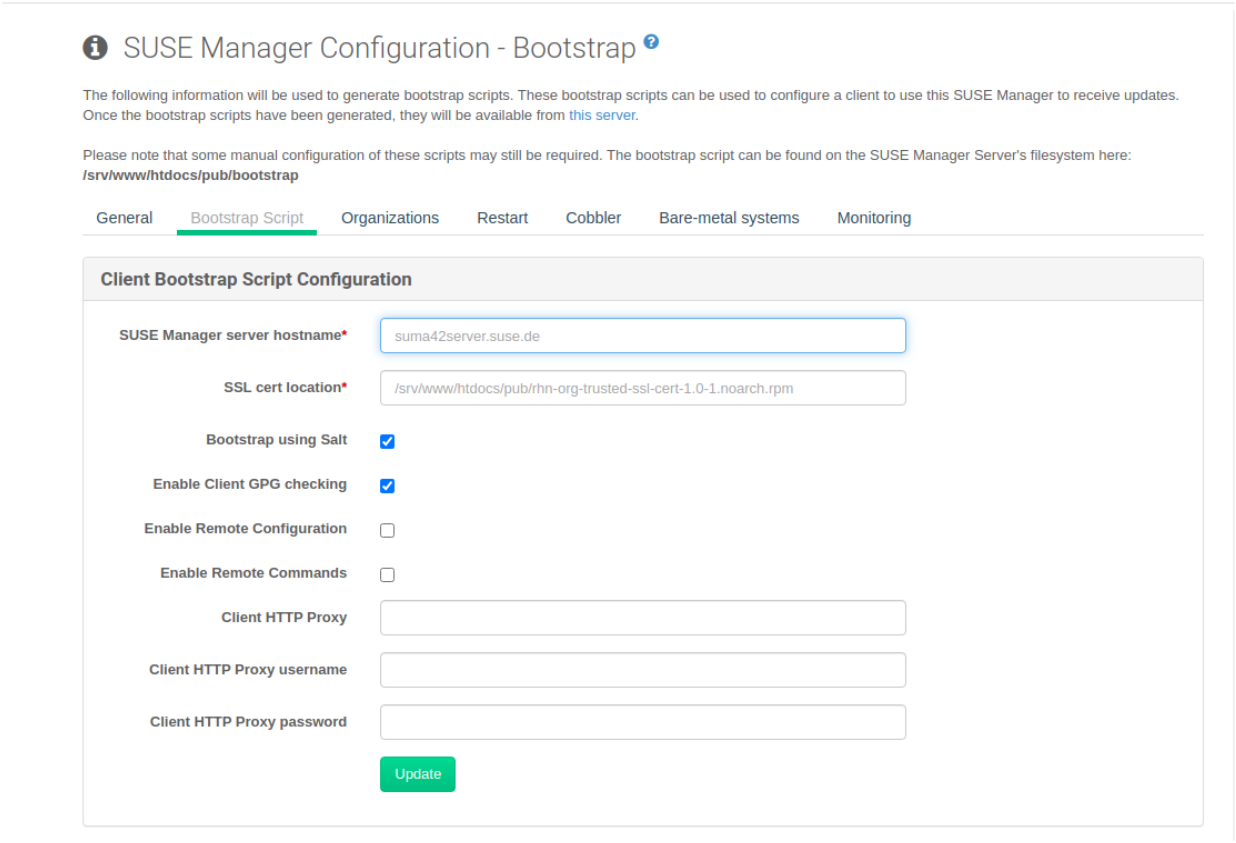


그림 3. 부트스트랩 스크립트 수정

4. 아니면, SUSE Manager Web UI에서 **시스템 › 부트스트랩**으로 이동합니다.

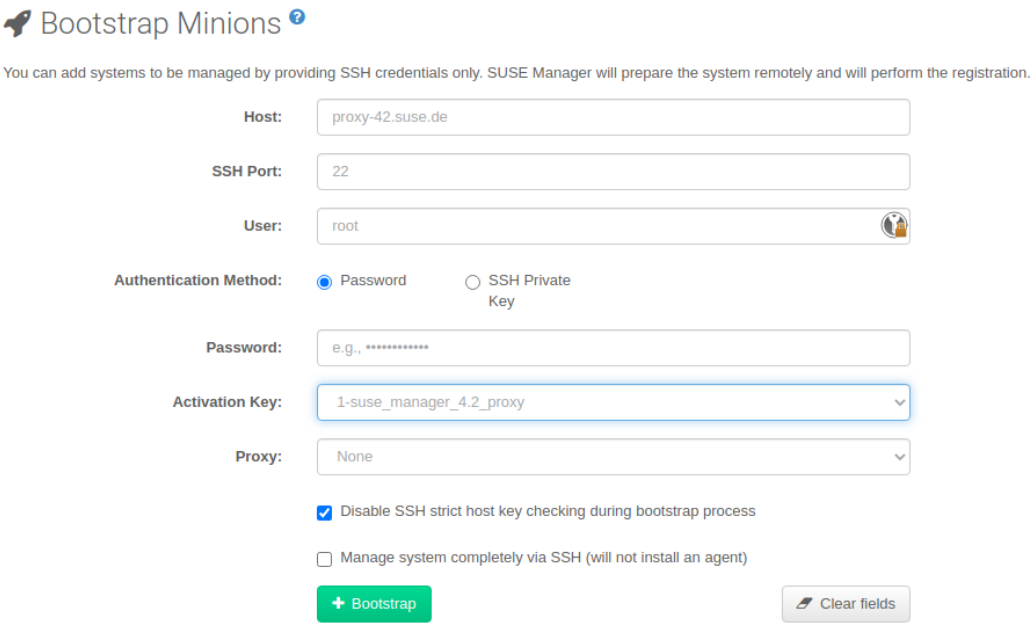


그림 4. GUI에서 프록시 부트스트랩

5. **시스템 정보 › 소프트웨어 › 소프트웨어 채널**로 이동한 후 프록시 채널 4개(**풀** 및 **업데이트**는 **SLE-PRODUCT** 및 **SLE-MODULE**의 경우)와 권장 채널이 선택되었는지 확인합니다. **SLE-PRODUCT-Pool**이 기본 채널이고 다른 채널은 하위 채널이어야 합니다.

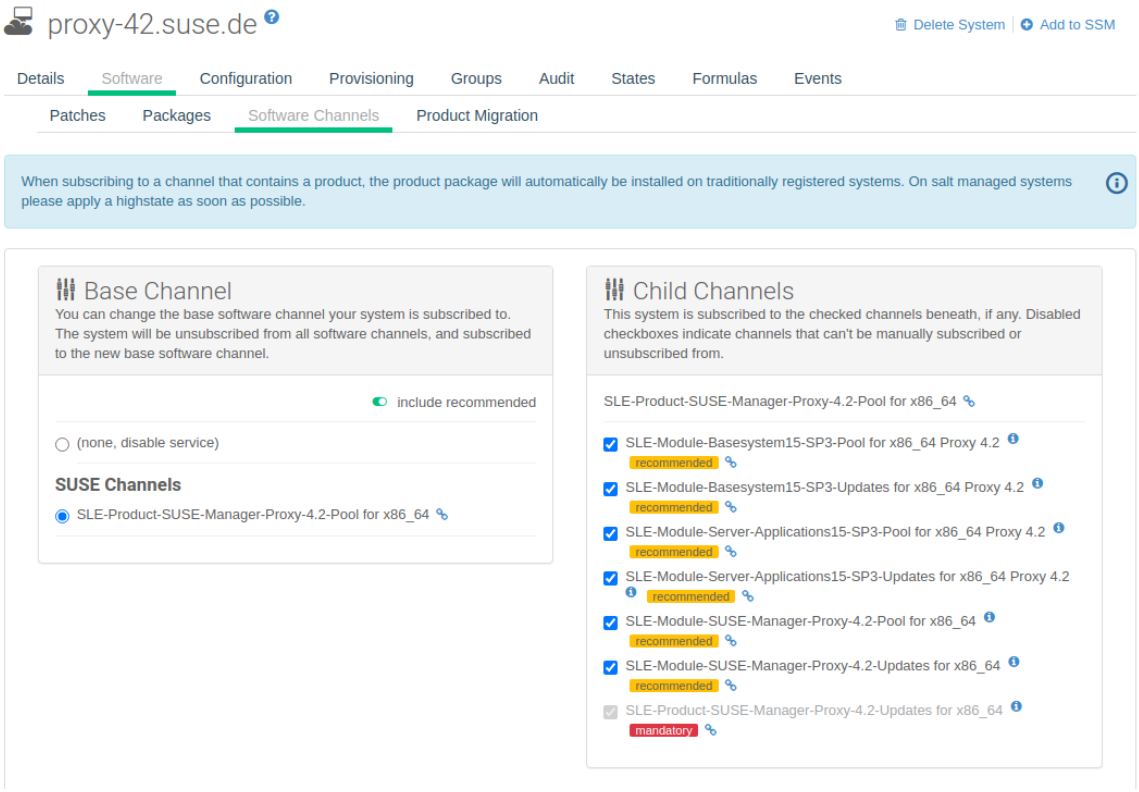


그림 5. 프록시 채널

등록한 SUSE Manager 프록시 설정: **Installation-and-upgrade › Proxy-setup**를 진행합니다.

4.2.2. SUSE Manager 프록시 설정

SUSE Manager 프록시를 추가적으로 구성해야 합니다.

Salt 프록시를 체인에서 정렬할 수 있습니다. 이 경우 업스트림 프록시의 이름은 **parent** 입니다.

TCP 포트 **4505** 및 **4506**이 프록시에서 열려 있는지 확인합니다. 프록시는 해당 포트에서 SUSE Manager 서버 또는 상위 프록시로 연결할 수 있어야 합니다.

서버 인증서 및 키 복사

프록시는 일부 SSL 정보를 SUSE Manager 서버와 공유합니다. SUSE Manager 서버 또는 상위 프록시에서 인증서 및 키를 복사합니다.

루트로 SUSE Manager 서버 또는 상위 프록시(이름: **PARENT**)를 사용하여 프록시에서 다음 명령을 입력합니다.

```
mkdir -m 700 /root/ssl-build
cd /root/ssl-build
scp root@PARENT:/root/ssl-build/RHN-ORG-PRIVATE-SSL-KEY .
scp root@PARENT:/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT .
```

```
scp root@PARENT:/root/ssl-build/rhn-ca-openssl.cnf .
```

보안 체인을 원래 상태로 유지하려면 SUSE Manager 프록시 기능의 SSL 인증서가 SUSE Manager 서버 인증서와 동일한 CA에 의해 서명되어야 합니다. 프록시와 서버에서 다른 CA로 서명된 인증서를 사용하는 것은 지원되지 않습니다.

configure-proxy.sh 실행

configure-proxy.sh 스크립트는 SUSE Manager 프록시 설정을 완료합니다.

대화형 **configure-proxy.sh** 스크립트를 실행합니다. 추가적으로 입력하지 않고 `Enter`를 눌러 스크립트가 괄호 **[]** 사이에 입력된 기본값을 사용하도록 합니다. 요청되는 설정에 대한 정보는 다음과 같습니다.

SUSE Manager 상위 항목

SUSE Manager 상위 항목은 다른 프록시 또는 SUSE Manager 서버일 수 있습니다.

HTTP 프록시

HTTP 프록시를 사용하면 SUSE Manager 프록시가 웹에 액세스할 수 있습니다. 방화벽에 의해 웹에 직접 액세스할 수 없는 경우 HTTP 프록시가 필요합니다.

전자 메일 역추적

문제를 보고할 전자 메일 주소입니다.

기존 인증서를 임포트하시겠습니까?

N을 선택합니다. 그러면 이전에 SUSE Manager 서버에서 복사한 새 인증서가 사용됩니다.

조직

다음 질문은 프록시의 SSL 인증서 사용 특성에 대한 것입니다. 물론 프록시가 기본 서버와 동일한 조직에 위치하지 않는 경우 조직은 서버에서 사용된 조직과 동일할 수 있습니다.

조직 단위

기본값은 프록시의 호스트 이름입니다.

Common Name

프록시의 인증서에 첨부된 추가 정보입니다.

시/도

프록시의 인증서에 첨부된 추가 정보입니다.

시/도

프록시의 인증서에 첨부된 추가 정보입니다.

국가 코드

SUSE Manager 설치 중 설정한 국가 코드를 **국가 코드** 필드에 입력합니다. 예를 들어, 프록시가 미국에 위치하고 SUSE Manager가 독일에 위치한 경우 프록시에 'DE'를 입력합니다.

국가 코드는 대문자 2자여야 합니다. 전체 국가 코드 목록은 https://www.iso.org/obp/

ui/#search를 참조하십시오.

E-mail

Use this field for e-mail address.

Cname 별칭(공백으로 구분)

여러 DNS CNAME 별칭으로 프록시에 액세스할 수 있는 경우 사용합니다. 그러지 않으면 비워둘 수 있습니다.

CA 비밀번호

SUSE Manager 서버의 인증서에서 사용한 비밀번호를 입력합니다.

SSH-Push Salt Minion을 프록시하기 위해 기존 SSH 키를 사용하시겠습니까?

서버의 SSH-Push Salt 클라이언트에서 사용한 SSH 키를 재사용하려면 이 옵션을 사용합니다.

구성 채널 rhn_proxy_config_1000010001을 생성하고 채우시겠습니까?

기본값 **Y**를 사용합니다.

SUSE Manager 사용자 이름

SUSE Manager 서버와 동일한 사용자 이름 및 비밀번호를 사용합니다.

Activate Advertising via SLP

Select one of the options.

CA 키 및 공인 인증서와 같이 일부가 누락된 경우, 스크립트는 필요한 파일을 통합하기 위해 실행해야 하는 명령을 출력합니다. 필수 파일이 복사되면 **configure-proxy.sh** 명령을 다시 실행합니다. 스크립트를 실행하는 동안 HTTP 오류가 수신되면 스크립트를 다시 실행합니다.

configure-proxy.sh는 **squid**, **apache2**, **salt-broker** 및 **jabberd** 등 SUSE Manager 프록시에 필요한 서비스를 활성화합니다.

프록시 시스템 및 클라이언트의 상태를 확인하려면 Web UI에서 프록시 시스템의 상세 정보 페이지(**시스템 › 프록시**, 시스템 이름)를 클릭합니다. **연결** 및 **Proxy** 하위 탭에는 다양한 상태 정보가 표시됩니다.

PXE 부팅 활성화

프로파일과 시스템 정보 동기화

프록시를 통한 PXE 부팅을 활성화하려면 SUSE Manager 프록시와 SUSE Manager 서버에서 모두 추가 소프트웨어가 설치 및 구성되어야 합니다.

1. SUSE Manager 프록시에 **susemanager-tftpsync-recv** 패키지를 설치합니다.

```
zypper in susemanager-tftpsync-recv
```

2. SUSE Manager 프록시에서 **configure-tftpsync.sh** 설정 스크립트를 실행한 후 요청되는 정보를 입력합니다.

```
configure-tftpsync.sh
```

SUSE Manager 서버 및 프록시의 호스트 이름과 IP 주소를 입력해야 합니다. 또한 프록시의 tftpboot 디렉토리 경로도 입력해야 합니다.

3. SUSE Manager 서버에 **susemanager-tftpsync**를 설치합니다.

```
zypper in susemanager-tftpsync
```

4. SUSE Manager 서버에서 **configure-tftpsync.sh**를 실행합니다. 그러면 구성이 생성되어 SUSE Manager 프록시에 업로드됩니다.

```
configure-tftpsync.sh FQDN_of_Proxy
```

5. SUSE Manager 서버에서 최초 동기화를 시작합니다.

```
cobbler sync
```

Cobbler에서 즉시 동기화해야 하는 변경을 수행한 후에도 동기화가 완료될 수 있습니다. 그러지 않으면 필요한 경우 Cobbler 동기화가 자동으로 수행됩니다. Cobbler에서 제공하는 자동 설치에 대한 자세한 내용은 **Client-configuration › Autoinst-intro**에서 확인할 수 있습니다.

SUSE Manager 프록시를 통해 PXE용 DHCP 구성

SUSE Manager에서는 클라이언트 프로비저닝을 위해 Cobbler를 사용합니다. 기본적으로 PXE(tftp)가 설치되고 활성화됩니다. 클라이언트가 DHCP를 사용하여 SUSE Manager 프록시에서 PXE 부팅을 찾을 수 있어야 합니다. 프로비저닝할 클라이언트가 포함된 영역에서 이 DHCP 구성을 사용하십시오.

```
next-server: <IP_Address_of_Proxy>
파일 이름: "pxelinux.0"
```

SUSE Manager 프록시 바꾸기

프록시는 연결된 클라이언트에 대한 정보를 저장하지 않으므로 언제든지 프록시를 바꿀 수 있습니다. 이 프로세스는 재활성화 키를 사용하여 처리되므로 프록시 기록이 손실되지 않습니다. 재활성화 키를 사용하지 않으면 대체 프록시가 새 ID를 가진 새 프록시가 됩니다. 대체 프록시의 이름 및 IP 주소는 이전 프록시와 동일해야 합니다.

또한, 기존 프록시에서 Salt 프록시로 프록시를 다시 설치하여 변경할 수도 있습니다.

프록시를 설치하는 동안 클라이언트는 SUSE Manager 서버와 통신할 수 없습니다. 프록시를 삭제한 후에는 시스템 목록이 일시적으로 올바르지 않을 수 있습니다. 이전에 프록시에 연결된 모든 클라이언트는 대신 서버에 직접 연결된 것으로 표시됩니다. 클라이언트에서 첫 번째 작업(예: 원격 명령 실행 또는 패키지나 패치 설치)이 수행된 후 이 정보가 자동으로 수정됩니다. 이 작업에는 몇 시간이 걸릴 수 있습니다.

프록시 바꾸기

기존 프록시를 종료한 후 대체 프록시를 준비하는 동안 설치된 상태를 유지하십시오. 이 시스템을 위한 재활성화 키를 생성한 후 재활성화 키를 사용하여 새 프록시를 등록하십시오. 재활성화 키를 사용하지 않으면 새 프록시에 모든 클라이언트를 다시 등록해야 합니다.

절차: 기존 프록시 바꾸기 및 등록된 클라이언트 유지

1. 마이그레이션을 시작하기 전, 필요한 경우 이전 프록시의 데이터를 저장하십시오. 새 프록시에서도 액세스할 수 있는 중앙 위치에 중요한 데이터 또는 사용자 정의 데이터를 복사하는 것이 좋습니다.
2. 기존 프록시를 종료하십시오.
3. 새 SUSE Manager 프록시를 설치합니다. 설치 지침은 **Installation-and-upgrade › Install-proxy-unified**에서 확인할 수 있습니다.
4. SUSE Manager Web UI에서 새로 설치한 SUSE Manager 프록시를 선택한 후 시스템 목록에서 삭제합니다.
5. Web UI에서 이전 프록시 시스템에 대한 재활성화 키를 만듭니다. 이전 프록시의 **System Details**탭에서 **Reactivation**을 클릭합니다. **Generate New Key**를 클릭하고 새 키를 기록해 둡니다.
6. **Installation-and-upgrade › Proxy-registration**에서의 설명과 같이 부트스트랩 스크립트를 사용하여 새 프록시를 등록하십시오. 부트스트랩 스크립트에서 **REACTIVATION_KEY** 매개변수로 재활성화 키를 설정합니다.
7. 이전에 생성한 백업에서 프록시 데이터를 복구하십시오. 이 절차의 1단계를 참조하십시오.

Salt 프록시의 경우 일부 추가 단계를 수행한 후 새 프록시를 부트스트랩해야 합니다.

절차: Salt 프록시 바꾸기 및 등록된 클라이언트 유지

1. 마이그레이션을 시작하기 전, 필요한 경우 이전 프록시의 데이터를 저장하십시오. 새 프록시에서도 액세스할 수 있는 중앙 위치에 중요한 데이터 또는 사용자 정의 데이터를 복사하는 것이 좋습니다.
2. 기존 프록시를 종료하십시오.
3. Web UI에서 이전 프록시 시스템에 대한 재활성화 키를 만듭니다. 이전 프록시의 **System Details**탭에서 **Reactivation**을 클릭합니다. **Generate New Key**를 클릭하고 새 키를 기록해 둡니다.
4. Web UI에서 **Salt › 키**로 이동하여 이전 프록시와 연결된 Salt 키를 찾은 다음 **[삭제]**를 클릭합니다.
5. 새 SUSE Manager 프록시를 설치합니다. 설치 지침은 **Installation-and-upgrade › Install-proxy-unified**에서 확인할 수 있습니다.
6. **Installation-and-upgrade › Proxy-registration**에서의 설명과 같이 부트스트랩 스크립트를 사용하여 새 프록시를 등록하십시오. 부트스트랩 스크립트에서 **REACTIVATION_KEY** 매개변수로 재활성화 키를 설정합니다.
7. 이전에 생성한 백업에서 프록시 데이터를 복구하십시오. 이 절차의 1단계를 참조하십시오.

재활성화 키 사용에 대한 자세한 내용은 **Client-configuration › Activation-keys**을 참조하십시오.

새 프록시를 설치한 후에는 다음을 수행해야 할 수도 있습니다.

- 중앙에 저장한 데이터를 새 프록시 시스템에 복사
- 필요한 다른 소프트웨어 설치
- 자동 설치를 위해 프록시가 사용되는 경우 TFTP 동기화 설정

기존에서 Salt로 프록시 변경

프록시를 다시 설치하여 기존 프록시에서 Salt 프록시로 전환할 수 있습니다. 이 방법에서는 재활성화 키 대신 원래 프록시를 등록할 때 사용한 것과 동일한 활성화 키를 다시 사용합니다. 즉, 클라이언트를 다시 등록할 필요가 없습니다.

절차: 기존 프록시를 Salt 프록시로 바꾸기

1. 마이그레이션을 시작하기 전, 필요한 경우 이전 프록시의 데이터를 저장하십시오. 새 프록시에서도 액세스할 수 있는 중앙 위치에 중요한 데이터 또는 사용자 정의 데이터를 복사하는 것이 좋습니다.
2. 프록시를 종료합니다.
3. 새 SUSE Manager 프록시를 설치한 후 바꾸려는 프록시와 IP 주소가 동일한지 확인합니다. 설치 지침은 **Installation-and-upgrade › Install-proxy-unified**에서 확인할 수 있습니다.
4. **Installation-and-upgrade › Proxy-registration**에서의 설명과 같이 부트스트랩 스크립트를 사용하여 프록시를 등록하십시오. 부트스트랩 스크립트에서 **ACTIVATION_KEYS** 매개변수로 이전 프록시와 함께 사용되는 활성화 키를 설정합니다.

새 프록시를 설치한 후에는 다음을 수행해야 할 수도 있습니다.

- 중앙에 저장한 데이터를 새 프록시 시스템에 복사
- 필요한 다른 소프트웨어 설치
- 자동 설치를 위해 프록시가 사용되는 경우 TFTP 동기화 설정

대용량 파일 제공

ISO 이미지와 같은 대용량 파일을 프록시를 통해 네트워크에 배포해야 하는 경우 PROXY_HOSTNAME 시스템으로 이동하여 대용량 파일을 **/srv/www/htdocs/pub** 디렉토리에 복사하십시오.

그 후에는 다음에서 파일을 다운로드할 수 있습니다.

```
http://PROXY_HOSTNAME/pub
```

4.2.3. 컨테이너화된 SUSE Manager 프록시 설정

SUSE Manager 프록시 컨테이너에 대한 컨테이너 호스트가 준비되면 컨테이너 설정에서 구성을 완료하기 위해 몇 가지 추가 단계가 필요합니다.

1. SUSE Manager 프록시 구성 아카이브 파일 생성
2. 설치 단계에서 준비한 컨테이너 호스트로 구성 아카이브를 전송하고 압축을 풉니다.
3. **systemd** 프록시 서비스 시작

SUSE Manager 프록시 구성 만들기 및 생성

SUSE Manager 프록시의 구성은 SUSE Manager 서버에 의해 생성되며 이 구성 생성은 컨테이너화된 각 프록시에 대해 수행되어야 합니다. SUSE Manager 구성을 생성하는 방법으로는 Web UI 또는 **spacecmd** 명령을 사용하는 두 가지 방법이 있습니다.

절차: 웹 UI를 사용한 컨테이너 서비스 구성

1. Web UI에서 **Systems › 프록시 구성**으로 이동하여 필요한 데이터를 입력합니다.
2. **Proxy FQDN** 필드에 프록시의 정규화된 도메인 이름을 입력합니다.

3. **상위 FQDN** 필드에 SUSE Manager Server 또는 다른 SUSE Manager Proxy에 대한 정규화된 도메인 이름을 입력하십시오.
4. **프록시 SSH 포트** 필드에 SSH 서비스가 SUSE Manager Proxy에서 수신 대기하는 SSH 포트를 입력하십시오. 권장 사항은 기본 포트인 8022를 유지하는 것입니다.
5. **최대 Squid 캐시 크기 [MB]** 필드에 Squid 캐시에 허용되는 최대 크기를 입력하십시오. 일반적으로 이는 컨테이너에 사용할 수 있는 저장소의 최대 60%여야 합니다.

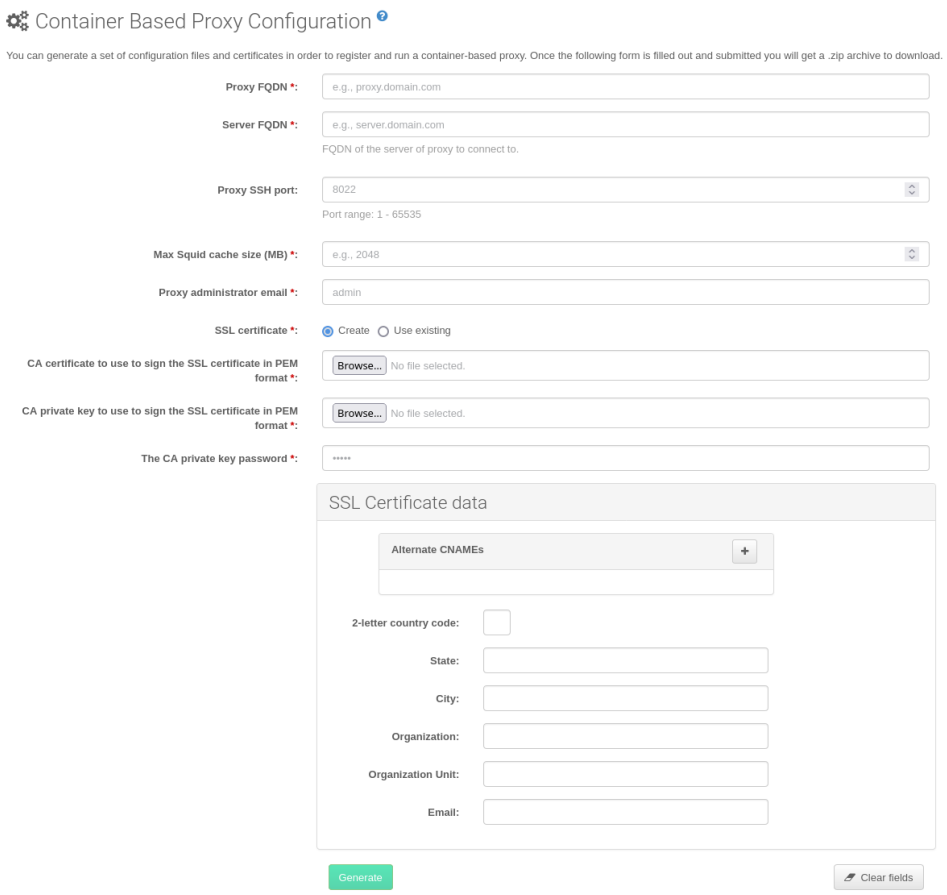
SSL 인증서 선택 목록에서 SUSE Manager 프록시에 대해 새 서버 인증서를 생성해야 하는지 또는 기존 인증서를 사용해야 하는지 선택합니다. 생성된 인증서를 SUSE Manager 기본 제공(자체 서명) 인증서로 간주할 수 있습니다.

+ 선택에 따라 새 인증서를 생성하기 위해 CA 인증서에 서명할 경로 또는 프록시 인증서로 사용할 기존 인증서 및 해당 키에 대한 경로를 입력하십시오.

+ 서버에서 생성된 CA 인증서는 **/root/ssl-build** 디렉토리에 저장됩니다.

+ 기존 또는 사용자 정의 인증서와 기업 및 중간 인증서의 개념에 대한 자세한 내용은 **Administration › Ssl-certs-imported**에서 확인할 수 있습니다.

1. **[생성]**을 클릭하여 SUSE Manager Server에 새 프록시 FQDN을 등록하고 컨테이너 호스트에 대한 세부 정보가 포함된 구성 아카이브를 생성하십시오.
2. 잠시 후 다운로드할 파일이 표시됩니다. 이 파일을 로컬에 저장하십시오.



절차: spacecmd 명령을 사용하여 컨테이너 서비스 구성

1. 콘솔에서 다음 명령 실행:

```
spacecmd proxy_container_config_generate_cert -- <proxy_fqdn> <parent_fqdn>
<squid_max_cache> <admin_email>
```

2. 스크립트에서 제공하는 질문, 즉 SUSE Manager 자격 증명 및 CA 암호에 답하십시오.

   그러면 SUSE Manager 프록시 컨테이너에 대한 구성이 포함된 **config.tar.gz** 파일이 생성됩니다.

   spacecmd 컨테이너 프록시 생성에 대한 자세한 내용은 **Reference › Spacecmd**를 참조하십시오.

등록된 미니언이 아닌 SUSE Manager 프록시 컨테이너 구성을 생성하기 위해 **Proxy FQDN**을 사용하는 경우 시스템 목록에 새 시스템 항목이 표시됩니다. 이 새 항목은 이전에 입력한 **프록시 FQDN** 값 아래에 표시되며 **외부** 시스템 유형이 됩니다.

SUSE Manager 프록시 구성 전송

spacecmd명령 및 웹 UI 방식 모두 구성 아카이브를 생성합니다. 이 아카이브는 컨테이너 호스트에서 사용할 수 있어야 합니다.

생성된 아카이브를 컨테이너 호스트로 전송하고 구성 디렉토리(기본적으로 **/etc/uyuni/proxy**)에 압축을 풉니다.

SUSE Manager 프록시 컨테이너 시작

이제 단일 **systemctl** 명령으로 컨테이너 시작 가능:

목록 1. 절차: SUSE Manager 프록시 컨테이너 시작

```
systemctl start uyuni-proxy-pod
```

목록 2. 절차: SUSE Manager 프록시 컨테이너 시작 및 설정 영구적으로 만들기

```
systemctl enable --now uyuni-proxy-pod
```

호출하여 모든 컨테이너가 예상대로 시작되었는지 확인하십시오.

```
podman ps
```

5개의 SUSE Manager 프록시 컨테이너가 있어야 합니다.

- proxy-salt-broker
- proxy-httpd
- proxy-tftpd
- proxy-squid
- proxy-ssh

그리고 **proxy-pod** 컨테이너 포드의 일부여야 합니다.

4.2.4. 내부 레지스트리를 사용한 컨테이너화된 프록시 배포

컨테이너화된 이미지는 인터넷에 연결되지 않은 환경에서 배포할 수 있습니다. 이 경우 SUSE 레지스트리에서 내부 레지스트리로 이미지를 복사하거나 **tar** 파일에 저장할 수 있습니다.

SUSE 레지스트리에서 내부 레지스트리로 이미지 복사

이 예는 Salt 프록시의 배포만을 보여줍니다.

절차: 내부 이미지 레지스트리에서 Salt 프록시 배포

1. **registry.suse.com**에 액세스할 수 있는 시스템에서 **skopeo** 설치:

```
skopeo의 zypper
```

   이는 SUSE Manager 서버일 수 있습니다.

2. 레지스트리 간 이미지 복사:

```
httpd salt-broker squid ssh tftpd에 있는 이미지의 경우, 수행
    skopeo copy docker://registry.suse.com/suse/manager/4.3/proxy-$image:latest
docker://<your_server>/registry.suse.com/suse/manager/4.3/proxy-$image
완료
skopeo copy docker://k8s.gcr.io/pause:latest
docker://<your_server>/k8s.gcr.io/pause:latest
```

   레지스트리가 보안되지 않은 경우 모든 **skopeo** 명령에 **--dest-tls-verify=false**를 추가합니다.

3. 레지스트리가 보안되지 않은 경우(예: SSL로 구성되지 않은 경우) 다음을 편집하여 컨테이너화된 프록시 가상 머신의 **registries.insecure** 섹션에 레지스트리 도메인을 추가합니다.

```
/etc/containers/registries.conf
```

4. 포드를 시작하기 전, 내부 레지스트리에서 **pause** 이미지를 가져올 위치를 Podman에 지정합니다.

```
echo -e '[engine]\ninfra_image =
"<your_server>/pause:latest"'>>/etc/containers/containers.conf
```

5. 내부 레지스트리에서 이미지 사용을 시작하려면 **/etc/sysconfig/uyuni-proxy-systemd-services.config** 파일에서 **NAMESPACE** 값을 조정합니다.

   k3s 배포의 경우 helm install 명령 줄에 **--set repository=<your_server>**를 추가합니다.

Podman용 에어 갭 솔루션

이 예는 인터넷에 연결되지 않은 시스템에 컨테이너화된 이미지를 배포하는 방법을 보여줍니다.

절차: 에어 갭 프록시 배포

1. 포드를 시작하기 전, 내부 레지스트리에서 **pause** 이미지를 가져올 위치를 Podman에 지정합니다.

```
echo -e '[engine]\ninfra_image =
"<your_server>/pause:latest"'>>/etc/containers/containers.conf
```

이 명령은 SLE 15 SP3 및 이전 컨테이너 호스트에서 작동하지 않습니다.

2. 인터넷에 연결된 시스템의 경우 다음을 실행:

```
httpd salt-broker squid ssh tftpd에 있는 이미지의 경우, 실행
    podman pull registry.suse.com/suse/manager/4.3/proxy-$image
완료
podman pull k8s.gcr.io/pause

podman save -m -o proxy-images.tar \
    k8s.gcr.io/pause \
    registry.suse.com/suse/manager/4.3/proxy-httpd \
    registry.suse.com/suse/manager/4.3/proxy-salt-broker \
    registry.suse.com/suse/manager/4.3/proxy-squid \
    registry.suse.com/suse/manager/4.3/proxy-ssh \
    registry.suse.com/suse/manager/4.3/proxy-tftpd
```

k3s 배포의 경우 helm install 명령 줄에 **--set repository=<your_server>**를 추가합니다.

3. **proxy-images.tar**을 에어 갭 프록시로 전송합니다.
4. 필요할 때 이미지를 시작할 수 있도록 하려면 다음 명령을 실행합니다.

```
podman load -i proxy-images.tar
```

Chapter 5. 업그레이드 소개

업데이트 날짜: 2025-09-24

SUSE Manager에는 3개의 주요 구성 요소가 있으며, 이러한 구성 요소에는 모두 일반 업데이트가 필요합니다. 이 가이드에서는 SUSE Manager 서버, 프록시 및 클라이언트와 함께 일부 기본 구성 요소(예: 데이터베이스)의 업데이트에 대해 설명합니다.

일부 업데이트를 자동화할 수 있지만, 수동으로 수행해야 하는 업데이트도 있습니다.

이 가이드를 처음부터 끝까지 읽을 필요는 없습니다. 대신, 업그레이드할 구성 요소로 이동한 다음 업그레이드 대상 버전을 확인하십시오.

SUSE Manager은(는) **X.Y.Z** 버전 관리 스키마를 사용합니다. 필요한 업그레이드 절차는 변경되는 버전 번호를 확인하여 결정할 수 있습니다.

아래 버전 번호는 예시입니다. 사용 가능한 최신 옵션으로 이해하지 마십시오. SUSE는 설명 목적으로만 이 번호를 사용합니다.

주 버전 업그레이드(X 업그레이드)

주 업그레이드는 일반적으로 X.Y에서 X+1.0 또는 X+1.1로 업그레이드하는 것을 의미하며, 여기서 Y는 X 시리즈의 최신 부 버전입니다. 예:

- 버전 3.2에서 4.0 또는 4.1로 업그레이드(3.2에서 4.2 이상으로의 직접 업그레이드는 지원되지 않음).

부 버전 업그레이드(Y 업그레이드)

부 업그레이드는 X.Y에서 X.Y+1로 다음 부 버전으로 업그레이드하는 것을 의미합니다. 이를 제품 마이그레이션, 서비스 팩 마이그레이션 또는 SP 마이그레이션이라고도 합니다. 예를 들면,

- 4.2에서 4.3으로

항상 부 버전의 최신 패치 레벨로 업그레이드해야 합니다.

예: 4.2.12에서 4.3.8 이상으로

패치 수준 업그레이드(Z 업그레이드)

동일한 부 버전으로 업그레이드합니다. 이를 유지 보수 업데이트 또는 MU라고 합니다. 예를 들면,

- 4.3.7에서 4.3.8로.

SUSE Manager 서버를 업그레이드하려면, **Installation-and-upgrade › Server-intro**에서 참조하십시오.

SUSE Manager 프록시를 업그레이드하려면, **Installation-and-upgrade › Proxy-intro**에서 참조하십시오.

클라이언트를 업그레이드하는 경우 **Client-configuration › Client-upgrades**에서 참조하십시오.

서버 업그레이드 외에도 데이터베이스와 같은 기타 기본 기술도 업그레이드해야 합니다. 데이터베이스 업그레이드에 대한 자세한 정보는 **Installation-and-upgrade › Db-intro**에서 참조하십시오.

5.1. 서버 업그레이드

SUSE Manager은(는) **X.Y.Z** 버전 관리 스키마를 사용합니다. 필요한 업그레이드 절차는 변경되는 버전 번호를 확인하여 결정할 수 있습니다.

아래 버전 번호는 예시입니다. 사용 가능한 최신 옵션으로 이해하지 마십시오. SUSE는 설명 목적으로만 이 번호를 사용합니다.

주 버전 업그레이드(X 업그레이드)

주 업그레이드는 일반적으로 X.Y에서 X+1.0 또는 X+1.1로 업그레이드하는 것을 의미하며, 여기서 Y는 X 시리즈의 최신 부 버전입니다. 예:

- 버전 3.2에서 4.0 또는 4.1로 업그레이드(3.2에서 4.2 이상으로의 직접 업그레이드는 지원되지 않음).
- **Installation-and-upgrade › Server-x**에서 참조하십시오.

부 버전 업그레이드(Y 업그레이드)

부 업그레이드는 X.Y에서 X.Y+1로 다음 부 버전으로 업그레이드하는 것을 의미합니다. 이를 제품 마이그레이션, 서비스 팩 마이그레이션 또는 SP 마이그레이션이라고도 합니다. 예를 들면,

- 4.2에서 4.3으로

항상 부 버전의 최신 패치 레벨로 업그레이드해야 합니다.

예: 4.2.12에서 4.3.8 이상으로

- **Installation-and-upgrade › Server-y**에서 참조하십시오.

패치 수준 업그레이드(Z 업그레이드)

동일한 부 버전으로 업그레이드합니다. 이를 유지 보수 업데이트 또는 MU라고 합니다. 예를 들면,

- 4.3.7에서 4.3.8로.
- **Installation-and-upgrade › Server-z**에서 참조하십시오.

5.1.1. 서버 - 주 버전 업그레이드(X 업그레이드)

이 업그레이드 유형은 3.2에서 4.0으로의 업그레이드에 적용됩니다.

5.1.2. 서버 - 부 버전 업그레이드(Y 업그레이드)

YaST 온라인 마이그레이션 도구 또는 Zypper 명령줄 도구를 사용하여 SUSE Manager를 다음 부 버전으로 업그레이드할 수 있습니다. 이는 제품 마이그레이션, 서비스 팩 마이그레이션 또는 SP 마이그레이션이라고도 합니다. 이 절차는 서버를 업데이트된 복사본으로 바꾸지 않습니다. 이 작업을 현재 위치에 업그레이드라고 합니다.

예: * **4.2.x → 4.3.0** 또는 **4.1.x → 4.3.0**

버전 4.1에서 4.3으로의 업그레이드도 기본 OS를 SUSE Linux Enterprise Server 15 SP2에서 SUSE Linux Enterprise Server 15 SP4로 업그레이드하며 추가 단계를 통해 PostgreSQL 데이터베이스를 버전 12에서 14로 업그레이드할 수 있습니다. 데이터베이스 업그레이드에 대한 자세한 정보는 **Installation-and-upgrade › Db-**

migration-xy에서 확인할 수 있습니다.

업그레이드는 GNOME과 같은 그래픽 인터페이스가 아닌 텍스트 콘솔에서 실행해야 합니다. 마이그레이션을 수행할 시스템에서 실행 중인 GNOME 세션에 로그인한 경우 텍스트 콘솔로 전환해야 합니다. 원격 시스템에서 로그인한 경우는 여기에 해당하지 않습니다(GNOME을 사용하여 VNC 세션을 실행 중인 경우 제외).

업그레이드를 수행하기 전 스토리지 요구사항의 충족 여부를 확인합니다. 자세한 내용은 **Installation-and-upgrade › Hardware-requirements**에서 확인할 수 있습니다. 서비스 팩 마이그레이션 및 새 소프트웨어 패키지 다운로드로 인해 여유 공간이 충분하지 않은 경우 마이그레이션 절차로 인해 루트 파티션을 채울 수 있습니다. PostgreSQL을 업그레이드하는 경우 **/var/lib/pgsql**도 동일합니다. 이전 데이터베이스의 복사본을 사용하므로 데이터베이스 복사본을 처리할 수 있는 최소한의 충분한 공간이 있어야 합니다.

4.3으로 업그레이드 준비

업그레이드 프로세스를 시작하기 전 이전 4.1.x 또는 4.2.x SUSE Manager Server에서 Python 2 모듈(**sle-module-python2**)을 비활성화해야 합니다. 4.1.x의 경우 명령줄에서 루트로 다음을 실행:

```
SUSEConnect -d -p sle-module-python2/15.3/x86_64
```

4.2.x의 경우 명령줄에서 루트로 다음을 실행:

```
SUSEConnect -d -p sle-module-python2/15.3/x86_64
```

새 SUSE Manager 4.3에서 Python 2 모듈을 더 이상 사용할 수 없기 때문에 이 비활성화 단계가 필요합니다. SUSE Manager Server 4.3에서 Python 3 모듈(**sle-module-python3**)이 설치됩니다.

자세한 내용은 SUSE Manager 4.3 릴리스 정보에서 참조하십시오.

서버 - YaST를 사용한 부 버전 업그레이드

YaST를 사용하여 업그레이드하려면 온라인 마이그레이션 도구를 사용하십시오.

YaST에 사용할 수 있는 온라인 마이그레이션 도구가 없는 경우 **yast2-migration** 패키지 및 필요한 모든 패키지를 설치합니다. 설치한 후 YaST를 재시작하여 YaST에서 도구를 사용할 수 있도록 합니다.

절차: YaST를 사용한 업그레이드

1. 명령 프롬프트에서 루트로 Spacewalk 서비스를 중지합니다.

```
spacewalk-service stop
```

2. YaST 온라인 마이그레이션 도구를 실행합니다.

```
yast2 migration
```

사용할 수 있는 기존 업데이트가 있는 경우 YaST에서 사용자에게 알리고 먼저 설치할 것을 요청합니다. 모든 패키지 업데이트를 설치한 후 마이그레이션을 수행해야 합니다. 자세한 내용은 **Installation-and-upgrade › Server-z**에서 참조하십시오.

YaST에 가능한 마이그레이션 대상과 함께 자세한 요약 정보가 표시됩니다.

3. 적절한 대상을 선택하고 프롬프트를 따라 마이그레이션을 완료합니다.
4. 서버를 재부팅합니다.
5. 재부팅되면, PostgreSQL 데이터베이스가 버전 14로 마이그레이션될 때까지 Spacewalk 서비스가 실행되지 않습니다. 텍스트 콘솔에 root로 로그인하고 4.1 또는 4.2에서 4.3로 업그레이드하는 경우, 데이터베이스 마이그레이션 스크립트를 실행합니다.

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh
```

6. Spacewalk 서비스가 실행 중인지 확인합니다.

```
spacewalk-service start
```

spacewalk-schema-upgrade는 더 이상 필요하지 않습니다. **spacewalk-service start** 중에 자동으로 실행됩니다.

업그레이드 중 YaST가 모든 권장 패키지를 설치합니다. 이 작업으로 인해 시스템의 설치 크기가 크게 증가할 수 있습니다. 필수 패키지만 설치하려면 **/etc/zypp/zypp.conf** 구성 파일을 열고 변수를 다음과 같이 설정합니다.

```
solver.onlyRequires = true
installRecommends = false
```

이 작업으로 모든 향후 패키지 작업의 동작이 변경됩니다.

서버 - zypper를 사용한 부 버전 업그레이드

Zypper를 사용하여 업그레이드하려면 Zypper 마이그레이션 도구를 사용하십시오.

절차: zypper를 사용한 업그레이드

1. 명령 프롬프트에서 루트로 Spacewalk 서비스를 중지합니다.

```
spacewalk-service stop
```

2. Zypper 마이그레이션 도구를 실행합니다.

```
zypper migration
```

Zypper에 가능한 마이그레이션 대상과 함께 자세한 요약 정보가 표시됩니다.

3. 적절한 대상을 선택하고 프롬프트를 따라 마이그레이션을 완료합니다.

4. 서버를 재부팅합니다.
5. 재부팅되면, PostgreSQL 데이터베이스가 버전 14로 마이그레이션될 때까지 Spacewalk 서비스가 실행되지 않습니다.
6. 텍스트 콘솔에 root로 로그인하고 4.1 또는 4.2에서 4.3로 업그레이드하는 경우, 데이터베이스 마이그레이션 스크립트를 실행합니다.

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh
```

7. Spacewalk 서비스가 실행 중인지 확인합니다.

```
spacewalk-service start
```

프로세스가 실패하면 먼저 다음 문제를 확인합니다.

- Zypper에 사용할 수 있는 마이그레이션 도구가 없으면 **zypper-migration-plugin** 패키지를 설치합니다.
- 사용할 수 있는 기존 업데이트가 있는 경우 Zypper가 먼저 알림을 전송해 설치를 요청합니다. 업그레이드를 수행하기 전에 모든 업데이트를 설치해야 합니다.

5.1.3. 서버 - 패치 수준 업그레이드(Z 업그레이드)

이 업데이트 절차는 단순한 패키지 업데이트 또는 일관적인 마이크로 업데이트를 다루며, 유지보수 업데이트(MU)라고 합니다. MU 중에 사용자는 서비스를 중지하고 패키지를 업데이트하며 스크립트를 실행하여 데이터베이스를 업데이트하고 서비스를 재시작합니다.

예: **4.3.0** → **4.3.1**.

즉, 먼저 사용자는 설치된 모든 패키지의 최신 버전이 설치되어 있는지 확인합니다. 그런 다음에 데이터베이스 스키마를 업그레이드할 수 있습니다.

절차: SUSE Manager 서버에서 패키지 업데이트

기본적으로 여러 업데이트 채널은 SUSE Manager 서버를 위해 구성 및 활성화됩니다. 새 패키지와 업데이트된 패키지는 자동으로 제공됩니다.

서버를 백업한 후 업그레이드하는 것이 좋습니다.

1. SUSE Manager 서버의 명령 프롬프트에서 루트로 Spacewalk 서비스를 중지합니다.

```
spacewalk-service stop
```

2. 소프트웨어 리포지토리 새로 고침:

```
zypper ref
```

3. 사용할 수 있는 패치를 나열합니다.

```
zypper list-patches
```

4. 사용할 수 있는 모든 패치를 적용합니다.

```
zypper patch
```

이 명령은 패치에만 적용됩니다. 적용되지 않은 모든 업데이트를 적용하려면 **zypper up**을 대신 사용합니다.

5. Spacewalk 서비스를 다시 시작합니다.

```
spacewalk-service start
```

기본적으로 zypper는 10분마다 리포지토리를 새로 고칩니다(**/etc/zypp/zypp.conf**의 **repo.refresh.delay** 참조). **autorefresh**가 비활성화되면 **zypper ref**를 실행하여 모든 리포지토리를 새로 고칩니다.

명령 **spacewalk-schema-upgrade**는 더 이상 필요하지 않습니다. **spacewalk-service start** 중에 자동으로 실행됩니다.

패키지 업데이트의 영향을 받는 서비스는 업데이트 후에 자동으로 재시작되지 않습니다. 장애가 발생하지 않도록 하려면 이러한 서비스를 수동으로 재시작해야 합니다. 기존 코드를 사용하고 재시작해야 하는 애플리케이션을 확인하려면 **zypper ps**를 사용합니다.

패치 업데이트에서 재부팅이 권장되면 서버를 재시작합니다.

5.2. 프록시 업그레이드

SUSE Manager 프록시는 클라이언트와 동일한 방식으로 관리됩니다.

유지보수 업데이트(MU)는 기타 클라이언트와 동일한 방식으로 SUSE Manager 프록시에 설치할 수 있습니다. MU 업데이트는 프록시 서비스를 다시 시작해야 합니다.

프록시를 업데이트하기 전, 유지보수 기간을 예약합니다. 프록시를 통해 SUSE Manager에 등록된 클라이언트는 업데이트를 진행하는 동안 SUSE Manager에 연결할 수 없습니다. 유지보수 기간에 대한 자세한 정보는 **Administration › Maintenance-windows**에서 참조하십시오.

SUSE Manager은(는) **X.Y.Z** 버전 관리 스키마를 사용합니다. 필요한 업그레이드 절차는 변경되는 버전 번호를 확인하여 결정할 수 있습니다.

주 버전 업그레이드(X 업그레이드)

다음 주 버전으로 업그레이드합니다. 예를 들면, 3.2에서 4.0 또는 4.1로 업그레이드가 해당합니다. 이 유형의 업그레이드는 4.3에 적용되지 않습니다. **Installation-and-upgrade › Proxy-x**를 참조하십시오.

부 버전 업그레이드(Y 업그레이드)

다음 부 버전으로 업그레이드합니다. 이를 서비스 팩(SP) 마이그레이션이라고 합니다. 예를 들면, 4.1에서 4.3로의 업그레이드 또는 4.2에서 4.3로의 업그레이드가 이에 해당합니다. **Installation-and-upgrade › Proxy-y-z**를 참조하십시오.

패치 수준 업그레이드(Z 업그레이드)

동일한 부 버전으로 업그레이드합니다. 이를 유지보수 업데이트라고 합니다. 예를 들면, 4.3.0에서 4.3.1로의 업그레이드가 이에 해당합니다. **Installation-and-upgrade › Proxy-y-z**를 참조하십시오.

5.2.1. 프록시 - 주 버전 업그레이드(X 업그레이드)

SUSE Manager 프록시는 하나의 주 버전에서 다음 버전으로 업그레이드할 수 있습니다. 예를 들면, 프록시는 3.2에서 4.1로 업그레이드할 수 있지만 3.2에서 4.3로 업그레이드할 수 없습니다.

4.2에서 4.3로 업그레이드하는 방법에 대한 자세한 내용은 **Installation-and-upgrade › Proxy-y-z**에서 참조하십시오.

5.2.2. 프록시 - 부 버전 또는 패치 수준 업그레이드(Y 또는 Z 업그레이드)

프록시를 업데이트하기 전, 유지보수 기간을 예약합니다. 프록시를 통해 SUSE Manager에 등록된 클라이언트는 업데이트를 진행하는 동안 SUSE Manager에 연결할 수 없습니다. 유지보수 기간에 대한 자세한 정보는 **Administration › Maintenance-windows**에서 참조하십시오.

SUSE Manager Proxy 4.0을 업그레이드할 때 버전 4.1 또는 4.2를 대상 제품으로 업그레이드하는 옵션을 무시하십시오. 항상 SUSE Manager Proxy 4.0에서 SUSE Manager Proxy 4.3로 업그레이드만 선택하십시오.

JeOS 이미지 기반 SUSE Manager Proxy 4.2 업그레이드를 수행하는 경우 **kernel-default-base** 패키지를 제거한 후 마이그레이션을 진행하십시오.

프록시 업데이트(Y)

프록시를 업데이트하려면 **제품 마이그레이션**을 사용합니다.

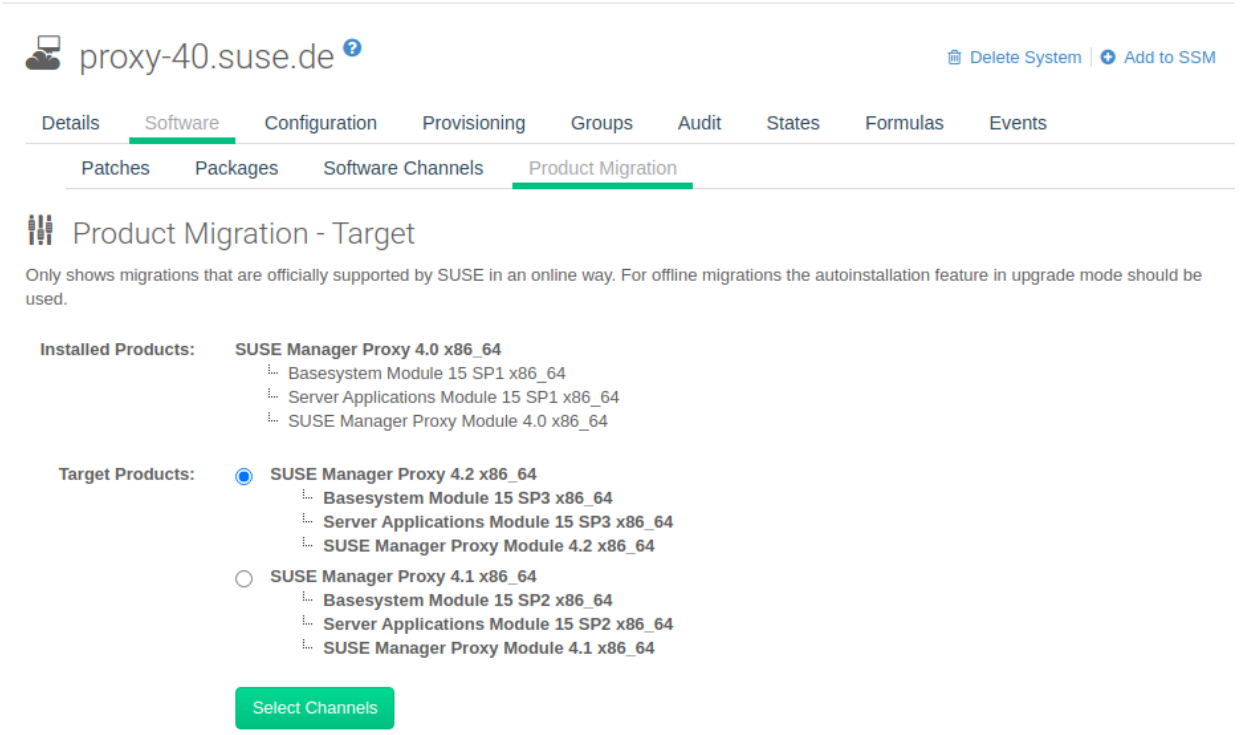


그림 6. 프록시 제품 마이그레이션(대상)

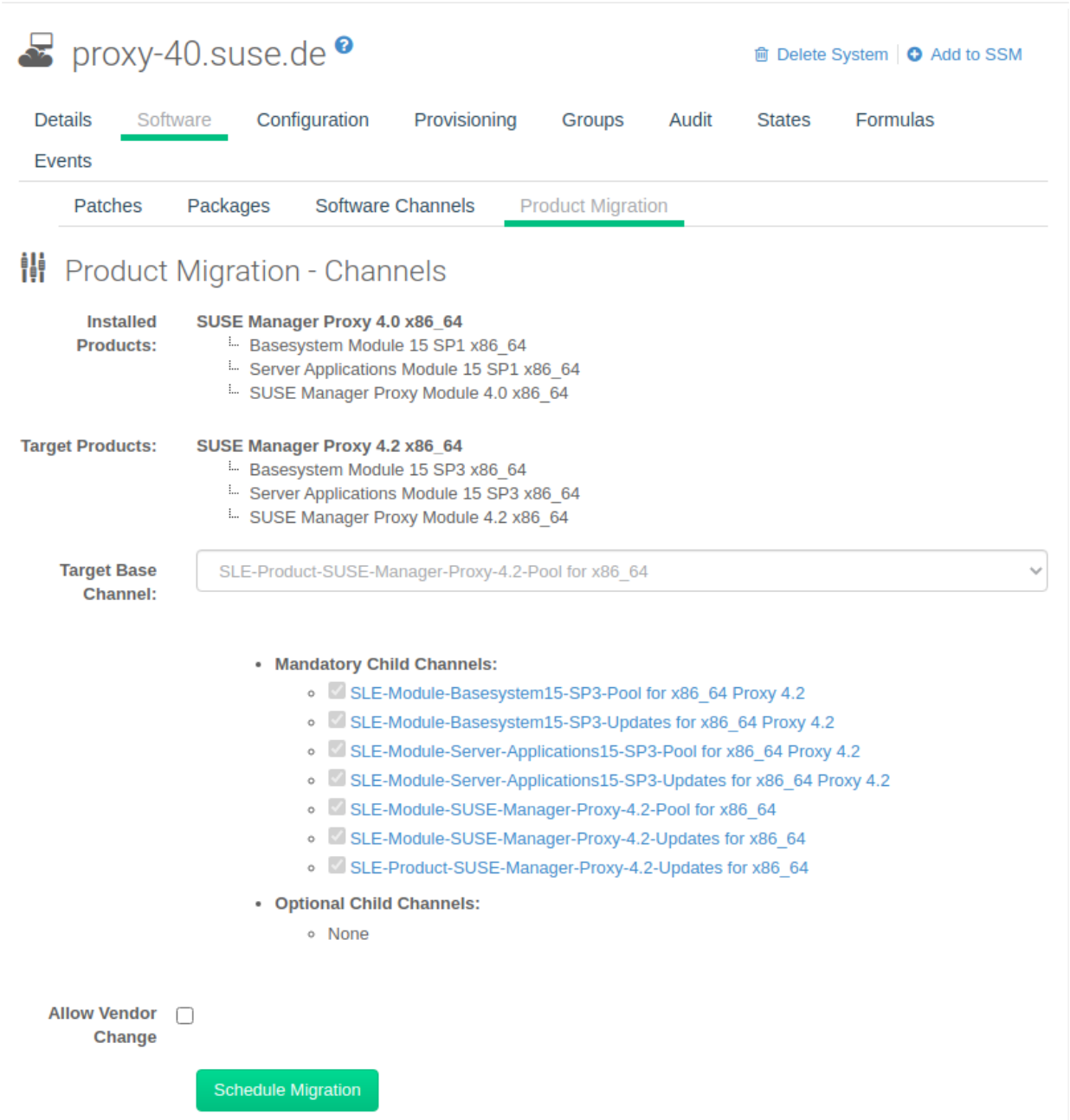


그림 7. 프록시 제품 마이그레이션(채널)

프록시 업데이트(Z)

프록시를 업데이트하려면 먼저 프록시 서비스를 중지한 후 소프트웨어를 업데이트하고 마지막으로 프록시 서비스를 재시작합니다.

절차: SUSE Manager 프록시 업데이트

1. SUSE Manager 프록시에서 프록시 서비스를 중지합니다.

```
spacewalk-proxy stop
```

2. SUSE Manager 서버 Web UI에서 **시스템 › 프록시**로 이동하여 프록시의 이름을 클릭합니다.

3. 프록시에서 업데이트할 패키지를 선택한 후 선택 사항을 적용합니다.
4. SUSE Manager 프록시에서 프록시 서비스를 시작합니다.

```
spacewalk-proxy start
```

여러 프록시를 업데이트해야 할 경우 SUSE Manager 서버에서 이 명령 시퀀스의 작업 체인을 생성할 수 있습니다. 작업 체인을 사용하여 여러 프록시에서 동시에 업데이트를 수행할 수 있습니다.

5.3. 데이터베이스 업그레이드

SUSE Manager의 주요 업데이트를 수행하려면 기본 데이터베이스를 업그레이드해야 할 수 있습니다.

최신 PostgreSQL로 업그레이드하려면, **Installation-and-upgrade › Db-migration-xy**에서 참조하십시오.

이 테이블은 SUSE Manager 및 SUSE Linux Enterprise Server의 각 버전에 필요한 PostgreSQL 버전을 보여줍니다.

표 17. PostgreSQL 버전

SUSE Manager 버전	운영 체제 버전	PostgreSQL 버전
SUSE Manager 4.0.0	SLES 15 SP1	PostgreSQL 10
SUSE Manager 4.1.0	SLES 15 SP2	PostgreSQL 12
SUSE Manager 4.2.0	SLES 15 SP3	PostgreSQL 13
SUSE Manager 4.3.0	SLES 15 SP4	PostgreSQL 14

5.3.1. 최신 버전으로 데이터베이스 마이그레이션

이 섹션에서는 최신 버전으로의 PostgreSQL 데이터베이스 업그레이드에 대해 설명합니다. PostgreSQL 14를 이미 사용 중인 경우에는 이 마이그레이션을 수행할 필요가 없습니다.

최신 SUSE Manager 버전으로 업그레이드하려면 기본 운영 체제에 따라 PostgreSQL 버전 13 또는 14를 사용해야 합니다.

- SUSE Linux Enterprise Server 15 SP3을 실행 중인 경우에는 PostgreSQL 13을 사용하십시오.
- SUSE Linux Enterprise Server 15 SP4를 실행 중인 경우에는 PostgreSQL 14를 사용하십시오.

업그레이드 준비

업그레이드하기 전에 기존 SUSE Manager 서버를 준비한 후 데이터베이스를 백업합니다.

PostgreSQL에서는 데이터가 **/var/lib/pgsql/data/**에 저장됩니다.

절차: 업그레이드 준비

1. 활성 PostgreSQL 버전을 확인합니다.

```
psql --version
```

2. 활성 smdba 버전을 확인합니다.

```
rpm -q smdba
```

PostgreSQL 14에는 **smdba**버전 1.7.6 이상이 필요합니다.

3. 데이터베이스를 백업하십시오. 백업에 대한 자세한 정보는 **Administration › Backup-restore**에서 참조하십시오.

PostgreSQL 업그레이드

항상 데이터베이스를 백업한 후 마이그레이션을 수행해야 합니다.

PostgreSQL 업그레이드는 일반 업그레이드와 빠른 업그레이드의 두 가지 방법으로 수행할 수 있습니다.

정기적으로 업그레이드하면 데이터베이스의 완전한 사본이 생성되므로 두 배의 기존 데이터베이스 여유 공간 크기가 필요합니다. 정기 업그레이드를 수행하기 위해서는 데이터베이스의 크기 및 스토리지 시스템의 속도에 따라 상당한 시간이 걸릴 수 있습니다.

빠른 업그레이드에는 몇 분이 걸릴 수 있으며, 추가적인 디스크 공간을 거의 사용하지 않습니다. 그러나 빠른 업그레이드가 실패하면 백업에서 데이터베이스를 복원해야 합니다. 빠른 업그레이드는 디스크 공간이 부족해지는 위험을 줄여주지만, 백업이 없거나 다시 수행할 수 없는 경우 데이터 위험이 증가합니다. 일반 업그레이드는 파일 간의 하드 링크를 생성하는 대신 데이터베이스 파일을 복사합니다.

PostgreSQL에서는 데이터가 **/var/lib/pgsql/data/**에 저장됩니다.

DB 업그레이드를 실행하기 전, PostgreSQL 사용자가 시스템에 있는지 확인하십시오. **/etc/passwd** 항목은 다음과 같아야 합니다.

```
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
```

절차: 일반 업그레이드 수행

1. 데이터베이스를 백업하십시오. 백업에 대한 자세한 정보는 **Administration › Backup-restore**에서 참조하십시오.
2. 업그레이드를 시작합니다. 스크립트 실행:

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh
```

3. 업그레이드가 완료되면, 기존 데이터베이스 디렉토리를 삭제하고 손실된 디스크 공간을 회수할 수 있습니다. 이전 디렉토리는 시작한 버전에 따라 **/var/lib/pgsql/data-pg12** 또는 **/var/lib/pgsql/data-pg10**으로 이름이 변경됩니다.

pg-migrate-x-to-y.sh 스크립트가 다음 작업을 수행합니다.

- Spacewalk 서비스 중지
- 실행 중인 데이터베이스 종료
- 최신 PostgreSQL이 설치되었는지 확인한 후 필요한 경우 설치
- 이전 버전의 PostgreSQL에서 새 기본값인 최신 버전으로 전환
- 데이터베이스 마이그레이션 시작
- SUSE Manager에서 사용할 수 있도록 조정된 PostgreSQL 구성 파일 생성
- 데이터베이스 및 Spacewalk 서비스 시작

업그레이드에 실패하면 마이그레이션 스크립트가 데이터베이스를 원래 상태로 복원하려고 시도합니다.

절차: 빠른 PostgreSQL 업그레이드 수행

1. 데이터베이스 백업을 실행하십시오. 검증된 데이터베이스 백업이 없으면 빠른 업그레이드를 시작할 수 없습니다. 백업에 대한 자세한 내용은 **Administration › Backup-restore**에서 참조하십시오.
2. 업그레이드를 시작합니다. 스크립트를 실행합니다.

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh -f
```

3. 업그레이드가 완료되면, 기존 데이터베이스 디렉토리를 삭제하고 손실된 디스크 공간을 회수할 수 있습니다. 이전 디렉토리는 시작한 버전에 따라 **/var/lib/pgsql/data-pg12** 또는 **/var/lib/pgsql/data-pg10**으로 이름이 변경됩니다.

데이터베이스 마이그레이션이 성공적으로 완료되면, 이전 버전의 PostgreSQL 데이터베이스 소프트웨어는 더 이상 필요하지 않습니다.

5.4. 클라이언트 업그레이드

클라이언트는 기본 운영 체제의 버전 관리 시스템을 사용합니다. SUSE 운영 체제를 사용하는 클라이언트의 경우, SUSE Manager Web UI 내에서 업그레이드할 수 있습니다.

클라이언트 업그레이드에 대한 자세한 정보는 **Client-configuration › Client-upgrades**에서 참조하십시오.

Chapter 6. GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections

then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum

below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document’s license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this

License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
   Permission is granted to copy, distribute and/or modify this document
   under the terms of the GNU Free Documentation License, Version 1.2
   or any later version published by the Free Software Foundation;
   with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
   A copy of the license is included in the section entitled "GNU
   Free Documentation License.
```