



U Y U N I

Uyuni 2024.01

설치 및 업그레이드 가이드

2024년02월15일



차례

설치 및 업그레이드 가이드 개요	1
1. 요구사항	2
1.1. 서버 요구사항	2
1.2. 프록시 요구사항	2
1.3. 네트워크 요구사항	3
1.3.1. 필수 네트워크 포트	4
1.4. 지원되는 클라이언트 시스템	9
1.5. 공용 클라우드 요구사항	10
1.5.1. 네트워크 요구사항	11
1.5.2. 스토리지 볼륨 준비	11
2. 설치	12
2.1. Uyuni 서버	12
2.1.1. openSUSE를 사용한 Uyuni 서버 설치	12
2.1.2. Deployment as a container	13
2.1.3. Container Management	17
2.1.4. Uyuni server and the Public Cloud	21
2.2. Uyuni 프록시	21
2.2.1. openSUSE Leap을 사용한 Uyuni 프록시 설치	21
2.2.2. Install containerized Uyuni Proxy	22
2.2.3. 컨테이너화된 Uyuni 프록시를 k3s에 설치합니다.....	24
3. 설정	26
3.1. Uyuni 서버	26
3.1.1. Uyuni 서버 설정	26
3.1.2. 설치 마법사	30
3.1.3. Web Interface Setup	31
3.1.4. 공용 클라우드 설정	35
3.1.5. PAYG 인스턴스 연결	37
3.2. Uyuni 프록시	40
3.2.1. Uyuni 프록시 등록	40
3.2.2. Uyuni 프록시 설정	41
3.2.3. 컨테이너화된 Uyuni 프록시 설정	45
3.2.4. 내부 레지스트리를 사용한 컨테이너화된 프록시 배포	48
4. 업그레이드 소개	51
4.1. 서버 업그레이드	51
4.1.1. 서버 - 부분 업그레이드	51
4.1.2. 서버 - 주요 업그레이드	53
4.2. 프록시 업그레이드	54
4.2.1. 프록시 - 주요 업그레이드	54
4.2.2. 프록시 - 부분 업그레이드	55
4.3. 데이터베이스 업그레이드	56
4.3.1. 최신 버전으로 데이터베이스 마이그레이션	56
4.4. 클라이언트 업그레이드	58
5. GNU Free Documentation License	59

설치 및 업그레이드 가이드 개요

업데이트 날짜: 2024-02-15

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

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

It is possible to use a public cloud instance to install Uyuni.

- For more information on using Uyuni on a public cloud, see [Specialized-guides > Public-cloud-guide](#).
- For more information on upgrading clients, see [Client-configuration > Client-upgrades](#).

Chapter 1. 요구사항

다음 테이블은 최소 서버 및 프록시 요구사항을 지정합니다.

1.1. 서버 요구사항

표 1. x86-64 아키텍처에 대한 서버 요구사항

소프트웨어 및 하드웨어	세부 정보	권장
openSUSE Leap 15.5	클린 설치, 최신	openSUSE Leap 15.5
CPU	-	최소 4개의 전용 64비트 CPU 코어 (x86-64)
RAM	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 360 GB for each Red Hat product
	/var/cache	Minimum 10 GB. Add 100 MB per SUSE product, 1 GB per Red Hat or other product. Double the space if the server is an ISS Master.
	Swap space	3 GB

1.2. 프록시 요구사항

표 2. 프록시 요구사항

Software and Hardware	Details	Recommendation
openSUSE Leap 15.5	Clean installation, up-to-date	openSUSE Leap 15.5
CPU		Minimum 2 dedicated 64-bit CPU cores
RAM	Test Server	Minimum 2 GB
	Production Server	Minimum 8 GB
Disk Space	/ (root directory)	Minimum 40 GB
	/srv	Minimum 100 GB
	/var/cache (Squid)	Minimum 100 GB

Uyuni 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 Uyuni 서버 간의 트래픽이 감소합니다.
- 프록시에서 `/var/cache/` 디렉토리의 크기와 Uyuni 서버에서 `/var/spacewalk/`의 크기를 동일하게 설정하면, 최초 동기화 후 대규모 트래픽이 발생하는 것을 방지할 수 있습니다.
- Uyuni 서버의 `/var/cache/` 디렉토리는 프록시에 비해 작을 수 있습니다. 크기 예상에 대한 설명은 [\[server-hardware-requirements\]](#) 섹션을 참조하십시오.

1.3. 네트워크 요구사항

이 섹션에서는 Uyuni의 네트워크 및 포트 요구사항에 대한 자세한 설명을 제공합니다.

FQDN(정규화된 도메인 이름)

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

For more information about configuring the hostname and DNS, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-network.html#sec-network-yast-change-host>.

호스트 이름 및 IP 주소

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

For more information about setting up a DNS server, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-dns.html>.

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.

For more information about configuring a proxy for access to SUSE Customer Center during a SUSE Linux Enterprise installation, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-boot-parameters.html#sec-boot-parameters-advanced-proxy>.



- Uyuni의 호스트 이름에는 대문자가 포함되지 않아야 합니다. 그렇지 않으면 `_jabberd_`에서 오류가 발생하게 됩니다. Uyuni의 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 Uyuni 서버와 클라이언트는 항상 방화벽을 사용해야 합니다. 전체 필수 포트 목록은 **Installation-and-upgrade > Ports**를 참조하십시오.

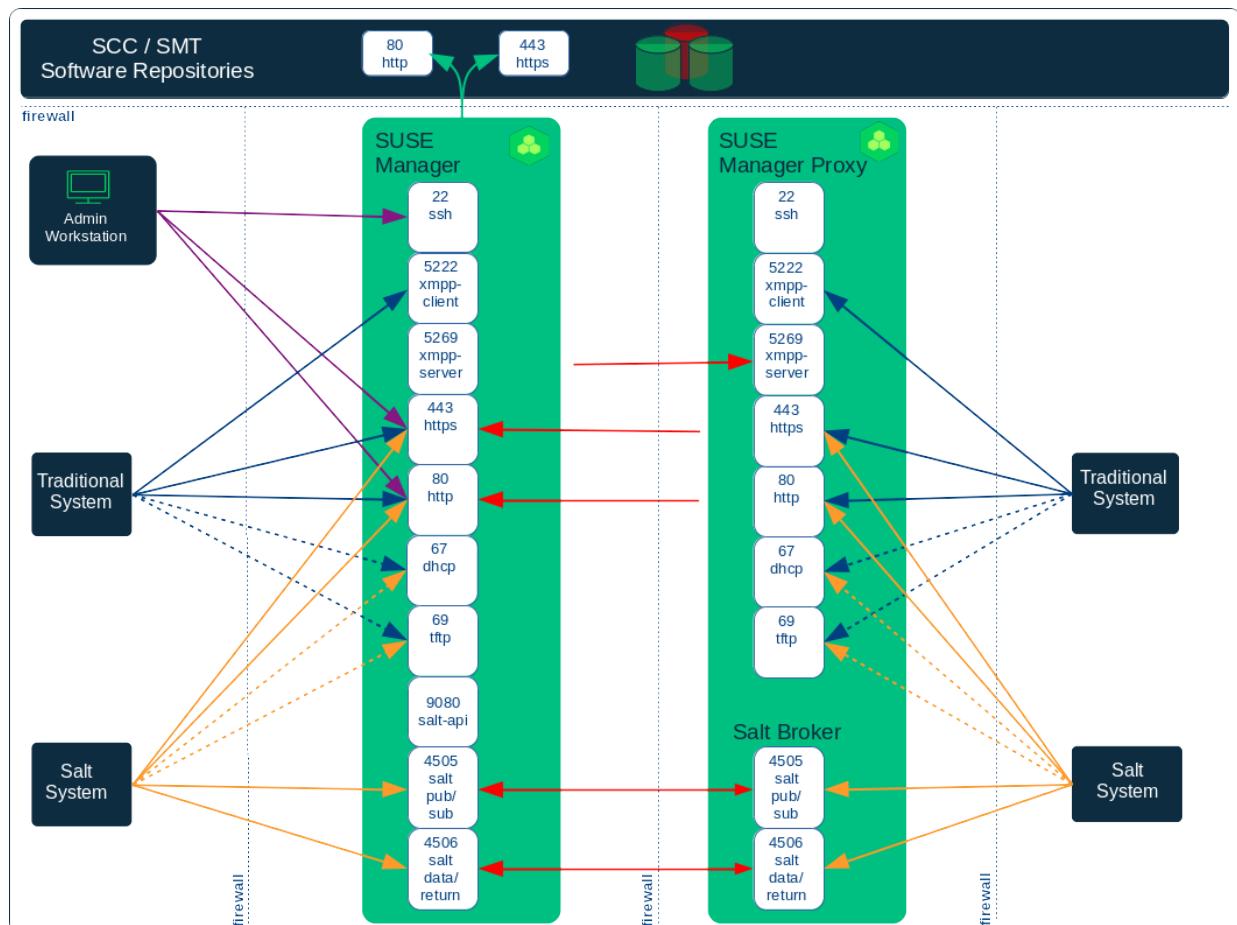
연결이 끊긴 설정 및 포트 구성에 대한 자세한 내용은 **Administration > Disconnected-setup**을 참조하십시오.

1.3.1. 필수 네트워크 포트

이 섹션에서는 Uyuni에서의 다양한 통신을 위해 사용되는 전체 포트 목록이 제공됩니다.

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

이 이미지는 Uyuni에서 사용되는 기본 포트를 보여줍니다.



1.3.1.1. 외부 인바운드 서버 포트

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

이러한 포트를 열면 외부 네트워크 트래픽이 Uyuni 서버에 액세스할 수 있습니다.

표 3. Uyuni 서버의 외부 포트 요구사항

포트 번호	프로토콜	사용 대상	참고
22			ssh-push 및 ssh-push-tunnel 통신 방법에서 필요합니다.

포트 번호	프로토콜	사용 대상	참고
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(<code>tftpsync</code>) 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	OSAD 동작을 클라이언트로 푸시하기 위해 필요합니다.
5269	TCP	jabberd	프록시와 동작을 서로 푸시하기 위해 필요합니다.
25151	TCP	Cobbler	

1.3.1.2. 외부 아웃바운드 서버 포트

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

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

표 4. Uyuni 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.
25151	TCP	Cobbler	

1.3.1.3. 내부 서버 포트

내부 포트는 Uyuni 서버에 의해 내부적으로 사용됩니다. 내부 포트는 `localhost`에서만 액세스할 수 있습니다.

대부분의 경우에는 이러한 포트를 조정할 필요가 없습니다.

표 5. Uyuni 서버의 내부 포트 요구사항

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

1.3.1.4. 외부 인바운드 프록시 포트

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

이러한 포트를 열면 외부 네트워크 트래픽이 Uyuni 프록시에 액세스할 수 있습니다.

표 6. Uyuni 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.
443	TCP	HTTPS	Web UI, 클라이언트, 서버 및 프록시(<code>tftpsync</code>) 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.

1.3.1.5. 외부 아웃바운드 프록시 포트

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

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

표 7. Uyuni 프록시의 외부 포트 요구사항

포트 번호	프로토콜	사용 대상	참고
80			서버에 연결하기 위해 사용됩니다.
443	TCP	HTTPS	SUSE Customer Center를 위해 필요합니다.
5269	TCP		서버와 동작을 서로 푸시하기 위해 필요합니다.

1.3.1.6. 외부 클라이언트 포트

Uyuni 서버와 클라이언트 사이에서 방화벽을 구성하려면 외부 클라이언트 포트가 열려 있어야 합니다.

대부분의 경우에는 이러한 포트를 조정할 필요가 없습니다.

표 8. Uyuni 클라이언트의 외부 포트 요구사항

포트 번호	방향	프로토콜	참고
22	인바운드	SSH	ssh-push 및 ssh-push-tunnel 통신 방법에서 필요합니다.
80	아웃바운드		서버 또는 프록시에 연결하기 위해 사용됩니다.
5222	아웃바운드	TCP	OSAD 동작을 서버 또는 프록시로 푸시하기 위해 필요합니다.
9090	아웃바운드	TCP	Prometheus 사용자 인터페이스에 필요합니다.
9093	아웃바운드	TCP	Prometheus 경고 관리자에 필요합니다.
9100	아웃바운드	TCP	Prometheus 노드 엑스포터에 필수입니다.
9117	아웃바운드	TCP	Prometheus Apache 엑스포터에 필수입니다.
9187	아웃바운드	TCP	Prometheus PostgreSQL에 필요합니다.

1.3.1.7. 필수 URL

Uyuni에서 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

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.

1.4. 지원되는 클라이언트 시스템

Supported operating systems for clients are listed in this table.

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 Uyuni에서 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.

표 9. 지원되는 클라이언트 시스템

Operating System	Architecture	Clients
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	✓
openSUSE Leap Micro	x86-64, aarch64	✓
openSUSE Leap 15	x86-64, aarch64	✓
Alibaba Cloud Linux 2	x86-64, aarch64	✓
AlmaLinux 9, 8	x86-64, aarch64	✓
Amazon Linux 2	x86-64, aarch64	✓
Amazon Linux 2023	x86-64, aarch64	✓
CentOS 7	x86-64, ppc64le, aarch64	✓
Debian 12, 11, 10	x86-64	✓
Oracle Linux 9, 8, 7	x86-64, aarch64	✓
Raspberry Pi OS 12	arm64, armhf	✓
Red Hat Enterprise Linux 9, 8, 7	x86-64	✓
Rocky Linux 9, 8	x86-64, aarch64	✓
Ubuntu 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-systems>를 참조하십시오.



Debian 및 Ubuntu에서는 x86-64 아키텍처가 amd64로 표시됩니다.



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

클라이언트 하드웨어를 설정할 때, Uyuni에 대한 다음 추가 사항과 함께 운영 체제 및 클라이언트에서 수행할 워크로드에 충분한 공간이 있는지 확인해야 합니다.

표 10. 클라이언트 추가 하드웨어 요구사항

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

1.5. 공용 클라우드 요구사항

이 섹션에서는 공용 클라우드 인프라에 Uyuni를 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.

- Uyuni 설정 절차는 정방향 확인 된 역방향 DNS 조회를 수행합니다. 설정 절차를 완료하고 Uyuni이 예상대로 작동하려면 이 작업이 성공해야 합니다. Uyuni를 설정하기 전에 호스트 이름 및 IP 구성을 수행하는 것이 중요합니다.
- Uyuni 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 -f에서 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.

1.5.1. 네트워크 요구사항

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



Running Uyuni on the public cloud means implementing robust security measures. It is essential to limit, filter, monitor, and audit access to the instance. SUSE strongly advises against a globally accessible Uyuni instance that lacks adequate perimeter security.

Uyuni Web UI에 액세스하려면, 네트워크 액세스 제어를 구성할 때 HTTPS를 허용하십시오. 이렇게 하면 Uyuni Web UI에 액세스할 수 있습니다.

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

1.5.2. 스토리지 볼륨 준비

Uyuni용 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 Uyuni 설정 절차를 실행하기 전에 저장소 장치를 설정해야 합니다.

리포지토리 저장소를 위한 디스크 크기는 Uyuni로 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.

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

인스턴스를 시작할 때 Uyuni 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_storage에 마운트된 XFS 파티션이 생성되고 이를 데이터베이스 및 리포지토리의 위치로 사용합니다.

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

Chapter 2. 설치

이 섹션은 Uyuni 구성 요소의 설치 프로세스를 설명합니다.

공용 클라우드 인스턴스를 사용하여 Uyuni를 설치할 수 있습니다. 공용 클라우드에서 Uyuni 사용에 대한 자세한 내용은 **Specialized-guides > Public-cloud-guide**을 참조하십시오.

2.1. Uyuni 서버

2.1.1. openSUSE를 사용한 Uyuni 서버 설치

Uyuni 서버를 openSUSE에 설치할 수 있습니다.

요구사항은 **Installation-and-upgrade > Uyuni-install-requirements**을 참조하십시오.



openSUSE Leap의 최신 버전 및 업데이트에 대한 자세한 내용은 <https://doc.opensuse.org/release-notes/>를 참조하십시오.

2.1.1.1. openSUSE Leap에 Uyuni 설치

절차: Uyuni를 사용한 openSUSE Leap 설치

1. 사용할 수 있는 모든 서비스 팩 및 패키지 업데이트를 적용하여 openSUSE Leap을 기본 시스템으로 설치합니다.
2. **yast > 시스템 > 네트워크 설정 > 호스트 이름/DNS**를 통해 확인 가능한 FQDN(정규화된 도메인 이름)을 구성합니다.
3. 리포지토리를 생성하기 위해 사용할 변수를 `root`로 설정합니다.

```
repo=repositories/systemsmanagement:/  
repo=${repo}Uyuni:/Stable/images/repo/Uyuni-Server-Pool-x86_64-  
Media1/
```

4. --로 Uyuni 서버 소프트웨어를 설치하기 위한 리포지토리를 추가합니다.

```
zypper ar https://download.opensuse.org/$repo uyuni-server-stable
```

5. --로 리포지토리에서 메타데이터를 새로 고칩니다.

```
zypper ref
```

6. --로 Uyuni 서버에 대한 패턴을 설치합니다.

```
zypper in patterns-uyuni_server
```

7. 재부팅합니다.

- Uyuni의 안정화 버전에 대한 자세한 내용은 <https://www.uyuni-project.org/pages/stable-version.html>을 참조하십시오.
- Uyuni의 개발 버전에 대한 자세한 내용은 <https://www.uyuni-project.org/pages/development-version.html>을 참조하십시오.

설치가 완료되면 Uyuni의 설정을 진행할 수 있습니다. 자세한 내용은 **Installation-and-upgrade** > **Uyuni-server-setup**에서 참조하십시오.

2.1.2. Deployment as a container

This section provides instruction on deployment of Uyuni as a container.

2.1.2.1. Deploying Uyuni as a container

2.1.2.1.1. Deployment preparations

In this section, you will gain expertise in setting up and deploying a Uyuni Server. The process encompasses the installation of Podman, Uyuni container utilities, deployment, and then initiating interaction with the container through `mgrctl`.



This section assumes you have already configured an openSUSE Leap 15.5 server, whether it is running on a physical machine or within a virtual environment.

2.1.2.1.2. Installing Podman on openSUSE Leap 15.5

To install Podman on openSUSE Leap 15.5, proceed with the following steps.

Procedure: Installing Podman

1. Open a terminal window.
2. Update the package manager's repository information to ensure you have the latest package information:

```
sudo zypper refresh
```

3. Install Podman by running the following command:

```
sudo zypper -y install podman
```

Zypper will download and install Podman along with its dependencies.

4. When the installation is complete, verify that Podman is installed by running:

```
podman --version
```

This command should display the installed version of Podman. You should now have Podman successfully installed on your openSUSE Leap 15.5 system, and you can start using it to manage containers on your system.

For more information, see <https://podman.io/>.

2.1.2.1.3. Installing Uyuni tools for use with containers

openSUSE 15.5

Procedure: Installing Uyuni Tools on openSUSE 15.5

1. Add the following repository to your openSUSE 15.5 server and accept the key.

```
sudo zypper ar
https://download.opensuse.org/repositories/systemsmanagement:/Uyuni:
/Master:/ContainerUtils/openSUSE_Leap_15.5/systemsmanagement:Uyuni:M
aster:ContainerUtils.repo
```

2. Install tools:

```
sudo zypper in mgradm mgrctl mgradm-bash-completion mgrctl-bash-
completion netavark
```

For more information on the Uyuni Container Utilities see,
[link:https://build.opensuse.org/repositories/systemsmanagement:Uyuni:
/Master:ContainerUtils\[Uyuni Container Utilities\]](https://build.opensuse.org/repositories/systemsmanagement:Uyuni:
/Master:ContainerUtils[Uyuni Container Utilities])

Repositories providing the Uyuni Container Utilities are located at:
[link:https://build.opensuse.org/repositories/systemsmanagement:Uyuni:
/Master:ContainerUtils\[Uyuni Container Utilities\]](https://build.opensuse.org/repositories/systemsmanagement:Uyuni:
/Master:ContainerUtils[Uyuni Container Utilities])

2.1.2.1.4. Deploying an Uyuni container with Podman

mgradm overview

Uyuni is deployed as a container using the mgradm tool. There are two approaches to deploying a Uyuni

server as a container. However, this section will focus on basic container deployment:

Basic deployment

You can start basic container deployment by executing the `mgradm` command. This will guide you through entering basic server variables.

For additional information, you can explore further by running `mgradm --help` from the command line.



`mgradm` will prompt for basic variables if they are not provided using command line parameters or the `mgradm.yaml` configuration file.

For security, **using command line parameters to specify passwords should be avoided**: use a configuration file with proper permissions instead.

Procedure: Deploying an Uyuni container with Podman

1. from the terminal run the following command a the sudo user.

```
sudo mgradm install podman
```



You must deploy the container as sudo or root. The following error will be displayed at the terminal if you miss this step.

```
INF Setting up uyuni network
9:58AM INF Enabling system service
9:58AM FTL Failed to open
/etc/systemd/system/uyuni-server.service for
writing error="open /etc/systemd/system/uyuni-
server.service: permission denied"
```

2. Wait for deployment to complete.
3. Open a browser and proceed to your servers FQDN.

In this section you learned how to deploy an Uyuni Server container.

Persistent volumes

Many users will want to specify locations for their persistent volumes.



If you are just testing out Uyuni you do not need to specify these volumes. `mgradm` will setup the correct volumes by default.

Specifying volume locations will generally be used for larger production deployments.

By default Podman stores its volumes in `/var/lib/containers/storage/volumes/`.

You can provide custom storage for the volumes by mounting disks on this path or the expected volume path inside it such as: `/var/lib/containers/storage/volumes/var-spacewalk`. This is especially important for the database and package mirrors.

For a list of all persistent volumes in the container see, [Installation-and-upgrade](#) → [Container-management](#)

2.1.2.2. Migrating the Uyuni server to a containerized environment

To migrate a regular Uyuni server to a container, a new machine is required.



| It is not possible to perform an in-place migration.

The old server is designated as the source server and the new machine is the destination one.

The migration procedure does not perform any hostname rename. The fully qualified domain name will be the same on the new server than on the source one. This means the DNS records need to be adjusted after the migration to use the new server.

2.1.2.2.1. Initial preparation

1. Stop the source server:

```
spacewalk-service stop
```

2. Stop the source services:

```
systemctl stop postgresql
```

2.1.2.2.2. Preparing the SSH connection

The SSH configuration and agent should be ready on the host for a passwordless connection to the source server. The migration script only uses the source server fully qualified domain name in the SSH command. This means that every other configuration required to connect needs to be defined in the `~/.ssh/config` file.

For a passwordless connection, the migration script will use an SSH agent on the server. If none is running yet, run `eval $(ssh-agent)`. Add the SSH key to the running agent using `ssh-add /path/to/the/private/key`. The private key password will be prompted.

2.1.2.2.3. Is SELinux enabled?

Verify that SELinux is enabled on the new host by running `getenforce`. If the output is `Enforcing`, SELinux is enabled. In such case, we temporarily provide this [Installation-and-upgrade](#) → [Container-management](#)

management to allow the migration script to run.

This file needs to be copied to `/root/uyuni-selinux-policy.cil` on the **new host**. The migration script will load the policy into the new host and pass it as podman argument to run the migration script.

2.1.2.2.4. Prepare for Kubernetes

Since the migration job will start the container from scratch the Persistent Volumes need to be defined before running the mgradm migrate command. Refer to the installation section for more details on the volumes preparation.

See: [Installation-and-upgrade > Container-management](#)

2.1.2.2.5. Migrating

Run the following command to install a new Uyuni server from the source one after replacing the `uyuni.source.fqdn` by the proper source server FQDN: This command will synchronize all the data from the source server to the new one: this can take time!

```
mgradm migrate podman uyuni.source.fqdn
```

또는

```
mgradm migrate kubernetes uyuni.source.fqdn
```

2.1.3. Container Management

2.1.3.1. Starting and Stopping Containers

The Uyuni 2024.01 Server container can be restarted, started, and stopped using the following commands:

To `restart` the Uyuni 2024.01 Server execute the following command:

```
# mgradm restart
5:23PM INF Welcome to mgradm
5:23PM INF Executing command: restart
```

To `start` the server execute the following command:

```
# mgradm start
5:21PM INF Welcome to mgradm
5:21PM INF Executing command: start
```

To stop the server execute the following command:

```
# mgradm stop
5:21PM INF Welcome to mgradm
5:21PM INF Executing command: stop
```

2.1.3.2. Update containers

The Uyuni 2024.01 Server container can be updated using the following command:

```
mgradm update
```

This command will bring the status of the container up-to-date and restart the server.

2.1.3.3. Update container images

2.1.3.4. Monitoring container storage space

2.1.3.5. List of persistent storage volumes

Modifications performed within containers are not retained. Any alterations made outside of persistent volumes will be discarded. Below is a list of persistent volumes for Uyuni 2024.01.

To customize the default volume locations, ensure you create the necessary volumes before launching the pod for the first time, utilizing the `podman volume create` command.



Ensure that this table aligns precisely with the volumes mapping outlined in both the Helm chart and the systemctl services definitions.

11. Persistent Volumes: **root**

Volume Name	Volume Directory
root	/root

12. Persistent Volumes: **var/**

Volume Name	Volume Directory
var-cobbler	/var/lib/cobbler
var-salt	/var/lib/salt
var-pgsql	/var/lib/pgsql
var-cache	/var/cache
var-spacewalk	/var/spacewalk
var-log	/var/log

표 13. Persistent Volumes: **srv/**

Volume Name	Volume Directory
srv-salt	/srv/salt
srv-www	/srv/www/
srv-tftpboot	/srv/tftpboot
srv-formulametadata	/srv/formula_metadata
srv-pillar	/srv/pillar
srv-susemanager	/srv/susemanager
srv-spacewalk	/srv/spacewalk

표 14. Persistent Volumes: **etc/**

Volume Name	Volume Directory
etc-apache2	/etc/apache2
etc-rhn	/etc/rhn
etc-systemd-multi	/etc/systemd/system/multi-user.target.wants
etc-systemd-sockets	/etc/systemd/system/sockets.target.wants
etc-salt	/etc/salt
etc-tomcat	/etc/tomcat
etc-cobbler	/etc/cobbler
etc-sysconfig	/etc/sysconfig
etc-tls	/etc/pki/tls
etc-postfix	/etc/postfix
ca-cert	/etc/pki/trust/anchors

2.1.3.6. Custom yaml configuration and deployment with mgradm

You also have the option to create a custom `mgradm.yaml` file, which the `mgradm` tool can utilize during deployment.

Procedure: Deploying an Uyuni container with Podman using a custom configuration file

1. Prepare an `mgradm.yaml` file similar to the following example:

```

# Database password
db:
  password: MySuperSecretDBPass
# Certificate password
cert:
  password: MySuperSecretCAPass
# SSL password
ssl:
  password: MySuperSecretSSLPassword

# If you have these you can provide them to setup your organization
# credentials
scc:
  user: ccUsername
  password: ccPassword

# Administrators email
email: email@example.com

```

- from the terminal run the following command as the sudo user. Replace uyuni.example.com with your FQDN.

```
sudo mgradm -c mgradm.yaml install podman uyuni.example.com
```

You must deploy the container as sudo or root. The following error will be displayed at the terminal if you miss this step.



```

INF Setting up uyuni network
9:58AM INF Enabling system service
9:58AM FTL Failed to open
/etc/systemd/system/uyuni-server.service for
writing error="open /etc/systemd/system/uyuni-
server.service: permission denied"

```

- Wait for deployment to complete.
- Open a browser and proceed to your servers FQDN.

In this section you learned how to deploy an Uyuni 2024.01 Server container using a custom yaml configuration.

2.1.3.7. Custom policy

2.1.4. Uyuni server and the Public Cloud

Public clouds provide Uyuni under a Bring Your Own Subscription (BYOS) or Pay-as-you-go models.

For more information on using Uyuni in the public cloud, see, [Specialized-guides > Public-cloud-guide](#).

2.2. Uyuni 프록시

2.2.1. openSUSE Leap을 사용한 Uyuni 프록시 설치

Uyuni 프록시를 openSUSE Leap15.5에 설치할 수 있습니다.

절차: Uyuni 프록시를 사용한 openSUSE Leap 설치

1. openSUSE Leap을 설치하고 사용할 수 있는 모든 패키지 업데이트를 적용합니다.
2. **yast** > 시스템 > 네트워크 설정 > 호스트 이름/DNS를 통해 확인 가능한 FQDN(정규화된 도메인 이름)을 구성합니다.
3. Uyuni 프록시 소프트웨어를 사용하여 리포지토리를 추가합니다. --로 다음을 입력합니다.

```
repo=repositories/systemsmanagement:/  
repo=${repo}Uyuni:/Stable/images/repo/Uyuni-Proxy-Pool-x86_64-  
Media1/  
zypper ar https://download.opensuse.org/$repo uyuni-proxy-stable
```

4. 리포지토리에서 메타 데이터를 새로 고칩니다. --로 다음을 입력합니다.

```
zypper ref
```

5. Uyuni 프록시용 패턴 설치: --로 다음을 입력합니다.

```
zypper in patterns-uyuni_proxy
```

6. Uyuni 프록시를 재부팅합니다.

- For more information about the stable version of Uyuni, see <https://www.uyuni-project.org/pages/stable-version.html>.
- For more information about the development version of Uyuni, see <https://www.uyuni-project.org/pages/devel-version.html>.

설치가 완료되면 Uyuni의 설정을 진행할 수 있습니다. 자세한 내용은 [Installation-and-upgrade > Uyuni-proxy-registration](#)에서 참조하십시오.

2.2.2. Install containerized Uyuni Proxy



openSUSE Leap 15.3 이상만 Uyuni 프록시 컨테이너의 컨테이너 호스트로 사용할 수 있도록 지원됩니다.

2.2.2.1. Container host requirements

표 15. Proxy Container host hardware requirements

Hardware	Details	Recommendation
CPU		Minimum 2 dedicated 64-bit CPU cores
RAM	Test Server	Minimum 2 GB
	Production Server	Minimum 8 GB
Disk Space		Minimum 100 GB

표 16. Proxy Container host software requirements

Software	Details	Remark
Connection Method	Salt	Host must be configured as a Salt client



To ensure that domain name of the Uyuni Server can be resolved by the clients:
 * 컨테이너 프록시와 클라이언트 머신 모두 DNS 서버에 연결되어 있어야 합니다. * 역방향 조회가 작동해야 합니다.

2.2.2.2. Install container services on the host system



Container host to be used as a base for Uyuni Proxy containers needs to be first registered as a client to the Uyuni Server.

For more information about registering client to the Uyuni Server, see **Client-configuration > Registration-overview**.

Uyuni Proxy 컨테이너는 podman 및 systemd를 사용하여 모든 프록시 컨테이너를 실행 및 관리합니다.

First step is to install the `mgrpxy` utility provided by the package of the same name.

The `mgrpxy` package is available in the container utils repository: pick the one matching the distribution in: <https://download.opensuse.org/repositories/systemsmanagement:/Uyuni:/Stable:/ContainerUtils/>.

To install them run:

```
zypper in helm mgrpxy
```

Procedure: Installation of container utility tool `mgrpxy` for Uyuni Proxy

Uyuni의 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 root로 로그인합니다.
2. Manually install `mgrpxy` package:

```
zypper install mgrpxy
```

2.2.2.3. Install Uyuni Proxy containers

Uyuni 프록시 컨테이너는 장기 저장을 위해 일부 볼륨을 마운트해야 합니다. 이러한 볼륨은 podman에 의해 자동으로 생성되며, `podman volume ls` 명령을 사용하여 나열할 수 있습니다. 기본적으로 podman은 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.

To install the systemd service starting the Uyuni proxy, run the `mgrpxy install podman /path/to/config.tar.gz` command.

It is possible to add custom arguments passed to podman container pod with the one or more `--podman-arg` parameters to the install command.

It is possible to modify the tag to use for container images with the `--tag=latest` parameter to the install command.



Changing the containers images and version parameters is dangerous and can cause a non-functional system.

2.2.2.3.1. 서비스에 사용자 지정 컨테이너 이미지 사용

By default, the Uyuni Proxy suite is set to use the same image version and registry path for each of its services. However, it is possible to override the default values for a specific service using the `install` parameters ending with `-tag` and `-image`.

예를 들어, 다음과 같이 사용합니다.

```
mgrpxy install podman --httpd-tag 0.1.0 --httpd-image
registry.opensuse.org/uyuni/proxy-httpd /path/to/config.tar.gz
```

It adjusts the configuration file for the httpd service, where `registry.opensuse.org/uyuni/proxy-
httpd:0.1.0` is the image to use and `0.1.0` is the version tag, before restarting it.

To reset the values to defaults, run the install command again without those parameters:

```
mgrpwy install podman /path/to/config.tar.gz
```

This command first resets the configuration of all services to the global defaults and then reloads it.

2.2.2.4. 컨테이너 호스트 방화벽에서 제공되는 서비스에 대한 네트워크 액세스 허용

Uyuni Proxy 컨테이너는 노드 포트 서비스로 작동합니다. 즉, 프록시 컨테이너 포드가 컨테이너 호스트 네트워크 TCP 및 UDP 포트 공간을 공유합니다. 이러한 이유로 컨테이너 호스트 방화벽은 Uyuni 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-setup](#)에서 설치된 Uyuni 프록시를 컨테이너로 계속 설정합니다.

2.2.3. 컨테이너화된 Uyuni 프록시를 k3s에 설치합니다.

2.2.3.1. k3s 설치

On the container host machine, install k3s (replace `<K3S_HOST_FQDN>` with the FQDN of your k3s host):

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

2.2.3.2. Installing tools

The installation requires the `mgrpwy` and `helm` packages.

The `mgrpwy` package is available in the container utils repository: pick the one matching the distribution in: <https://download.opensuse.org/repositories/systemsmanagement:/Uyuni:/Stable:/ContainerUtils/>.

To install them run:

```
zypper in helm mgrpxy
```

2.2.3.3. Uyuni 프록시 helm 차트 배포

To configure the storage of the volumes to be used by the Uyuni Proxy pod, define persistent volumes for the following claims. If you do not customize the storage configuration, k3s will automatically create the storage volumes for you.

The persistent volume claims are named:

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

Create the configuration for the Uyuni Proxy as documented in **Installation-and-upgrade > Proxy-container-setup**. Copy the configuration `tar.gz` file and then install:

```
mgrpxy install kubernetes /path/to/config.tar.gz
```

For more information see <https://kubernetes.io/docs/concepts/storage/persistent-volumes/> (kubernetes) or <https://rancher.com/docs/k3s/latest/en/storage/> (k3s) documentation.

Chapter 3. 설정

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

3.1. Uyuni 서버

3.1.1. Uyuni 서버 설정

이 섹션에서는 다음 절차를 사용한 Uyuni 서버 설정에 대해 설명합니다.

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

3.1.1.1. YaST를 사용한 Uyuni 설정

이 섹션에서는 Uyuni 설정 절차를 설명합니다.

절차: Uyuni 설정

1. Uyuni 서버에 로그인하고 YaST를 시작합니다.
2. YaST에서 **네트워크 서비스** > **Uyuni 설정**으로 이동하여 설정을 시작합니다.
3. 소개 화면에서 **Uyuni 설정** > **처음부터 Uyuni 설정**을 선택한 후 **[다음]**을 클릭하여 계속 진행합니다.
4. 상태 알림을 수신할 전자 메일 주소를 입력하고 **[다음]**을 클릭하여 계속 진행합니다. Uyuni는 종종 대용량 알림 전자 메일을 전송합니다. 필요한 경우 설정 후 전자 메일 알림을 Web UI에서 비활성화할 수 있습니다.
5. 인증서 정보 및 비밀번호를 입력합니다. 암호의 길이는 7자 이상이어야 하며, 공백, 작은따옴표 또는 큰따옴표(' 또는 \"), 느낌표(!) 또는 달러 기호(\$)를 사용할 수 없습니다. 항상 암호를 안전한 곳에 보관하십시오.



Uyuni 프록시를 설정하려면 인증서 비밀번호가 있어야 합니다.

6. **[다음]**을 클릭하여 계속합니다.
7. **Uyuni 설정** > **데이터베이스 설정** 화면에서 데이터베이스 사용자 및 암호를 입력하고 **[다음]**을 클릭하여 계속 진행합니다. 암호의 길이는 7자 이상이어야 하며, 공백, 작은따옴표 또는 큰따옴표(' 또는 \"), 느낌표(!) 또는 달러 기호(\$)를 사용할 수 없습니다. 항상 암호를 안전한 곳에 보관하십시오.
8. **[다음]**을 클릭하여 계속합니다.
9. 메시지가 표시되면 **[예]**를 클릭하여 설정을 실행합니다.
10. 설정이 완료되면 **[다음]**을 클릭하여 계속 진행합니다. Uyuni Web UI의 주소가 표시됩니다.
11. **[완료]**를 클릭하여 Uyuni의 설정을 완료합니다.

3.1.1.2. 기본 관리 계정 생성

이 섹션에서는 Uyuni에서 조직의 기본 관리 계정을 생성하는 방법을 설명합니다.



기본 관리 계정은 Uyuni에서 최상위 권한을 갖습니다. 이 계정에 대한 액세스 정보를 안전하게 유지해야 합니다.

조직 및 그룹을 위한 낮은 수준의 관리 계정을 생성하는 것이 좋습니다. 기본 관리 액세스 세부 정보를 공유하지 마십시오.



최신 브라우저 버전에서는 HSTS로 인해 Uyuni 서버 FQDN에 대한 웹 액세스가 차단될 수 있습니다.

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

1. 서버에서 <http://<server>.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT>로 이동하십시오.
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. 웹 브라우저에 Uyuni Web UI의 주소를 입력합니다. 이 주소는 설정 완료 후 제공됩니다. 자세한 내용은 [installation-and-upgrade:uyuni-server-setup.pdf](#)에서 확인할 수 있습니다.
2. Web UI에 로그인하고 **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.

Uyuni Web UI의 설정이 완료되면 **홈** > **개요** 페이지로 이동됩니다.

3.1.1.3. 옵션: 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.



Uyuni의 경우 SUSE Customer Center에서 제품 동기화는 선택 사항입니다.

소프트웨어 리포지토리를 SCC와 동기화하기 전, Uyuni에 조직 인증서를 입력해야 합니다. 조직 인증서를 통해 SUSE 제품 다운로드에 액세스할 수 있습니다. <https://scc.suse.com/organizations>에서 조직 인증서는 찾을 수 있습니다.

Uyuni Web UI에 조직 인증서를 입력합니다.

절차: 조직 인증서 입력

1. SUSE Manager Web UI에서 **기본 메뉴**, **관리**, **설정 마법사**로 이동합니다.
2. →→→ 페이지에서 **[조직 인증서]** 탭으로 이동합니다.
3. **[새 인증서 추가]**를 클릭합니다.
4. 사용자 이름 및 암호를 입력한 후 **[저장]**을 클릭합니다.

인증서가 확인되면 확인 표시 아이콘이 표시됩니다. 새 인증서를 입력하면 SUSE Customer Center와 동기화할 수 있습니다.

절차: SUSE Customer Center를 사용한 동기화

1. Uyuni Web UI에서 **관리**, **설정 마법사**로 이동합니다.
2. →→→ 페이지에서 **[SUSE 제품]** 탭을 선택합니다. 제품 목록이 채워질 때까지 잠시 기다립니다. 이전에 SUSE Customer Center로 등록한 경우 제품 목록이 테이블에 채워집니다. 이 테이블에는 아키텍처, 채널 및 상태 정보가 나열됩니다. 자세한 내용은 **Reference** > **Admin**에서 참조하십시오.

3.1. Uyuni 서버

The screenshot shows the 'Setup Wizard' interface with the 'SUSE Products' tab selected. On the left, a list of products is displayed with columns for 'Product Description', 'Arch', and 'Channels'. On the right, there's a sidebar with options to refresh the catalog and a message explaining why not all products are shown. At the bottom, there are navigation buttons for the wizard.

3. SUSE Linux Enterprise 클라이언트가 x86_64 아키텍처 기반인 경우 페이지의 스크롤을 내려 이 채널에 대한 확인란을 선택합니다.

- 각 채널의 왼쪽에 있는 확인란을 선택하여 채널을 Uyuni에 추가합니다. 설명의 왼쪽에 있는 화살표 기호를 클릭하여 제품을 펼치고 사용할 수 있는 모듈을 나열합니다.
- [제품 추가]를 클릭하여 제품의 동기화를 시작합니다.

채널을 추가하면 Uyuni가 동기화할 채널을 예약합니다. Uyuni가 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 Pages로 인해 PostgreSQL 워크로드의 속도가 크게 느려질 수 있습니다.

Transparent Huge Pages를 비활성화하려면 transparent_hugepage 커널 파라미터를 `-n`으로 설정합니다. 또한, `/etc/default/grub` 파일을 열고 `GRUB_CMDLINE_LINUX_DEFAULT` 라인을 추가하거나 수정할 수도 있습니다. 예:

```
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.

3.1.2. 설치 마법사

When you have completed your Uyuni installation, you can use the setup wizard to complete the last few steps. The setup wizard allows you to configure the HTTP proxy, organization credentials, and SUSE products.

설정 마법사는 Uyuni Web UI에 처음으로 로그인하면 기본적으로 표시됩니다. 관리 > 설정 마법사로 이동하여 설정 마법사에 직접 액세스할 수도 있습니다.

3.1.2.1. Configure the HTTP Proxy

Uyuni는 프록시를 사용하여 SUSE Customer Center(SCC) 또는 기타 원격 서버에 연결할 수 있습니다. 프록시를 구성하려면 HTTP `-->`로 이동합니다.

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

필드를 지워 프록시의 사용을 비활성화할 수 있습니다.



Uyuni 프록시의 사용자 이름 또는 암호를 선택할 때 `@` 또는 `:` 문자가 포함되지 않아야 합니다. 이러한 문자는 예약되어 있습니다.

3.1.2.2. Configure Organization Credentials

SUSE Customer Center 계정은 조직의 관리 계정과 연결됩니다. SUSE Customer Center 액세스는 조직 내의 다른 사용자와 공유될 수 있습니다. ← → 템으로 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).

3.1.2.3. 제품 구성

SUSE 서브스크립션을 통해 다양한 제품에 액세스할 수 있습니다. ← 템으로 이동하여 사용할 수 있는 제품을 찾아보고 SUSE Customer Center를 통해 Uyuni와(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 Uyuni에서 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.

3.1.3. Web Interface Setup

Uyuni Web UI를 사용하려면 브라우저에서 Uyuni URL로 이동합니다. Uyuni 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 마법사로 이동하여 설정 마법사에 언제라도 액세스할 수도 있습니다.

초기 설정이 완료된 후 로그인하면 홈 > 개요 섹션으로 이동됩니다. 이 섹션에는 시스템 관련 중요 정보를 제공하는 요약창이 포함되어 있습니다.

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

--> 창은 Uyuni 서버로의 체크인이 중지된 모든 클라이언트를 보여줍니다. 이러한 클라이언트를 확인해야 합니다.

The Most Critical Systems pane shows any clients that require software updates. Click the name of a client in the list to be taken to the Systems > System Details section for that client. From this page, you can apply any required updates.

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

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

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

The Recently Registered Systems pane shows all clients registered in the past thirty days. Click the name of a client in the list to be taken to the Systems > System Details section for that client.

3.1.3.1. 웹 인터페이스 탐색

Uyuni Web UI에서는 탐색을 지원하는 일부 표준 요소가 사용됩니다. Web UI를 사용하는 ③ 아이콘을 클릭하면 해당 섹션의 문서에 액세스할 수 있습니다.

3.1.3.1.1. 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 메시지로 이동합니다.

검색

검색 돋보기 아이콘을 클릭하여 검색 상자를 엽니다. 시스템(클라이언트), 패키지, 패치 또는 문서를 검색할 수 있습니다. [검색]을 클릭하여 관련 --> 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 > 개요로 이동합니다. 지우개 아이콘을 클릭하여 모든 시스템의 선택을 취소합니다. 시스템 세트 관리자에 대한 자세한 내용은 Client-configuration > System-set-manager에서 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 활성 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 Uyuni 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
```

3.1.3.1.2. 왼쪽 탐색줄

왼쪽 탐색줄은 Uyuni 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 **...** 필드에 입력하여 메뉴 트리의 항목을 검색합니다. 사용할 수 있는 메뉴 항목은 사용자의 역할에 따라 다릅니다.



Uyuni 관리자만 다음 섹션에 액세스할 수 있습니다.

- **...**
- **...**
- **...**

3.1.3.1.3. 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.

3.1.3.1.4. 패치 경고 아이콘

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

Icon	Description
	The shield icon is a security alert. A red shield is the highest priority security alert.
	The bug icon is a bug fix alert.
	The squares icon is an enhancement alert.

추가적인 정보를 제공하기 위해 몇 개의 추가 아이콘이 사용됩니다.

Icon	Description
	The circling arrows icon indicates that applying a patch will require a reboot.
	The archive box icon indicates that a patch will have an effect on package management.

3.1.3.1.5. 인터페이스 사용자 정의

기본적으로 Uyuni 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 ⏪ ⏩ 섹션을 찾습니다.

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

3.1.3.1.6. 요청 시간 초과 값

Web UI를 사용 중이므로 Uyuni 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.

3.1.4. 공용 클라우드 설정

로그인하기 전 업데이트를 수신하려면 Uyuni 서버를 SUSE Customer Center에 등록해야 합니다.



YaST Uyuni 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.

```
yast2 susemanager_setup
```

메시지를 따르고 설정이 완료될 때까지 기다리십시오.

YaST를 사용하여 Uyuni를 설정하는 방법에 대한 자세한 지침은 **Installation-and-upgrade > Server-setup**에서 참조하십시오.

3.1.4.1. 공용 클라우드 모듈 활성화

공용 클라우드 인스턴스에서 Uyuni를 사용하려면 공용 클라우드 모듈을 활성화해야 합니다.

절차: 공용 클라우드 모듈 활성화

1. Uyuni 서버에서 YaST 관리 도구를 열고 **소프트웨어 > 소프트웨어 리포지토리**로 이동합니다.
2. **[추가]**를 클릭한 후 **Public Cloud**을 선택합니다.
3. **필드**에서 **Public Cloud**을 선택합니다.

명령줄을 사용하려면 다음 명령으로 모듈을 추가할 수 있습니다.

```
SUSEConnect -p sle-module-public-cloud/{sles-version}.{sp-version-number}/x86_64
```

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

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

공용 클라우드의 Uyuni 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

3.1.4.2. Web UI에서 설정을 완료합니다.

다음과 같은 주소를 사용하여 웹 브라우저에서 Uyuni Web UI(를) 엽니다.

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

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

표 17. 기본 관리자 계정 상세 정보

Provider	Default Username	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.

Uyuni 서버 설정과 관련한 자세한 내용은 **Installation-and-upgrade > Server-setup**에서 참조하십시오.

3.1.4.3. 제품 추가 및 리포지토리 동기화 시작

Uyuni 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.

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

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

Before using the PAYG feature ensure:

- 원하는 리포지토리에 액세스할 수 있도록 올바른 SUSE 제품 이미지(예: SLES, SLES for SAP 또는 SLE HPC)에서 PAYG 인스턴스가 시작됩니다.
- Uyuni 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 Uyuni 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.

3.1.5.1. PAYG 인스턴스 연결

절차: 새 PAYG 인스턴스 연결

1. Uyuni Web UI에서 **관리 > 설치 마법사 > PAYG**으로 이동하고 **[PAYG 추가]**를 클릭합니다.

2. 페이지 섹션 PAYG ➔ ➔으로 시작하십시오.
3. ➔ 필드에 설명을 추가합니다.
4. ➔➔➔ SSH ➔ ➔ ➔ 페이지 섹션으로 이동합니다.
5. ➔➔➔ 필드에 Uyuni에서 연결할 인스턴스 DNS 또는 IP 주소를 입력합니다.
6. SSH ➔ ➔ 필드에 포트 번호를 입력하거나 기본값 22를 사용합니다.
7. ➔➔➔ 필드에 클라우드에 지정된 대로 사용자 이름을 입력합니다.
8. ➔ ➔ 필드에 암호를 입력합니다.
9. SSH ➔ ➔ ➔ 필드에 인스턴스 키를 입력합니다.
10. SSH ➔ ➔ ➔ ➔ ➔ 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 추가](#)를 진행합니다.

그렇지 않으면, [절차: PAYG 연결 종료](#) 명령을 수행하십시오.

[절차: SSH 배스천 연결 데이터 추가](#)

1. SSH ➔ ➔ ➔ ➔ ➔ 페이지 섹션으로 이동합니다.
2. ➔➔➔ 필드에 배스천 호스트 이름을 입력합니다.
3. SSH ➔ ➔ 필드에 배스천 포트 번호를 입력합니다.
4. ➔➔➔ 필드에 배스천 사용자 이름을 입력합니다.
5. ➔ ➔ 필드에 배스천 암호를 입력합니다.
6. SSH ➔ ➔ ➔ 필드에 배스천 키를 입력합니다.
7. SSH ➔ ➔ ➔ ➔ ➔ 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 ➔ ➔ 페이지로 돌아갑니다. 업데이트된 연결 상태는 ➔ 상단 섹션에 표시됩니다.
3. 연결 상태는 ➔ ➔ > ➔ ➔ ➔ > Pay-as-you-go 화면에도 표시됩니다.
4. 인스턴스에 대한 인증 데이터가 올바르면, ➔ 열에 "자격 증명이 업데이트됨" 메시지가 표시됩니다.



언제든 잘못된 데이터를 입력하면 새로 생성된 인스턴스가 ➔ ➔ > ➔ ➔ ➔ > PAYG에 표시되고 ➔ 열에 오류 메시지가 표시됩니다.

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

Available products are all versions of the same product family and architecture as the one installed in the PAYG instance. For example, if the instance has the SLES 15 SP1 product installed, SLES 15 SP2,

SLES 15 SP3, SLES 15 SP4 and SLES 15 SP5 are automatically shown in Admin > Setup Wizard > Products.

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

성공 메시지가 표시되면 **→→→→** > **→→** > **→**로 이동하여 Web UI에서 새로 추가된 채널을 확인할 수 있습니다.

각 채널의 동기화 진행 상황을 모니터링하려면 Uyuni 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.

3.1.5.1.1. 인스턴스 연결 데이터 삭제

다음 절차는 인스턴스의 SSH 연결 데이터를 삭제하는 방법을 설명합니다.

절차: 인스턴스에 대한 연결 데이터 삭제

1. **→→→** > **→→** > PAYG를 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.

3.1.5.2. 인스턴스 자격 증명 수집 상태

Uyuni 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.

The status of the PAYG instance credentials collect is shown in the column `Status` or on the instance details page. When the instance is unreachable, the credential update process will fail and the credentials will become invalid after the second failed refresh. Synchronization of channels will fail when the credentials are invalid. To avoid this keep the connected instances running.

SSH 연결 데이터가 명시적으로 삭제된 경우를 제외하고, PAYG 인스턴스는 Uyuni 서버에 연결된 상태를 유지합니다. 인스턴스에 대한 SSH 연결 데이터를 삭제하려면 [절차: 인스턴스에 대한 연결 데이터 삭제](#) 명령을 사용하십시오.

항상 Uyuni 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/hosts에서 클라우드 관련 항목 제거

3.1.5.3. 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.

3.1.5.4. 문제 해결

자격 증명 확인

- 스크립트가 자격 증명 수집에 실패하면 로그 및 Web UI에 적절한 오류 메시지가 표시되어야 합니다.
- 자격 증명이 작동하지 않으면 reposync에 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 --clean을 실행하면 문제가 발생할 수 있습니다.

3.2. Uyuni 프록시

3.2.1. Uyuni 프록시 등록

Proxy systems are registered as clients using bootstrap script or Web UI.

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

절차: 프록시 등록

- Uyuni 서버에서 `spacewalk-common-channels` 명령을 사용하여 openSUSE Leap 및 Uyuni 프록시 채널을 생성합니다. `spacewalk-common-channels`는 `spacewalk-utils` 패키지의 일부입니다.

```
spacewalk-common-channels \
opensuse_leap15_5 \
opensuse_leap15_5-non-oss \
opensuse_leap15_5-non-oss-updates \
opensuse_leap15_5-updates \
opensuse_leap15_5-backports-updates \
opensuse_leap15_5-sle-updates \
uyuni-proxy-stable-leap-155
```

Instead of `uyuni-proxy-stable-leap-155` you can also try `uyuni-proxy-devel-leap` which is the current development version.



활성화 키를 생성하는 동안 올바른 하위 채널을 선택할 수 있기 전, openSUSE Leap 채널이 필요한 모든 하위 채널 및 Uyuni 프록시 채널과 올바르게 동기화되었는지 확인합니다.

- openSUSE Leap을 기본 채널로 그리고 다른 채널을 하위 채널로 하여 활성화 키를 생성합니다. 활성화 키에 대한 자세한 내용은 **Client-configuration > Activation-keys**에서 확인할 수 있습니다.
- 프록시의 부트스트랩 스크립트를 만든 다음 조정합니다. GPG 키를 `ORG_GPG_KEY=` 매개변수에 추가합니다.
- 스크립트를 사용하여 클라이언트를 부트스트랩합니다. 자세한 내용은 **Client-configuration > Registration-bootstrap**에서 참조하십시오.
- Salt > 키**로 이동하고 키를 수락합니다. 키가 수락되면, 새 프록시가 → → → 섹션의 **시스템 > 개요**에 표시됩니다.
- 아니면, Uyuni Web UI에서 **시스템 > 부트스트랩**으로 이동합니다.
- 시스템 정보 > 소프트웨어 > 소프트웨어 채널**로 이동한 후 프록시 채널이 선택되었는지 확인합니다.

등록된 Uyuni 프록시를 설정하려면 [uyuni-proxy-setup.pdf](#)을 참조하십시오.

3.2.2. Uyuni 프록시 설정

Uyuni 프록시를 추가적으로 구성해야 합니다.

3.2.2.1. `uyuni_proxy` 프록시 패턴을 설치합니다.

프록시 패턴이 올바르게 설치되었는지 확인합니다. 이 단계는 **Installation-and-upgrade > Install-proxy-uyuni**의 일부입니다. 설치 성공을 확인하려면, 서버에서 설치를 위한 `pattern_uyuni_proxy` 패키지를 선택합니다.

The salt-broker service will be automatically started after installation is complete. This service forwards Salt interactions to the Uyuni Server.



프록시 체인

It is possible to arrange proxies in a chain. In such a case, the upstream proxy is named `parent`.

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

3.2.2.2. 서버 인증서 및 키 복사

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

루트로 Uyuni 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 Uyuni 프록시 기능의 SSL 인증서가 Uyuni 서버 인증서와 동일한 CA에 의해 서명되어야 합니다. 프록시와 서버에서 다른 CA로 서명된 인증서를 사용하는 것은 지원되지 않습니다.

3.2.2.3. `configure-proxy.sh` 실행

`configure-proxy.sh` 스크립트는 Uyuni 프록시 설정을 완료합니다.

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

Uyuni 상위 항목

Uyuni 상위 항목은 다른 프록시 또는 Uyuni 서버일 수 있습니다.

HTTP 프록시

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

전자 메일 역추적

문제를 보고할 전자 메일 주소입니다.

SSL 사용

보안을 위해 Y를 누릅니다.

기존 인증서를 임포트하시겠습니까?

N을 선택합니다. 그러면 이전에 Uyuni 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.

시/도

프록시의 인증서에 첨부된 추가 정보입니다.

시/도

프록시의 인증서에 첨부된 추가 정보입니다.

국가 코드

Uyuni 설치 중 설정한 국가 코드를 -- 필드에 입력합니다. 예를 들어, 프록시가 미국에 위치하고 Uyuni가 독일에 위치한 경우 프록시에 ‘DE’를 입력합니다.



국가 코드는 대문자 2자여야 합니다. 전체 국가 코드 목록은 <https://www.iso.org/obp/ui/#search>를 참조하십시오.

Cname 별칭(공백으로 구분)

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

CA 비밀번호

Uyuni 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.

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.sh`는 squid, apache2, salt-broker 및 jabberd 등 Uyuni 프록시에 필요한 서비스를 활성화합니다.

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

3.2.2.4. PXE 부팅 활성화

3.2.2.4.1. 프로파일과 시스템 정보 동기화

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

1. Uyuni 프록시에 `susemanager-tftpsync-recv` 패키지를 설치합니다.

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

2. Uyuni 프록시에서 `configure-tftpsync.sh` 설정 스크립트를 실행한 후 요청되는 정보를 입력합니다.

```
configure-tftpsync.sh
```

Uyuni 서버 및 프록시의 호스트 이름과 IP 주소를 입력해야 합니다. 또한 프록시의 `tftpboot` 디렉토리 경로도 입력해야 합니다.

3. Uyuni 서버에 `susemanager-tftpsync`를 설치합니다.

```
zypper in susemanager-tftpsync
```

4. Uyuni 서버에서 `configure-tftpsync.sh`를 실행합니다. 그러면 구성이 생성되어 Uyuni 프록시에 업로드됩니다.

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

5. Uyuni 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. PXE 부팅에 대한 자세한 내용은 **Client-configuration** > **Autoinst-pxeboot**에서 참조하십시오.

3.2.2.4.2. 프록시를 통한 PXE를 위한 DHCP 구성

Uyuni에서는 클라이언트 프로비저닝을 위해 Cobbler를 사용합니다. 기본적으로 PXE(tftp)가 설치되고 활성화됩니다. 클라이언트는 DHCP를 사용하여 Uyuni 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"
```

3.2.2.5. Uyuni 프록시 바꾸기

프록시에는 연결된 클라이언트에 대한 정보가 포함되어 있지 않습니다. 그러므로 프록시는 언제든지 새 프록시로 대체할 수 있습니다. 대체 프록시는 이름과 IP 주소가 이전 프록시와 동일해야 합니다.

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.



재활성화 키는 시스템의 이력이 손실되지 않도록 하려는 경우에만 필요합니다. 재활성화 키를 사용하지 않으면 대체 프록시는 새 ID를 갖는 새 프록시가 됩니다.

절차: 프록시 대체 및 클라이언트 등록 유지

Before starting the actual migration procedure, save the data from the old proxy, if needed. Consider copying important or manually created data to a central place that can also be accessed by the new proxy.

1. 프록시를 종료합니다.
2. 새 Uyuni 프록시를 설치합니다. 설치 지침은 [프록시 설치](#)를 참조하십시오.
3. Uyuni Web UI에서 새로 설치한 Uyuni 프록시를 선택한 후 시스템 목록에서 삭제합니다.
4. Web UI에서 기존 프록시 시스템을 위한 재활성화 키를 생성합니다. 기존 프록시의 시스템 정보 탭에서 **...**를 클릭합니다. **...**을 클릭하고 나중에 편집할 때 필요하므로 새 키를 메모해 둡니다. 재활성화 키에 대한 자세한 내용은 [Reference > Systems](#)를 참조하십시오.
5. 선택 사항: 새 프록시를 설치한 후에는 다음 작업도 수행해야 할 수 있습니다.
 - 중앙에 저장한 데이터를 새 프록시 시스템에 복사
 - 필요한 다른 소프트웨어 설치
 - 자동 설치를 위해 프록시가 사용되는 경우 TFTP 동기화 설정



프록시를 설치하는 동안 클라이언트는 Uyuni 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.

3.2.3. 컨테이너화된 Uyuni 프록시 설정

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

1. Uyuni 프록시 구성 아카이브 파일 생성

2. 설치 단계에서 준비한 컨테이너 호스트로 구성 아카이브를 전송하고 압축을 풉니다.
3. `systemd` 프록시 서비스 시작

3.2.3.1. Uyuni 프록시 구성 만들기 및 생성

Uyuni 프록시의 구성은 Uyuni 서버에 의해 생성되며 이 구성 생성은 컨테이너화된 각 프록시에 대해 수행되어야 합니다. Uyuni 구성 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. ↵ **FQDN** 필드에 Uyuni Server 또는 다른 Uyuni Proxy에 대한 정규화된 도메인 이름을 입력하십시오.
4. ↵ ↵ **SSH** ↵ **SSH** 필드에 SSH 서비스가 Uyuni Proxy에서 수신 대기하는 SSH 포트를 입력하십시오. 권장 사항은 기본 포트인 8022를 유지하는 것입니다.
5. ↵ ↵ **Squid** ↵ ↵ **[MB]** 필드에 Squid 캐시에 허용되는 최대 크기를 입력하십시오. 일반적으로 이는 컨테이너에 사용할 수 있는 저장소의 최대 60%여야 합니다.

SSL ↵ 선택 목록에서 Uyuni 프록시에 대해 새 서버 인증서를 생성해야 하는지 또는 기존 인증서를 사용해야 하는지 선택합니다. 생성된 인증서를 Uyuni 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 Uyuni Server에 새 프록시 FQDN을 등록하고 컨테이너 호스트에 대한 세부 정보가 포함된 구성 아카이브를 생성하십시오.
2. 잠시 후 다운로드할 파일이 표시됩니다. 이 파일을 로컬에 저장하십시오.

Container Based Proxy Configuration ?

You can generate a set of configuration files and certificates in order to register and run a container-based proxy. Once the following form is filled out and submitted you will get a .zip archive to download.

Proxy FQDN *: e.g., proxy.domain.com

Server FQDN *: e.g., server.domain.com

FQDN of the server of proxy to connect to.

Proxy SSH port: 8022
Port range: 1 - 65535

Max Squid cache size (MB) *: e.g., 2048

Proxy administrator email *: admin

SSL certificate *:

- Create
- Use existing

CA certificate to use to sign the SSL certificate in PEM format *:

CA private key to use to sign the SSL certificate in PEM format *:

The CA private key password *:

.....

SSL Certificate data

Alternate CNAMEs	<input type="button" value="+"/>
2-letter country code:	<input type="text"/>
State:	<input type="text"/>
City:	<input type="text"/>
Organization:	<input type="text"/>
Organization Unit:	<input type="text"/>
Email:	<input type="text"/>

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 Uyuni 자격 증명 및 CA 암호에 답하십시오.

그러면 Uyuni 프록시 컨테이너에 대한 구성이 포함된 config.tar.gz 파일이 생성됩니다.

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

등록된 미니언이 아닌 Uyuni 프록시 컨테이너 구성 생성하기 위해 Proxy FQDN을 사용하는 경우 시스템 목록에 새 시스템 항목이 표시됩니다. 이 새 항목은 이전에 입력한 --> FQDN 값 아래에 표시되며 -- 시스템 유형이 됩니다.

3.2.3.2. Uyuni 프록시 구성 전송

spacecmd 명령 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 풁니다.

3.2.3.3. Uyuni 프록시 컨테이너 시작

이제 단일 `systemctl` 명령으로 컨테이너 시작 가능:

목록 1. 절차: Uyuni 프록시 컨테이너 시작

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

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

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

호출하여 모든 컨테이너가 예상대로 시작되었는지 확인하십시오.

```
podman ps
```

5개의 Uyuni 프록시 컨테이너가 있어야 합니다.

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

그리고 `proxy-pod` 컨테이너 포드의 일부여야 합니다.

3.2.4. 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.

3.2.4.1. SUSE 레지스트리에서 내부 레지스트리로 이미지 복사

Machines must have access to `registry.suse.com`.

Procedure: Deploying Proxy from an internal image registry

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

`skopeo`의 `zypper`



이는 Uyuni 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=false를 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]\nninfra_image =
"<your_server>/pause:latest"'>/etc/containers/containers.conf
```

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



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

3.2.4.2. 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]\nninfra_image =
"<your_server>/pause:latest"'>/etc/containers/containers.conf
```



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

- 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.

- proxy-images.tar을 에어 갭 프록시로 전송합니다.

- 필요할 때 이미지를 시작할 수 있도록 하려면 다음 명령을 실행합니다.

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

Chapter 4. 업그레이드 소개

업데이트 날짜: 2024-02-15

Uyuni에는 3개의 주요 구성 요소가 있으며, 이러한 구성 요소에는 모두 일반 업데이트가 필요합니다. 이 가이드에서는 Uyuni 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, 업그레이드 할 구성 요소로 이동한 다음 업그레이드 대상 버전을 확인하십시오.

Uyuni에서는 룰링 릴리스에 적합한 YYYY.MM 버전 관리 스키마를 사용합니다.

Uyuni 서버를 업그레이드하려면, **Installation-and-upgrade > Server-intro-uyuni**에서 참조하십시오.

Uyuni 프록시를 업그레이드하려면, **Installation-and-upgrade > Proxy-intro**에서 참조하십시오.

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

4.1. 서버 업그레이드

Uyuni은(는) 룰링 릴리스 버전 관리 스키마를 사용합니다. 다음 버전으로 업그레이드하기 위해 사용할 수 있는 업그레이드 전략에 대한 내용은 릴리스 노트에서 확인할 수 있습니다.

부분 업그레이드

부분 업그레이드는 일반 업그레이드로 간주할 수 있습니다. 자세한 내용은 **Installation-and-upgrade > Server-minor-upgrade-uyuni**에서 참조하십시오.

주요 업그레이드

주요 업그레이드는 특별 업그레이드로 간주할 수 있습니다. 이 경우 기본 운영 체제, Salt 또는 PostgreSQL 데이터베이스 등의 구성 요소가 업그레이드됩니다. 자세한 내용은 **Installation-and-upgrade > Server-major-upgrade-uyuni**에서 참조하십시오.

4.1.1. 서버 - 부분 업그레이드

Uyuni 팀은 연중 몇 차례 Uyuni 서버의 부분 업그레이드를 제공합니다. 이러한 업데이트에는 버그 수정과 기능 개선이 포함되며 새로운 기능이 종종 제공됩니다.



Some additional manual steps might be required, and this information is only available in the release notes. For more information about such a major upgrade, see **Installation-and-upgrade > Server-major-upgrade-uyuni**.

For information about your upgrade, see the release notes at <https://www.uyuni-project.org/pages/stable-version.html>.

부분 업그레이드를 수행하는 것은 운영 체제 패키지 업데이트를 설치하는 것과 유사합니다.

절차: Uyuni 서버에서 패키지 업데이트

기본적으로 여러 업데이트 리포지토리는 Uyuni 서버를 위해 구성 및 활성화됩니다. 새 패키지와 업데이트된 패키지는 자동으로 제공됩니다.

It is recommended you make a backup of the server before upgrading. For more information about backing up Uyuni, see [Administration > Backup-restore](#).

1. Uyuni 서버의 명령 프롬프트에서 루트로 Spacewalk 서비스를 중지합니다.

```
spacewalk-service stop
```

2. 소프트웨어 리포지토리 새로 고침:

```
zypper ref
```

3. 새 패키지 업데이트: (zypper에서 메시지가 표시되면 이 작업을 반복)

```
zypper up
```

Uyuni is different from SUSE Manager in this step. SUSE Manager uses `zypper patch`, but Uyuni requires `zypper up`.

+

1. If zypper reports that the Uyuni package will not be upgraded, run the command manually:

```
zypper install Uyuni-Server-release
```

2. Spacewalk 서비스를 다시 시작합니다.

```
spacewalk-service start
```

패치 업데이트에서 재부팅이 권장되면 서버를 재시작합니다.



기본적으로 zypper는 10분마다 리포지토리를 새로 고칩니다(
`/etc/zypp/zypp.conf`의 `repo.refresh.delay` 참조). autorefresh가
 비활성화되면 zypper ref를 실행하여 모든 리포지토리를 새로 고칩니다.



Uyuni 2020.04부터는 `spacewalk-schema-upgrade`가 더 이상 필요하지 않습니다.



스키마 업그레이드는 Spacewalk 서비스가 `spacewalk-service start`로 시작될 때 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.

4.1.2. 서버 - 주요 업그레이드

Uyuni 핵심 구성 요소가 새로운 주 버전으로 업그레이드되면 Uyuni 서버에서 주요 업그레이드를 수행해야 합니다. PostgreSQL, Salt 또는 openSUSE Leap의 버전이 업그레이드되는 경우가 해당합니다. openSUSE Leap은 내부 기본 운영 체제(OS)입니다.



추가적인 수동 단계가 몇 가지 필요할 수 있으며 이 정보는 릴리스 노트에서만 제공됩니다. 업그레이드와 관련된 중요한 추가 정보는 릴리스 노트를 참조하십시오.

<https://www.uyuni-project.org/pages/stable-version.html>.



You will not be able to fix issues that arise during the migration. Ensure you have created a backup before you start the migration. For more information about backing up Uyuni, see **Administration > Backup-restore**. If you are running Uyuni Server on a virtual machine, we recommend that you create a snapshot before you start.



업그레이드를 수행하기 전 스토리지 요구사항의 총족 여부를 확인하십시오. 자세한 내용은 [uyuni-install-requirements.pdf](#)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.

`server-migrator.sh` 스크립트를 통해 Uyuni 서버가 최신 버전으로 마이그레이션됩니다. 또한 기본 운영 체제도 15.5 버전으로 업그레이드됩니다. 스크립트는 `susemanager` 패키지의 일부입니다.

절차: Uyuni 서버 마이그레이션

1. `server-migrator.sh` 스크립트를 실행하기 전, `susemanager` 패키지의 가장 최신 버전이 설치되어 있는지 확인합니다.

```
zypper ref
zypper up susemanager
```

2. `/usr/lib/susemanager/bin/server-migrator.sh` 스크립트를 실행하여 기본 OS 및 Uyuni 서버를 실행합니다.



마이그레이션이 완료된 후에는, Uyuni 서버를 수동으로 재부팅합니다.

4.2. 프록시 업그레이드

Uyuni 프록시는 클라이언트와 동일한 방식으로 관리됩니다.

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



2024.01의 업그레이드 절차는 주요 업그레이드 또는 부분 업그레이드가 될 수 있습니다.
자세한 내용은 Uyuni 2024.01 릴리스 정보를 참조하십시오.

주요 업그레이드

Installation-and-upgrade > Proxy-uyuni의 내용을 참조하십시오.

부분 업그레이드

Installation-and-upgrade > Proxy-minor-uyuni의 내용을 참조하십시오.

4.2.1. 프록시 - 주요 업그레이드

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



주요 프록시 업그레이드에는 운영 체제의 버전 업그레이드가 포함됩니다. 자세한 내용은 Uyuni 2024.01 릴리스 정보를 참조하십시오.

4.2.1.1. 업그레이드 준비

절차: 명령 프롬프트에서 openSUSE Leap 15.5 소프트웨어 채널 추가

1. Uyuni 서버의 명령 프롬프트에서 루트로 `spacewalk-common-channels` 명령을 사용하여 적절한 채널을 추가합니다.

```
spacewalk-common-channels opensuse_leap15_5 \
opensuse_leap15_5-non-oss \
opensuse_leap15_5-non-oss-updates \
opensuse_leap15_5-updates \
opensuse_leap15_5-backports-updates \
opensuse_leap15_5-sle-updates \
uyuni-proxy-stable-leap-155
```

2. `spacewalk-repo-sync`을 사용하여 모든 채널을 완전히 동기화합니다.

4.2.1.2. 프록시 업그레이드

프록시를 업그레이드하려면 먼저 프록시 서비스를 중지한 후 소프트웨어 리포지토리를 바꾸고 소프트웨어를 업데이트한 후 마지막으로 프록시 서비스를 재시작합니다.

절차: Uyuni 프록시 업데이트

1. Uyuni 프록시에서 프록시 서비스를 중지합니다.

```
spacewalk-proxy stop
```

2. Uyuni 서버 Web UI에서 **시스템** > **프록시**로 이동하여 프록시의 이름을 클릭합니다.
3. **소프트웨어** > **소프트웨어 채널**을 클릭하고 Customs Channels 목록에 나열된 openSUSE Leap 15.5 채널을 기본 채널로 선택합니다.
4. ← ← 창에서 15.5 하위 채널을 선택합니다.
5. [다음]을 클릭하고 ←←←←←에서 [확인]을 클릭합니다.
6. **세부 정보** > **원격 명령**을 클릭하고 스크립트 필드에 zypper --non-interactive dup --allow -vendor-change --replacefiles를 추가한 후 [예약]을 클릭합니다.
7. 원격 명령이 실행될 때까지 기다립니다.
8. Uyuni 프록시에서 프록시 서비스를 시작합니다.

```
spacewalk-proxy start
```

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

4.2.2. 프록시 - 부분 업그레이드

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



부분 프록시 업그레이드의 경우 운영 체제의 버전 업그레이드가 포함되지 않습니다. 자세한 내용은 Uyuni 2024.01 릴리스 정보를 참조하십시오.

4.2.2.1. 프록시 업그레이드

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

절차: Uyuni 프록시 업데이트

1. Uyuni 프록시에서 프록시 서비스를 중지합니다.

```
spacewalk-proxy stop
```

2. Uyuni 서버 Web UI에서 **시스템** > **프록시**로 이동하여 프록시의 이름을 클릭합니다.
3. 프록시에서 업데이트할 패키지를 전체 선택한 후 선택 사항을 적용합니다.
4. Uyuni 프록시에서 프록시 서비스를 시작합니다.

```
spacewalk-proxy start
```

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

4.3. 데이터베이스 업그레이드

Uyuni의 주요 업데이트를 수행하려면 기본 데이터베이스를 업그레이드해야 할 수 있습니다.

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

이 테이블은 Uyuni 및 openSUSE의 각 버전에 필요한 PostgreSQL 버전을 보여줍니다.

표 18. PostgreSQL 버전

Uyuni version	Operating System version	PostgreSQL version
Uyuni >= 2020.07	openSUSE 15.2	PostgreSQL 12
Uyuni >= 2021.06	openSUSE 15.3	PostgreSQL 13
Uyuni >= 2022.06	openSUSE 15.4	PostgreSQL 14
Uyuni >= 2023.09	openSUSE 15.5	PostgreSQL 14

4.3.1. 최신 버전으로 데이터베이스 마이그레이션

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

If you want to upgrade to the latest Uyuni version, you must be using PostgreSQL version 13, 14, or 15 depending on the underlying operating system:

- If you are running openSUSE Leap 15.3, use PostgreSQL 13.
- openSUSE Leap 15.4를 실행 중인 경우에는 PostgreSQL 14를 사용하십시오.
- If you are running openSUSE Leap 15.5, use PostgreSQL 14.

4.3.1.1. 업그레이드 준비

업그레이드하기 전에 기존 Uyuni 서버를 준비한 후 데이터베이스를 백업합니다.

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

절차: 업그레이드 준비

- 활성 PostgreSQL 버전을 확인합니다.

```
psql --version
```

- 활성 smdba 버전을 확인합니다.

```
rpm -q smdba
```

PostgreSQL 14에는 smdba 버전 1.7.6 이상이 필요합니다.

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

4.3.1.2. 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

- 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
```

- 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-pg10으로 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
- Uyuni에서 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

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

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

- 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-pg10으로 이름이 변경됩니다.

4.4. 클라이언트 업그레이드

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

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

Chapter 5. GNU Free Documentation License

Copyright © 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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".