第十七节：组复制安全---进阶篇

1.组复制IP地址白名单：

使用组复制插件，可以指定集群的白名单，从白名单中确认可接受组通信系统传入的连接。如果在server s1上指定了一个白名单，则当server s2为了进行通信而与s1建立连接时，s1首先遍历白名单，然后再接受s2的连接。如果s2在白名单中，则s1接受s2的连接，否则s1拒绝s2的连接。

MySQL 从8.0.22开始，系统变量group_replication_ip_allowlist用于制定白名单，对于MySQL 8.0.22之前的版本，使用系统变量group_replication_ip_whitelist。新的系统变量的工作方式与旧系统变量的工作方式相同，仅名称改变而已。

如果未指定白名单，则组通信引擎（XCom）会自动扫描主机上的活跃网关，并根据这些活跃网卡上配置的IP地址生成相应的子网地址。(包括IPV4和IPV6地址）。根据这些生成的子网地址来自动创建一个组复制的白名单设置。自动生成的IP白名单地址可能包含如下范围：

```
IPv4 (as defined in RFC 1918)

10/8 prefix       (10.0.0.0 - 10.255.255.255) - Class A

172.16/12 prefix  (172.16.0.0 - 172.31.255.255) - Class B

192.168/16 prefix (192.168.0.0 - 192.168.255.255) - Class C

IPv6 (as defined in RFC 4193 and RFC 5156)

fc00:/7 prefix    - unique-local addresses

fe80::/10 prefix  - link-local unicast addresses

127.0.0.1 - localhost for IPv4

::1       - localhost for IPv6
```

ps:在MySQL的错误日志中会记录自动为主机添加的白名单地址信息。

自动生成的白名单地址都是私有网络地址（即便主机上配置有公网IP地址，也不会生成公网地址网络的白名单）,d但私有地址只允许在内网访问，不允许接入到公网上对外提供服务。如果要使用公网地址作为白名单，需要使用系统变量group_replication_ip_whitelist来显式指定允许开放访问的公网地址范围，另外，一旦为系统变量group_replication_ip_whitelist指定值之后，自动生成白名单的功能就失效了，未在系统变量group_replication_ip_whitelist中指定的任何地址都不允许访问，因此，任何允许访问的IP地址范围，都需要在该系统变量中指定。

要手动指定白名单，使用group_replication_ip_allowlist（MySQL 8.0.22及更高版本）或group_replication_ip_whitelist系统变量。如果server是集群中的online节点，则无法在该online节点上在线动态配置白名单。如果该节点处于online状态，则必须在修改白名单之前执行STOP GROUP_REPLICATION，配置完白名单后，然后再执行START GROUP_REPLICATION。

否则会报错：ERROR 3093 (HY000): The IP whitelist cannot be set while Group Replication is running。

白名单必须包含集群每个节点的group_replication_local_address系统变量中指定的IP地址或主机名。该地址与MySQL的SQL协议的主机和端口不同，（系统变量group_replication_local_address指定的地址和端口是用于组成员之间的组通讯的，而不是对外提供业务访问的）。并且未在实例的bind_address系统变量中指定。如果用作该实例的组复制本地地址的主机名同时支持解析为IPv4和IPv6地址，则组复制连接将首选IPv4地址。

指定为分布式恢复的IP地址，以及集群节点的标准SQL客户端连接的IP地址（如果用于分布式恢复），无需添加到白名单中。白名单仅适用于由group_replication_local_address为每个节点指定的地址。加入节点必须具有与白名单允许的集群节点列表，以便检索一个或多个地址以进行分布式恢复。

在白名单中，可以指定以下任意IP地址的组合：

```
IPv4地址（示例：198.51.100.44）

具有CIDR表示法的IPv4地址（示例：192.0.2.21/24）

IPv6地址（MySQL8.0.14开始）（2001:db8:85a3:8d3:1319:8a2e:370:7348）

具有CIDR表示法的IPv6地址（从MySQL8.0.14开始）（示例：2001:db8:85a3:8d3::/64）

主机名（示例：example.org）

具有CIDR表示法的主机名（示例：www.example.com/24）
```

在MySQL 8.0.14之前，主机名只能解析为IPv4地址。从MySQL 8.0.14开始，主机名可以解析为IPv4地址和/或IPv6地址。如果主机名支持同时解析为IPv4和IPv6地址，则IPv4地址始终用于组复制连接。可以将CIDR表示法与主机名或IP地址结合使用，允许使用具有特定网络前缀的IP地址块来配置白名单（带有子网掩码的IP地址范围的白名单），但是要确保指定子网中的所有IP地址都在允许访问的范围之内。

必须停止并重新启动节点上的组复制才能修改白名单，用逗号来分割白名单中的每一项。

例如：

```
mysql> STOP GROUP_REPLICATION;

mysql> SET GLOBAL
group_replication_ip_allowlist="192.0.2.21/24,198.51.100.44,203.0.113.0/24,2001:
db8:85a3:8d3:1319:8a2e:370:7348,example.org,www.example.com/24";

mysql> START GROUP_REPLICATION;
```

要加入集群，给定的待加入集群的Server的IP地址需要在其请求加入集群的种子节点的白名单中允许其发起组通讯请求。通常，是根据种子节点的系统变量group_replication_group_seeds设置的IP进行筛选，也可以根据集群中的任意节点的系统变量group_replication_group_seeds指定的值进行设定，例如：集群中的节点混合使用了IPV4和IPV6地址，那么，建议将所有节点可能会用于组通讯的网络的IPV4和IPV6协议地址一并配置到白名单中，以避免出现有Server申请加入集群时被拒绝连接的情况发生。

当复制组重新配置（例如，当选举新的primary节点或者有节点离开集群时），集群内所有节点重新建立它们自己之间的连接。如果集群中的所有节点的白名单地址配置不一致，在重新配置集群之后，可能导致某个节点在重新配置集群之前允许加入集群，而在重新配置集群之后无法重新加入。

例如：集群中有3个节点S1、S2、S3，当S3脱离集群并重新配置集群时，因为白名单不一致的原因，S2不允许S1访问，S3允许S1访问，但是现在S3已经不在集群中了，这就会导致S3脱离集群之后，S1和S2也无法组成新的集群。为了完全避免这种情况，需要为集群内所有节点指定相同的白名单。

ps:可以根据安全要求在不同的节点上配置不同的白名单，以使不同的子网分开。如果需要配置其他白名单以满足安全要求，请确保复制组中的白名单之间有足够的重叠，以最大程度地提高server在没有种子节点的情况下能够重新连接的可能性。

对于主机名，仅当另一个主机发出连接请求时，才进行名称解析。无法解析的主机名不会用于白名单的验证，并且警告消息会写入错误日志。对已解析的主机名执行反向DNS验证。

注意：主机名本质上不如白名单中的IP地址安全。 FCrDNS验证提供了良好的保护，但可能会受到某些类型的攻击。仅在绝对必要时在白名单中指定主机名，并确保所有用于名称解析的组件（例如DNS服务器）都在你的控制下。如果实在不可避免，可以临时使用hosts文件在本地实现名称解析，以避免使用外部组件。

2.组复制对SSL的支持：

安全套接字可用于集群内各个节点之间的组通信连接。组复制系统变量group_replication_ssl_mode用于激活对组通信连接使用SSL，并指定连接的方式。默认设置表示不使用SSL。该参数具有以下的有效值：

值	意义
DISABLED	不启用SSL
REQUIRED	如果集群内的节点支持SSL连接，则建立连接
VERIFY_CA	类似于REQUIRED，但是要根据配置CA证书来验证TLS证书
VERIFY_IDENTITY	与VERIFY_CA类似，但是还要验证证书是否与尝试连接的主机匹配

组复制的通信连接的其余配置来自MySQL server的SSL配置。应用于组复制的组通信连接的SSL参数如下：

Server配置选项（系统变量）	描述
ssl_key	PEM格式的SSL私钥文件的路径名。在客户端，用于指定客户端私钥文件（例如：mysql命令行客户端的ssl_key选项）；在服务端，用于指定服务端的私钥文件
ssl_cert	PEM格式的SSL公钥证书文件的路径名。在客户端，用于指定客户端的公钥证书文件；在服务端，用于指定服务端的公钥证书文件
ssl_ca	PEM格式的证书颁发机构(CA)证书文件的路径名
ssl_capath	包含PEM格式的受信SSL证书颁发机构(CA)证书文件的目录的路径名
ssl_crl	包含PEM格式的证书撤销列表的文件的路径名
ssl_crlpath	包含PEM格式证书撤销列表文件的目录的路径名
ssl_cipher	用于加密连接握手中允许使用的密码列表
tls_version	Server允许的用于加密连接的TLS协议的列表
tls_ciphersuites	Server允许的用于加密连接的TLSv1.3加密套件

ps：从MySQL 8.0.16开始，MySQL Server中提供了对TLSv1.3协议的支持，前提是MySQL是使用OpenSSL 1.1.1或更高版本进行编译的。MySQL 8.0.18中的组复制支持TLSv1.3。在MySQL 8.0.16和MySQL 8.0.17中，如果server支持TLSv1.3，组通信引擎中不支持该协议，则组复制不能使用该协议。

在TLS_version系统变量中指定的TLS协议列表中，确保指定的版本是连续的（例如TLSv1，TLSv1.1，TLSv1.2）。如果协议列表中有任何空白（例如，如果指定TLSv1，TLSv1.2，而忽略TLS 1.1），则组复制可能无法建立组通信连接。

在MySQL 8.0.18中，TLSv1.3可以在组复制中用于分布式恢复连接，但是group_replication_recovery_tls_version和group_replication_recovery_tls_ciphersuites系统变量不可用。因此，至少一个引导节点必须允许使用默认启用的TLSv1.3密码套件。从MySQL 8.0.19开始，如果需要的话，可以使用这些选项来配置对任何密码套件选择的客户端支持，仅包括非默认密码套件。

在复制组中，使用OpenSSL来在集群所有节点之间协商大家支持的最高TLS协议的版本。如果某个新加入集群的节点配置为仅支持TLSv1.3 (tls_version=TLSv1.3)，则如果集群中的现有节点不支持TLSv1.3时（例如：设置 tls_version=TLSv1,TLSv1.1,TLSv1.2 ）的情况下，则配置为仅使用TLSv1.3（tls_version = TLSv1.3）的节点无法加入其中任何现有节点都不支持TLSv1.3的集群，因为在这种情况下，该集群内的节点使用的是较低的TLS协议版本。要将新节点加入集群，必须将加入节点配置为允许使用现有集群节点支持的较低TLS协议版本。相反，如果加入的节点不支持TLSv1.3，但是现有集群的节点都支持并且正在使用该版本相互连接，如果集群现有的节点已经允许使用合适的较低TLS协议，则该节点可以加入集群。在这种情况下，OpenSSL使用较低的TLS协议版本进行从集群内每个节点到加入节点的连接。集群内每个节点与其他现有节点的连接继续使用两个节点都支持的最高可用协议。

- 如果只是修改集群中现有节点的TLS版本，但不重启组复制，则集群中的现有节点之间已建立连接的TLS版本不会改变（不影响现有节点之间的连接）。
- 如果想要使用TLSv1.3版本，则可能需要先升级集群中现有节点的MySQL Server版本到MySQL 8.0.18及其以上的版本，然后将TLS版本都修改为支持TLSv1.3（例如：tls_version=TLSv1,TLSv1.1,TLSv1.2,TLSv1.3）。

从MySQL 8.0.16开始，可以在线变更tls_version系统变量，以更改MySQL server允许的TLS协议版本列表。对于组复制，执行ALTER INSTANCE RELOAD TLS语句（从定义上下文的系统变量的当前值重新配置MySQL server的TLS上下文）不会在组复制运行时更改组复制的组通信连接使用的TLS上下文。要将配置重新应用于这些连接，必须执行STOP GROUP_REPLICATION，然后执行START GROUP_REPLICATION，在更改了tls_version系统变量的一个或多个节点上重新启动组复制。同样，如果要使集群的所有节点更改为使用更高或更低的TLS协议版本，则必须在更改允许的TLS协议版本的列表后对节点进行组复制的滚动重启，以便OpenSSL协商滚动重启完成后，使用更高版本的TLS协议。

以下示例显示了my.cnf文件中的一部分，该部分在MySQL server上配置SSL，并为组复制组通信连接激活SSL：

```
[mysqld]
ssl_ca = "cacert.pem"
ssl_capath = "/.../ca_directory"
ssl_cert = "server-cert.pem"
ssl_cipher = "DHE-RSA-AEs256-SHA"
ssl_crl = "crl-server-revoked.crl"
ssl_crlpath = "/.../crl_directory"
ssl_key = "server-key.pem"
group_replication_ssl_mode= REQUIRED
```

ps：ALTER INSTANCE RELOAD TLS语句从定义上下文的系统变量的当前值重新配置MySQL server的TLS上下文，并且在运行组复制时不会更改组复制的组通信连接的TLS上下文。要将配置重新应用于这些连接，必须执行STOP GROUP_REPLICATION，然后执行START GROUP_REPLICATION，以重新启动组复制。

上述选项未涵盖在加入节点与集群现有节点之间进行的用于分布式恢复的连接。

3.为分布式恢复配置SSL：

当节点加入集群时，将结合使用远程克隆操作和异步复制连接来执行分布式恢复。

集群现有节点提供给加入节点以进行分布式恢复的连接与组复制用于集群的online成员之间的通信的连接不同。在MySQL 8.0.20之前的版本中，集群节点向加入节点提供其标准SQL客户端连接以进行分布式恢复，这由MySQL Server的主机名和端口系统变量指定。从MySQL 8.0.21开始，集群节点可以发布分布式恢复端点的替代列表，作为加入成员的专用客户端连接。

要保护集群中的分布式恢复连接，请确保正确保护复制用户的用户凭据，并在可能的情况下将SSL用于分布式恢复连接。

从二进制日志进行状态传输需要具有正确权限的复制用户，以便组复制可以建立直接的节点到节点的复制通道。同一复制用户用于所有组成员上的分布式恢复。如果已将组成员设置为支持将远程克隆操作用作分布式恢复的一部分（可从MySQL 8.0.17获得），则此复制用户还用作引导节点上的克隆用户，并且这个节点需要正确的权限。

为了保护用户凭据，可以要求与用户帐户建立SSL连接，并且（从MySQL 8.0.21开始）可以在启动组复制时提供用户凭据，而不是将其存储在副本状态表中。另外，如果使用缓存SHA-2身份验证，则必须在集群节点上设置RSA密钥对。

默认情况下，在MySQL 8中创建的用户使用SHA-2缓存可插拔身份验证。如果为分布式恢复配置的复制用户使用SHA-2身份验证插件，并且没有将SSL用于分布式恢复连接，则RSA密钥对将用于密码交换。

在这种情况下，可以将rpl_user的公钥复制到加入节点，也可以配置引导节点以在需要时提供公钥。更为安全的方法是将复制用户帐户的公钥复制到加入节点上。然后，需要在加入节点上配置group_replication_recovery_public_key_path系统变量，并使用复制用户帐户的公钥路径。

安全性较差的方法是在引导节点上设置group_replication_recovery_get_public_key = ON，以便它们将复制用户的公钥提供给加入节点。因此，当确定存在无法验证MySQL server的身份风险时，仅将group_replication_recovery_get_public_key 设置为ON。

在加入节点连接到引导节点之前，必须创建需要SSL连接的复制用户。通常，这是在配置服加入节点加入集群时设置的。要为需要SSL连接的分布式恢复创建复制用户，请在将要加入该集群的所有节点上执行以下语句：

```
mysql> SET SQL_LOG_BIN=0;
mysql> CREATE USER 'rec_ssl_user'@'%' IDENTIFIED BY 'password' REQUIRE SSL;
mysql> GRANT replication slave ON *.* TO 'rec_ssl_user'@'%';
mysql> GRANT BACKUP_ADMIN ON *.* TO 'rec_ssl_user'@'%';
mysql> FLUSH PRIVILEGES;
mysql> SET SQL_LOG_BIN=1;
```

要为复制用户提供用户凭据，可以使用CHANGE MASTER TO语句将它们永久设置为group_replication_recovery通道的凭据。另外，从MySQL 8.0.21开始，可以在每次启动组复制时在START GROUP_REPLICATION语句中指定它们。在START GROUP_REPLICATION上指定的用户凭据优先于使用CHANGE MASTER TO语句设置的任何用户凭据。

使用CHANGE MASTER TO设置的用户凭据以纯文本格式存储在MySQL server上的复制元数据存储库中，但是在START GROUP_REPLICATION上指定的用户凭据仅保存在内存中，并通过STOP GROUP_REPLICATION语句或MySQL server关闭将其删除。因此，使用START GROUP_REPLICATION指定用户凭据有助于保护组复制server免遭未经授权的访问。但是，此方法与group_replication_start_on_boot系统变量指定的自动启动组复制不兼容。

如果要使用CHANGE MASTER TO语句永久设置用户凭据，请在将要加入该集群的节点上执行以下语句：

```
mysql> CHANGE MASTER TO MASTER_USER='rec_ssl_user', MASTER_PASSWORD='password'
FOR CHANNEL 'group_replication_recovery';
```

要在START GROUP_REPLICATION上提供用户凭据，请在首次启动组复制时或在服务器重新启动后执行以下语句：

```
mysql> START GROUP_REPLICATION USER='rec_ssl_user', PASSWORD='password';
```

如果切换到使用START GROUP_REPLICATION以前使用CHANGE MASTER TO提供凭据的服务器上指定用户凭据，则必须完成以下步骤才能获得此更改：

使用STOP GROUP_REPLICATION语句在集群节点上停止组复制。尽管可以在运行组复制的同时执行以下两个步骤，但是需要重新启动组复制以应用变更。

将group_replication_start_on_boot系统变量的值设置为OFF（默认值为ON）。

通过执行以下语句从副本状态表中删除分布式恢复凭据：

```
mysql> CHANGE MASTER TO MASTER_USER='', MASTER_PASSWORD='' FOR CHANNEL
'group_replication_recovery';
```

使用指定分布式恢复用户凭据的START GROUP_REPLICATION语句在集群节点上重新启动组复制。如果不执行这些步骤，则凭据仍存储在副本状态表中，并且在进行远程复制操作以进行分布式恢复时也可以将凭据转移到其他组成员。然后，可能会在原始成员或从其克隆的成员上意外地使用存储的凭据启动group_replication_recovery通道。MySQL server启动时（包括在远程克隆操作之后）自动启动组复制将使用存储的用户凭据，并且如果未在START GROUP_REPLICATION命令上指定分布式恢复凭据，也将使用它们。

假设在集群中的所有节点中都已经配置好了一个启用SSL的复制用户，则可以通过如下语句来为组复制的恢复通道配置使用该用户，当启动组复制时，复制恢复通道将使用这些凭据来连接其他组成员，如下所示：

```
CHANGE MASTER TO MASTER_USER="rec_ssl_user" FOR CHANNEL
"group_replication_recovery";
```

无论是使用标准SQL客户端连接还是使用分布式恢复端点进行分布式恢复连接，为了安全地配置连接，请使用组复制专用的分布式恢复SSL系统变量。这些变量对应用于组通信连接的Server SSL系统变量值，但它们仅适用于分布式恢复的连接。默认情况下，分布式恢复连接不使用SSL，即使为组通信连接激活了SSL，这些Server SSL系统变量也不会应用于分布式恢复连接。必须单独配置组复制专用的SSL系统变量才会生效。

如果将远程克隆操作用作分布式恢复的一部分，则组复制会自动配置克隆插件的SSL选项，以匹配分布式恢复SSL选项的设置。

分布式恢复SSL参数如下：

group_replication_recovery_use_ssl：设置为ON，以使组复制将SSL用于分布式恢复连接，包括远程克隆操作和来自引导节点二进制日志的状态转移。只能设置此选项，而不能设置其他任何分布式恢复SSL选项，在这种情况下，MySQL server会自动生成用于连接的证书，并使用默认的密码套件。如果要为连接配置证书和密码套件，请使用其他分布式恢复SSL选项执行此操作。

group_replication_recovery_ssl_ca：用于分布式恢复连接的证书颁发机构（CA）文件的路径名。组复制会根据此系统变量的值自动配置为克隆插件的SSL系统变量clone_ssl_ca的值。

group_replication_recovery_ssl_capath：包含受信任的SSL证书颁发机构（CA）证书文件的目录的路径名。

group_replication_recovery_ssl_cert：用于分布式恢复连接的SSL公钥证书文件的路径名。组复制会自动将克隆SSL选项clone_ssl_cert配置为与此匹配。

group_replication_recovery_ssl_key：用于分布式恢复连接的SSL私钥文件的路径名。组复制会自动将克隆SSL选项clone_ssl_cert配置为与此匹配。

group_replication_recovery_ssl_verify_server_cert：使分布式恢复连接检查引导节点发送的证书中Server的公共名称值。将此系统变量设置为ON与系统变量group_replication_ssl_mode设置为VERIFY_IDENTITY值等效。

group_replication_recovery_ssl_crl：包含证书吊销列表的文件的路径名。

group_replication_recovery_ssl_crlpath：包含证书吊销列表的目录的路径名。

group_replication_recovery_ssl_cipher：分布式恢复连接的连接加密的允许密码列表。指定一个或多个密码名称的列表，以冒号分隔。

为组复制的分布式恢复连接配置SSL的示例如下：

```
SET GLOBAL group_replication_recovery_use_ssl=1;
SET GLOBAL group_replication_recovery_ssl_ca= '.../cacert.pem';
SET GLOBAL group_replication_recovery_ssl_cert= '.../client-cert.pem';
SET GLOBAL group_replication_recovery_ssl_key= '.../client-key.pem';
```

group_replication_recovery_tls_version：当此实例是分布式恢复连接中的客户端（即加入节点）时，一个或多个允许用于连接加密的TLS协议的逗号分隔列表。确保指定的版本是连续的（例如，“ TLSv1，TLSv1.1，TLSv1.2”）。如果未设置此系统变量，则使用默认的“ TLSv1，TLSv1.1，TLSv1.2，TLSv1.3”。每个分布式恢复连接中涉及的组成员（作为客户端（加入节点）和（引导节点））协商它们都设置为支持的最高协议版本。该系统变量可从MySQL 8.0.19获得。

group_replication_recovery_tls_ciphersuites：使用TLSv1.3进行分布式恢复连接的连接加密时，以冒号分隔的一个或多个允许密码组的列表，并且此实例是分布式恢复连接中的客户端，即加入节点。如果在使用TLSv1.3时将此系统变量设置为NULL（如果未设置系统变量，则为默认值），则允许默认启用的密码套件。如果将此系统变量设置为空字符串，则不允许使用密码套件，因此不使用TLSv1.3。从MySQL 8.0.19开始，此系统变量可用。