Main page: Cisco Unified MeetingPlace, Release 8.0

Back to: Configuration

Back to: Maintenance

The Cisco Unified MeetingPlace backup and restore functions ensure that the system can recover with minimal data loss in case of database failure or corruption.

- About Database Backups, Archives, and Restoration
- How to Back Up, Archive, and Restore Data

Contents

About Database Backups, Archives, and Restoration

Database Backups

There are three types of database backups:

- L0 (Level 0) backup. This is the most common database backup. This is a complete physical and logical backup of the database from which data can be restored.
- L1 (Level 1) backup. The L1 backup is an incremental backup. It contains a backup of all the data that has been changed since the last L0 backup. It takes much less disk space than an L0 backup; however, it cannot be used for full restoration. If the system fails, you must use both the L0 and L1 backup files to restore data.
- L2 (Level 2) backup. The L2 backup is incremental to the L1 backup, so it needs both the L0 and the L1 backups to restore data.

Cisco Unified MeetingPlace uses a combination of L0, L1, and L2 backups and uses an Informix command called **ontape** for the backup mechanism.

The database backup file is physically located on the system disk of the Application Server. The system disk can contain up to three automatically-created L0 backups: the current L0, plus the previous one or two L0 backups. The L1 and L2 backups are also kept there. All of the older backups are removed from the system disk during the cleanup process.

Caution! Use caution if you manually modify the backup files on the local disk or in the archive location. For successful data restoration, the three levels of backup files must be present in the correct order. For example, if the correct L0 and L2 backup files are present while the appropriate L1 backup file is missing, the data cannot be restored.

You can enable or disable an automatic backup. If the automatic backup is enabled, an L0 backup happens twice a week, every Monday and Thursday at 11:00PM, local server time. The L1 backup runs each day at 1:00AM, local server time, while the L2 backups run daily at 4:00AM, 8:00AM, 12:00PM, 4:00PM, and 8:00PM, local server time.

Note: In this release, you cannot use the crontab command to view or edit cron jobs. Instead, advanced system administrator (the root user) can edit the corresponding cron job file under the /etc/cron.d/ directory, the directory under which all cron job files are installed. For database backup and archive, you can change the frequency of automatic backups or archives by editing the /etc/cron.d/cron_root file. Be careful when modifying the cron schedule, which determines the order of the backups.

The automatic backup process also incorporates archiving (if enabled) and cleanup. This ensures that if there

is a database corruption or disk failure, in the worst case, less than five hours of data is lost.

Related Topics

- About Database Backups, Archives, and Restoration
- How to Back Up, Archive, and Restore Data

Cleanup Process for Database Backups

The cleanup process occurs before every scheduled backup. During the cleanup process, these files are deleted:

- Backup files older than seven days.
- Unusable files, such as L1 and L2 backup files that are older than the oldest remaining L0 backup file.

Note: If you disable automatic backups, the cleanup process continues to run as scheduled in the crontab file. Therefore, if you want to keep backup files that are older than seven days, you must archive them.

Related Topics

- About Database Backups, Archives, and Restoration
- How to Back Up, Archive, and Restore Data

About Archiving the Database Backup Files and Other Files

Archiving makes a remote copy of all the backup files and external files, such as licenses, and voice recordings that have not yet been deleted by the automatic system cleanup processes. If a newly archived file has the same name as an existing archived file, the new file overwrites the old file. Maintaining the archive and the remote system used for storing the archive is the responsibility of the system administrator.

Note: Backup files and archives do not include backup configuration settings, SNMP configuration settings, or SMTP configuration settings.

You can enable or disable automatic archiving. When enabled, it is initiated by and happens after the automatic database backup. There are two options:

- SSH/rsync Archiving Method (Recommended)
- FTP Archiving Method

SSH/rsync Archiving Method (Recommended)

The remote server to which you archive files must support rsync and SSH connections:

- To archive to a UNIX or Linux server, you must enable SSH service and rsync on that server. Both SSH service and rsync are included in most UNIX and Linux distributions.
- To archive to a Windows-based server, you must install both an SSH server and an rsync utility on that server.

Related Topics

- About Database Backups, Archives, and Restoration
- How to Back Up, Archive, and Restore Data

FTP Archiving Method

These restrictions apply to the FTP archiving method:

- The FTP archiving method does not use a secure connection to transfer files to the remote server.
- The FTP archiving method enables the Cisco Unified MeetingPlace server to transfer backup files and other critical files to the remote server; FTP clients cannot transfer files to the Cisco Unified MeetingPlace server.
- Make sure that the remote host sign-in credentials provide the permissions required to create new directories within in the directory specified in the Pathname location of archive field. For example, if you enter "pub" in the Pathname location of archive field, these directories are automatically created when the archiving script runs:
    - pub/compressed_backup
    - pub/licenses
    - pub/custom

The destination archive directory on the remote server might contain files or directories that are not present in the Cisco Unified MeetingPlace directory that is being archived. Those extra files and directories in the remote server will be left undisturbed.

Therefore, when archiving information to an FTP server, you might see messages such as the following:

- Old directory `test' is not removed
- Old directory `mpx-record/conf/001005' is not removed
- Old directory `mpx-record/conf/001192' is not removed
- Old file `tape_2009-06-19-16-00-02-Level-2.gz' is not removed
- Old file `tape_2009-06-19-20-00-02-Level-2.gz' is not removed

These messages are for information only and refer to the FTP server file system. They do not refer to the Cisco Unified MeetingPlace Application Server. It is the responsibility of the network administrator of the remote server to manage the archive directory on that server.

Most FTP servers can be used for archiving MeetingPlace database. The following FTP servers are known to work: FileZilla, Serv-U, and Titan FTP servers. freeFTPd is known to have issues with directory permissions and should not be used.

Related Topics

- About Database Backups, Archives, and Restoration
- How to Back Up, Archive, and Restore Data

How to Back Up, Archive, and Restore Data

Configuring Backups and Archiving

You can use the Cisco Unified MeetingPlace Administration Center to configure the system to automatically back up data. This section describes how to configure the parameters for the automatic backups that the system performs.

Procedure

1. Sign in to the Administration Center.
2. Select **Maintenance > Backup and Archive**.
3. Configure the fields on the Backup and Archive Page.
4. Perform one of these actions:
    - ♦ To save these values without running the backup program, select **Save**.
    - ♦ To save these values and run the backup process, select **Save and Run Backup**.
    - ♦ To save these values and run the archive process, select **Save and Run Archiving**.

Related Topics

- Table: Field Reference: Backup and Archive Page in the Administration Center Page References for Cisco Unified MeetingPlace (A - C pages)
- About Database Backups, Archives, and Restoration
- How to Back Up, Archive, and Restore Data

Backing Up Data By Using the CLI on the Application Server

If you disable the automatic back up feature (by selecting **No** for the Enable automatic backup field on the Backup and Archive Page), you can still manually back up data.

Restriction

Only run one backup (L0, L1, or L2) at a time.

Procedure

1. Sign in to the Cisco Unified MeetingPlace operating system as the **mpxadmin** user.
2. At the password prompt, enter the mpxadmin password.
3. Right-click on the desktop.
4. From the menu, select **New Terminal**. This brings up a terminal session.
5. Manually back up the data by entering this command:
   sudo $MP_DATABASE/db-maintenance/backup.sh <number>
   where **<number>** is the number of the backup you are running. To make sure you run only one backup at a time, specify 0 for an L0 backup, 1 for an L1 backup, or 2 for an L2 backup.
   When the system finishes the backup, it displays a "Backup ended" message.
6. On the desktop, select **RedHat > Network Services**.
7. Select **Log out**.

Related Topics

- About Database Backups, Archives, and Restoration
- How to Back Up, Archive, and Restore Data

Archiving Data By Using the CLI on the Application Server

Regardless if auto-archiving is on or off, the archive.sh script forces archiving as described in the Configuring Backups and Archiving.

Procedure

1. Sign in to the Cisco Unified MeetingPlace operating system as the **mpxadmin** user.
2. At the password prompt, enter the mpxadmin password.
3. Right-click on the desktop.
4. From the menu, select **New Terminal**. This brings up a terminal session.
5. Manually archive the data by entering this command:
   sudo $MP_DATABASE/db-maintenance/archive.sh
   Note: The archive.sh script uses remote sign-in credentials that are defined in the $MP_DATABASE/db-maintenance/settings.config file. You set these credentials using the procedure described in the Configuring Backups and Archiving.
   When the system finishes the archive, it displays "Archive ended" and "Archive external files ended" messages.
6. On the desktop, select **RedHat > Network Services**.
7. Select **Log out**.

Related Topics

- About Database Backups, Archives, and Restoration
- How to Back Up, Archive, and Restore Data

Restoring Data By Using the CLI on the Application Server

Restoring the data recreates database server data from backed-up storage spaces and logical log files. You might need to restore your data if you need to replace a failed disk that contains database server data, if there is a logic error in a program that has corrupted the database, if you need to move your database server data to a new computer, or if a user accidentally corrupts or destroys data.

Before You Begin

- To restore data up to the time of the failure, you must have at least one L0 backup.
- You must have the backup files in the correct order. For example, if you have the correct L0 and L2 backup files, but not the appropriate L1 backup file, you cannot restore the data on the L2 backup file. You will still be able to restore from L0. This requires extra caution if you manually back up files on a local disk or in the archiving location.
- You can only restore the data to a server with the same IP and hostname as was originally configured for your backup.
- If you are restoring two Application Servers that are configured in a failover deployment, make sure that the servers are in standby mode before running the restore on them.
- If you are restoring two Application Servers that are configured in a failover deployment, make sure that you turn off replication before running the restore.

Restrictions

- You can only restore a database that is from the same version of Cisco Unified MeetingPlace. You cannot restore a database from a previous version.
- The names of the databases that you are restoring from and restoring to must be the same.

Procedure

1. Sign in to the Cisco Unified MeetingPlace operating system as the **mpxadmin** user.
2. At the password prompt, enter the mpxadmin password.
3. Right-click on the desktop.
4. From the menu, select **New Terminal**.
   This brings up a terminal session.
5. Restore the data by entering this command:
   sudo $MP_DATABASE/db-maintenance/restore.sh
6. At the system prompt, press **S** to stop the Cisco Unified MeetingPlace application.
7. Choose the type of restore you want. Press **A** for archive or **L** for the local disk and follow the prompts on the screen.
8. Choose an entry from the displayed list of backups.
9. Enter the number associated with the backup entry.
10. When prompted, press **R** to perform the restore.

When the system finishes the archive, it displays the message: "You restored database successfully."

11. If you are restoring an Application Server that is configured in a failover deployment, reboot the server after the restore is completed.

    Note: If the server needs to be in active mode after it reboots, switch it to active mode.
12. On the desktop, select **RedHat > Network Services**.
13. Select **Log out**.

Troubleshooting Tips

- If you restore archived data after you reinstall the Cisco Unified MeetingPlace Web Server software or the entire Cisco Unified MeetingPlace system, the system might not find meetings because the Application Server cannot reach the Web Server. If this occurs, you need to manually edit the Web Server connection to use the new Installation key, which changed during the reinstallation process. For details, see Adding or Editing a Web Server Connection in the Connecting the Cisco Unified MeetingPlace Application Server to a Web Server module.

- If the Web Server page in the Administration Center appears to have duplicate entries after completing the restore, make the old entries inactive, then log in to the Application Server CLI as root user and use the gwstatus command to verify that the inactive entries have been removed.

Related Topics

- About Database Backups, Archives, and Restoration
- How to Back Up, Archive, and Restore Data
- Sending Email Blasts from Cisco Unified MeetingPlace
- Configuring Two New Application Servers in a Failover Deployment After Failure of Both Existing Servers

What To Do Next

- When updating (synchronizing) all meetings on the Web Server, the system deletes all the data for meetings that do not exist on the Application Server. Therefore, the next time you or the system updates all meetings, the system deletes these items from the Web Server:
  - ♦ Recordings for meetings that occurred between the backup time and the restore time.
  - ♦ Meetings that were scheduled between the backup time and the restore time. Nevertheless, you or your users might save local copies of recordings before they are deleted. You can use an email blast to inform your users of the following:
  - ♦ Time period (between the most recent backup time and the restore time) of affected meetings.
  - ♦ How to save local copies of recordings. See the *User Guide for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_user_guide_list.html.
  - ♦ Deadline for saving local copies of recordings. This is determined by the next update-all-meetings event, which occurs automatically at midnight every Saturday night (local server time), or when you complete the Updating All Meetings section in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module.

- If you restored two Application Servers that were configured in a failover deployment, complete the failover setup on Node 1 and Node 2. See How to Configure Application Server Failover.