FortiNAC

Backup and Restore

Version: 9.x

Date: March 6, 2023

Rev: F

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET KNOWLEDGE BASE

https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

FORTINET BLOG

http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

http://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

NSE INSTITUTE

http://training.fortinet.com

FORTIGUARD CENTER

http://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contents

Overview

What it Does

Administering FortiNAC should include a backup plan in case of data corruption or equipment failure. This document describes the best practices for backing up and restoring the FortiNAC components, whether for a single server, a Control Server/Application Server pair, a High Availability (HA) system, or multiple servers managed by a FortiNAC Control Manager (NCM).

How it Works

FortiNAC has the ability to backup the following:

- **Database**: FortiNAC's mysql database contains the components and configurations viewed/modified through the Administration UI and the last known state of those components. Everything seen in the Administration UI is kept in the database except for Alarms and Events, Connection Logs and Scan Results. Passwords are encrypted.
- **System files**: Files associated with the configurations done through Configuration Wizard as well as additional files required for appliance operation.
- **Alarms and Events:**
- **Connection Logs:** List of historical host/user network connections.
- **Scan Results**

Backups of the database and other files occur when their corresponding scheduled tasks run. The backup files are stored on the local appliance. The Administrator can additionally configure FortiNAC to place a copy of the database and other directories on an ftp and/or other remote server for safekeeping.

FortiNAC includes these backup/restore capabilities:

- **Database Backup:** A scheduled task that backs up the entire database to the FortiNAC itself.
- **Database Archive and Purge:** Use Database Archive to set age times for selected log files (Connections, Events/Alarms, and Scan Results). Log files are archived and then purged from the FortiNAC database when the age time elapses. Archived data can be imported back into the database if necessary.
- **System Backup:** A scheduled task that creates a backup of all system files that are used to configure FortiNAC, such as license key and web server configurations.
- **Remove local backups:** The number of days desired to keep backups before deleting from the local drive. This setting is available for each of the above backup types.
- **Backup to Remote Server:** Uploads a copy of the Database Backup, Database Archive and System Backup files to a remote server.

Recommendations and Considerations

Virtual Appliance

Recommendations

- Database: Run backup daily
- Run virtual machine snapshots regularly*
- Alarms & Events
- Connection Logs
- Scan Results

*Virtual machine snapshots restore the entire appliance. This is a much simpler and quicker restoration method than restoring files separately. If the database included in the snapshot is not for the appropriate time period, the database can be restored separately once the desired snapshot has been loaded.

Considerations

- When the snapshot is being reverted and FortiNAC services are halted:
    - VLANs will not switch
    - Rogue devices will not be able to register
    - FortiNAC will not answer RADIUS requests
    - Scans will not be performed
- Devices registered since the time of the snapshot will need to re-register
- Devices added to Inventory since the time of the snapshot will need to be re-added
- Reverting the snapshot: System should start up once snapshot is reverted
- Moving the VM to another host: UUID and eth0 MAC will change. License key will need to be updated with new UUID and MAC (contact Customer Service)

Due to the above, performing these tasks after hours would be advisable.

Physical

Recommendations

- Database: Run backup daily
- System Files: Run backup weekly
- Alarms & Events
- Connection Logs
- Scan Results

Considerations

- Restoration process does not recover the following:
    - Basic Network configuration
        - Host Name
        - Eth0 IP address/mask
        - Eth0 default gateway
    - DNS
        - Server IP address(es)
        - Domain
    - CLI Passwords
- While FortiNAC services are halted:
    - VLANs will not switch
    - Rogue devices will not be able to register
    - FortiNAC will not answer RADIUS requests
    - Scans will not be performed
- Devices registered since the time of the restored database will need to re-register
- Devices added to Inventory since the time of the restored database will need to be re-added
- Restoring database to the same appliance: System should start up once database is restored
- Moving database to another appliance: License key will need to be updated with new Serial number and eth0 MAC address (Contact Customer service for assistance)

Due to the above, performing these tasks after hours would be advisable.

Database and Database Archive

Full database backups and log files that are periodically archived and purged, are stored in a compressed, date-stamped format on the Control Server (in control on an HA) in the */bsc/campusMgr/master_loader/mysql/backup* directory. The database backup is named:
<database>_<yyyy_mm_dd_hh_mm_ss>.gz
The table archive is named:
<table>_<yy_mm_dd_hh_mm_ss>.gz

The following is a listing of backup files. Notice that there are entries for the complete database (DataBase_BackUp) and the archived records (e.g., ALARMS_Archive). Note that file size will vary.

```
52M   FortiNAC_DataBase_BackUp_2017_08_21_00_01_35_bcm.gz
4.6M  EVENTS_Archive_2017_08_21_01_01_15_bcm.bua.gz
67K   TESTS_RESULTS_Archive_2017_08_21_01_01_15_bcm.bua.gz
43K   RESULTS_Archive_2017_08_21_01_01_15_bcm.bua.gz
52K   MAC_RESULTS_Archive_2017_08_21_01_01_15_bcm.bua.gz
116K  ALARMS_Archive_2017_08_21_01_01_15_bcm.bua.gz
3.1M  DYNAMICLOG_Archive_2017_08_21_01_01_15_bcm.bua.gz
1.2M  CONNECTIONS_Archive_2017_08_21_23_44_15.bua.gz
```

The following table maps the type of records that are archived to the backup filename.

Database Backup Filenames

Database Records	Filename
Database	Database_BackUp
Events	EVENTS_Archive
Alarms	ALARMS_Archive
Scan Results	RESULTS_Archive (coupled with TEST_RESULTS and MAC_RESULTS)
Connections	DYNAMICLOG_Archive (coupled with CONNECTIONS_Archive)

System Backups

A system backup creates a backup of all system files that are used to configure FortiNAC, such as license key and web server configurations. Backups of selected files and directories are stored in a compressed, date-stamped format on the same server where they reside in the */bsc/backups/<hostname>* directory as:
<hostname>.<yyyy_mm_dd>.<directory>.tar.gz

For example, for a Control/Application Server pair, qa192/qa229, the files on qa192 would be backed up to */bsc/backups/qa192* on qa192, and the files on qa229 would be backed up to */bsc/backups/qa229* on the qa229.

Remote Backups

If FortiNAC data is not backed up to a remote server, there is the potential of losing file and database backups if a disk/appliance fails. The Remote Backup feature copies the database and file backups to the specified remote server, using either FTP or SSH. The best practice is to include remote offsite backup using SSH. For details, see Remote backup configuration in the Administration Guide.

FTP access utilizes the login credentials (user name and password) set up in the Admin UI, whereas SSH uses an encrypted key which must be copied from the FortiNAC to the remote server, preferably in some account other than ROOT. (See Configure SSH Backups)

Note: FortiNAC does not manage backups on a remote server.

Scheduling

Scheduling options are available for each of the backup configurations:

- Database
- System files
- Database Archive
    - Alarms and Events
    - Connection Logs
    - Scan Results

Determine Backup Frequency

How often the various backups are run depends upon the anticipated network activity. Consider the frequency of change for the following, and determine the frequency based on the most frequent occurrence.

- Database
    - New registrations (BYOD, company assets, headless devices, etc)
    - Network infrastructure configuration models added or modified in FortiNAC Topology
    - **Best practice:** Backup the database daily
- System files
    - Changes made via configWizard (DHCP scopes, etc)
    - **Best practice:** Unless needed more often, backup the system files weekly.
- Database Archive
    - Alarms and Events: The frequency alarms and events are generated
    - Connection Logs: Devices connecting and disconnecting from the network
    - Scan Results: How often hosts are scanned

    Note: Once logs are archived, they are no longer searchable via the Alarms, Events or Connection Logs view.

Determine Purging Frequency

Decide how long to keep backups before deleting. Keep in mind the possible conflicts between scheduled backups and configured backup removal, and the configured timeout for the backup process:

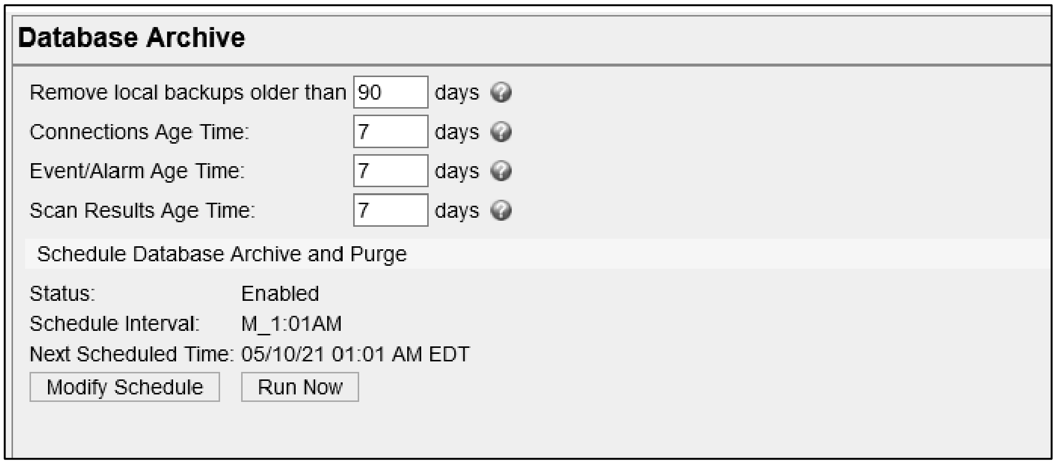
The **Remove Backups Older Than** field is available for all three backup configurations and are independent of each other. This field value should always be larger than the frequency used for the backup. For example, if the field is set to 5 days and the backup task runs every 15 days, all of the backups may be removed inadvertently. However, if the remove option is set to 15 days and the backup task runs every 5 days, then there would always be backup files available.

Note: This parameter affects the backups on the local server only, not backups on the remote server.

Configure Archive/Purge Database Records Schedule

When the Events Archive and Purge task is run, records older than the corresponding Age Time field (in Topology view, FortiNAC Properties tab) are archived to the local Control Server and purged from the database.

1. Navigate to **System > Settings > System Management > Database Archive**



Database Archive

Remove local backups older than 90 days

Connections Age Time: 7 days

Event/Alarm Age Time: 7 days

Scan Results Age Time: 7 days

Schedule Database Archive and Purge

Status: Enabled

Schedule Interval: M_1:01AM

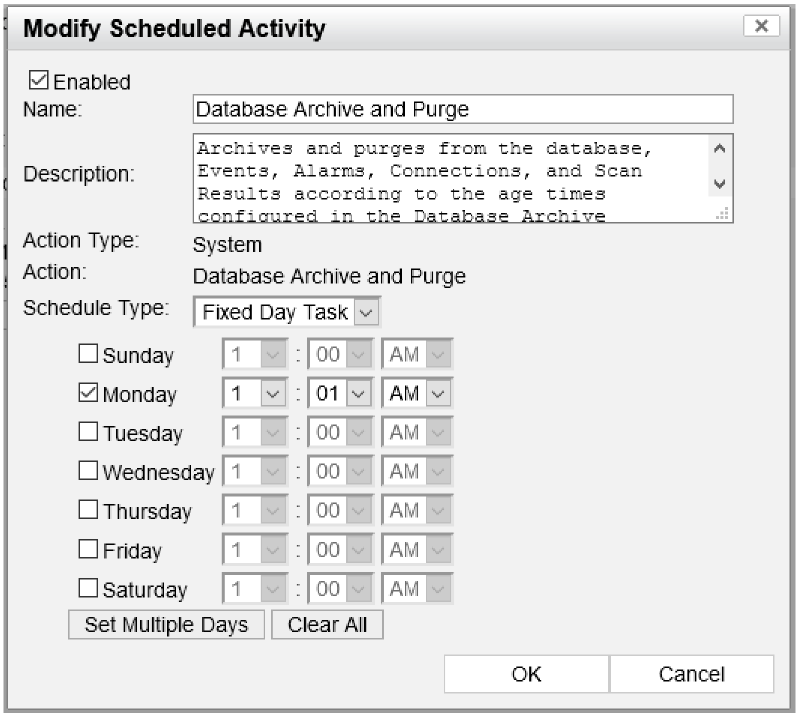
Next Scheduled Time: 05/10/21 01:01 AM EDT

2. Set **Remove local backups older than** to desired value. See Purging Frequency.

3. Set Age Times as desired.

4. Click **Modify Schedule**.

Note: This same view can be accessed by navigating to **System > Scheduler.** Double click **Database Archive and Purge.**



Modify Scheduled Activity

☑ Enabled

Name: Database Archive and Purge

Description:
```
Archives and purges from the database,
Events, Alarms, Connections, and Scan
Results according to the age times
configured in the Database Archive
```

Action Type: System

Action: Database Archive and Purge

Schedule Type: Fixed Day Task

□ Sunday	1	:	00	AM
☑ Monday	1	:	01	AM
□ Tuesday	1	:	00	AM
□ Wednesday	1	:	00	AM
□ Thursday	1	:	00	AM
□ Friday	1	:	00	AM
□ Saturday	1	:	00	AM

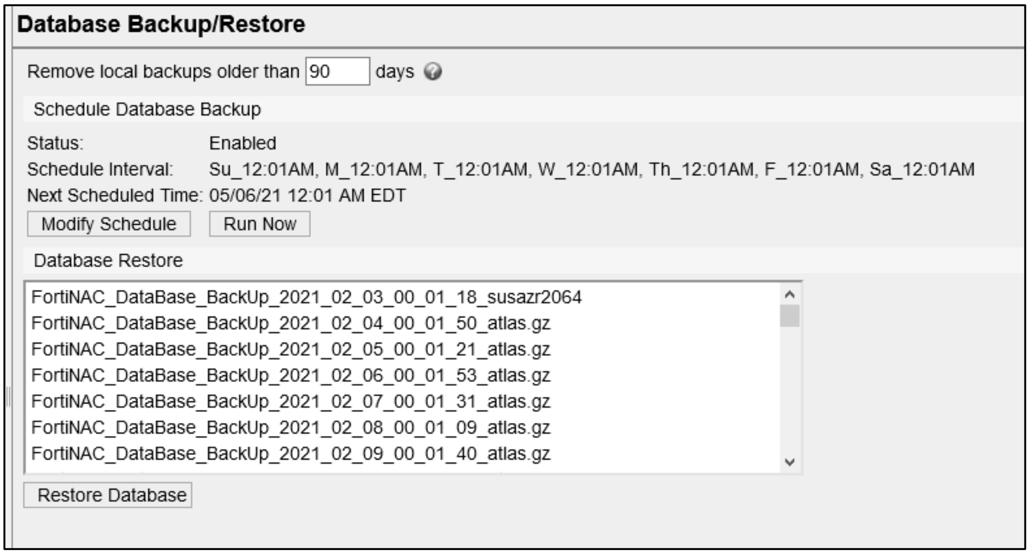
5. Enable the task and edit as appropriate. For details see [Database archive]() in the Administration Guide.

6. Click **OK**.

7. Click **Save Settings**.

Configure Database Backups Schedule

1. Navigate to **System > Settings > System Management > Database Backup/Restore**.



Database Backup/Restore

Remove local backups older than 90 days

Schedule Database Backup

Status: Enabled

Schedule Interval: Su_12:01AM, M_12:01AM, T_12:01AM, W_12:01AM, Th_12:01AM, F_12:01AM, Sa_12:01AM

Next Scheduled Time: 05/06/21 12:01 AM EDT

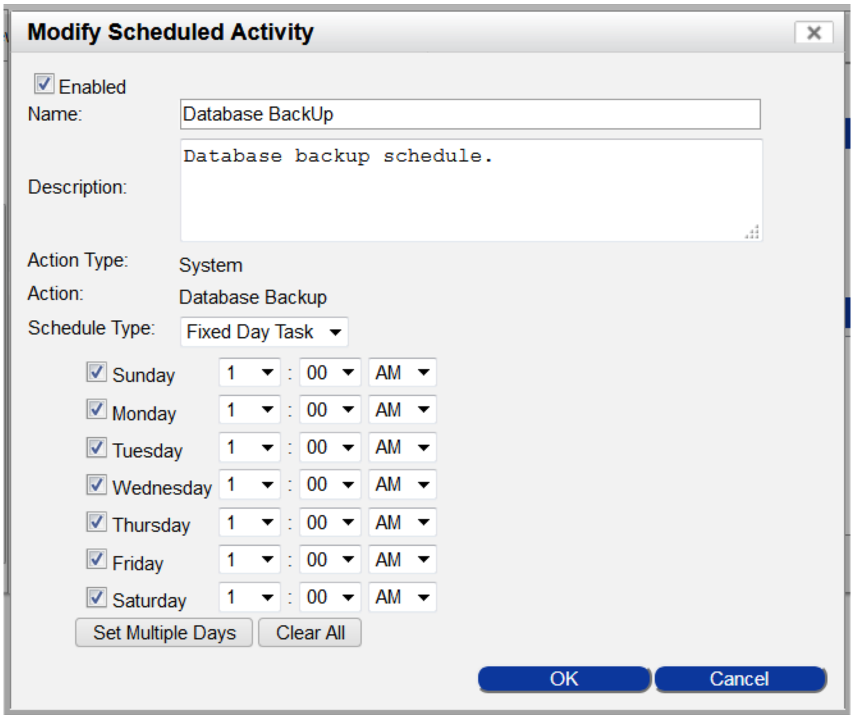
Database Restore

```
FortiNAC_DataBase_BackUp_2021_02_03_00_01_18_susazr2064
FortiNAC_DataBase_BackUp_2021_02_04_00_01_50_atlas.gz
FortiNAC_DataBase_BackUp_2021_02_05_00_01_21_atlas.gz
FortiNAC_DataBase_BackUp_2021_02_06_00_01_53_atlas.gz
FortiNAC_DataBase_BackUp_2021_02_07_00_01_31_atlas.gz
FortiNAC_DataBase_BackUp_2021_02_08_00_01_09_atlas.gz
FortiNAC_DataBase_BackUp_2021_02_09_00_01_40_atlas.gz
```

2. Set **Remove local backups older than** to desired value. See Purging Frequency.

3. Click **Modify Schedule**.

Note: This same view can be accessed by navigating to **System > Scheduler.** Double click **Database BackUp.**



Modify Scheduled Activity

☑ Enabled

Name: Database BackUp

Description: Database backup schedule.

Action Type: System

Action: Database Backup

Schedule Type: Fixed Day Task

☑	Sunday	1	00	AM
☑	Monday	1	00	AM
☑	Tuesday	1	00	AM
☑	Wednesday	1	00	AM
☑	Thursday	1	00	AM
☑	Friday	1	00	AM
☑	Saturday	1	00	AM

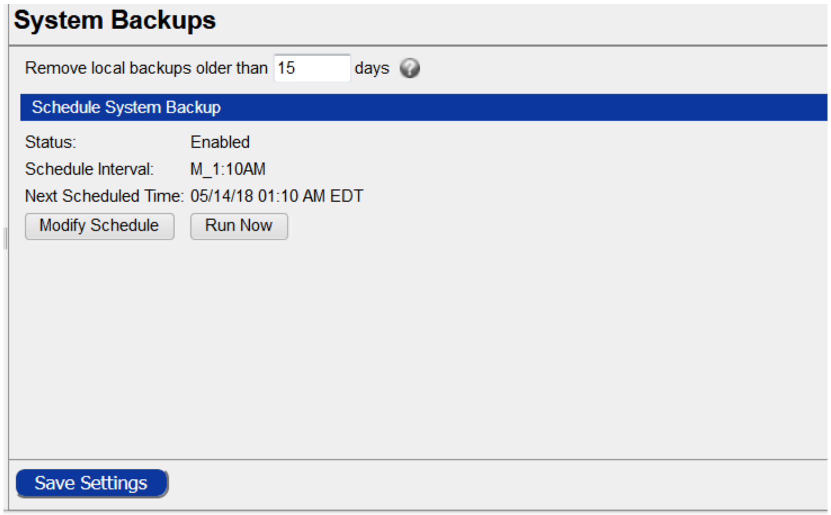
4. Enable the task and edit as appropriate. For details see Database backup/restore in the Administration Guide.

5. Click **OK** to save schedule settings.

6. Click **Save Settings**.

Configure System Backups Schedule

1. Click **System > Settings > System Management > System Backups.**



System Backups

Remove local backups older than 15 days

Schedule System Backup

Status: Enabled

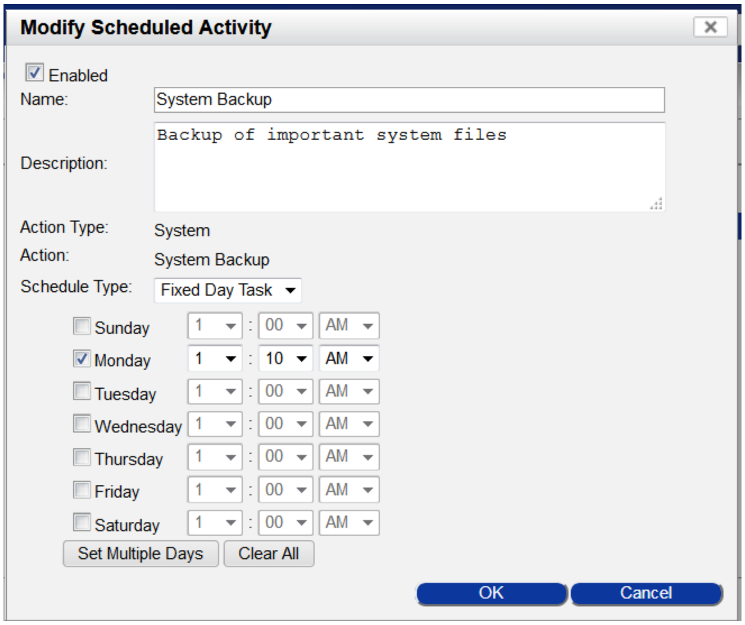
Schedule Interval: M_1:10AM

Next Scheduled Time: 05/14/18 01:10 AM EDT

2. Set the **Remove local backups older than** to desired value. See Purging Frequency.

3. Click **Modify Schedule**.

Note: This same view can be accessed by navigating to **System > Scheduler.** Double click **System Backup.**



Modify Scheduled Activity

☑ Enabled

Name: System Backup

Description: Backup of important system files

Action Type: System

Action: System Backup

Schedule Type: Fixed Day Task

□ Sunday	1	00	AM
☑ Monday	1	10	AM
□ Tuesday	1	00	AM
□ Wednesday	1	00	AM
□ Thursday	1	00	AM
□ Friday	1	00	AM
□ Saturday	1	00	AM

4. Enable the task and edit as appropriate. For details see System backups in the Administration Guide.

5. Click **OK**.

6. Click **Save Settings**.

Manual Backups

Scheduled backups should be run before:

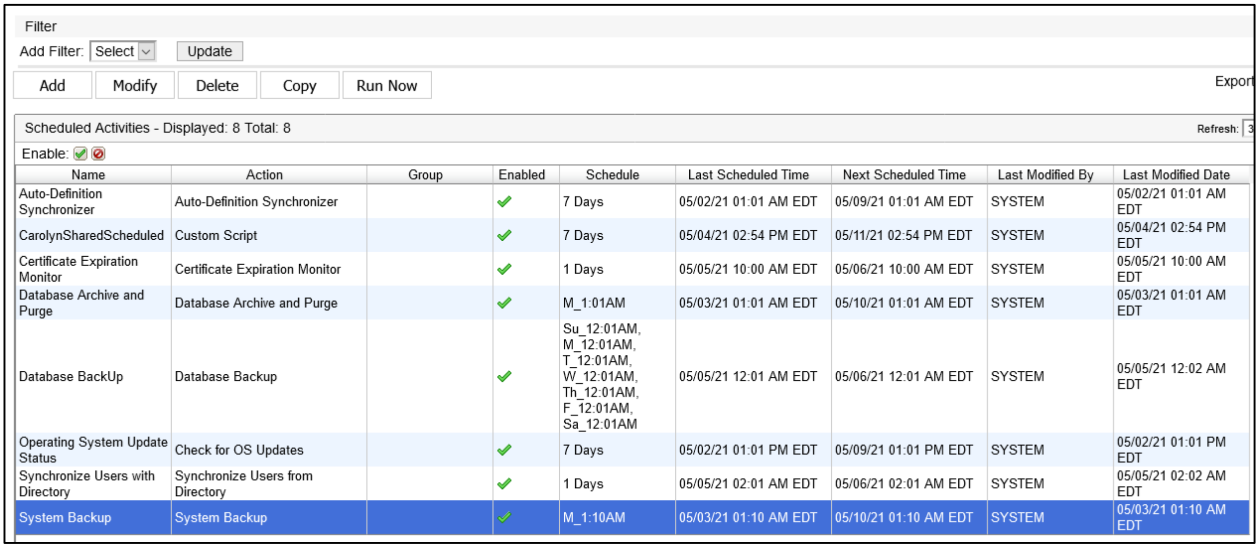
- Any major changes to FortiNAC's configuration
- Upgrading hardware. Before replacing the hardware, back up the database and files/directories list to a remote server.

Note: FortiNAC automatically backs up files during software upgrades.

Run Manual Backup

In addition to the individual configuration views, each backup can be scheduled and run from the Scheduler view.

1. Navigate to **System > Scheduler**.



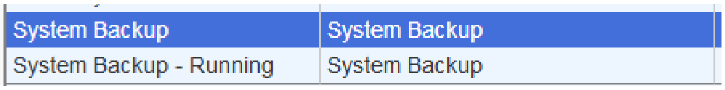
Scheduled Activities - Displayed: 8 Total: 8

Name	Action	Group	Enabled	Schedule	Last Scheduled Time	Next Scheduled Time	Last Modified By	Last Modified Date
Auto-Definition Synchronizer	Auto-Definition Synchronizer		✓	7 Days	05/02/21 01:01 AM EDT	05/09/21 01:01 AM EDT	SYSTEM	05/02/21 01:01 AM EDT
CarolynSharedScheduled	Custom Script		✓	7 Days	05/04/21 02:54 PM EDT	05/11/21 02:54 PM EDT	SYSTEM	05/04/21 02:54 PM EDT
Certificate Expiration Monitor	Certificate Expiration Monitor		✓	1 Days	05/05/21 10:00 AM EDT	05/06/21 10:00 AM EDT	SYSTEM	05/05/21 10:00 AM EDT
Database Archive and Purge	Database Archive and Purge		✓	M_1:01AM	05/03/21 01:01 AM EDT	05/10/21 01:01 AM EDT	SYSTEM	05/03/21 01:01 AM EDT
Database BackUp	Database Backup		✓	Su_12:01AM, M_12:01AM, T_12:01AM, W_12:01AM, Th_12:01AM, F_12:01AM, Sa_12:01AM	05/05/21 12:01 AM EDT	05/06/21 12:01 AM EDT	SYSTEM	05/05/21 12:02 AM EDT
Operating System Update Status	Check for OS Updates		✓	7 Days	05/02/21 01:01 PM EDT	05/09/21 01:01 PM EDT	SYSTEM	05/02/21 01:01 PM EDT
Synchronize Users with Directory	Synchronize Users from Directory		✓	1 Days	05/05/21 02:01 AM EDT	05/06/21 02:01 AM EDT	SYSTEM	05/05/21 02:02 AM EDT
System Backup	System Backup		✓	M_1:10AM	05/03/21 01:10 AM EDT	05/10/21 01:10 AM EDT	SYSTEM	05/03/21 01:10 AM EDT

2. Highlight the desired activity:
   Database Archive and Purge
   Database Backup
   System Backup

3. Click **Run Now**.

   A second instance of the activity will appear under the original activity, indicating the activity is running.



System Backup	System Backup
System Backup - Running	System Backup

   This instance will disappear upon refresh once the backup has completed.

Remote Backups

Configuration

Remote Backup Configuration defines the connection details used to copy files to a third party (remote) server when the Database Backup task is run in Scheduler. Transferring the backup files can be done using FTP and/or SSH protocols.

For instructions see section Remote backup configuration in the Administration Guide.

Restore

This section describes how and when (typical scenarios) to restore from a backup file.

High Availability configurations: Database is restored to the FortiNAC Server that is in control at the time of restore.

Database Using Administration UI

Typical Scenarios

- Data was accidentally deleted which would take extensive time to restore manually, e.g., a domain from Topology view, a list of registered clients from Clients view.
- Database was corrupted.

In these cases, the Admin UI is functioning properly and you just need to restore lost data.

Note: Restoring the database will not include any data captured between the time of the backup and the current time.

Procedure

1. Click **System > Settings > System Management > Database Backup/Restore**.

2. Click on a backup to select it.

3. Click **Restore Database**.

Database Using CLI

Typical Scenarios

- The disk fails on a RAID-less appliance.
- The appliance has been reset to factory defaults, and you want to restore the pre-reset remote backup of the database.
- You have upgraded the FortiNAC hardware and want to restore the most recent remote backup from the previous FortiNAC appliance.

Procedure

1. Copy (e.g., use winscp) the most recent backup from the remote server to the **/bsc/campusMgr/master_loader/mysql/backup** directory on the FortiNAC Control Server.

2. Log into the CLI on the Control Server with root privileges.

3. Stop the the FortiNAC processes:
   ```
   shutdownCampusMgr
   ```

4. Navigate to the **/bsc/campusMgr/master_loader/mysql/backup** directory and identify the filename of the backup to be used.
   Example:
   ```
   FortiNAC_DataBase_BackUp_2018_05_14_00_01_06_qa6-74.gz
   ```

5. Navigate to the **/bsc/campusMgr/master_loader/mysql** directory and restore the database:
   ```
   ydb_restore_full_backup <database_name>
   ```

   Example:
   ```
   ydb_restore_full_backup
   FortiNAC_DataBase_BackUp_2018_05_14_00_01_06_qa6-74.gz
   ```

6. Start the FortiNAC processes:
   ```
   startupCampusMgr
   ```

Archived Data

When the Purge Events task runs, FortiNAC creates an archive of several different types of records. You can reimport this data if necessary. Importing archived data does not overwrite existing data. It adds the archived records back into the database.

Records that are archived and can be re-imported include the following:

- Alarms View
- Events View
- Scan Results
- Connections

Procedure

Note: If the archived data is not currently in the **/bsc/campusMgr/master_loader/mysql/backup** directory on the Control Server (in control for HA), transfer a copy from the remote server (use WinSCP) to that directory.

1. Navigate to one of the views listed above.

2. Click the Import button at the bottom of the view to display the Import window.

3. Select the archive from the drop-down list. The archives are listed by date with the name of the view at the beginning. For example, for the Connections View the archive would have the following format:
   DYNAMICLOG_Archive_YY_MM_DD.bua.gz

4. Click **OK**.

Some archive files can be quite large and may take several minutes to import. A progress dialog is displayed as the import is taking place. A message is displayed when the import is complete.

System Files/Directories

Typical Scenarios

- Files are corrupted or accidentally deleted
- The disk fails on a RAID-less appliance.
- The appliance has been reset to factory defaults and need to restore customized files from the pre-reset remote backup.
- FortiNAC hardware has been upgraded and need to restore customized files from the pre-reset remote backup from the previous FortiNAC appliance.

Procedure

1. If the failed appliance held the endpoint license entitlements, ensure the entitlements have been moved from the old appliance to the new device's serial number. Contact Customer Service for assistance.

2. Run the Config Wizard on the new appliance to configure the basic network settings (IP address, host name, domain for etc).

   a. Complete **Basic Network** and **Passwords**
   b. Click **Summary** and **Apply**
   c. Reboot appliance

   For instructions, see the applicable Configuration Wizard Guide:
   Versions 9.2 & 9.4
   Versions 8.x & 9.1

3. Access the appliance CLI as `root`.

4. Create a temporary directory.

5. Locate the backup file (e.g., on appliance in the **/bsc/backups/<hostname>** directory, or on a remote server) from which you will restore the file(s).

6. Copy (use WinSCP if copying from a remote server) the following backup files to the temporary directory:

   ```
   <hostname>.<yyyymmdd>.bsc-.runtime-data.tar.gz
   <hostname>.<yyyymmdd>.bsc-Registration.tar.gz
   <hostname>.<yyyymmdd>.bsc-Remediation.tar.gz
   <hostname>.<yyyymmdd>.bsc-Hub.tar.gz
   <hostname>.<yyyymmdd>.bsc-Authentication.tar.gz
   <hostname>.<yyyymmdd>.bsc-DeadEnd.tar.gz
   <hostname>.<yyyymmdd>.bsc-CommonJspFiles.tar.gz
   <hostname>.<yyyymmdd>.bsc-VPN.tar.gz
   <hostname>.<yyyymmdd>.bsc-www.tar.gz
   <hostname>.<yyyymmdd>.bsc-siteConfiguration.tar.gz
   <hostname>.<yyyymmdd>.bsc-services-tomcat-admin-conf.tar.gz
   <hostname>.<yyyymmdd>.bsc-services-tomcat-portal-conf.tar.gz
   <hostname>.<yyyymmdd>.bsc-campusMgr-master_loader-telnetMibs.tar.gz
   <hostname>.<yyyymmdd>.bsc-campusMgr-master_loader-customTraps.tar.gz
   <hostname>.<yyyymmdd>.bsc-campusMgr-.keystore.gz
   <hostname>.<yyyymmdd>.bsc-campusMgr-bin-.backup_config.gz
   <hostname>.<yyyymmdd>.bsc-campusMgr-bin-.config.properties.gz
   <hostname>.<yyyymmdd>.bsc-campusMgr-bin-.networkConfig.gz
   <hostname>.<yyyymmdd>.bsc-campusMgr-agent-scanConfig.tar.gz
   <hostname>.<yyyymmdd>.bsc-campusMgr-agent-customScanConfig.tar.gz
   ```

7. Extract the contents of the backup files to the temporary folder, retaining the original directory structure:
   `tar -xzvf <filename>`

   Example:
   ```
   tar -xzvf qa228.20091102.bsc-Authentication.tar.gz
   ```

8. Locate the files to be restored, and copy them to the appropriate directory(ies).

9. Reboot system.

Contact Support for assistance.