Red Hat Directory Server 12

配置和管理复制

将数据复制到其他目录服务器实例

Last Updated: 2024-05-09

Red Hat Directory Server 12 配置和管理复制

将数据复制到其他目录服务器实例

法律通告

摘要

要将一个目录服务器实例的数据自动同步到另一个目录服务器实例，您可以使用单个供应商、多供应商和级联复制机制。要管理复制更改日志，您可以使用修剪和加密。

目录

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。要做到这一点：

- 要通过 JIRA 提交反馈（需要帐户）：
  1. 登录到 Jira 网站。
  2. 在顶部导航栏中点 **Create**
  3. 在 **Summary** 字段中输入描述性标题。
  4. 在 **Description** 字段中输入您对改进的建议。包括到文档相关部分的链接。
  5. 点对话框底部的 **Create**。
- 要通过 Bugzilla 提交反馈（需要帐户）：
  1. 进入 Bugzilla 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。

第 1 章 使用命令行配置单层次复制

在单层次复制环境中，一个可写供应商将数据复制到一个或多个只读消费者。例如，如果后缀收到大量搜索请求，则设置单层次复制，但只有少量写入请求。要分发负载，客户端可以在只读消费者中搜索后缀，并将写入请求发送到供应商。

本节假设您在名为 provider. **example.com** 的主机上运行现有的 Directory 服务器实例，它将充当要设置的复制拓扑中的供应商。该流程描述了如何将名为 **consumer.example.com** 的只读消费者添加到拓扑中，以及如何为 **dc=example,dc=com** 后缀配置单层次复制。

1.1. 使用命令行准备新消费者

要准备 **consumer.example.com** 主机，请启用复制。这个过程：

- 在复制拓扑中配置此服务器的角色
- 定义复制的后缀
- 创建供应商用来连接到此主机的复制管理器帐户

在您要添加到复制拓扑的消费者上执行这个步骤。

前提条件

- 已安装 Directory 服务器实例。
- **dc=example,dc=com** 后缀的数据库存在。

流程

- 为 **dc=example,dc=com** 后缀启用复制：

```
# dsconf -D "cn=Directory Manager" ldap://consumer.example.com replication enable
--suffix "dc=example,dc=com" --role "consumer" --bind-dn "cn=replication
manager,cn=config" --bind-passwd "password"
```

此命令将 **consumer.example.com** 主机配置为 **dc=example,dc=com** 后缀的使用者。此外，命令还会创建具有指定密码的 **cn=replication managercn=config** 用户，并允许此帐户将后缀更改复制到此主机。

验证

- 显示复制配置：

```
# dsconf -D "cn=Directory Manager" ldap://consumer.example.com replication get --
suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 2
...
```

这些参数表示：

- **nsDS5ReplicaBindDN** 指定复制管理器帐户。
- **nsDS5ReplicaRoot** 设置复制的后缀。
- **nsDS5ReplicaType** 设置为 **2** 定义此主机是消费者。

其他资源

- 安装 Red Hat Directory Server
- 在单独的数据库中存储后缀
- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

1.2. 使用命令行将现有服务器配置为消费者的供应商

要准备 provider **.example.com** 主机，您需要：

- 为后缀启用复制。
- 创建到消费者的复制协议。
- 初始化消费者。

在复制拓扑中的现有供应商上执行这个步骤。

前提条件

- 您在使用者上启用了 **dc=example,dc=com** 后缀的复制。

流程

1. 为 **dc=example,dc=com** 后缀启用复制：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication enable --suffix "dc=example,dc=com" --role "supplier" --replica-id 1
```

此命令将 provider. **example.com** 主机配置为 **dc=example,dc=com** 后缀的供应商，并将此条目的副本 ID 设置为 **1**。

重要

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数。

2. 添加复制协议并初始化消费者：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt create --suffix "dc=example,dc=com" --host "consumer.example.com" --port 389 --conn-protocol=LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method=SIMPLE --init example-agreement
```

此命令创建名为 **example-agreement** 的复制协议。复制协议定义设置，如消费者的主机名、协议和身份验证信息，如供应商在将数据连接和复制到此消费者时使用的身份验证信息。

创建协议后，目录服务器会初始化 **consumer.example.com**。根据要复制的数据量，初始化可能会非常耗时。

验证

1. 显示复制配置：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication get --suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 3
...
```

这些参数表示：

- **nsDS5ReplicaRoot** 设置复制的后缀。
- **nsDS5ReplicaType** 设置为 **3** 定义此主机是一个供应商。

2. 验证初始化是否成功：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt init-status --suffix "dc=example,dc=com" example-agreement
Agreement successfully initialized.
```

3. 显示复制状态：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement
Status For Agreement: "example-agreement" (consumer.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20210330075608Z
Last Update End: 20210330075608Z
Number Of Changes Sent: 1:3/0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210330074603Z
Last Init End: 20210330074606Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: Not in Synchronization: supplier (6062d73c000000010000) consumer (Unavailable) State (green) Reason (error (0) replica acquired successfully: incremental update succeeded)
Replication Lag Time: Unavailable
```

验证 **Replication Status** 和 **Last Update Status** 字段。

故障排除

1. 默认情况下，服务器上所有协议的复制闲置超时为 1 小时。如果因为超时而导致大型数据库的初始化失败，请将 **nsslapd-idletimeout** 参数设置为更高的值。例如，要将参数设置为 **7200** (2 小时)，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com config replace
nsslapd-idletimeout=7200
```

要设置无限周期，请将 **nsslapd-idletimeout** 设置为 **0**。

其他资源

- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

第 2 章 使用 WEB 控制台配置单层次复制

在单层次复制环境中，一个可写供应商将数据复制到一个或多个只读消费者。例如，如果后缀收到大量搜索请求，则设置单层次复制，但只有少量写入请求。要分发负载，客户端可以在只读消费者中搜索后缀，并将写入请求发送到供应商。

本节假设您在名为 provider. **example.com** 的主机上运行现有的 Directory 服务器实例，它将充当要设置的复制拓扑中的供应商。该流程描述了如何将名为 **consumer.example.com** 的只读消费者添加到拓扑中，以及如何为 **dc=example,dc=com** 后缀配置单层次复制。

2.1. 使用 WEB 控制台准备新消费者

要准备 **consumer.example.com** 主机，请启用复制。这个过程：

- 在复制拓扑中配置此服务器的角色
- 定义复制的后缀
- 创建供应商用来连接到此主机的复制管理器帐户

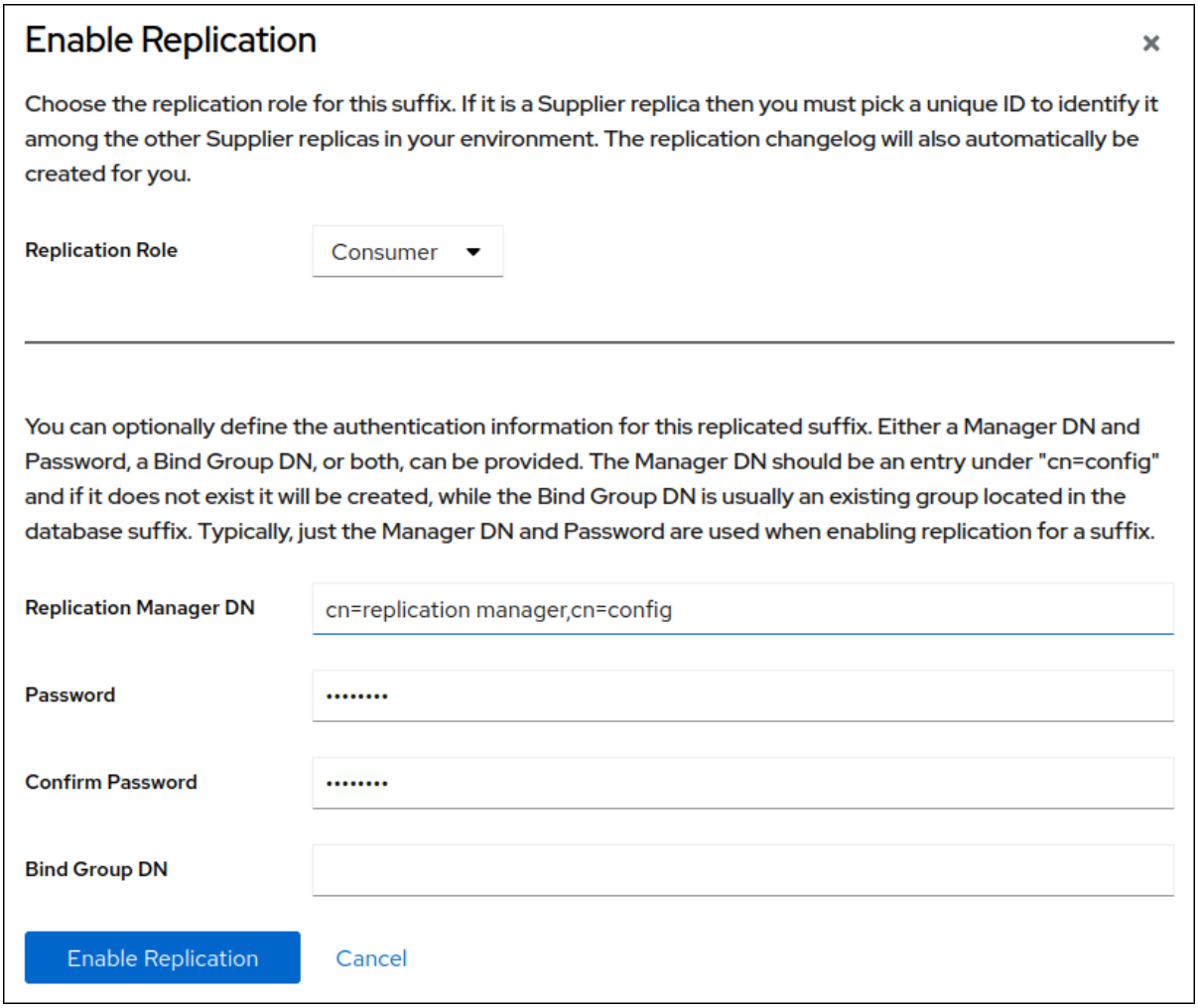
在您要添加到复制拓扑的消费者上执行这个步骤。

前提条件

- 已安装 Directory 服务器实例。
- **dc=example,dc=com** 后缀的数据库存在。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 点 **Enable Replication**。
4. 在 **Replication Role** 字段中选择 **Consumer**，并输入要创建的复制管理器帐户和密码：



这些设置将主机配置为 **dc=example,dc=com** 后缀的消费者。此外，服务器还会创建具有指定密码的 **cn=replication managercn=config** 用户，并允许此帐户将后缀更改复制到此主机。

5. 点 **Enable Replication**。

验证

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 如果 **Replica Role** 字段包含值 **Consumer**，则启用复制，主机被配置为消费者。

其他资源

- 安装 Red Hat Directory Server
- 在单独的数据库中存储后缀

2.2. 使用 WEB 控制台将现有服务器配置为消费者的供应商

要准备 provider **.example.com** 主机，您需要：

- 为后缀启用复制。
- 创建到消费者的复制协议。

- 初始化消费者。

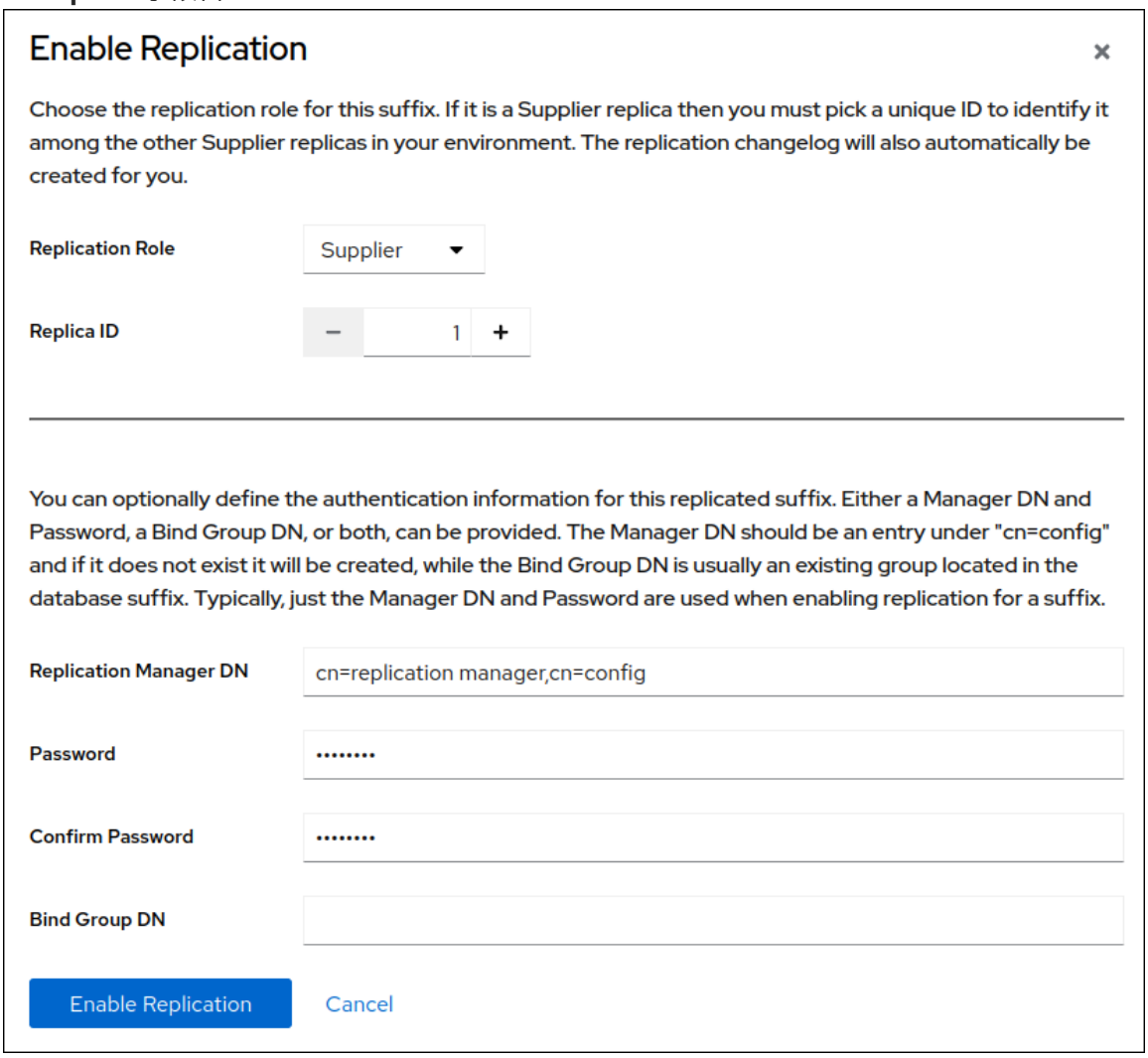
在复制拓扑中的现有供应商上执行这个步骤。

前提条件

- 您在使用者上启用了 **dc=example,dc=com** 后缀的复制。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 启用复制：
   a. 点 **Enable Replication**。
   b. 在 **Replication Role** 字段中选择 **Supplier**，输入副本 ID、复制管理器凭证，并将 **Bind Group DN** 字段留空：



这些设置将主机配置为 **dc=example,dc=com** 后缀的供应商，并将此条目的副本 ID 设置为 **1**。

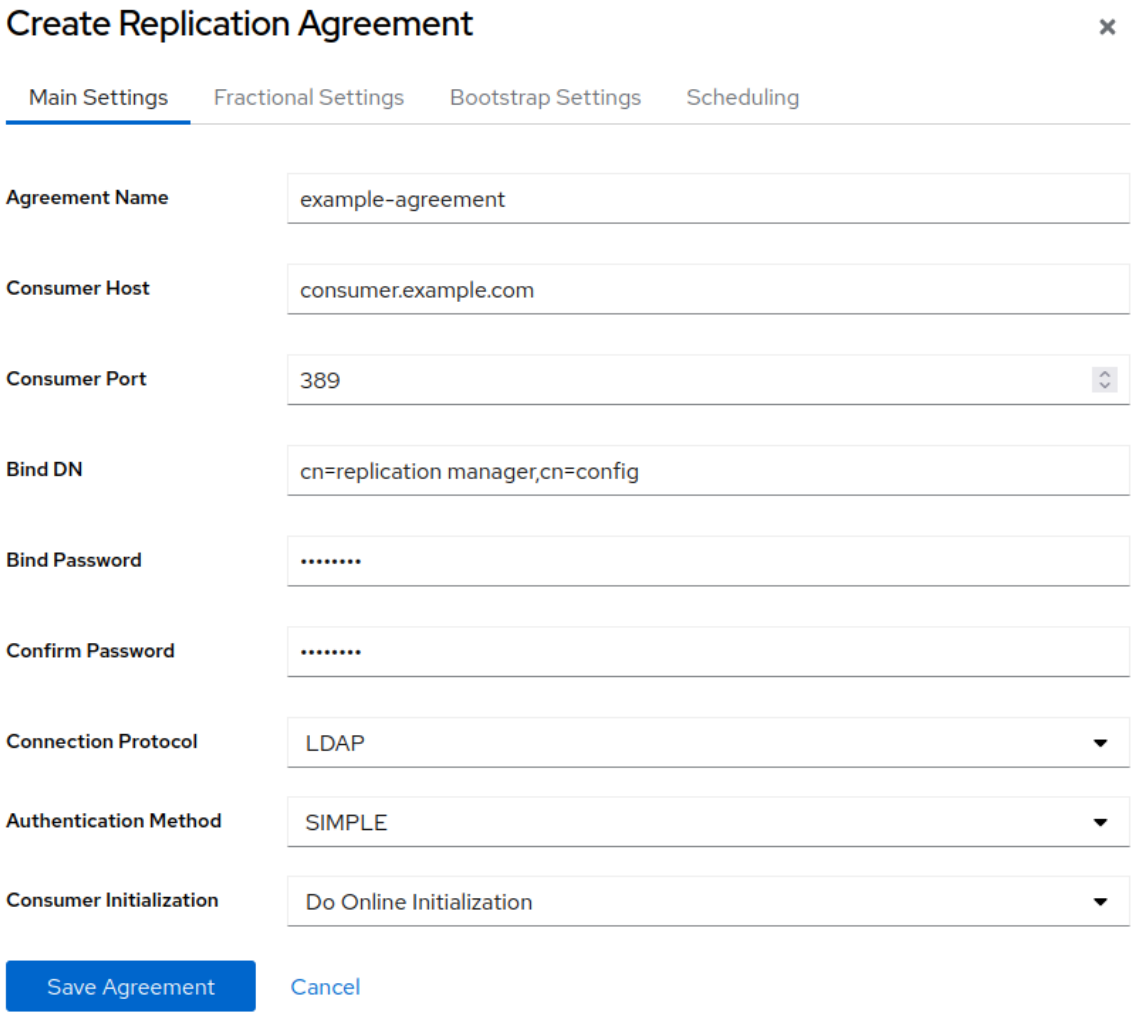
重要

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数。

c. 点 **Enable Replication**。

4. 添加复制协议并初始化消费者：

a. 在 **Agreements** 选项卡中，点 **Create Agreement**，并填写字段：



这些设置创建一个名为 **example-agreement** 的复制协议。复制协议定义设置，如消费者的主机名、协议和身份验证信息，如供应商在将数据连接和复制到此消费者时使用的身份验证信息。

b. 在 **Consumer Initialization** 字段中选择 **Do Online Initialization**，以在保存协议后自动初始化消费者。

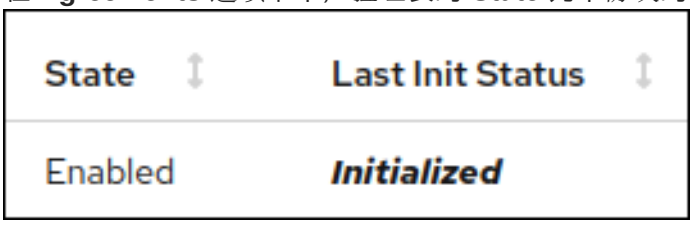
c. 点 **Save Agreement**。
创建协议后，目录服务器会初始化 **consumer.example.com**。根据要复制的数据量，初始化可能会非常耗时。

验证

1. 打开 **Replication** 菜单。

2. 选择 **dc=example,dc=com** 后缀。

3. 在 **Agreements** 选项卡中，验证表的 **State** 列中协议的状态。



第 3 章 使用命令行配置多层次复制

在多层次复制环境中，两个或多个可写供应商相互复制数据。例如，设置多层次复制以提供故障转移环境，并将负载分发到多个服务器。然后，客户端可以在任何属于读写副本的主机上执行读写操作。

本节假设您在名为 provider **1.example.com** 的主机上运行现有的 Directory 服务器实例。该流程描述了如何将名为 provider **2.example.com** 的另一个读写副本添加到拓扑中，以及如何为 **dc=example,dc=com** 后缀配置多层次复制。

3.1. 使用命令行准备新供应商

要准备 provider **2.example.com** 主机，请启用复制。这个过程：

- 在复制拓扑中配置此服务器的角色
- 定义复制的后缀
- 创建供应商用来连接到此主机的复制管理器帐户

在您要添加到复制拓扑的供应商上执行这个步骤。

前提条件

- 已安装 Directory 服务器实例。
- **dc=example,dc=com** 后缀的数据库存在。

流程

- 为 **dc=example,dc=com** 后缀启用复制：

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com replication enable --suffix "dc=example,dc=com" --role "supplier" --replica-id 1 --bind-dn "cn=replication manager,cn=config" --bind-passwd "password"
```

此命令将 provider **2.example.com** 主机配置为 **dc=example,dc=com** 后缀的供应商，并将此条目的副本 ID 设置为 **1**。此外，命令还会创建具有指定密码的 **cn=replication managercn=config** 用户，并允许此帐户将后缀更改复制到此主机。

重要

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数。

验证

- 显示复制配置：

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com replication get --suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
```

```
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 3
...
```

这些参数表示：

- **nsDS5ReplicaBindDN** 指定复制管理器帐户。
- **nsDS5ReplicaRoot** 设置复制的后缀。
- **nsDS5ReplicaType** 设置为 **3** 定义此主机是一个供应商。

其他资源

- 安装 Red Hat Directory Server
- 在单独的数据库中存储后缀
- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

3.2. 使用命令行将现有服务器配置为新服务器的供应商

要准备现有服务器 provider **1.example.com** 作为供应商，您需要：

- 为后缀启用复制。
- 为新供应商创建复制协议。
- 初始化新供应商。

在复制拓扑中的现有供应商上执行这个步骤。

前提条件

- 您在供应商上启用了 **dc=example,dc=com** 后缀的复制来加入。

流程

1. 为 **dc=example,dc=com** 后缀启用复制：

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com replication enable --suffix "dc=example,dc=com" --role "supplier" --replica-id 2 --bind-dn "cn=replication manager,cn=config" --bind-passwd "password"
```

此命令将 provider **1.example.com** 主机配置为 **dc=example,dc=com** 后缀的供应商，并将此条目的副本 ID 设置为 **2**。此外，命令还会创建具有指定密码的 **cn=replication managercn=config** 用户，并允许此帐户将后缀更改复制到此主机。

重要

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数。

2. 添加复制协议并初始化新的服务器：

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com repl-agmt create --suffix "dc=example,dc=com" --host "supplier2.example.com" --port 389 --conn-protocol LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method SIMPLE --init example-agreement-supplier1-to-supplier2
```

此命令创建一个名为 **example-agreement-supplier1-to-supplier2** 的复制协议。复制协议定义设置，如供应商的主机名、协议和身份验证信息，供应商在将数据连接并复制到新供应商时使用的身份验证信息。

创建协议后，目录服务器会初始化 vendor **2.example.com**。根据要复制的数据量，初始化可能会非常耗时。

验证

1. 显示复制配置：

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com replication get --suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 3
...
```

这些参数表示：

- **nsDS5ReplicaBindDN** 指定复制管理器帐户。
- **nsDS5ReplicaRoot** 设置复制的后缀。
- **nsDS5ReplicaType** 设置为 **3** 定义此主机是一个供应商。

2. 验证初始化是否成功：

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com repl-agmt init-status --suffix "dc=example,dc=com" example-agreement-supplier1-to-supplier2
Agreement successfully initialized.
```

3. 显示复制状态：

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement-supplier1-to-supplier2
Status For Agreement: "example-agreement-supplier1-to-supplier2" (supplier2.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20210331071545Z
Last Update End: 20210331071546Z
Number Of Changes Sent: 2:1/0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210331071541Z
Last Init End: 20210331071544Z
Last Init Status: Error (0) Total update succeeded
```

```
Reap Active: 0
Replication Status: Not in Synchronization: supplier (6064219e000100020000) consumer
(Unavailable) State (green) Reason (error (0) replica acquired successfully: incremental
update succeeded)
```

验证 **Replication Status** 和 **Last Update Status** 字段。

故障排除

1. 默认情况下，服务器上所有协议的复制闲置超时为 1 小时。如果因为超时而导致大型数据库的初始化失败，请将 **nsslapd-idletimeout** 参数设置为更高的值。例如，要将参数设置为 **7200** (2 小时)，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com config replace
nsslapd-idletimeout=7200
```

要设置无限周期，请将 **nsslapd-idletimeout** 设置为 **0**。

其他资源

- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

3.3. 使用命令行将新服务器配置为现有服务器的供应商

要将新的服务器 provider **2.example.com** 准备为供应商，请使用以下方法之一：

- 为后缀启用复制。
- 创建到现有服务器的复制协议。

警告

不要从新服务器初始化现有供应商。否则，新服务器中的空数据库会覆盖现有供应商上的数据库。

在现有供应商中应用以下步骤：

- 创建到新服务器的复制协议。
- 初始化新服务器。

前提条件

- 您可以在新服务器上为 **dc=example,dc=com** 后缀启用复制。
- 您在现有服务器上为 **dc=example,dc=com** 后缀启用复制。
- 要加入的新服务器已被成功初始化。

流程

- 在现有实例中添加复制协议：

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com repl-agmt create --suffix "dc=example,dc=com" --host "supplier1.example.com" --port 389 --conn-protocol LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method SIMPLE example-agreement-supplier2-to-supplier1
```

- 使用 **--init** 选项将复制协议添加到新实例：

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com repl-agmt create --suffix "dc=example,dc=com" --host "supplier2.example.com" --port 389 --conn-protocol LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method SIMPLE --init example-agreement-supplier1-to-supplier2
```

验证

1. 显示协议状态：

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com repl-agmt init-status --suffix "dc=example,dc=com" example-agreement-supplier2-to-supplier1
Agreement successfully initialized.
```

2. 显示复制状态：

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement-supplier2-to-supplier1
Status For Agreement: ""example-agreement-supplier2-to-supplier1 (supplier1.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20210331073540Z
Last Update End: 20210331073540Z
Number Of Changes Sent: 7:1/0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210331073535Z
Last Init End: 20210331073539Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: Not in Synchronization: supplier (60642649000000070000) consumer (Unavailable) State (green) Reason (error (0) replica acquired successfully: incremental update succeeded)
Replication Lag Time: Unavailable
```

验证 **Replication Status** 和 **Last Update Status** 字段。

故障排除

1. 默认情况下，服务器上所有协议的复制闲置超时为 1 小时。如果因为超时而导致大型数据库的初始化失败，请将 **nsslapd-idletimeout** 参数设置为更高的值。例如，要将参数设置为 **7200** (2 小时)，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://supplier2.example.com config replace
nsslapd-idletimeout=7200
```

要设置无限周期，请将 **nsslapd-idletimeout** 设置为 **0**。

第 4 章 使用 WEB 控制台配置多层次复制

在多层次复制环境中，两个或多个可写供应商相互复制数据。例如，设置多层次复制以提供故障转移环境，并将负载分发到多个服务器。然后，客户端可以在任何属于读写副本的主机上执行读写操作。

本节假设您在名为 provider **1.example.com** 的主机上运行现有的 Directory 服务器实例。该流程描述了如何将名为 provider **2.example.com** 的另一个读写副本添加到拓扑中，以及如何为 **dc=example,dc=com** 后缀配置多层次复制。

4.1. 使用 WEB 控制台准备新供应商

要准备 provider **2.example.com** 主机，请启用复制。这个过程：

- 在复制拓扑中配置此服务器的角色
- 定义复制的后缀
- 创建供应商用来连接到此主机的复制管理器帐户

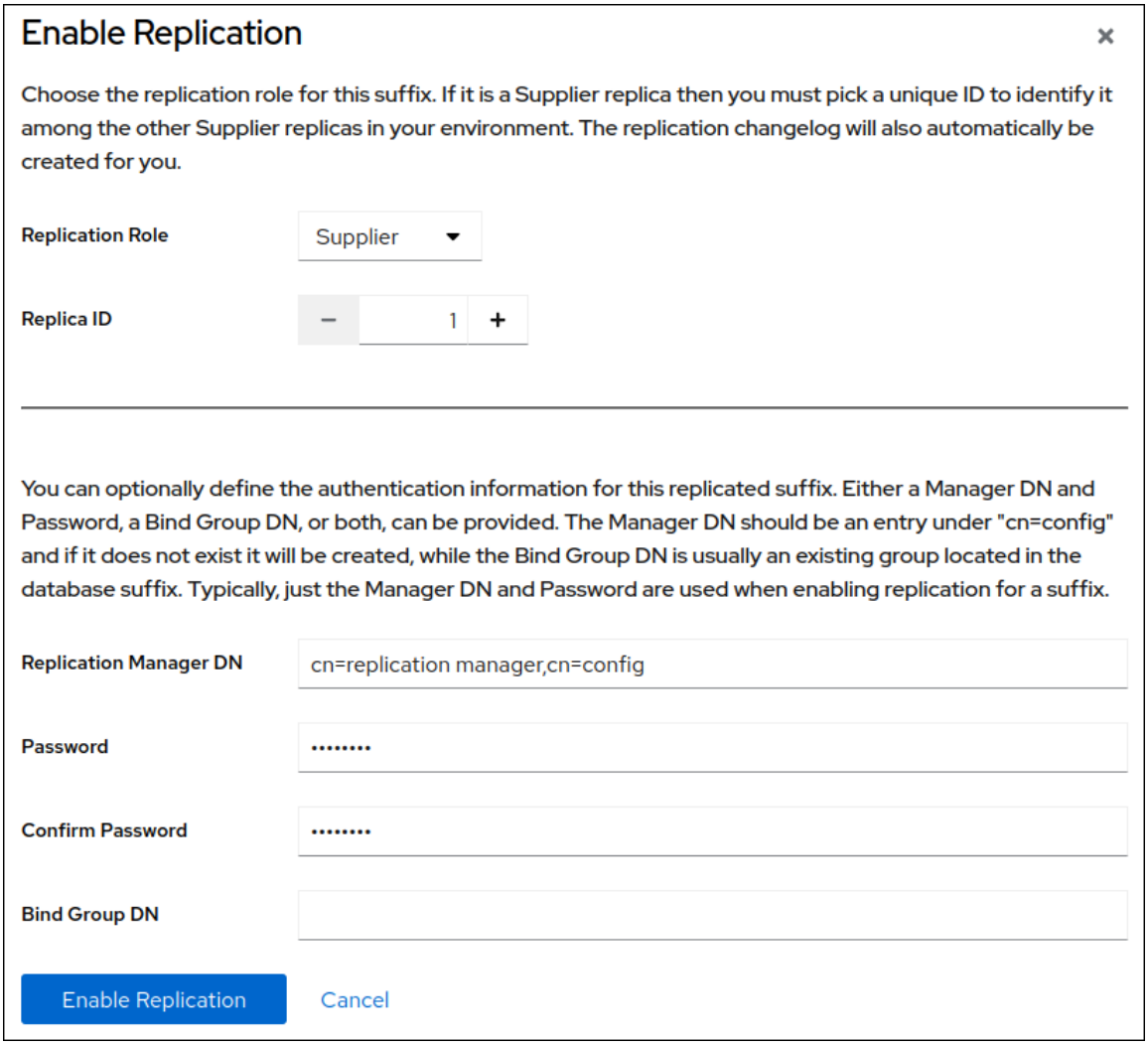
在您要添加到复制拓扑的供应商上执行这个步骤。

前提条件

- 已安装 Directory 服务器实例。
- **dc=example,dc=com** 后缀的数据库存在。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 启用复制：
    a. 点 **Enable Replication**。
    b. 在 **Replication Role** 字段中选择 **Supplier**，输入副本 ID，以及要创建的复制管理器帐户的可分辨名称(DN)和密码：



这些设置将主机配置为 **dc=example,dc=com** 后缀的供应商，并将此条目的副本 ID 设置为 **1**。

重要

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数。

如果没有设置复制管理器 DN，请设置绑定组 DN。然后您可以在复制协议中使用此组的任何成员。

c. 点 **Enable Replication**。

验证

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 如果 **Replica Role** 字段包含值 **Supplier**，则启用复制，主机被配置为供应商。

其他资源

- 安装 Red Hat Directory Server
- 在单独的数据库中存储后缀

4.2. 使用 WEB 控制台将现有服务器配置为新服务器的供应商

要准备现有服务器 provider **1.example.com** 作为供应商，您需要：

- 为后缀启用复制。
- 为新供应商创建复制协议。
- 初始化新供应商。

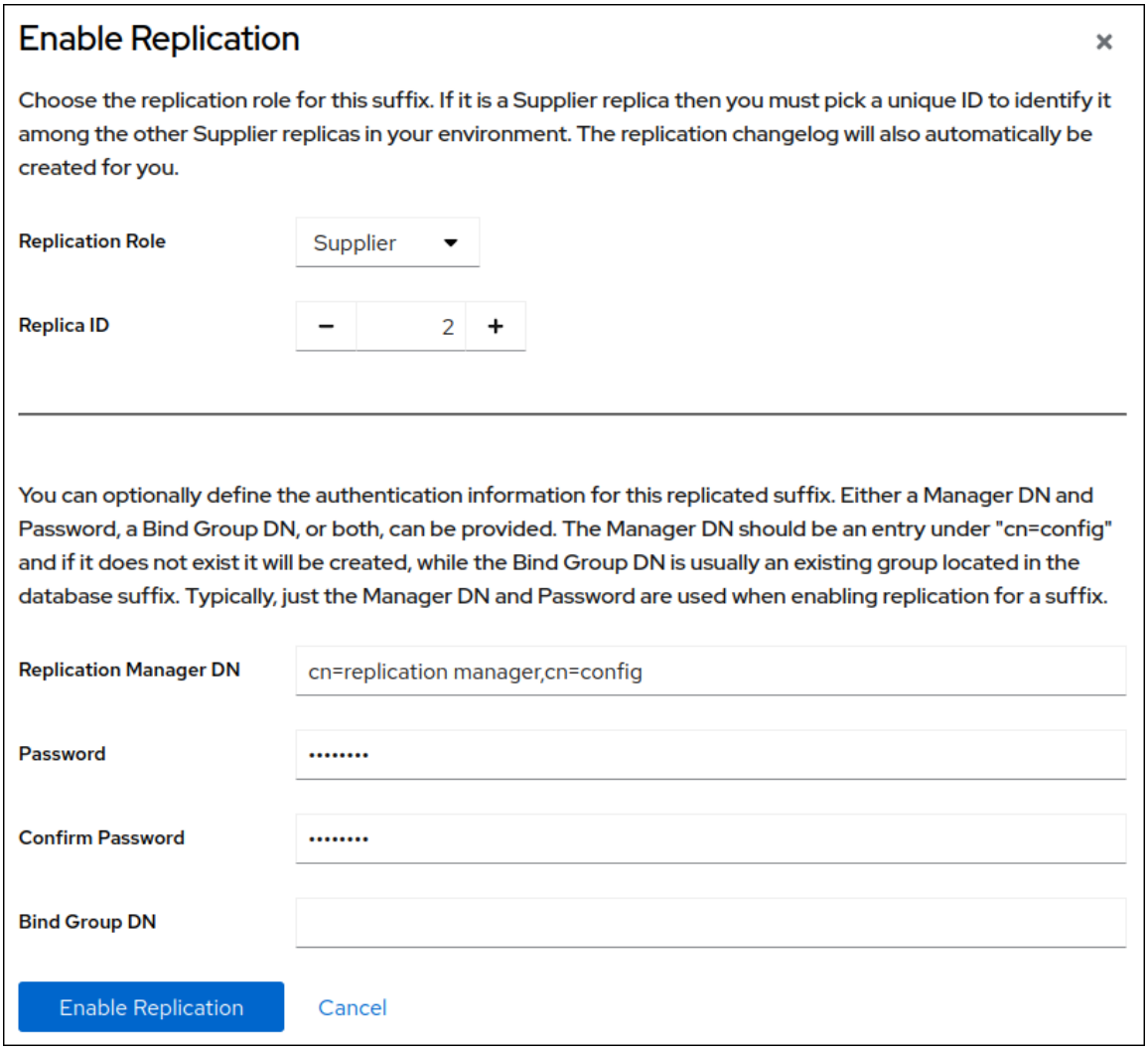
在复制拓扑中的现有供应商上执行这个步骤。

前提条件

- 您在供应商上启用了 **dc=example,dc=com** 后缀的复制来加入。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 启用复制：
   a. 点 **Enable Replication**。
   b. 在 **Replication Role** 字段中选择 **Supplier**，输入副本 ID，以及要创建的复制管理器帐户的可分辨名称(DN)和密码：



这些设置将主机配置为 **dc=example,dc=com** 后缀的供应商，并将此条目的副本 ID 设置为 **2**。

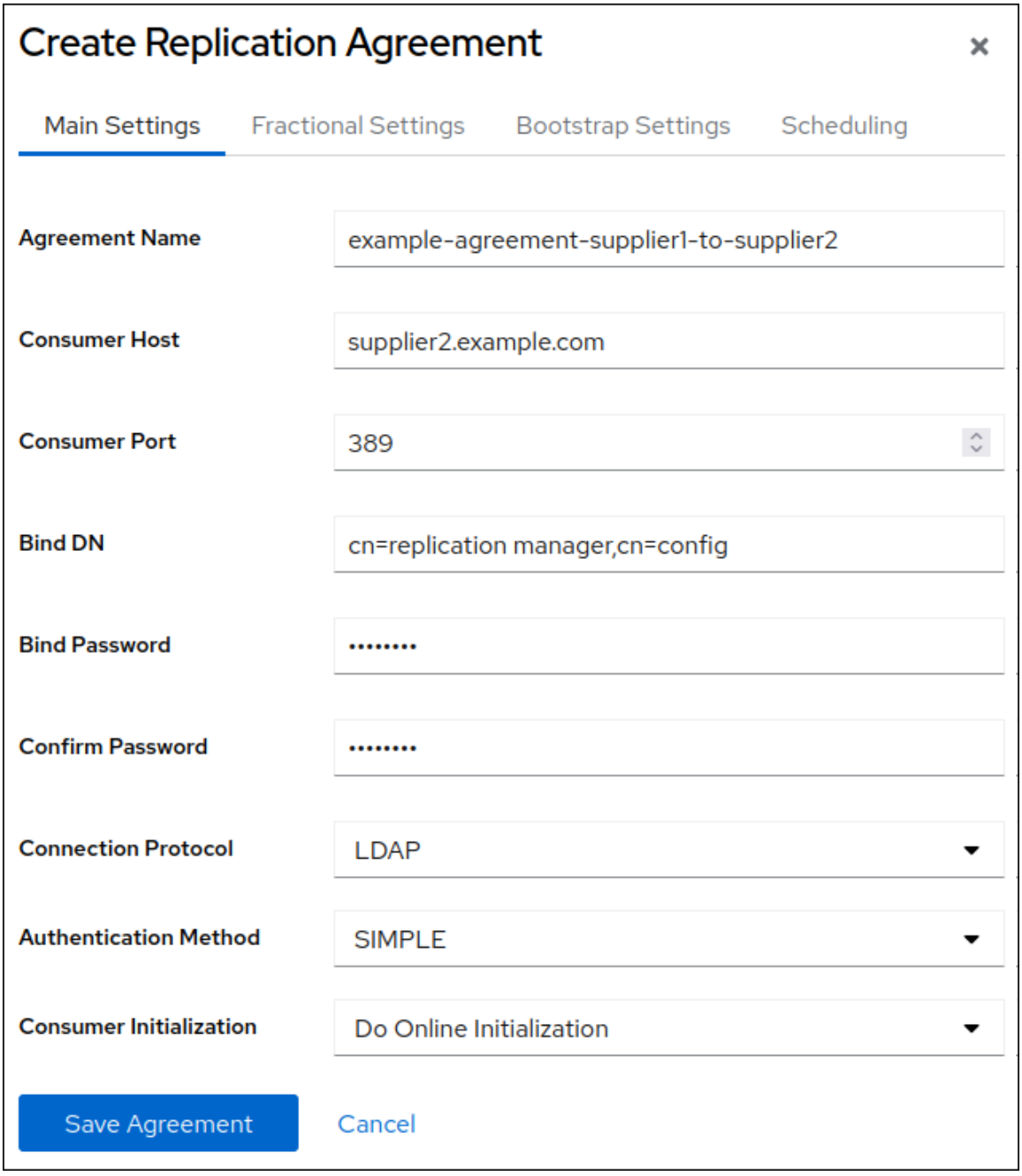
重要

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数。

c. 点 **Enable Replication**。

4. 添加复制协议并初始化新的服务器：

a. 在 **Agreements** 选项卡中，点 **Create Agreement**，并填写字段：



这些设置创建一个名为 **example-agreement-supplier1-to-supplier2** 的复制协议。复制协议定义设置，如供应商的主机名、协议和身份验证信息，供应商在将数据连接并复制到新供应商时使用的身份验证信息。

b. 在 **Consumer Initialization** 字段中选择 **Do Online Initialization**，以在保存协议后自动初始化新的服务器。

c. 点 **Save Agreement**。
创建协议后，目录服务器会初始化 vendor **2.example.com**。根据要复制的数据量，初始化可能会非常耗时。

验证

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 在 **Agreements** 选项卡中，验证表的 **State** 列中协议的状态。

4.3. 使用 WEB 控制台将新服务器配置为现有服务器的供应商

要准备新的服务器 provider **2.example.com** 作为供应商，您需要：

- 为后缀启用复制。
- 创建到现有服务器的复制协议。
- 初始化现有服务器。

在复制拓扑中的现有供应商上执行这个步骤。

警告

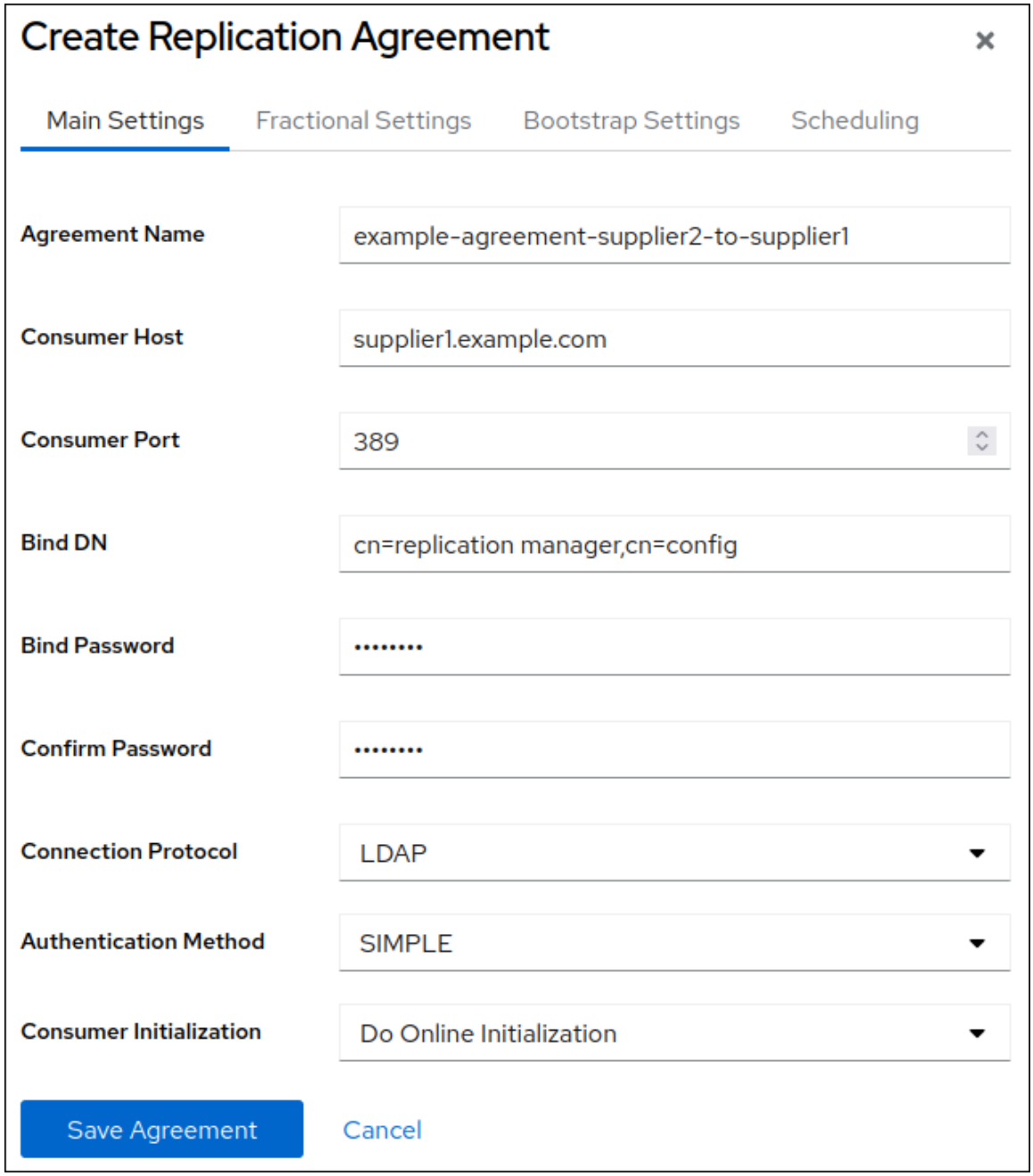
如果您没有在现有服务器上初始化复制协议，请不要继续。否则，新服务器中的空数据库会覆盖现有供应商上的数据库。

前提条件

- 您可以在新服务器上为 **dc=example,dc=com** 后缀启用复制。
- 您在现有服务器上为 **dc=example,dc=com** 后缀启用复制。
- 要加入的新服务器已被成功初始化。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 添加复制协议并初始化现有服务器：
    a. 在 **Agreements** 选项卡中，点 **Create Agreement**，并填写字段：



这些设置创建一个名为 **example-agreement-supplier2-to-supplier1** 的复制协议。复制协议定义了设置，如现有服务器的主机名、协议和身份验证信息，供应商在将数据连接并复制到现有供应商时使用的身份验证信息。

b. 在 **Consumer Initialization** 字段中选择 **Do Online Initialization**，以在保存协议后自动初始化新的服务器。

c. 点 **Save Agreement**。
创建协议后，目录服务器会初始化 provider **1.example.com**。根据要复制的数据量，初始化可能会非常耗时。

验证

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 在 **Agreements** 选项卡中，验证表的 **State** 列中协议的状态。

State	Last Init Status
Enabled	***Initialized***

第 5 章 使用基于证书的身份验证配置多层次复制

当您在两个目录服务器实例之间建立复制时，您可以使用基于证书的身份验证，而不使用绑定 DN 和密码对复制合作伙伴进行身份验证。

您可以通过在复制拓扑中添加新服务器并使用基于证书的身份验证在新主机和现有服务器之间设置复制协议。

重要

基于证书的验证需要 TLS 加密连接。

5.1. 准备帐户和绑定组，以便在带有基于证书的验证的复制协议中使用

要在复制协议中使用基于证书的身份验证，首先准备帐户，并将客户端证书存储在这些帐户的 **userCertificate** 属性中。另外，这个流程会创建一个稍后在复制协议中使用的绑定组。

在现有主机 **server1.example.com** 上执行此流程。

前提条件

- 您在目录服务器中启用了 TLS 加密。
- 您以区分编码规则(DER)格式存储客户端证书，格式为 **/root/server1.der** 和 **/root/server2.der** 文件。
  有关客户端证书以及如何从您的证书颁发机构(CA)请求它们的详情，请查看您的 CA 文档。

流程

1. 如果 **ou=services** 条目不存在，请创建它：

```
# ldapadd -D "cn=Directory Manager" -W -H ldaps://server1.example.com -x

dn: ou=services,dc=example,dc=com
objectClass: organizationalunit
objectClass: top
ou: services
```

2. 为两个服务器创建帐户，如 **cn=server1、ou=services,dc=example,dc=com** 和 **cn=server1,ou=services,dc=example,dc=com** ：

```
# ldapadd -D "cn=Directory Manager" -W -H ldaps://server1.example.com -x

dn: cn=server1,ou=services,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: inetOrgPerson
sn: server1
cn: server1
userPassword: password
userCertificate:< file:///root/server1.der

adding new entry "cn=server1,ou=services,dc=example,dc=com"
```

```
dn: cn=server2,ou=services,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: inetOrgPerson
sn: server2
cn: server2
userPassword: password
userCertificate:< file:///root/server2.der

adding new entry "cn=server2,ou=services,dc=example,dc=com"
```

3. 创建一个组，如 **cn=repl_servers,dc=groups,dc=example,dc=com** ：

```
# dsidm -D "cn=Directory Manager" ldaps://server1.example.com -b
"dc=example,dc=com" group create --cn "repl_servers"
```

4. 将两个复制帐户作为成员添加到组中：

```
# dsidm -D "cn=Directory Manager" ldaps://server1.example.com -b
"dc=example,dc=com" group add_member repl_servers
"cn=server1,ou=services,dc=example,dc=com"

# dsidm -D "cn=Directory Manager" ldaps://server1.example.com -b
"dc=example,dc=com" group add_member repl_servers
"cn=server2,ou=services,dc=example,dc=com"
```

其他资源

- 启用到目录服务器的 TLS 加密连接

5.2. 使用临时复制管理器帐户初始化新的服务器

基于证书的验证使用 目录中存储的证书。但是，在初始化新服务器前，**server2.example.com** 上的数据库为空，相关证书的帐户不存在。因此，在数据库初始化前无法使用证书复制。您可以使用临时复制管理器帐户初始化 **server2.example.com** 来解决这个问题。

前提条件

- 您已在 **server2.example.com** 上安装 Directory 服务器实例。
- **dc=example,dc=com** 后缀的数据库存在。
- 您可以在服务器(**server1.example.com** 和 **server2.example.com** 上的目录服务器)中启用了 TLS 加密。

流程

1. 在 **server2.example.com** 上，为 **dc=example,dc=com** 后缀启用复制：

```
# dsconf -D "cn=Directory Manager" ldaps://server2.example.com replication enable --
suffix "dc=example,dc=com" --role "supplier" --replica-id 2 --bind-dn "cn=replication
manager,cn=config" --bind-passwd "password"
```

此命令将 **server2.example.com** 主机配置为 **dc=example,dc=com** 后缀的供应商，并将此主机的副本 ID 设置为 **2**。此外，命令还会创建具有指定密码的临时 **cn=replication managercn=config** 用户，并允许此帐户将后缀更改复制到此主机。

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数。

2. 在 **server1.example.com** 上：

   a. 启用复制：

   ```
   # dsconf -D "cn=Directory Manager" ldaps://server1.example.com replication
   enable --suffix="dc=example,dc=com" --role="supplier" --replica-id="1"
   ```

   b. 创建一个临时复制协议，它使用上一步中的临时帐户进行身份验证：

   ```
   # dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt create
   --suffix="dc=example,dc=com" --host="server1.example.com" --port=636 --conn-
   protocol=LDAPS --bind-dn="cn=Replication Manager,cn=config" --bind-
   passwd="password" --bind-method=SIMPLE --init temporary_agreement
   ```

验证

1. 验证初始化是否成功：

   ```
   # dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt init-status
   --suffix "dc=example,dc=com" temporary_agreement
   Agreement successfully initialized.
   ```

其他资源

- Installing Red Hat Directory Server
- 启用到目录服务器的 TLS 加密连接

5.3. 使用基于证书的身份验证配置多层次复制

在带有基于证书的身份验证的多层次复制环境中，副本使用证书验证其他副本。

前提条件

- 您可以在两个主机上(**server1.example.com** 和 **server2.example.com**)上设置基于证书的身份验证。
- 目录服务器信任发布客户端证书的证书颁发机构(CA)。
- 客户端证书满足服务器上 **/etc/dirsrv/slapd-instance_name/certmap.conf** 中设置的要求。

流程

1. 在 **server1.example.com** 上：

   a. 删除临时复制协议：

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt delete
--suffix="dc=example,dc=com" temporary_agreement
```

b. 将 **cn=repl_servers,dc=groups,dc=example,dc=com** 绑定组添加到复制设置中：

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com replication set --
suffix="dc=example,dc=com" --repl-bind-group
"cn=repl_servers,dc=groups,dc=example,dc=com"
```

c. 配置 Directory Server 以自动检查 bind 组中的更改：

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com replication set --
suffix="dc=example,dc=com" --repl-bind-group-interval=0
```

2. 在 **server2.example.com** 上：

a. 删除临时复制管理器帐户：

```
# dsconf -D "cn=Directory Manager" ldaps://server2.example.com replication
delete-manager --suffix="dc=example,dc=com" --name="Replication Manager"
```

b. 将 **cn=repl_servers,dc=groups,dc=example,dc=com** 绑定组添加到复制设置中：

```
# dsconf -D "cn=Directory Manager" ldaps://server2.example.com replication set --
suffix="dc=example,dc=com" --repl-bind-group
"cn=repl_servers,dc=groups,dc=example,dc=com"
```

c. 配置 Directory Server 以自动检查 bind 组中的更改：

```
# dsconf -D "cn=Directory Manager" ldap://server2.example.com replication set --
suffix="dc=example,dc=com" --repl-bind-group-interval=0
```

d. 使用基于证书的身份验证创建复制协议：

```
dsconf -D "cn=Directory Manager" ldaps://server2.example.com repl-agmt create --
suffix="dc=example,dc=com" --host="server1.example.com" --port=636 --conn-
protocol=LDAPS --bind-method="SSLCLIENTAUTH" --init server2-to-server1
```

3. 在 **server1.example.com** 上，使用基于证书的身份验证创建复制协议：

```
dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt create --
suffix="dc=example,dc=com" --host="server2.example.com" --port=636 --conn-
protocol=LDAPS --bind-method="SSLCLIENTAUTH" --init server1-to-server2
```

验证

1. 在每个服务器上验证初始化是否成功：

```
# dsconf -D "cn=Directory Manager" ldaps://server1.example.com repl-agmt init-status
--suffix "dc=example,dc=com" server1-to-server2
Agreement successfully initialized.
```

```
# dsconf -D "cn=Directory Manager" ldaps://server2.example.com repl-agmt init-status
--suffix "dc=example,dc=com" server2-to-server1
Agreement successfully initialized.
```

其他资源

- 设置基于证书的身份验证
- 更改 CA 信任标记

第 6 章 使用命令行配置级联复制

在级联复制场景中，一个服务器(hub)作为消费者和供应商。hub 是一个只读副本，维护更改日志。它从供应商接收更新，并将这些更新提供给消费者。使用级联复制来平衡大量流量负载，或在地理分布环境中保持基于供应商的本地。

6.1. 使用命令行准备新的 HUB 服务器

要准备 **hub.example.com** 主机，启用复制。这个过程：

- 在复制拓扑中配置此服务器的角色
- 定义复制的后缀
- 创建供应商用来连接到此主机的复制管理器帐户

在您要添加到复制拓扑的 hub 上执行这个步骤。

前提条件

- 已安装 Directory 服务器实例。
- dc=example,dc=com 后缀的数据库存在。

流程

- 为 **dc=example,dc=com** 后缀启用复制：

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com replication enable --suffix "dc=example,dc=com" --role "hub" --bind-dn "cn=replication manager,cn=config" --bind-passwd "password"
```

此命令将 **hub.example.com** 主机配置为 **dc=example,dc=com** 后缀的 hub。此外，命令还会创建具有指定密码的 **cn=replication managercn=config** 用户，并允许此帐户将后缀更改复制到此主机。

验证

- 显示复制配置：

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com replication get --suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 2
nsDS5ReplicaId: 65535
...
```

这些参数表示：

  - **nsDS5ReplicaBindDN** 指定复制管理器帐户。

- **nsDS5ReplicaRoot** 设置复制的后缀。
- **nsDS5ReplicaType** 设置为 **2** 定义此主机是一个消费者，它也对 hub 有效。
- **nsDS5ReplicaId** 设置为 **65535** 定义此主机是一个 hub。如果您定义 **--role "hub"** 选项，则 **dsconf** 工具会自动设置这个值。

其他资源

- 安装 Red Hat Directory Server
- 在单独的数据库中存储后缀
- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

6.2. 使用命令行将现有服务器配置为 HUB 服务器的供应商

要将现有服务器准备为供应商，您需要：

- 为后缀启用复制。
- 创建到 hub 的复制协议。
- 初始化 hub。

在复制拓扑中的现有供应商上执行这个步骤。

前提条件

- 您在 hub 上为 **dc=example,dc=com** 后缀启用复制以加入。

流程

1. 为 **dc=example,dc=com** 后缀启用复制：

```
# [command]`dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication enable --suffix "dc=example,dc=com" --role "supplier" --replica-id 1
```

此命令将 provider. **example.com** 主机配置为 **dc=example,dc=com** 后缀的供应商，并将此条目的副本 ID 设置为 **1**。

重要

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数。

2. 添加复制协议并初始化新的服务器：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt create --suffix "dc=example,dc=com" --host "hub.example.com" --port 389 --conn-protocol LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method SIMPLE --init example-agreement-supplier-to-hub
```

此命令创建一个名为 **example-agreement-supplier-to-hub** 的复制协议。复制协议定义设置，如 hub 的主机名、协议和供应商在将数据连接到 hub 时使用的身份验证信息。

创建协议后，目录服务器会初始化 **hub.example.com**。根据要复制的数据量，初始化可能会非常耗时。

验证

1. 显示复制配置：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication get --suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 3
...
```

这些参数表示：

- **nsDS5ReplicaRoot** 设置复制的后缀。
- **nsDS5ReplicaType** 设置为 **3** 定义此主机是一个供应商。

2. 验证初始化是否成功：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt init-status --suffix "dc=example,dc=com" example-agreement-supplier-to-hub
Agreement successfully initialized.
```

3. 显示复制状态：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement-supplier-to-hub
Status For Agreement: "example-agreement-supplier-to-hub" (hub.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20210331105030Z
Last Update End: 20210331105030Z
Number Of Changes Sent: 0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210331105026Z
Last Init End: 20210331105029Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: Not in Synchronization: supplier (Unknown) consumer (Unknown) State (green) Reason (error (0) replica acquired successfully: incremental update succeeded)
Replication Lag Time: Unavailable
```

验证 **Replication Status** 和 **Last Update Status** 字段。

故障排除

1. 默认情况下，服务器上所有协议的复制闲置超时为 1 小时。如果因为超时而导致大型数据库的初始化失败，请将 **nsslapd-idletimeout** 参数设置为更高的值。例如，要将参数设置为 **7200** (2 小时)，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://supplier1.example.com config replace
nsslapd-idletimeout=7200
```

要设置无限周期，请将 **nsslapd-idletimeout** 设置为 **0**。

其他资源

- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

6.3. 使用命令行准备 HUB 的新消费者

要准备 **consumer.example.com** 主机，请启用复制。这个过程：

- 在复制拓扑中配置此服务器的角色
- 定义复制的后缀
- 创建复制管理器帐户，hub 用来连接到此主机

在您要添加到复制拓扑的消费者上执行这个步骤。

前提条件

- 已安装 Directory 服务器实例。
- **dc=example,dc=com** 后缀的数据库存在。

流程

- 为 **dc=example,dc=com** 后缀启用复制：

```
# dsconf -D "cn=Directory Manager" ldap://consumer.example.com replication enable
--suffix "dc=example,dc=com" --role "consumer" --bind-dn "cn=replication
manager,cn=config" --bind-passwd "password"
```

此命令将 **consumer.example.com** 主机配置为 **dc=example,dc=com** 后缀的使用者。此外，命令还会创建具有指定密码的 **cn=replication managercn=config** 用户，并允许此帐户将后缀更改复制到此主机。

验证

- 显示复制配置：

```
# dsconf -D "cn=Directory Manager" ldap://consumer.example.com replication get --
suffix "dc=example,dc=com"
dn: cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
...
nsDS5ReplicaBindDN: cn=replication manager,cn=config
nsDS5ReplicaRoot: dc=example,dc=com
nsDS5ReplicaType: 2
...
```

这些参数表示：

- **nsDS5ReplicaBindDN** 指定复制管理器帐户。
- **nsDS5ReplicaRoot** 设置复制的后缀。
- **nsDS5ReplicaType** 设置为 **2** 定义此主机是消费者。

其他资源

- 安装 Red Hat Directory Server
- 在单独的数据库中存储后缀
- cn=replica,cn=suffix_DN,cn=mapping tree,cn=config

6.4. 使用命令行将 HUB 服务器配置为消费者的供应商

要准备 hub，您需要：

- 创建到消费者的复制协议。
- 初始化消费者。

在复制拓扑的 hub 上执行这个步骤。

前提条件

- hub 被初始化，从供应商复制到 hub 可以正常工作。
- 您在 hub 上为 **dc=example,dc=com** 后缀启用复制。

流程

- 添加复制协议并初始化消费者：

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com repl-agmt create --suffix "dc=example,dc=com" --host "consumer.example.com" --port 389 --conn-protocol LDAP --bind-dn "cn=replication manager,cn=config" --bind-passwd "password" --bind-method SIMPLE --init example-agreement-hub-to-consumer
```

此命令创建一个名为 **example-agreement-hub-to-consumer** 的复制协议。复制协议定义设置，如消费者的主机名、协议和身份验证信息，如供应商在将数据连接和复制到此消费者时使用的身份验证信息。

创建协议后，目录服务器会初始化 **consumer.example.com**。根据要复制的数据量，初始化可能会非常耗时。

验证

1. 验证初始化是否成功：

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com repl-agmt init-status --suffix "dc=example,dc=com" example-agreement-hub-to-consumer
Agreement successfully initialized.
```

2. 显示复制状态：

```
# dsconf -D "cn=Directory Manager" ldap://hub.example.com repl-agmt status --suffix
"dc=example,dc=com" example-agreement-hub-to-consumer
Status For Agreement: "example-agreement-hub-to-consumer"
(consumer.example.com:389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20210331131534Z
Last Update End: 20210331131534Z
Number Of Changes Sent: 0
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
Last Init Start: 20210331131530Z
Last Init End: 20210331131533Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: Not in Synchronization: supplier (Unknown) consumer (Unknown) State
(green) Reason (error (0) replica acquired successfully: incremental update succeeded)
Replication Lag Time: Unavailable
```

验证 **Replication Status** 和 **Last Update Status** 字段。

故障排除

1. 默认情况下，服务器上所有协议的复制闲置超时为 1 小时。如果因为超时而导致大型数据库的初始化失败，请将 **nsslapd-idletimeout** 参数设置为更高的值。例如，要将参数设置为 **7200** (2 小时)，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://hub .example.com config replace nsslapd-
idletimeout=7200
```

要设置无限周期，请将 **nsslapd-idletimeout** 设置为 **0**。

第 7 章 使用 WEB 控制台配置级联复制

在级联复制场景中，一个服务器(hub)作为消费者和供应商。hub 是一个只读副本，维护更改日志。它从供应商接收更新，并将这些更新提供给消费者。使用级联复制来平衡大量流量负载，或在地理分布环境中保持基于供应商的本地。

7.1. 使用 WEB 控制台准备新的 HUB 服务器

要准备 **hub.example.com** 主机，启用复制。这个过程：

- 在复制拓扑中配置此服务器的角色
- 定义复制的后缀
- 创建供应商用来连接到此主机的复制管理器帐户

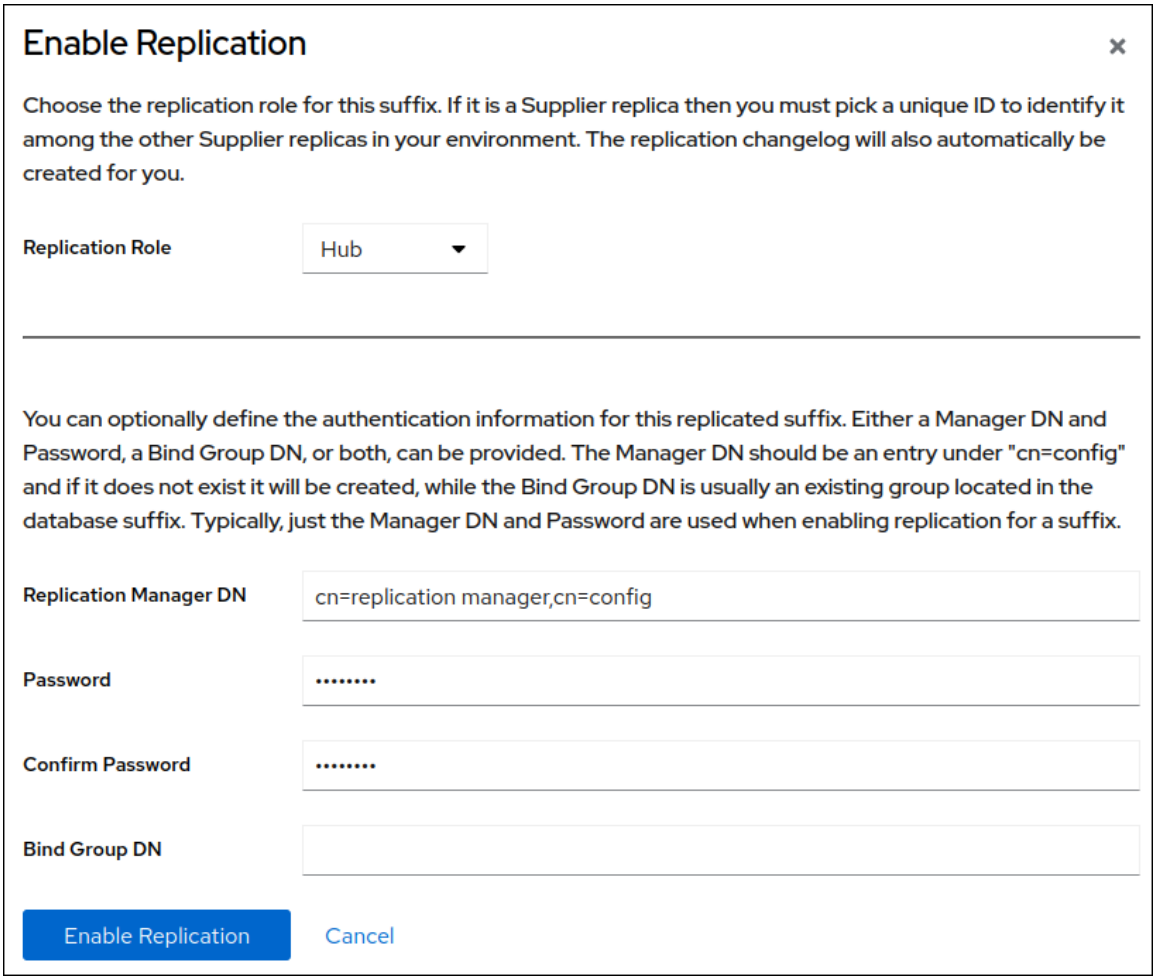
在您要添加到复制拓扑的 hub 上执行这个步骤。

前提条件

- 已安装 Directory 服务器实例。
- dc=example,dc=com 后缀的数据库存在。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 启用复制：
    a. 点 **Enable Replication**。
    b. 在 **Replication Role** 字段中选择 **Consumer**，并输入要创建的复制管理器帐户和密码：



这些设置将主机配置为 **dc=example,dc=com** 后缀的 hub。

c. 点 **Enable Replication**。

验证

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 如果 **Replica Role** 字段包含值 **Hub**，则启用复制，并且主机被配置为消费者。

其他资源

- 安装 Red Hat Directory Server
- 在单独的数据库中存储后缀

7.2. 使用 WEB 控制台将现有服务器配置为 HUB 服务器的供应商

要将现有服务器准备为供应商，您需要：

- 为后缀启用复制。
- 创建到 hub 的复制协议。
- 初始化 hub。

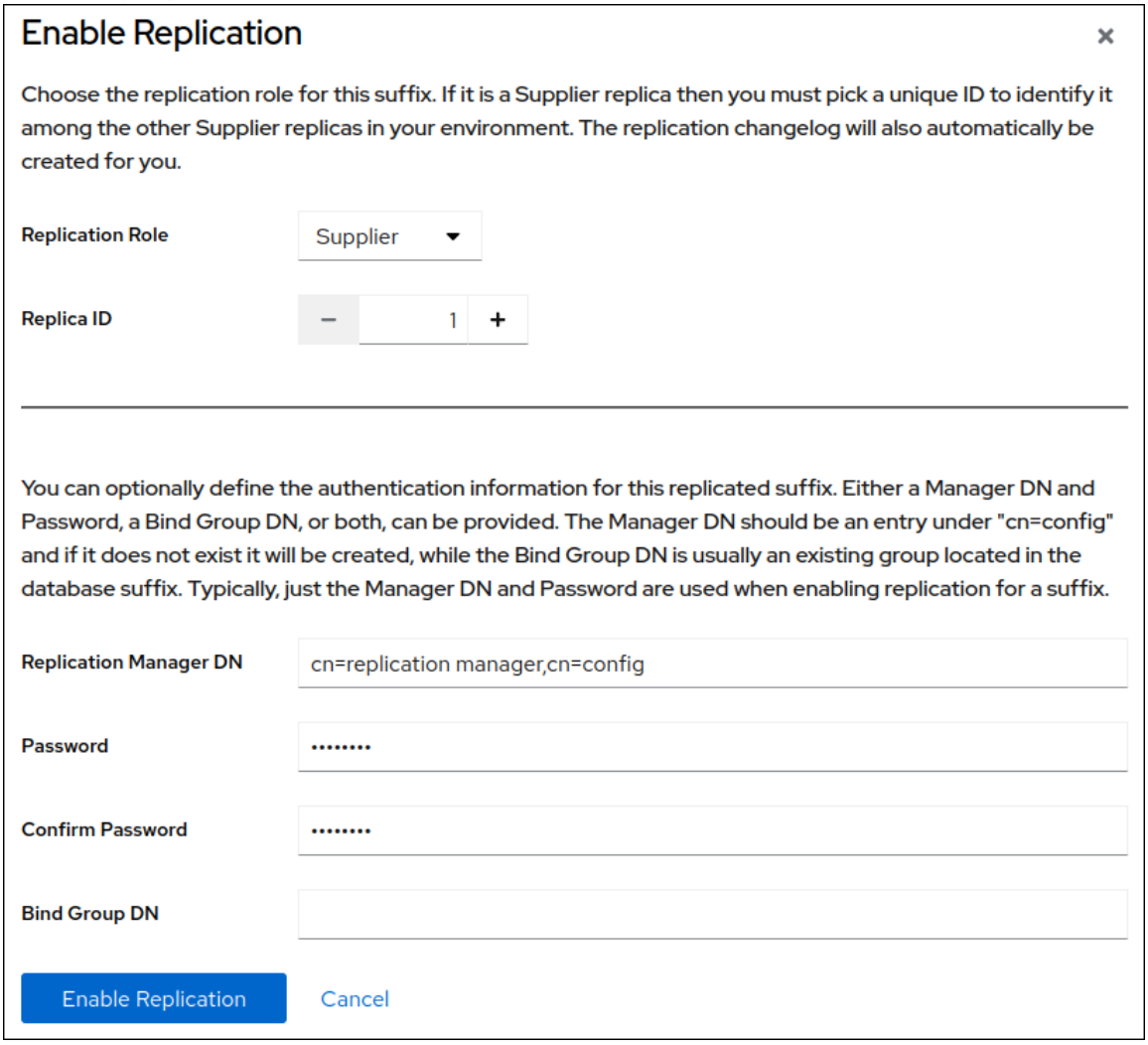
在复制拓扑中的现有供应商上执行这个步骤。

前提条件

- 您在 hub 上为 **dc=example,dc=com** 后缀启用复制以加入。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 启用复制：
   a. 点 **Enable Replication**。
   b. 在 **Replication Role** 字段中选择 **Supplier**，输入副本 ID，以及要创建的复制管理器帐户的可分辨名称(DN)和密码：



这些设置将主机配置为 **dc=example,dc=com** 后缀的供应商，并将此条目的副本 ID 设置为 **1**。

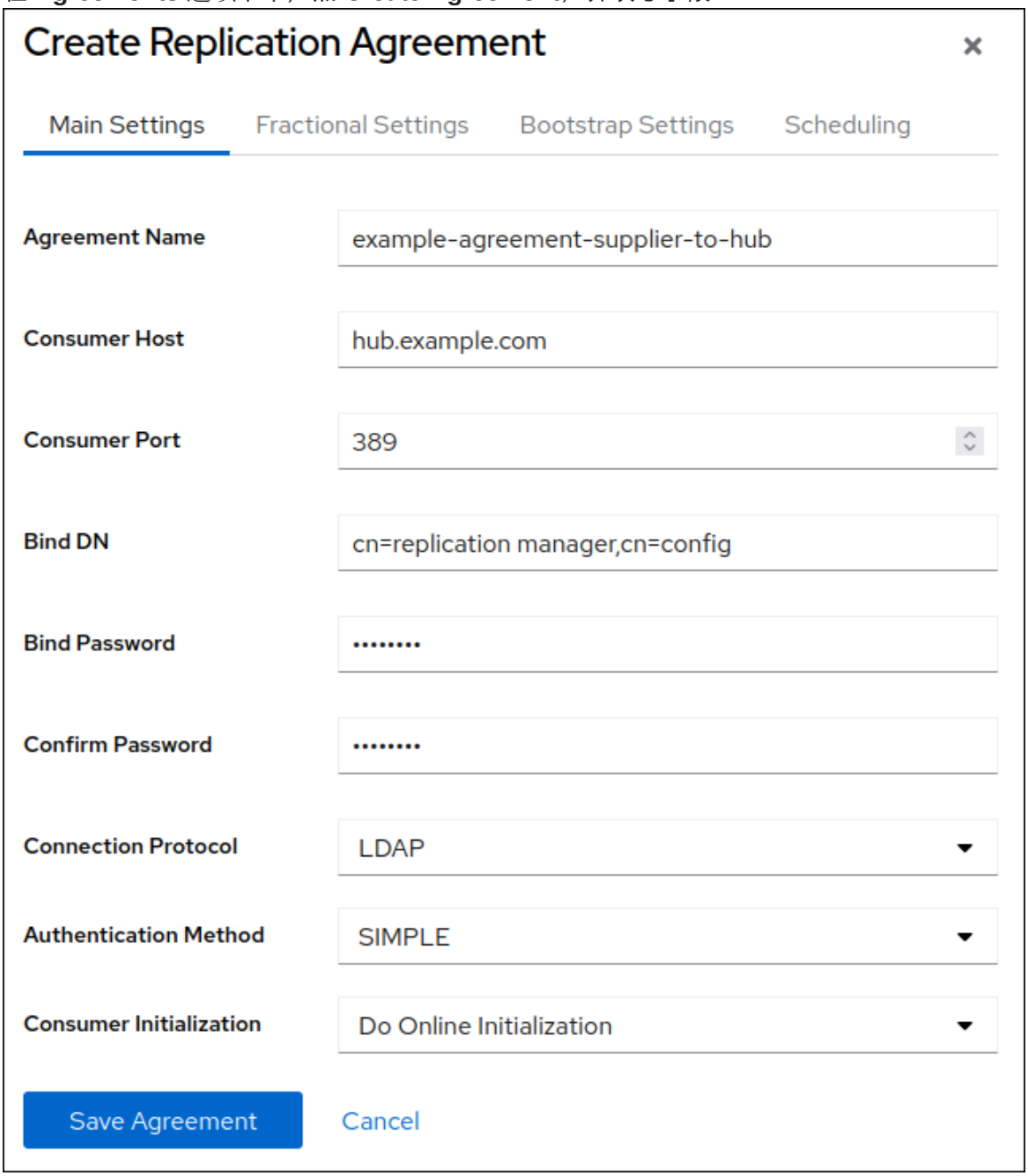
重要

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数。

c. 点 **Enable Replication**。

4. 添加复制协议并初始化新的服务器：

a. 在 **Agreements** 选项卡中，点 **Create Agreement**，并填写字段：



这些设置创建一个名为 **example-agreement-supplier-to-hub** 的复制协议。复制协议定义了设置，如 hub 的主机名、协议和身份验证信息，供应商在将数据连接并复制到此 hub 时使用的身份验证信息。

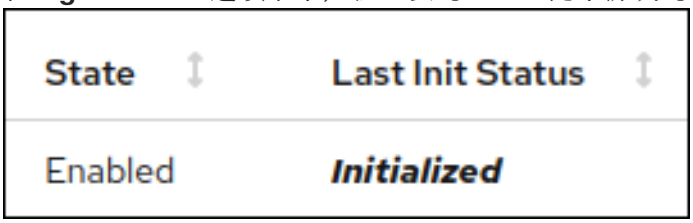
b. 在 **Consumer Initialization** 字段中选择 **Do Online Initialization**，以在保存协议后自动初始化新的服务器。

c. 点 **Save Agreement**。
创建协议后，目录服务器会初始化 **hub.example.com**。根据要复制的数据量，初始化可能会非常耗时。

验证

1. 打开 **Replication** 菜单。

2. 选择 **dc=example,dc=com** 后缀。
3. 在 **Agreements** 选项卡中，验证表的 **State** 列中协议的状态。



7.3. 使用 WEB 控制台准备 HUB 的新消费者

要准备 **consumer.example.com** 主机，请启用复制。这个过程：

- 在复制拓扑中配置此服务器的角色
- 定义复制的后缀
- 创建供应商用来连接到此主机的复制管理器帐户

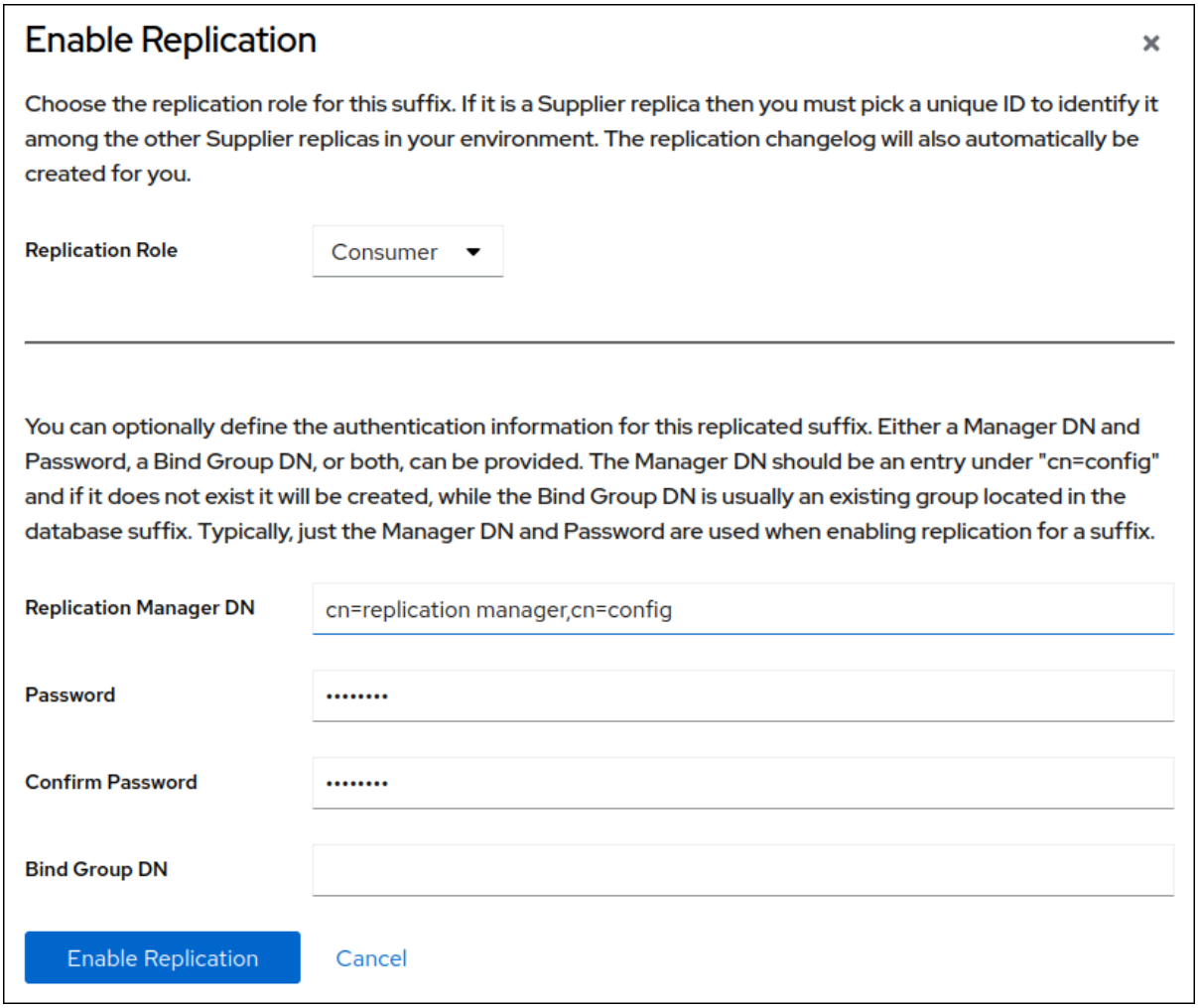
在您要添加到复制拓扑的消费者上执行这个步骤。

前提条件

- 已安装 Directory 服务器实例。
- **dc=example,dc=com** 后缀的数据库存在。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 点 **Enable Replication**。
4. 在 **Replication Role** 字段中选择 **Consumer**，并输入要创建的复制管理器帐户和密码：



这些设置将主机配置为 **dc=example,dc=com** 后缀的消费者。此外，服务器还会创建具有指定密码的 **cn=replication managercn=config** 用户，并允许此帐户将后缀更改复制到此主机。

5. 点 **Enable Replication**。

验证

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 如果 **Replica Role** 字段包含值 **Consumer**，则启用复制，主机被配置为消费者。

其他资源

- 安装 Red Hat Directory Server
- 在单独的数据库中存储后缀

7.4. 使用 WEB 控制台将 HUB 服务器配置为消费者的供应商

要准备 hub，您需要：

- 创建到消费者的复制协议。
- 初始化消费者。

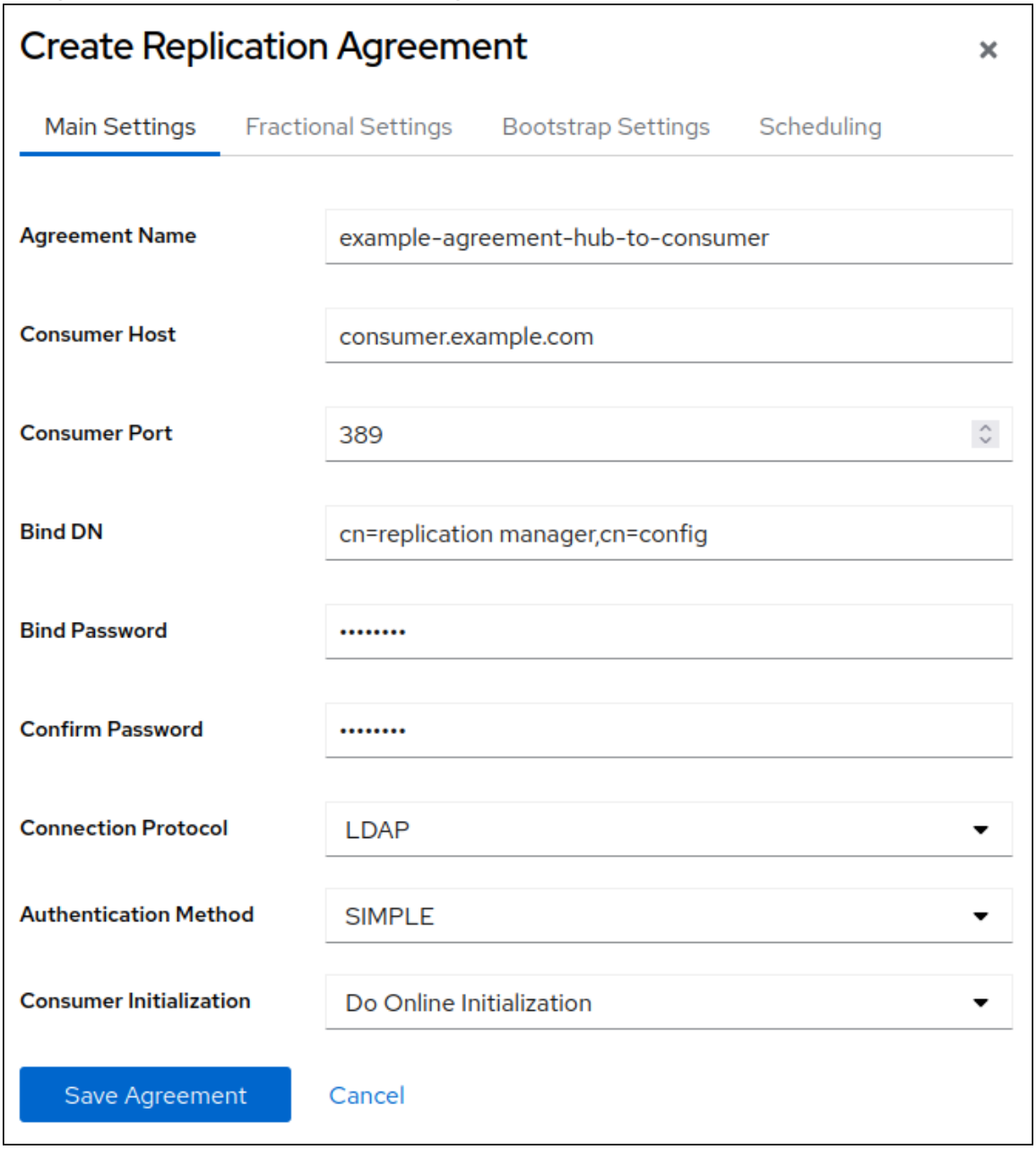
在复制拓扑的 hub 上执行这个步骤。

前提条件

- hub 被初始化，从供应商复制到 hub 可以正常工作。
- 您在 hub 上为 dc=example,dc=com 后缀启用复制。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 添加复制协议并初始化消费者：
   a. 在 **Agreements** 选项卡中，点 **Create Agreement**，并填写字段：



这些设置创建一个名为 **example-agreement-hub-to-consumer** 的复制协议。复制协议定义设置，如消费者的主机名、协议和身份验证信息，如 hub 连接和复制数据到这个消费者时使用的身份验证信息。

b. 在 **Consumer Initialization** 字段中选择 **Do Online Initialization**，以在保存协议后自动初始化消费者。

c. 点 **Save Agreement**。
创建协议后，目录服务器会初始化 **consumer.example.com**。根据要复制的数据量，初始化可能会非常耗时。

验证

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 在 **Agreements** 选项卡中，验证表的 **State** 列中协议的状态。

第 8 章 提高多层次复制环境中的延迟

在某些多层次复制环境中，例如，如果服务器通过广域网络(WAN)连接，则当多个供应商同时接收更新时，复制延迟可能会很高。当一个供应商只只访问一个副本时，会出现这种情况。在这种情况下，其他供应商无法向这个消费者发送更新，这会增加复制延迟。

要在固定时间后释放副本，请在供应商和 hub 上设置 **nsds5ReplicaReleaseTimeout** 参数。

注意

60 秒默认值适用于大多数环境。设置得太高或太低，可能会对复制性能造成负面影响。如果您设置的值太低，则复制服务器会持续相互清理，并且服务器无法发送许多更新。在高流量复制环境中，较长的超时时间可以提高一个供应商只访问副本的情况。但是，在大多数情形中，超过 **120** 秒的值会减慢复制速度。

8.1. 使用命令行设置复制发行超时

要在多层次复制环境中提高复制效率，请更新所有 hub 和供应商上的复制发行超时值。

前提条件

- 您在多个供应商和 hub 之间配置了复制。

流程

1. 为后缀设置超时值：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication set --
suffix="dc=example,dc=com" --repl-release-timeout=70
```

   此命令将 **example,dc=com** 后缀的复制超时更改为 **70** 秒。

2. 重启实例：

```
# dsctl instance_name restart
```

8.2. 使用 WEB 控制台设置复制发行超时

要在多层次复制环境中提高复制效率，请更新所有 hub 和供应商上的复制发行超时值。

前提条件

- 您在多个供应商和 hub 之间配置了复制。

流程

1. 在 **Replication** 选项卡中，选择后缀条目。
2. 单击 **Show Advanced Settings**。
3. 更新 **Replication Release Timeout** 字段中的值。
4. 单击 **Save Configuration**。

第 9 章 从复制拓扑中删除实例

在某些情况下，如硬件中断或结构性更改，管理员希望从复制拓扑中删除目录服务器实例。删除实例的过程取决于您要删除的副本的角色。

9.1. 从复制拓扑中删除消费者或 HUB

如果复制拓扑中不再需要消费者或 hub，请删除它。

前提条件

- 要删除的实例是消费者或 hub。
- 如果要删除的主机是一个 hub，它也充当拓扑中其他服务器的供应商，您配置了其他供应商或 hub 将数据复制到这些服务器，以防止它们被隔离。

流程

1. 在要删除的消费者或 hub 中：
   a. 列出后缀及其对应的数据库：

   ```
   # dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend
   suffix list
   dc=example,dc=com (userroot)
   ```

   请注意数据库的名称。

   b. 将数据库设置为只读模式以防止进一步更新：

   ```
   # dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend
   suffix set --enable-readonly "userroot"
   ```

2. 在所有具有与您要删除的消费者或 hub 的复制协议的供应商中：
   a. 列出复制的后缀的复制协议：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt list --
   suffix "dc=example,dc=com"
   dn: cn=example-agreement,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
   tree,cn=config
   cn: example-agreement
   ...
   ```

   cn 属性包含下一步中所需的复制协议名称。

   b. 删除复制协议：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt delete --
   suffix "dc=example,dc=com" example-agreement
   ```

3. 在要删除的消费者或 hub 中，禁用所有后缀的复制：

```
# dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com replication
disable --suffix "dc=example,dc=com"
```

如果此主机是 hub，禁用复制会自动删除这个服务器上这个后缀的所有复制协议。

后续步骤

- 如果要使用删除的实例用于测试目的，请禁用只读模式：

```
# dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend
suffix set --disable-readonly userroot
```

重要

如果要使用从拓扑中删除的实例用于测试目的，请确保没有客户端继续使用它。

- 删除实例：

```
# dsctl instance_name remove --do-it
```

其他资源

- 使用命令行配置单层次复制
- 使用命令行配置多层次复制
- 使用命令行配置级联复制

9.2. 从复制拓扑中删除供应商

从复制拓扑中删除供应商比删除 hub 或消费者更复杂。这是因为拓扑中的每个供应商都存储了其他供应商的信息，即使供应商突然不可用，它们也会保留这些信息。

目录服务器在一组称为副本更新向量(RUV)的元数据中维护关于复制拓扑的信息。RUV 包含有关供应商的信息，如 ID、URL、最新的更改状态号(CSN)，以及第一次更改的 CSN。供应商和消费者均存储 RUV 信息，它们使用它来控制复制更新。

要完全删除供应商，您必须删除其元数据以及配置条目。

前提条件

- 要删除的实例是供应商。
- 如果要删除的主机也充当拓扑中其他服务器的供应商，您配置了其他供应商或中心将数据复制到这些服务器，以防止它们被隔离。

流程

1. 在要删除的供应商中：
   a. 列出后缀及其对应的数据库：

```
# dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend
suffix list
dc=example,dc=com (userroot)
```

请注意数据库的名称。

b. 将数据库设置为只读模式以防止进一步更新：

```
# dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend
suffix set --enable-readonly "userroot"
```

c. 等待拓扑中的所有其他服务器收到此供应商的所有数据。要验证，请确保其他服务器上的 CSN 等于或大于供应商上要删除的 CSN：

```
# ds-replcheck online -D "cn=Directory Manager" -w password -m ldap://host-to-
remove.example.com:389 -r ldap://server.example.com:389 -b dc=example,dc=com
================================================================================
========
        Replication Synchronization Report  (Tue Mar  5 09:46:20 2021)
================================================================================
========

Database RUV's
======================================================

Supplier RUV:
 {replica 1 ldap://host-to-remove.example.com:389} 5c7e8927000100010000
5c7e89a0000100010000
 {replicageneration} 5c7e8927000000010000

Replica RUV:
 {replica 1 ldap://host-to-remove.example.com:389} 5c7e8927000100010000
5c7e8927000400010000
 {replica 2 ldap://server.example.com:389}
 {replicageneration} 5c7e8927000000010000
```

d. 显示副本 ID：

```
# dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com
replication get --suffix "dc=example,dc=com" | grep -i "nsds5replicaid"
nsDS5ReplicaId: 1
```

在本例中，副本 ID 是 **1**。记住此步骤的最后一步的副本 ID。

2. 在所有具有与您要删除的主机的复制协议的供应商中：

a. 列出复制的后缀的复制协议：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt list --
suffix "dc=example,dc=com"
dn: cn=example-agreement,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
cn: example-agreement
...
```

cn 属性包含下一步中所需的复制协议名称。

b. 删除复制协议：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt delete --
suffix "dc=example,dc=com" example-agreement
```

3. 在要删除的供应商上，禁用所有后缀的复制：

```
# dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com replication
disable --suffix "dc=example,dc=com"
```

禁用复制也会删除这个服务器上此后缀的所有复制协议。

4. 在继续操作前，请确保 **ds-replcheck** 输出的 **Replica RUV** 部分中列出的所有目录服务器实例都是在线的。

5. 在拓扑中剩余的其中一个供应商上，清理副本 ID 的 RUV：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-tasks cleanallruv -
-suffix "dc=example,dc=com" --replica-id 1
```

此命令要求您指定此流程前面步骤中显示的副本 ID。

验证

- 在 **ds-replcheck** 命令的输出中验证您删除的主机没有副本 ID 和 URL 的条目是否已保留：

```
# ds-replcheck online -D "cn=Directory Manager" -w password -m ldap://host-to-
remove.example.com:389 -r ldap://server.example.com:389 -b dc=example,dc=com
```

后续步骤

- 如果要使用删除的实例用于测试目的，请禁用只读模式：

```
# dsconf -D "cn=Directory Manager" ldap://host-to-remove.example.com backend
suffix set --disable-readonly userroot
```

重要

如果要使用从拓扑中删除的实例用于测试目的，请确保没有客户端继续使用它。

- 删除实例：

```
# dsctl instance_name remove --do-it
```

其他资源

- 使用命令行配置单层次复制
- 使用命令行配置多层次复制
- 使用命令行配置级联复制

第 10 章 在多层次复制拓扑中防止副本的 MONOPOLIZATION

在多层次复制拓扑中，具有重度更新负载的供应商也可以对副本进行单调，以便其他供应商也无法更新它。

这部分论述了发生 monopolization 时的情况，如何识别此问题，并提供了有关如何配置供应商以避免出现 monopolization 的情况。

10.1. 当发生 MONOPOLIZATION 时

多层次复制的一个功能是供应商获得对副本的独占访问。如果在锁定时供应商试图获取访问，副本会发回一个忙碌的响应，并且供应商会在启动另一个尝试前等待 **nsds5ReplicaBusyWaitTime** 参数中设置的时间。同时，供应商将其更新发送到另一个副本。当第一个副本再次可用时，供应商会向这个主机发送更新。

如果锁定的供应商处于重度更新负载时，或者更改更改中有很多待处理的更新，则可能会出现问题。在这种情况下，锁定供应商完成发送更新，并立即尝试重新排序同一副本。在大多数情况下，这种尝试会成功，因为其他供应商可能仍在等待。您可以在 **nsds5ReplicaSessionPauseTime** 参数中设置两个更新会话之间的暂停。这可能导致单个供应商在几个小时或更长时间内对副本进行单调。

10.2. 启用复制日志记录来识别副本的合并

如果一个或多个供应商经常处于更新负载，且副本经常收到更新，则启用记录复制消息来识别 monopolization 的情况。

前提条件

- 复制拓扑中有多个供应商。

流程

1. 启用复制日志记录：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com config replace
   nsslapd-errorlog-level=8192
   ```

   请注意，这个命令只启用复制日志记录，并禁用了记录其他错误消息。

2. 监控 **/var/log/dirsrv/slapd-*instance_name*/errors** 日志文件，并搜索以下出错信息：

   ```
   Replica Busy! Status: [Error (1) Replication error acquiring replica: replica busy]
   ```

   请注意，如果 Directory 服务器偶尔记录此错误，则代表正常。但是，如果副本经常没有接收更新，并且供应商会记录这个错误，请考虑更新您的配置来解决这个问题。

10.3. 配置供应商以避免发生重复副本

此流程描述了如何在供应商上设置参数，以防止对副本进行 monopolization。

由于环境和负载的区别，仅设置与您的情况相关的参数，并根据您的环境调整值。

前提条件

- 复制拓扑中有多个供应商。
- 目录服务器频繁记录 **Replica Busy!Status: [Error (1) Replication error acquiring replica: replica busy]** 错误。

流程

1. 设置 **nsds5ReplicaBusyWaitTime** 参数，以配置供应商在启动另一个尝试在副本发送忙碌响应后获取对副本的访问前等待的时间：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt set --suffix "dc=example,dc=com" --busy-wait-time 5 replication_agreement_name
```

   此命令设定等待 **5** 秒的时间。此设置仅适用于指定的复制协议。

2. 设置 **nsds5ReplicaSessionPauseTime** 参数，以配置供应商在两个更新会话之间等待的时间：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt set --suffix "dc=example,dc=com" --session-pause-time 15 replication_agreement_name
```

   此命令将 pause 设为 **15** 秒。默认情况下，**nsds5ReplicaSessionPauseTime** 是 **nsds5ReplicaBusyWaitTime** 中的值之一。此设置仅适用于指定的复制协议。

3. 设置 **nsds5ReplicaReleaseTimeout** 参数，以便在给定时间后终止复制会话，而不考虑是否发送更新是否完成：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication set --suffix "dc=example,dc=com" --repl-release-timeout 90
```

   此命令将超时设置为 **90** 秒。此设置适用于指定后缀的所有复制协议。

4. 可选：为供应商设置一个超时时间，使其不会保持连接到消费者无限尝试通过缓慢或有问题的连接发送更新：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt set --conn-timeout 600 --suffix "dc=example,dc=com" replication_agreement_name
```

   此命令将超时设置为 **600** 秒(10 分钟)。要识别 optimum 值，请检查访问日志是否有复制过程的平均时间，并相应地设置超时时间。

其他资源

- 配置和架构参考

第 11 章 在复制环境中的实例离线后强制复制更新

如果您停止了涉及进行常规维护复制中的目录服务器实例，供应商必须在恢复在线时立即更新目录数据。您可以使用命令行和 Web 控制台强制进行这个更新。

11.1. 使用命令行强制复制更新

在供应商上执行以下步骤，以对 **example-agreement** 中的 **dc=example,dc=com** 后缀强制执行复制更新。

前提条件

- 复制已设置。
- 消费者已初始化。

流程

1. 检查复制协议是否配置了更新计划：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt get --suffix "dc=example,dc=com" example-agreement
```

   如果命令的输出包含 **nsDS5ReplicaUpdateSchedule: *** 或 **nsDS5ReplicaUpdateSchedule** 参数不存在，则不会配置更新调度。

   如果 **nsDS5ReplicaUpdateSchedule** 包含调度，如以下所示，请注意该值：

```
nsDS5ReplicaUpdateSchedule: 0800-2200 0246
```

2. 如果配置了更新调度，请输入以下命令临时禁用它：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt set --schedule \* --suffix "dc=example,dc=com" example-agreement
```

3. 临时禁用复制协议：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt disable --suffix "dc=example,dc=com" example-agreement
```

4. 重新启用复制协议以强制复制更新：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt enable --suffix "dc=example,dc=com" example-agreement
```

5. 如果在此流程开始时配置了复制调度，请将调度设置为以前的值：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt set --schedule "0800-2200 0246" --suffix "dc=example,dc=com" example-agreement
```

验证

- 显示复制状态：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement
...
Last Update Start: 20210406120631Z
Last Update End: 20210406120631Z
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
...
```

11.2. 使用 WEB 控制台强制复制更新

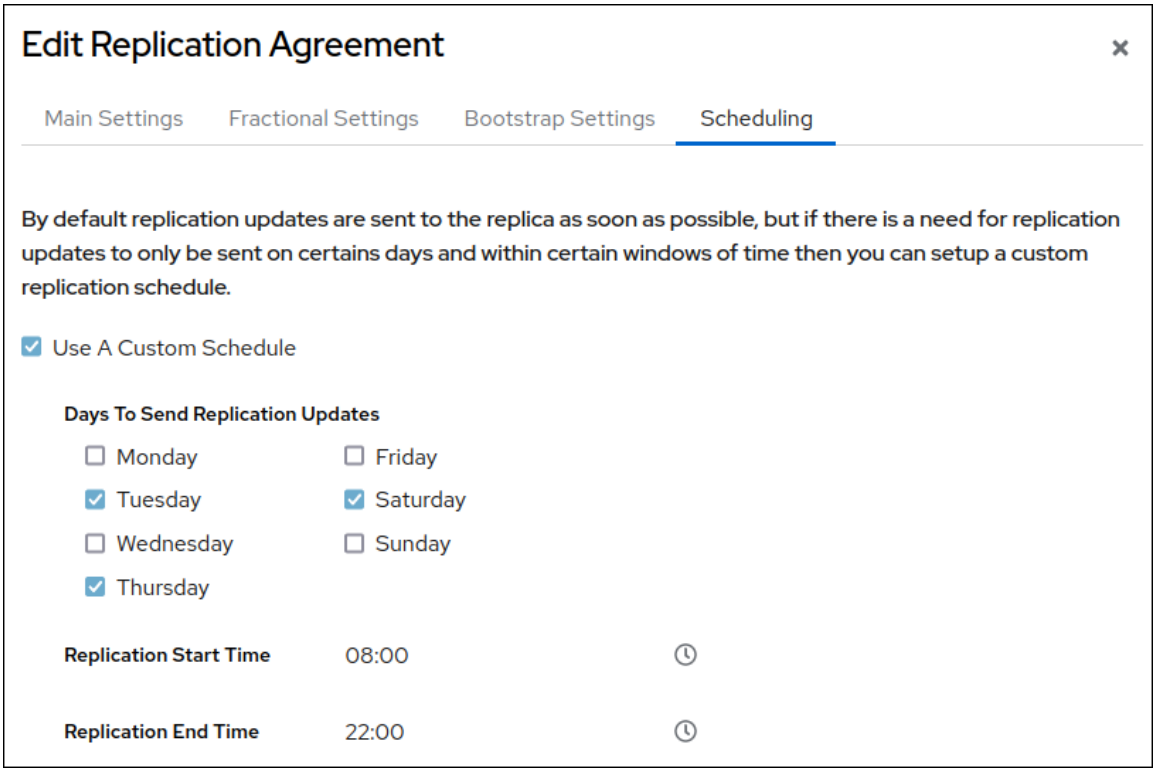
在供应商上执行以下步骤来强制实施复制更新。

前提条件

- 复制已设置。
- 消费者已初始化
- 在 web 控制台中登录到实例。

流程

1. 打开 **Replication** 菜单。
2. 选择 **dc=example,dc=com** 后缀。
3. 打开 **Agreements** 选项卡。
4. 检查复制协议是否配置了更新计划：
   a. 单击协议旁边的溢出菜单，然后选择 **Edit Agreement**。
   b. 在 **Scheduling** 选项卡中，记下当前设置的值。



如果没有选择 **Use A Custom Schedule**，则不会配置调度。

5. 单击复制协议旁边的 overflow 菜单，然后选择 **Disable/Enable Agreement** 来禁用协议。
State 列中协议的状态现在是 **Disabled**。

6. 再次单击复制协议旁边的 overflow 菜单，然后选择 **Disable/Enable Agreement** 来重新启用复制协议并强制实施复制更新。
State 列中协议的状态现在为 **Enabled**。

7. 如果在此流程开始时配置了复制调度，请将调度设置为以前的值：

   a. 单击 overflow 菜单，然后选择 **Actions → Edit Agreement**。

   b. 在 **Scheduling** 选项卡中，设置前面的值。

验证

- 显示复制状态：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com repl-agmt status --suffix "dc=example,dc=com" example-agreement
...
Last Update Start: 20210406120631Z
Last Update End: 20210406120631Z
Last Update Status: Error (0) Replica acquired successfully: Incremental update succeeded
...
```

第 12 章 更改副本的角色

在复制拓扑中，您可以更改副本的角色。例如，如果供应商因为硬件中断而不可用，您可以将消费者提升到供应商。另外，您可以降级（例如，具有低硬件资源的供应商）到消费者，并随后使用新硬件添加另一个供应商。

12.1. 使用命令行提升副本

您可以提升：

- hub 或供应商的消费者
- 供应商 hub

本节论述了如何提升 **dc=example,dc=com** 后缀的副本。

前提条件

- 目录服务器实例是复制拓扑的成员。
- 要提升的副本是消费者或 hub。

流程

1. 如果要提升的副本是带有复制协议的 hub，且 hub 在提升后不再将数据发送到其他主机，请删除复制协议：

   a. 列出 hub 上的复制协议：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt list --
   suffix "dc=example,dc=com"
   dn: cn=example-agreement,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
   tree,cn=config
   cn: example-agreement
   ...
   ```

   cn 属性包含下一步中所需的复制协议名称。

   b. 从 hub 中删除复制协议：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt delete --
   suffix "dc=example,dc=com" example-agreement
   ```

2. 提升实例：

   - 如果您将消费者或 hub 提升到供应商，请输入：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com replication
   promote --suffix "dc=example,dc=com" --newrole "supplier" --replica-id 2
   ```

   重要

   对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数值。

- 如果将消费者提升到 hub，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication
promote --suffix "dc=example,dc=com" --newrole "hub"
```

3. 如果新角色中的副本应该向拓扑中其他主机发送更新，则创建复制协议。

其他资源

- 使用命令行配置单层次复制
- 使用命令行配置多层次复制
- 使用命令行配置级联复制

12.2. 使用 WEB 控制台提升副本

您可以提升：

- hub 或供应商的消费者
- 供应商 hub

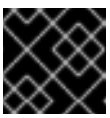
本节论述了如何提升 **dc=example,dc=com** 后缀的副本。

前提条件

- 目录服务器实例是复制拓扑的成员。
- 要提升的副本是消费者或 hub。
- 在 web 控制台中登录到实例。

流程

1. 如果要提升的副本是带有复制协议的 hub，且 hub 在提升后不再将数据发送到其他主机，请删除复制协议：
   a. 导航到 **复制协议** 。
   b. 单击您要删除的协议旁边的 **Actions**，然后选择 **Delete Agreement**。
2. 导航到 **Replication → Configuration**，然后单击 **Change Role** 按钮。
   - 如果您将消费者或 hub 提升到供应商，请选择 **Supplier**，并输入唯一的副本 ID。



重要

对于拓扑中的所有供应商，副本 ID 必须是 **1** 到 **65534** 之间的唯一整数值。

   - 如果将消费者提升到 hub，请选择 **Hub**。
3. 选择 **Yes, I am sure**。
4. 点 **Change Role**。

5. 如果新角色中的副本应该向拓扑中其他主机发送更新，则创建复制协议。

其他资源

- 使用 Web 控制台配置单层次复制
- 使用 Web 控制台配置多层次复制
- 使用 Web 控制台配置级联复制

12.3. 使用命令行降级副本

您可以降级：

- 消费者的供应商或 hub
- 消费者的 hub

本节论述了如何降级 **dc=example,dc=com** 后缀的副本。

前提条件

- 目录服务器实例是复制拓扑的成员。
- 要降级的副本是一个供应商或 hub。

流程

1. 如果要降级的副本具有不再需要的复制协议，例如，因为您要将副本降级为消费者，请删除复制协议：

   a. 列出副本中的复制协议：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt list --suffix "dc=example,dc=com"
   dn: cn=example-agreement,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config
   cn: example-agreement
   ...
   ```

   cn 属性包含下一步中所需的复制协议名称。

   b. 从副本中删除复制协议：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com repl-agmt delete --suffix "dc=example,dc=com" example-agreement
   ```

2. 降级实例：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com replication demote --suffix "dc=example,dc=com" --newrole "hub_or_consumer"
   ```

   根据您要配置的角色，将 **--newrole** 参数设置为 **hub** 或 **消费者**。

3. 如果您将副本配置为 hub，且应该向拓扑中的其他主机发送更新，请创建复制协议。

其他资源

- 使用命令行配置单层次复制
- 使用命令行配置多层次复制
- 使用命令行配置级联复制

12.4. 使用 WEB 控制台降级副本

您可以降级：

- 消费者的供应商或 hub
- 消费者的 hub

本节论述了如何降级 **dc=example,dc=com** 后缀的副本。

前提条件

- 目录服务器实例是复制拓扑的成员。
- 要降级的副本是一个供应商或 hub。
- 在 web 控制台中登录到实例。

流程

1. 如果要降级的副本具有不再需要的复制协议，例如，因为您要将副本降级为消费者，请删除复制协议：
   a. 导航到 **复制协议** 。
   b. 单击您要删除的协议旁边的 **Actions**，然后选择 **Delete Agreement**。
2. 导航到 **Replication → Configuration**，然后单击 **Change Role** 按钮。
3. 选择新的 replica 角色。
4. 选择 **Yes, I am sure**。
5. 点 **Change Role**。
6. 如果新角色中的副本应该向拓扑中其他主机发送更新，则创建复制协议。

其他资源

- 使用 Web 控制台配置单层次复制
- 使用 Web 控制台配置多层次复制
- 使用 Web 控制台配置级联复制

第 13 章 修剪复制更改日志

目录服务器更改日志管理接收和处理的更改的列表。它包括从复制合作伙伴接收的客户端更改和更改。

默认情况下，Directory 服务器会修剪 7 天旧的 changelog 条目。但是，您可以配置：

- **nsslapd-changelogmaxage** 参数中的 changelog 中条目的最大期限。
- **nsslapd-changelogmaxentries** 参数中更改日志的记录总数。

如果您至少启用了这些设置之一，Directory 服务器会默认每五分钟修剪 changelog (**nsslapd-changelogtrim-interval**)。

即使启用了修剪设置，之后创建的记录和记录都会保留在更改日志中，直到它们成功复制到拓扑中的所有服务器。如果您从拓扑中删除供应商，如从复制拓扑中删除 供应商 中所述，则目录服务器会从其他服务器上的 changelog 中修剪此供应商的所有更新。

13.1. 使用命令行配置复制 CHANGELOG 修剪

默认情况下，目录服务器会修剪 7 天以上的 changelog 条目。但是，您可以配置 Directory 服务器删除条目的时间。如果条目数量超过配置的值，您还可以将 Directory 服务器配置为自动删除条目。

本节描述了如何为 **dc=example,dc=com** 后缀配置 changelog 修剪。

注意

红帽建议设置最长期限，而不是最大条目数。最长期限应当与 **cn=replica,cn=suffixDN,cn=mapping tree,cn=config** 条目中的 **nsDS5ReplicaPurgeDelay** 参数中设置的复制清除延迟匹配。

在供应商上执行这个步骤。

前提条件

- 您为 **dc=example,dc=com** 后缀启用复制。

流程

1. 配置更改日志修剪：
   - 要设置更改日志条目的最长期限，请输入：

     ```
     # dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-changelog --suffix "dc=example,dc=com" --max-age "4w"
     ```

     此命令将最长期限设置为 4 周。参数支持以下单元：

     - **s** (**S**)秒数
     - **M** (**M**)表示分钟
     - **H** (**H**)小时
     - **D**(D)表示天

- W (W)周

- 要设置最大条目数，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-changelog --suffix "dc=example,dc=com" --max-entries "100000"
```

此命令将更改日志中的最大条目数设置为 100,000。

2. 默认情况下，Directory 服务器每 5 分钟(300 秒)修剪更改日志。要设置不同的间隔，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-changelog --suffix "dc=example,dc=com" --trim-interval 600
```

此命令将间隔设置为 10 分钟(600 秒)。

验证

- 显示后缀的 changelog 设置：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication get-changelog --suffix "dc=example,dc=com"
dn: cn=changelog,cn=userroot,cn=ldbm database,cn=plugins,cn=config
cn: changelog
nsslapd-changelogmaxage: 4w
nsslapd-changelogtrim-interval: 600
...
```

命令仅显示与其默认值不同的参数。

13.2. 手动缩小大量更改日志的大小

在某些情况下，如未启用复制 changelog 修剪，则更改日志可能会增加到非常大的大小。要解决这个问题，您可以手动减少更改日志大小。

这个步骤描述了如何修剪 dc=example,dc=com 后缀的 changelog。在供应商上执行这个步骤。

前提条件

- 您为 dc=example,dc=com 后缀启用复制。

流程

1. 可选：显示 changelog 的大小：

   a. 识别 dc=example,dc=com 后缀的后端数据库：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com backend suffix list
   dc=example,dc=com (userroot)
   ```

   括号中的名称是后端数据库，用于存储对应后缀的数据。

   b. 显示 userroot 后端的 changelog 文件的大小：

   ```
   # ls -lh /var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db
   -rw-------. 1 dirsrv dirsrv 517M Jul  5 12:58
   /var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db
   ```

2. 要在缩小 changelog 大小后重置参数，显示并记录相应参数的当前值：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com replication get-
   changelog --suffix "dc=example,dc=com"
   dn: cn=changelog,cn=userroot,cn=ldbm database,cn=plugins,cn=config
   cn: changelog
   nsslapd-changelogmaxage: 4w
   nsslapd-changelogtrim-interval: 300
   ```

   如果您没有在输出中看到任何特定属性，Directory 服务器将使用它们的默认值。

3. 临时减少与修剪相关的参数：

   ```
   # dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-
   changelog --suffix "dc=example,dc=com" --max-age "300s" --max-entries 500 --trim-
   interval 60
   ```

重要

出于性能的原因，请不要永久使用太短间隔设置。

4. 等待 --trim-interval 参数中设置的时间过期。

5. 紧凑更改日志以重新获得磁盘空间：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backend compact-db --only-changelog
```

6. 在临时减少前，将 changelog 参数重置为它们的值：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-changelog --suffix "dc=example,dc=com" --max-age "4w" --trim-interval 300
```

验证

- 显示 changelog 的大小：

```
# ls -lh /var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db
-rw-------. 1 dirsrv dirsrv 12M Jul  5 12:58 /var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db
```

第 14 章 加密复制更改日志

加密复制更改日志以提高实例的安全性，以防攻击者获得服务器文件系统的访问权限。

changelog 加密使用服务器的 TLS 加密密钥和相同的 PIN 来解锁密钥。您必须在服务器启动时手动输入 PIN，或使用 PIN 文件。

目录服务器使用随机生成的对称密码密钥来加密和解密更改日志。服务器为每个配置的密码都使用单独的密钥。这些密钥被嵌套使用服务器的 TLS 证书中的公钥，生成的封装密钥存储在服务器配置文件中。属性加密的有效强度与用于嵌套的服务器 TLS 密钥的强度相同。如果没有访问服务器的私钥和 PIN，无法从嵌套的副本恢复对称密钥。

14.1. 使用命令行加密更改日志

要在复制拓扑中提高安全性，请加密供应商和 hub 上的 changelog。这个步骤描述了如何为 dc=example,dc=com 后缀启用 changelog 加密。

前提条件

- 服务器启用了 TLS 加密。
- 主机是复制拓扑中的供应商或 hub。

流程

1. 将 changelog 导出，例如，将 /tmp/changelog.ldif 文件导出到 /tmp/changelog.ldif 文件中：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication export-changelog to-ldif -o /tmp/changelog.ldif -r "dc=example,dc=com"
```

2. 为 dc=example,dc=com 后缀启用更改日志加密：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication --suffix "dc=example,dc=com" --encrypt
```

3. 从 /tmp/changelog.ldif 文件中导入 changelog：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication import-changelog from-ldif -r "dc=example,dc=com" /tmp/changelog.ldif
```

4. 重启实例：

```
# dsctl instance_name restart
```

验证

1. 在 LDAP 目录中进行更改，如更新条目。

2. 停止实例：

```
# dsctl instance_name stop
```

3. 列出后缀及其对应的数据库：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backend suffix list
dc=example,dc=com (userroot)
```

请注意启用了更改日志加密的数据库名称。

4. 输入以下命令显示 changelog 的部分：

```
# dbscan -f /var/lib/dirsrv/slapd-instance_name/db/userroot/replication_changelog.db | tail -50
```

如果更改日志已加密，您只会看到加密数据。

5. 启动实例。

```
# dsctl instance_name start
```

其他资源

- 启用到目录服务器的 TLS 加密连接

第 15 章 对复制相关的问题进行故障排除

本节列出了复制环境中频繁的错误消息，解释可能的原因，并提供补救。

15.1. 配置目录服务器以记录与复制相关的错误

要记录与复制相关的错误，请启用复制调试。nsslapd-errorlog-level 参数是 additive。这意味着，要启用多个日志记录功能，您必须添加每个日志记录功能的值，并在 nsslapd-errorlog-level 中设置 sum。

流程

1. 显示当前错误日志级别：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-errorlog-level
nsslapd-errorlog-level: 16384
```

2. 启用复制调试的值为 8192。将 nsslapd-errorlog-level 参数设置为 24576 (8192 + 以前的值 16384)，除了当前启用的错误日志记录功能外，还要启用复制调试：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace nsslapd-errorlog-level=24576
```

15.2. 复制相关错误、原因和可能的解决方案概述

以下是复制相关错误和可能的解决方案概述：

agmt=*agreement_name* (*host_name*:*port*) Replica 具有与本地数据不同的生成 ID

- reason: 在消息的括号中指定的消费者尚未成功初始化，或者从不同的根供应商初始化。
- 影响：本地供应商不会将任何数据复制到消费者。
- 解决方案 ：如果在消费者初始化之前发生，则忽略此消息。否则，如果消息持久，重新初始化消费者。在多层次环境中，所有服务器都只需要从 root 供应商直接或间接初始化一次。例如，服务器 S1 初始化 S2 和 S4，S2 会初始化 S3，以此类推。请注意，需要注意的是，在 S2 初始

化完成前，S2 不得开始初始化 S3。为此，请从 S1 上的 web 控制台或 S1 或 S2 错误日志中检查总更新状态。此外，S2 不应重新初始化 S1。

warning: 重新载入副本的数据，它不再与更改日志中的数据匹配。重新创建 changelog 文件。这可能会影响带有副本消费者的复制，在这种情况下，应该重新初始化用户。

- 原因 ：只有在重启供应商时，才会显示此消息。这表示供应商无法写入更改日志，或者没有在最后一次关闭时清除其副本更新向量(RUV)。由于磁盘空间问题，以前的情况通常是因为服务器崩溃或未正常关闭的情况。

- 影响：如果服务器的 changelog 中不再存在使用者的 maxcsn 值，服务器将无法将更改发送到消费者。

- Remedy ：检查磁盘空间以及服务器日志目录下可能的核心文件。如果这是单层次复制，则重新初始化用户。否则，如果服务器稍后提示它无法找到消费者的序列号(CSN)，请验证消费者是否可以从其他供应商接收 CSN。如果没有，重新初始化消费者。

过长的时间偏移

- 原因：主机机器上的系统时钟非常不同步。

- 影响：目录服务器使用系统时钟生成 CSN 的一部分。为了反映多个供应商之间的更改序列，供应商将根据其他供应商的远程时钟转发其本地时钟。由于调整仅限于特定数量，超过允许的限制的任何差别都将中止复制会话。

- remedy：通过配置 chronyd 服务，同步目录服务器主机机器上的系统时钟。

agmt=*agreement_name* (*host_name*:*port*): Warning: Unable to send endReplication extended operation (*error_message*)

- reason: 消费者没有响应。

- 影响：如果消费者在没有重启的情况下恢复，则消费者中的副本会被锁定，如果它没有从供应商收到发行版本锁定消息。

- Remedy ：查看消费者是否可以从任何供应商收到任何新更改，或者启动复制监控器，并查看此消费者的所有供应商是否都处于忙碌状态。如果副本似乎被锁定，且没有供应商可以获得，

则重启消费者。

更改日志太大。

- 原因 ：关闭更改日志清除（这是默认设置），或者更改日志清除被打开，但有些消费者在供应商后面是方法。

- remedy ：默认情况下，更改日志清除会被关闭。要从命令行打开它，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication set-changelog --max-age 1d --suffix "dc=example,dc=com"
```

1d 表示 1 天。其他有效的时间单位为 s （秒）、m 表示分钟、h 表示小时，以及 w 周。值 0 可关闭清除。

打开 changelog 清除后，如果其年龄大于您设置的值，则每分钟唤醒一次清除线程会删除更改，如果它已重新执行到这个供应商或 hub 的所有直接消费者。

如果显示更改日志在达到清除阈值时没有清除，请检查所有消费者中复制监控器的最大时间。无论清除阈值是什么，所有消费者都会清除任何更改。

第 16 章 使用命令行监控复制拓扑

要监控供应商、消费者和 hub 之间目录数据复制的状态，您可以使用复制拓扑报告来提供有关复制进度、副本 ID、更改数和其他参数的信息。要更快地生成报告，并使其更易于阅读，您可以配置自己的凭证和别名。

16.1. 使用命令行显示复制拓扑报告

要查看复制拓扑中每个协议的复制状态的整体信息，您可以显示复制拓扑报告。为此，请使用 dsconf 复制监控器 命令。

先决条件

- 主机是复制拓扑的成员。
- 您初始化了消费者。

流程

- 要查看复制拓扑报告，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com replication monitor
```

dsconf 工具将为拓扑中的每个实例请求身份验证凭据：

```
Enter password for cn=Directory Manager on ldap://supplier.example.com: password
Enter a bind DN for consumer.example.com:389: cn=Directory Manager
Enter a password for cn=Directory Manager on consumer.example.com:389: password

Supplier: server.example.com:389
--------------------------------
Replica Root: dc=example,dc=com
Replica ID: 1
Replica Status: Online
Max CSN: 5e3acb77001d00010000

Status For Agreement: "example-agreement" (consumer.example.com:1389)
Replica Enabled: on
Update In Progress: FALSE
Last Update Start: 20211209122116Z
Last Update End: 20211209122116Z
Number Of Changes Sent: 1:21/0
```

```
Number Of Changes Skipped: None
Last Update Status: Error (0) Replica acquired successfully: Incremental update
succeeded
Last Init Start: 20211209122111Z
Last Init End: 20211209122114Z
Last Init Status: Error (0) Total update succeeded
Reap Active: 0
Replication Status: In Synchronization
Replication Lag Time: 00:00:00

Supplier: consumer.example.com:1389
---------------------------------
Replica Root: dc=example,dc=com
Replica ID: 65535
Replica Status: Online
Max CSN: 00000000000000000000
```

其他资源

- 在 .dsrc 文件中为复制监控设置凭证
- 在复制拓扑监控输出中使用别名
- 使用 Web 控制台显示复制拓扑报告

16.2. 在 .DSRC 文件中为复制监控设置凭证

默认情况下，dsconf 复制监控 命令在向远程实例进行身份验证时请求绑定 DN 和密码。要更快地生成报告，您可以更轻松地为用户的 ~/.dsrc 文件中的拓扑中的每个服务器设置绑定 DN 和可选密码。

先决条件

- 主机是复制拓扑的成员。
- 您初始化了消费者。

流程

1. 可选：创建 ~/.dsrc 文件。

2. 在 ~/.dsrc 文件中，设置绑定 DN 和密码。例如：

```
[repl-monitor-connections]
connection1 = server1.example.com:389:cn=Directory Manager:*
connection2 = server2.example.com:389:cn=Directory Manager:[~/pwd.txt]
connection3 = hub1.example.com:389:cn=Directory Manager:S3cret
```

这个示例使用 connection1 到 connection3 作为每个条目的密钥。但是，您可以使用任何唯一的密钥。

当您运行 dsconf replication monitor 命令时，dsconf 实用程序连接到实例复制协议中配置的所有服务器。如果实用程序在 ~/.dsrc 中查找主机名，它将使用定义的凭证向远程服务器进行身份验证。在上例中，dsconf 在连接到服务器时使用以下凭证：

Hostname	绑定 DN	密码设置方法
server1.example.com	cn=Directory Manager	请求密码
server2.example.com	cn=Directory Manager	从 ~/**pwd.txt**读取密码
hub1.example.com	cn=Directory Manager	S3cret

验证

- 运行 dsconf replication monitor 命令，以查看在 ~/.dsrc 文件中配置的 dsconf 工具是否使用了凭证。如需更多信息，请参阅 使用命令行显示复制拓扑报告。

其他资源

- 使用 Web 控制台为复制监控设置凭证

16.3. 在复制拓扑监控输出中使用别名

要使报告更易读，您可以设置自己的别名，该别名将在报告输出中显示。默认情况下，复制监控报告包含远程服务器的主机名。

先决条件

- 主机是复制拓扑的成员。
- 您初始化了消费者。

流程

如果要在报告中看到别名，请使用以下方法之一：

- 在 ~/.dsrc 文件中定义别名：

```
[repl-monitor-aliases]
M1 = server1.example.com:389
M2 = server2.example.com:389
```

- 通过将 -a alias=*host_name:port* 参数传给 dsconf 复制监控器命令来定义 别名：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com replication monitor -a
M1=server1.example.com:389 M2=server2.example.com:389
```

在这两种情况下，dsconf 复制监控器 命令在输出中显示别名：

```
...
Supplier: M1 (server1.example.com:389)
--------------------------------
Replica Root: dc=example,dc=com

...
Supplier: M2 (server2.example.com:389)
--------------------------------
Replica Root: dc=example,dc=com
```

其他资源

- 使用 Web 控制台配置复制命名别名

第 17 章 使用 WEB 控制台监控复制拓扑

要监控供应商、消费者和 hub 之间目录数据复制的状态，您可以使用复制拓扑报告来提供有关复制进度、副本 ID、更改数和其他参数的信息。要更快地生成报告，并使其更易于阅读，您可以配置自己的凭证和别名。

17.1. 使用 WEB 控制台显示复制拓扑报告

要查看复制拓扑中每个协议的复制状态的整体信息，您可以显示复制拓扑报告。

先决条件

- 主机是复制拓扑的成员。
- 您初始化了消费者。
- 已登陆到 web 控制台。

流程

1. 导航到 Monitoring → Replication。Replication Monitoring 页面将打开。
2. 点 Generate Report。
3. 输入用于登录到远程实例的密码，然后单击 Confirm Credentials Input。目录服务器使用现有复制协议中的绑定 DN 值。

   复制拓扑报告将在 Report Result 选项卡中生成。

注意

要生成另一个复制拓扑报告，请转至 Prepare Report 选项卡。

其他资源

- 使用 Web 控制台为复制监控设置凭证
- 使用 Web 控制台配置复制命名别名
- 使用命令行显示复制拓扑报告

17.2. 使用 WEB 控制台为复制监控设置凭证

要更快地生成复制拓扑报告，您可以为拓扑中的每个服务器设置自己的绑定 DN 和可选密码，以进行身份验证。在这种情况下，您不需要在每次您要生成复制拓扑报告时确认复制凭证。默认情况下，Directory 服务器从现有复制协议获取这些凭证。

先决条件

- 主机是复制拓扑的成员。
- 您初始化了消费者。
- 已登陆到 web 控制台。

流程

1. 导航到 Monitoring → Replication。Replication Monitoring 页面将打开。
2. 单击 Add Credentials。
3. 输入您要用来向远程实例进行身份验证的复制登录凭证：
   - 主机名.您希望服务器进行身份验证的远程实例主机名。
   - 端口.远程实例端口。

- 绑定 DN.用于向远程实例进行身份验证的绑定 DN。
- 密码.用于身份验证的密码。
- 交互式输入.如果选中，Directory 服务器每次生成复制拓扑报告时会要求输入密码。

4. 点 Save。

验证

生成复制拓扑报告，以查看报告是否请求凭证。如需更多信息，请参阅使用 Web 控制台显示复制拓扑报告。

17.3. 使用 WEB 控制台配置复制命名别名

要使报告更易读，您可以设置自己的别名，该别名将在报告输出中显示。默认情况下，复制监控报告包含服务器的主机名。

先决条件

- 主机是复制拓扑的成员。
- 您初始化了消费者。
- 已登陆到 web 控制台。

流程

1. 导航到 Monitoring → Replication。Replication Monitoring 页面将打开。
2. 单击 Add Alias。

3. 输入别名详情：

   - 别名.复制拓扑报告中显示的别名。
   - 主机名.实例主机名。
   - 端口.实例端口。

4. 点 Save。

验证

- 生成复制拓扑报告，以查看报告是否使用新的别名。如需更多信息，请参阅使用 Web 控制台显示复制拓扑报告。

第 18 章 比较两个目录服务器实例

您可以使用 ds-replcheck 程序验证两个 Directory Server 实例是否已同步。您可以在线比较两台服务器，或者在离线模式中使用两个 LDIF 格式文件。

18.1. 显示两个目录服务器实例的复制状态

您可以使用 ds-replcheck 工具来显示两个目录服务器实例的复制状态。

流程

- 使用以下命令显示两个 Directory Server 实例的复制状态：

```
# ds-replcheck state -D "cn=Directory Manager" -W -m ldap://server1.example.com:389
-r ldap://server2.example.com:389 -b "dc=example,dc=com"
Replication State: Replica is behind Supplier by: 264 seconds
```

18.2. 比较两个在线目录服务器实例

如果您比较了两个在线服务器，数据库的内容通常会不同，如果它们负载过重。要临时解决这个问题，ds-replcheck 通过将 -l *time_in_seconds* 参数传递给 ds-replcheck 来使用滞后时间值。默认情况下，这个值被设置为 300 秒(5 分钟)。如果工具检测到在滞后时间内的不一致，则工具不会报告它。这有助于减少误报。

默认情况下，如果您排除复制协议中的某些属性被复制，则 ds-replcheck 会报告这些属性不同。要忽略这些属性，请将 -i *attribute_list* 参数传递给 实用程序。

流程

- 要比较 provider.example,dc=com 的 dc= example,dc=com 后缀和 replica.example.com 在线，请输入：

```
# ds-replcheck online -D "cn=Directory Manager" -W -m
ldap://supplier.example.com:389 -r ldap://replica.example.com:389 -b
"dc=example,dc=com"
```

-m 和 -r 参数将 URL 设置为供应商和副本。

18.3. 离线两个目录服务器实例

要比较两个离线目录服务器实例，请导出两个主机上的数据库，并使用 ds-replcheck 进行比较。

默认情况下，如果您排除复制协议中的某些属性被复制，则 ds-replcheck 会报告这些属性不同。要忽略这些属性，请将 -i *attribute_list* 参数传递给 实用程序。

流程

1. 在供应商中，列出后缀及其对应的数据库：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com backend suffix list
dc=example,dc=com (userroot)
o=test (test_database)
```

请注意您要比较的数据库的名称或后缀。

2. 在实例运行时导出数据库：

```
# dsconf -D "cn=Directory Manager" ldap://supplier.example.com backend export -r -l
/var/lib/dirsrv/slapd-instance_name/ldif/export-supplier.ldif userRoot
```

r 参数确保导出包含复制状态信息，-l 设置导出文件的路径。请注意，dirsrv 用户必须在目标目录中具有写入权限才能创建该文件。

3. 在您要与供应商比较的副本中重复前面的步骤。

4. 将导出的文件从一个主机复制到另一个主机。例如，要将 LDIF 文件从 replica.example.com 复制到 provider.example.com，请在副本上输入以下命令：

```
# scp /var/lib/dirsrv/slapd-instance_name/ldif/export-replica.ldif
supplier.example.com:/var/lib/dirsrv/slapd-instance_name/ldif/
```

请注意，这个命令需要您可以使用 SSH 访问供应商。

5. 在供应商中，比较两个 LDIF 文件：

```
# ds-replcheck offline -m /var/lib/dirsrv/slapd-instance_name/ldif/export-supplier.ldif -r
/var/lib/dirsrv/slapd-instance_name/ldif/export-replica.ldif -rid 1 -b
"dc=example,dc=com"
```

-m 和 -r 参数设置到供应商和副本的路径，-rid 设置供应商的副本标识符。

18.4. DS-REPLCHECK 输出的说明

ds-replcheck 工具的输出包含以下部分：

数据库 RUV

列出数据库的 Replication Update Vectors (RUV)，包括最小和最大更改序列号(CSN)。例如：

```
Supplier RUV:
  {replica 1 ldap://supplier.example.com:389} 58e53b92000200010000
58e6ab46000000010000
  {replica 2 ldap://replica.example.com:389} 58e53baa000000020000
58e69d7e000000020000
  {replicageneration} 58e53b7a000000010000

Replica RUV:
  {replica 1 ldap://supplier.example.com:389} 58e53ba1000000010000
58e6ab46000000010000
  {replica 2 ldap://replica.example.com:389} 58e53baa000000020000
58e7e8a3000000020000
  {replicageneration} 58e53b7a000000010000
```

条目数

显示两个服务器中的条目总数，包括 tombstone 条目。例如：

```
Supplier:  12
Replica: 10
```

tombstones

显示每个副本上的 tombstone 条目数量。这些条目被添加到总条目数中。例如：

```
Supplier:  4
Replica: 2
```

冲突条目

列出每个冲突条目的可辨识名称(DN)、冲突类型及其创建日期。例如：

```
Supplier Conflict Entries: 1

 - nsuniqueid=48177227-2ab611e7-afcb801a-ecef6d49+uid=user1,dc=example,dc=com
   - Conflict:   namingConflict (add) uid=user1,dc=example,dc=com
   - Glue entry: no
   - Created:    Wed Apr 26 20:27:40 2021


Replica Conflict Entries: 1

 - nsuniqueid=48177227-2ab611e7-afcb801a-ecef6d49+uid=user1,dc=example,dc=com
   - Conflict:   namingConflict (add) uid=user1,dc=example,dc=com
   - Glue entry: no
   - Created:    Wed Apr 26 20:27:40 2021
```

缺少条目

列出每个缺失条目的 DN 以及条目所在的其他服务器的创建日期。例如：

```
Entries missing on Supplier:
 - uid=user2,dc=example,dc=com (Created on Replica at: Wed Apr 12 14:43:24 2021)
 - uid=user3,dc=example,dc=com (Created on Replica at: Wed Apr 12 14:43:24 2021)

Entries missing on Replica:
 - uid=user4,dc=example,dc=com (Created on Supplier at: Wed Apr 12 14:43:24 2021)
```

entry Inconsistencies

列出条目的 DN，其中包含与其他服务器上不同的属性。如果状态信息可用，也会显示它。如果没有属性的状态信息，则会将其列为原始值。这意味着该值没有更新，因为复制首次初始化。例如：

```
cn=group1,dc=example,dc=com
---------------------------
Replica missing attribute "objectclass":

 - Supplier's State Info: objectClass;vucsn-58e53baa000000020000: top
 - Date: Wed Apr  5 14:47:06 2021

 - Supplier's State Info: objectClass;vucsn-58e53baa000000020000: groupofuniquenames
 - Date: Wed Apr  5 14:47:06 2021
```

第 19 章 解决常见复制问题

多层次复制使用最终不一致的复制模型。这意味着在不同服务器上可以更改相同的条目。在这两个服务器之间发生复制时，目录服务器需要解决冲突的更改。主要是，根据与每台服务器上更改关联的时间戳自动进行解析。最近的更改具有优先级。然而，在某些情况下，冲突需要人工干预才能到达解决方案。

19.1. 识别和解决命名冲突

当多个供应商服务器收到一个请求来创建具有相同可分名称(DN)的条目时，每个服务器都会使用此 DN 和不同的条目唯一标识符(entry ID)创建条目。条目 ID 存储在 nsuniqueid 操作属性中。

例如，Server A 和 Server B 收到一个请求，以创建 uid=*user_name*,ou=people,dc=example,dc=com 用户条目。因此，每个服务器都有自己的条目：

- 在 Server A 中，该条目有：
  - uid=*user_name*,ou=people,dc=example,dc=com
  - nsuniqueid=a7f1758b-512211ec-b115e2e9-7dc2d46b
- 在 Server B 中，该条目有：
  - uid=*user_name*,ou=people,dc=example,dc=com
  - nsuniqueid=643a461e-b61311e1-b23be826-4afeed5f

在复制过程中，服务器 A 复制新创建的条目 uid=*user_name*,ou=people,dc=example,dc=com 到 Server B ，Server B 将新创建的条目复制到 Server A，并在每台服务器上发生命名冲突。通过比较更改序列号(CSN)，每台服务器决定了之前创建的条目。例如，之前创建了 Server B 中的条目。

自动冲突解析过程会通过以下方法更改创建的最后一个条目(服务器 A中的条目) ：

- 在非唯一 DN 中添加 nsuniqueid 值。
- 添加 nsds5replconflict 属性以及导致冲突的操作的描述。
- 添加 ldapsubentry objectclass。

现在，两个服务器上都存在以下条目：

- 有效的 条目包括：
  - uid=user_name,ou=people,dc=example,dc=com
  - nsuniqueid=643a461e-b61311e1-b23be826-4afeed5f
- 冲突 条目有：
  - nsuniqueid=a7f1758b-512211ec-b115e2e9-7dc2d46b+uid=user_name,ou=people,dc=example,dc=com
  - nsuniqueid=a7f1758b-512211ec-b115e2e9-7dc2d46b

要手动解决命名冲突，请在每台服务器上执行以下步骤。

流程

1. 列出冲突条目：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict list
dc=example,dc=com
dn: nsuniqueid=a7f1758b-512211ec-b115e2e9-
7dc2d46b+uid=user_name,ou=people,dc=example,dc=com
cn: user_name
displayName: user
```

```
gidNumber: 99998
homeDirectory: /var/empty
legalName: user name
loginShell: /bin/false
nsds5replconflict: namingConflict (ADD)
uid=user_name,ou=people,dc=example,dc=com
objectClass: top
objectClass: nsPerson
objectClass: nsAccount
objectClass: nsOrgPerson
objectClass: posixAccount
objectClass: ldapsubentry
uid: user_name
uidNumber: 99998
```

2. 如果存在冲突条目，决定如何进行：

- 要只保留有效的条目(uid=user_name,ou=people,dc=example,dc=com)并删除冲突条目，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict delete
nsuniqueid=a7f1758b-512211ec-b115e2e9-
7dc2d46b+uid=user_name,ou=People,dc=example,dc=com
```

- 要只保留冲突条目(nsuniqueid=a7f1758b-512211ec-b115e2e9-7dc2d46b+uid=user_name,ou=People,dc=example,dc=com)，并删除有效的条目，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict swap
nsuniqueid=a7f1758b-512211ec-b115e2e9-
7dc2d46b+uid=user_name,ou=People,dc=example,dc=com
```

- 要保留这两个条目，请指定一个新的相对可分辨名称(RDN)来重命名冲突条目：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict
convert --new-rdn=uid=user_name_NEW nsuniqueid=a7f1758b-512211ec-
b115e2e9-7dc2d46b+uid=user_name,ou=people,dc=example,dc=com
```

此命令将冲突条目重命名为 uid=user_name_NEW,ou=people,dc=example,dc=com。

警告

目录服务器复制在冲突条目上执行的 LDAP 操作。通常，使用原始操作条目的 nsuniqueid 而不是使用操作 dn 来复制操作以条目为目标。但是，在使用冲突条目时，行为可能会有所不同。

19.2. 识别和解决孤立条目冲突

当目录服务器复制删除操作且消费者服务器发现要删除的条目有子条目时，冲突解析过程会创建一个粘滞条目，以避免在目录中有孤立的条目。

同样，当目录服务器复制添加操作且消费者服务器无法找到父条目时，冲突解析过程会为父条目创建一个粘滞条目。

粘滞条目是包含对象类 glue 和 Scalable Object 的临时条目。可以通过几种方式创建粘合条目：

- 如果冲突解析过程找到一个带有匹配唯一标识符的已删除条目，glue 条目具有与已删除条目相同的属性，但增加了 glue 对象类和 nsds5ReplConflict 属性。

  在这种情况下，可以修改 glue 条目来删除 glue 对象类和 nsds5ReplConflict 属性，将条目保留为普通条目或删除 glue 条目及其子条目。

- 服务器使用 glue 和 scalable Object 对象类 创建一个条目。

流程

1. 列出孤立条目冲突：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict list-glue
suffix
dn: ou=parent,dc=example,dc=com
objectClass: top
objectClass: organizationalunit
objectClass: glue
objectClass: extensibleobject
ou: parent
```

2. 如果存在孤立条目冲突，请决定如何进行：

- 要删除粘滞条目及其子条目，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict delete-glue "ou=parent,dc=example,dc=com"
dn: ou=parent,dc=example,dc=com
objectClass: top
objectClass: organizationalunit
objectClass: extensibleobject
ou: parent
```

- 要将 glue 条目转换为常规条目，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com repl-conflict convert-glue "ou=parent,dc=example,dc=com"
```

19.3. 识别并解决有关过时或缺失供应商的错误

目录服务器将关于复制拓扑的信息（如所有将更新发送到其他副本的供应商）存储在一组称为副本更新向量(RUV)的元数据中。RUV 包含有关供应商的信息，如 ID 和 URL、本地服务器上的最后一次更改状态号(CSN)，以及第一次更改的 CSN。供应商和消费者均存储 RUV 信息，它们使用它来控制复制更新。

当您从复制拓扑中删除供应商时，可以保留到另一个副本的 RUV 的信息。您可以使用 cleanallruv 任务来删除拓扑中的所有供应商。

前提条件

- 复制启用在.

流程

1. 监控 /var/log/dirsrv/slapd-*instance_name*/errors 日志文件，并搜索类似如下的条目：

```
[22/Jan/2021:17:16:01 -0500] NSMMReplicationPlugin - ruv_compare_ruv: RUV [changelog max RUV] does not contain element [{replica 8 ldap://server2.example.com:389} 4aac3e59000000080000 4c6f2a02000000080000] which is present in RUV [database RUV]
...
[22/Jan/2021:17:16:01 -0500] NSMMReplicationPlugin - replica_check_for_data_reload:
```

```
Warning: for replica dc=example,dc=com there were some differences between the changelog max RUV and the database RUV. If there are obsolete elements in the database RUV, you should remove them using the CLEANALLRUV task. If they are not obsolete, you should check their status to see why there are no changes from those servers in the changelog.
```

在这种情况下，副本 ID 8 会导致这个错误。

2. 显示所有 RUV 记录和副本 ID，分别有效且无效：

```
# dsconf -D "cn=Directory Manager" ldap://server1.example.com replication get-ruv --suffix "dc=example,dc=com"
RUV:        {replica 1 ldap://server1.example.com} 61a4d8f8000100010000 61a4f5b8000000010000

Replica ID: 1
LDAP URL:   ldap://server1.example.com
Min CSN:    2021-11-29 13:43:20 1 0 (61a4d8f8000100010000)
Max CSN:    2021-11-29 15:46:00 (61a4f5b8000000010000)
RUV:        {replica 2 ldap://server2.example.com} 61a4d8fb000100020000 61a4f550000000020000

Replica ID: 2
LDAP URL:   ldap://server2.example.com
Min CSN:    2021-11-29 13:43:23 1 0 (61a4d8fb000100020000)
Max CSN:    2021-11-29 15:44:16 (61a4f550000000020000)
 RUV:       {replica 8 ldap://server3.example.com} 61a4d903000100080000 61a4d908000000080000

Replica ID: 8
LDAP URL:   ldap://server3.example.com
Min CSN:    2021-11-29 13:43:31 1 0 (61a4d903000100080000)
Max CSN:    2021-11-29 13:43:36 (61a4d908000000080000)
```

请注意返回的副本 ID 列表： 1、 2 和 8。

3. 为副本 ID 8 运行清理任务。

```
# dsconf -D "cn=Directory Manager" ldap://server1.example.com repl-tasks cleanallruv --suffix="dc=example,dc=com" --replica-id=8
```

请注意，目录服务器复制 RUV 清理任务。因此，您只需要在一个供应商上启动任务。

如果一个副本无法加入，例如，如果其停机，您可以使用 --force-cleaning 选项来实现 RUV 的即时清理。

验证

- 显示 RUV 记录和副本 ID：

```
# dsconf -D "cn=Directory Manager" ldap://server1.example.com replication get-ruv --
suffix "dc=example,dc=com"
RUV:        {replica 1 ldap://server1.example.com} 61a4d8f8000100010000
61a4f5b8000000010000

Replica ID: 1
LDAP URL:   ldap://server1.example.com
Min CSN:    2021-11-29 14:02:10 1 0 (61a4d8f8000100010000)
Max CSN:    2021-11-29 16:00:00 (61a4f5b8000000010000)
RUV:        {replica 2 ldap://server2.example.com} 61a4d8fb000100020000
61a4f550000000020000

Replica ID: 2
LDAP URL:   ldap://server2.example.com
Min CSN:    2021-11-29 14:02:10 1 0 (61a4d8fb000100020000)
Max CSN:    2021-11-29 15:58:22 (61a4f550000000020000)
```

该命令不再返回副本 ID 8 的 RUV 条目。