Table of Contents

yce_setup.pl

The **`yce_setup.pl`** script, located in `/opt/yce/system/`, is used for setting up the YCE application. The script is used at initial system setup, when changes to the system setup must be made, when the networking environment has changed, and when a software update is completed.

The **yce_setup** script is tasked to create configuration files for all components the NetYCE application is composed of and activating these configurations. These components include many background processes (often referred to as daemons) like http-, tftp-, ftp- and scp-servers, but also backend api's, process monitoring, database replication and maintenance.

In its interactive mode the user can add and delete NetYCE servers to its environment and define its roles. The resulting configuration setup file (`/opt/yce/etc/yce_setup.conf`) is then used in the non-interactive mode of **yce_setup** to re-generate the various configurations and restart their processes.

> Note: Each NetYCE server has it unique `yce_setup.conf` file. When making changes to the NetYCE environment (like adding a server or enabling SSL), it needs to be done for ***all servers*** successively.

net_setup dependency

The networking addresses for the local server are taken from the `net_setup.conf` file (also located in `/opt/yce/etc`). It is managed by running the **net_setup** script (see net_setup.pl) and can be automatically updated by the **yce_netmon** daemon when using dynamic ip-addresses using DHCP.

To setup a new NetYCE server, executing **net_setup** (as 'root') prior to executing **yce_setup** is the most logical, but not essential. When completing the net-setup, the yce-setup is automatically initiated in its non-interactive mode using common defaults.

Roles and settings

The yce_setup will prompt the user in a dialog to set NetYCE server parameters in several categories. The settings apply primarily to the local server, but because of the communication and replication with the remote NetYCE servers, the setup must include the full environment.

- Add new or delete existing NetYCE servers (depending on architecture license)
- Edit primary IPv4 and IPv6 addresses of remote servers
- IPv4 and IPv6 addresses of the local server are retrieved from the net_setup.conf
- Assign any server the role of Front-end server (Web GUI, API's, device management)
- Assign any server the role of Database server (up to two per environment)
- Set up the server to run in a non-DNS (ip-addresses only) network
- Enable the Web GUI to use SSL certificates (https)
- Limit SSL support to most hardened protocols
- Assign another than the default port 8080 to the GUI backend
- Assign the unique database id for replication
- Assign the primary and secondary database server for each server to use
- Define the single-sign-on parameters (dns-)domain and validity duration

- Select the use of the public NetYCE wiki server or a local private copy

Changes or additions to the setup must be repeated identically to the other servers in the environment.

NOTES:

> The yce_setup script should to be started as 'yce' user.
>
> In the dialog with yce_setup the (default) values and the user entries are shown using the color 'green' for easy legibility. This colour provides a good contrast on both white and black terminal backgrounds.
>
> Default values are shown between square brackets (`[` and `]`). An <enter> suffices to accept de default value. The use of these defaults is to permit the user to enter as few as possible values and re-use existing values where available.
>
> At each prompt a help message is available by entering the **?** as value.
>
> Abort the script by typing `quit` to any prompt or hitting `<control>`C.

Invocation

The **yce_setup** script is executed by the 'yce' user (not as root) from a SSH session or console (default credentials: user 'yce', password 'NetYCE01'). The interactive mode is started without any argument:

```
$ yce_setup.pl
-- ----------------------------------------
-- ----------------------------------------
-- Starting 'yce_setup' interactive
-- System release
   identified CentOS - 7.9.2009
   using setup for Redhat V7
-- Connected to database at '172.17.10.24' using version '10.2.36-MariaDB-
log'

NOTE:
  When prompted for input help on the question is available by entering '?'.
  Incorrect responses result in a message on the expect input.
  Just hitting <enter> will accept the existing or default value '[...]'.
  The proces can be aborted at any prompt by entering 'quit'.

YCE servers currently in setup:
1) devel7a.netyce.org (*)
   | IPv4-address          | IPv6-address
   |  172.17.10.24         |  3001::24
2) devel7b.netyce.org
   | IPv4-address          | IPv6-address
   |  172.17.10.25         |  3001::25
  local server is marked with (*)
  Select the server-number to Edit/Remove, or 'A' to add, 'C' to continue:
```

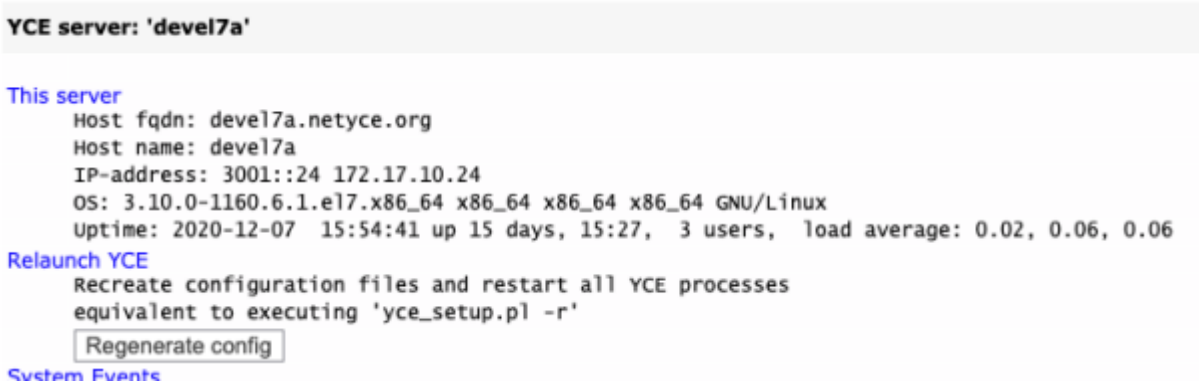
```
[C]
```

The non-interactive mode is normally invoked automatically when needed. It uses the **-r** option (for “regenerate”):

```
$ yce_setup7.pl -r
-- ----------------------------------------
-- Starting 'yce_setup' regenerate
-- System release
   identified CentOS - 7.9.2009
   using setup for Redhat V7
-- Connected to database at '172.17.10.24' using version '10.2.36-MariaDB-
log'

Current setup:
devel7a.netyce.org (*)
  | IP-address  | IPv4              | IPv6
  |  users      |  172.17.10.24     |  3001::24
  | Database    | Primary           | Secondary
  |  id=1       |  devel7a (*)      |  devel7b
devel7b.netyce.org
  | IP-address  | IPv4              | IPv6
  |  users      |  172.17.10.25     |  3001::25
  | Database    | Primary           | Secondary
  |  id=2       |  devel7b          |  devel7a (*)
  local server is marked with (*)
-- Create configs for server 'devel7a'
-- Yce: /opt/yce/etc/devel7a_yce.conf
-- Retrieving file-transfer configurations...
     can support 'sftp'
     can support 'scp'
     can support 'ftp'
     can support 'tftp'
-- Mojo: /opt/yce/htdocs/angular/app/host.js
     mojo url set to 'https://devel7a.netyce.org:8080/'
     wiki url set to 'http://wiki.netyce.com/'
-- Yce_psmon: /opt/yce/etc/devel7a_psmon.conf
-- Crontab: /opt/yce/etc/devel7a_crontab.conf
-- Httpd: /opt/yce/etc/devel7a_httpd.conf
-- Mysql: /opt/yce/etc/devel7a_mysql.conf

   ::

-- mojo: 6348 10365 17550 17551 20759 20763 20764
     mojo hot-deploy on pid 10365
     running 'mojo': 6348 10365 17550 17551 20759 20763 20764
-- yce_xch: 10426
     stop: /opt/yce/system/init/yce_xch stop
     wait stop 'yce_xch':
     start: /opt/yce/system/init/yce_xch start
     wait start 'yce_xch': 23348
```

```
-- Completed
```

The yce_setup “regenerate” option is also available as a front-end function using the “Admin - System - System status” tool. The tool also allows the regenerate command to be executed on remote servers, provided of-course that the local setup included these servers.



Adding servers

After starting **yce_setup**, the user is presented with a concise overview of the servers in the NetYCE environment. The example shows two servers, the top server is the local server.

```
$ yce_setup7.pl
-- ----------------------------------------
-- Starting 'yce_setup' interactive
-- System release
   identified CentOS - 7.9.2009
   using setup for Redhat V7
-- Connected to database at '172.17.10.24' using version '10.2.36-MariaDB-log'

NOTE:
  When prompted for input help on the question is available by entering '?'.
  Incorrect responses result in a message on the expect input.
  Just hitting <enter> will accept the existing or default value '[...]'.
  The proces can be aborted at any prompt by entering 'quit'.

YCE servers currently in setup:
1) devel7a.netyce.org (*)
   | IPv4-address          | IPv6-address
   |  172.17.10.24         |  3001::24
2) devel7b.netyce.org
   | IPv4-address          | IPv6-address
   |  172.17.10.25         |  3001::25
  local server is marked with (*)
  Select the server-number to Edit/Remove, or 'A' to add, 'C' to continue: [C]
```

The local server reads the IP-addresses from the net_setup and can therefore not be changed. Choosing a remote server permits the server to be removed or its addresses to be updated. Servers are identified by a number as displayed in the overview (in the example, 1 and 2)

```
  Select the server-number to Edit/Remove, or 'A' to add, 'C' to continue:
[C] 1
    cannot edit or remove the local server.
```

```
    use 'net_setup.pl' to change its ip-address
  Select the server-number to Edit/Remove, or 'A' to add, 'C' to continue:
[C] 2
    Delete server 'devel7b' from setup?       [no]
    Enter IPv4-address for 'devel7b'          [172.17.10.25]
    Enter IPv6-address for 'devel7b'          [3001::25]
```

After choosing the 'A' option a new server can be added:

```
  Select the server-number to Edit/Remove, or 'A' to add, 'C' to continue:
[C] a
  Add new server
    Hostname for new server (without domain):  devel7c
    Domain name for new server (fqdn without hostname):  [netyce.org]
    IPv4-address for new server:              172.17.10.26
    IPv6-address for new server:              3001::26
YCE servers currently in setup:
1) devel7a.netyce.org (*)
   | IPv4-address          | IPv6-address
   |  172.17.10.24         |  3001::24
2) devel7b.netyce.org
   | IPv4-address          | IPv6-address
   |  172.17.10.25         |  3001::25
3) devel7c.netyce.org
   | IPv4-address          | IPv6-address
   |  172.17.10.26         |  3001::26
  local server is marked with (*)
  Select the server-number to Edit/Remove, or 'A' to add, 'C' to continue:
[C]
```

To change the name or domain of a remote server first remove it before re-adding it. To finish this dialog type 'C' for continue.

Assigning roles

A NetYCE server can have two roles, that of a Front-end server and that of a Database server, or both. As with the server setup, an overview of the current roles is displayed first.

```
YCE server roles:
1) devel7a.netyce.org (*)
   | Front-end      | SSL       | URL        | Backend
   |  yes           |  https    |  name      |  8080
   | Database       | Db-id
   |  yes           |  1
2) devel7b.netyce.org
   | Front-end      | SSL       | URL        | Backend
   |  yes           |  https    |  name      |  8080
   | Database       | Db-id
   |  yes           |  2
3) devel7c.netyce.org
   | Front-end      | SSL       | URL        | Backend
   |  yes           |  http     |  name      |  8080
   | Database       | Db-id
   |  no            |
  local server is marked with (*)
  Select the server-number to change, 'C' to continue: [1] 3
```

Select the number of the server to edit and a series of prompts will collect the required values. Remember that a ? will offer help.

Front-end role

The term “Front-end” as a role is a bit of a misnomer as this role will enable all NetYCE tasks but that of a database server. These tasks include the user Web GUI, the support of the NetYCE API's and the different type of jobs when communicating with the network devices. And these 'jobs' range from executing configuration changes, fetching and restoring configurations (NCCM), and performing Compliance assessments on them.

Every front-end needs at least one database connection which can be local or remote. A basic (evaluation) NetYCE environment has one (virtual) server which has both the front-end and the database role. More production oriented setups have two of these servers. When environments scale up, more servers can be added to separate tasks into user, Command jobs, NCCM and Compliance.

As many as seven front-end servers and two database servers can combined into a single environment. For more information see the reference guide on the connection matrix.

A sample session to select the options available for front-end servers:

```
  Select the server-number to change, 'C' to continue: [1]
    'devel7a' is (also) a Front-end server?   [yes]
    'devel7a' is DNS resolvable (y/n)?        [yes] ?

  NetYCE servers are expected to be registered in a DNS to resolve their
fqdn into an ip-address.
  However, for non-production environments this might not be the case. By
selecting non-DNS the
  system will be setup to function using ip-addresses only.
```

```
  When setting up a NetYCE server for 'ip-only', the user MUST access the
front-end GUI by
  entering the server IP-address in the browser, not its DNS name. This is a
technical restriction
  enforced by the browser to prevent 'cross-domain' security issues.

    'devel7a' is DNS resolvable (y/n)?        [yes]
    'devel7a' uses SSL (y/n)?                 [yes]
    'devel7a' uses SSL-hardening (y/n)?       [yes] ?

  SSL can be setup to accept older (weaker) levels of TLS (transport-layer-
security)
  as well as the newer (hardened) level of TLS1.2. When selecting 'SLL-
hardening'
  the http server will only accept connections supporting TLS1.2 and reject
older
  levels.

    'devel7a' uses SSL-hardening (y/n)?       [yes]
    'devel7a' portnumber of backend server?   [8080]
    'devel7a' is (also) a Database server?    [yes]
```

The selection for 'SSL' enables https in the communication with the users. This applies to the Web GUI channel and the backend channel. To use https SSL certificates need to be generated by a trusted Certificate Authorization (CA) and installed.

Usually a new server is installed and made operational with the SSL certificate to be installed later. Please consult the article on the SSL certificate tool.

The option for SSL hardening will result in only accepting connections supporting TLS1.2 and reject older TLS levels.

Database role

The second example illustrates that only two database servers can be defined. These will automatically be configured for master/master replication to allow redundancy, failover and load balancing.

Each database server must have its unique id, either '1' or '2'. Make sure the database ids assigned are consistently configured in all servers or replication setup will fail.

```
  Select the server-number to change, 'C' to continue: [1] 2
    'devel7b' is (also) a Front-end server?   [yes]
    'devel7b' is DNS resolvable (y/n)?        [yes]
    'devel7b' uses SSL (y/n)?                 [yes]
    'devel7b' uses SSL-hardening (y/n)?       [yes]
    'devel7b' portnumber of backend server?   [8080]
    'devel7b' is (also) a Database server?    [yes]
    'devel7b' uses database-id value (1/2)?   [2] ?
```

```
      NetYCE servers running a database must be assigned a unique database-
id to setup
      replication. As there are only two databases permitted, one server is
must use the
      id '1' whereas the other must use '2'.

    'devel7b' uses database-id value (1/2)?   [2]
YCE server roles:
```

```
  Select the server-number to change, 'C' to continue: [2] 3
    'devel7c' is (also) a Front-end server?   [yes]
    'devel7c' is DNS resolvable (y/n)?        [yes]
    'devel7c' uses SSL (y/n)?                 [no]
    'devel7c' portnumber of backend server?   [8080]
    'devel7c' cannot be a database, two servers max
YCE server roles:
```

Database mapping

Every NetYCE server needs at least one connection to a database. When two database servers are present, one will be assigned as the 'primary', the other as 'secondary'. With the replication in place, the primary database will be used by the server when it is available. The moment the primary connection fails, all database requests will switch to the secondary. When the primary becomes active again, the databases will re-synchronize and when completed the connections switch back to the primary database.

It is customary to use the local database as the primary database if available. So in a standard two-server setup each server is the failover/standby database of the other. Additional servers without a database must be assigned a primary and secondary based on their proximity for best performance.

In situations where the replication is prone to fail frequently due to unstable connections between the databases, it is advisable to select one database as the primary for *all* servers. This will result in the secondary becoming a 'standby' only ensuring that the primary is leading.

```
YCE server database mapping:
1) devel7a.netyce.org (*)
   | Db-id     | Primary          |  Secondary
   |  1        |  devel7a (*)     |  devel7b
2) devel7b.netyce.org
   | Db-id     | Primary          |  Secondary
   |  2        |  devel7b         |  devel7a (*)
3) devel7c.netyce.org
   | Db-id     | Primary          |  Secondary
   |           |  devel7a (*)     |  devel7b
  local server is marked with (*)
  Select the server-number to change, 'C' to continue: [1]
```

To assign a database server select its number and you are prompted to answer if the first of the database servers will be its primary. Answer 'yes' and this databse becomes the primary, the other the secondary. Answer no and the assignment reverses.

```
  Select the server-number to change, 'C' to continue: [1] 3
    'devel7c' connects to 'devel7a' as primary database? [yes] no
YCE server database mapping:
1) devel7a.netyce.org (*)
   | Db-id     | Primary           |  Secondary
   |  1        |  devel7a (*)      |  devel7b
2) devel7b.netyce.org
   | Db-id     | Primary           |  Secondary
   |  2        |  devel7b          |  devel7a (*)
3) devel7c.netyce.org
   | Db-id     | Primary           |  Secondary
   |           |  devel7b          |  devel7a (*)
  local server is marked with (*)
  Select the server-number to change, 'C' to continue: [2]
```

Login setup

The NetYCE web GUI uses session cookies to keep you signed at all servers in an environment for a limited duration. To allow multiple servers to use the session cookies as a means for single-sign-on (SSO) the domain name used in the cookie must match.

The session cookies are stored in memory by the browser. While the browser was not quit and the cookie is valid, no logins are required for that user. Switching user names on the same browser will replace the cookie.

```
Login setup:
    Domain name for login (single-sign-on cookie)? [netyce.org] ?

  NetYCE uses a session cookie to allow single-sign-on for the servers
  that share the domain-name (or some trailing sections) specified here.
  The default is the domain name of this server.

    Domain name for login (single-sign-on cookie)? [netyce.org]
    Hours until Login session expiry (single-sign-on cookie)? [12] ?

  The single-sign-on session cookie will be valid for the duration specified
  here. The session cookie will be lost should the browser be restarted.

    Hours until Login session expiry (single-sign-on cookie)? [12]
Login setup:
  | Single-sign-on domain           | Expire (hrs)
  |  netyce.org
```

If all servers use the exact same DNS domain the SSO domain is the same. But if different DNS domains are used, the SSO domain should be modified to use the common part of the DNS domain

Example:

```
server fqdn                DNS domain         SSO domain
-----------                ----------         ----------
```

```
netyce01.ams.acme.com     ams.acme.com       acme.com
netyce02.ldn.acme.com     ldn.acme.com       acme.com
```

Only if all servers use the same SSO domain will the cookies be accepted and validated.

Wiki setup

The NetYCE public wiki is the default target for the 'Help' function in the GUI. As this requires Internet access which might not be permitted, the NetYCE wiki can also be installed locally on any of the NetYCE servers.

The procedure is described in the WIKI installation page. The corresponding configuration for the hosting server and the redirection must be entered here.

```
Wiki setup:
    'devel7a' will use the NetYCE public Wiki server? [yes] ?

  By default the public NetYCE Wiki server will be assigned to the 'Help'
button of
  the menu. When the internet is not accessible from the browser, the
administrator
  can install a local copy of the NetYCE Wiki on this server.
  The installation instructions located at:
  'https://wiki.netyce.com/doku.php/maintenance:downloads:wiki_updates'

    'devel7a' will use the NetYCE public Wiki server? [yes] n
    The (alias) name of the local Wiki server? [wiki] netyce-wiki
    the domain name of the local Wiki server? [netyce.org]
Wiki setup:
  Local    Protocol Hostname            Domain
Ip-address
  yes      http     netyce-wiki         netyce.org
  Is this Wiki setup correct?                [yes]
```

Config generation and activation

After all sections are completed, a summary of the new setup is shown along with the prompt to activate it. Activation will perform many steps that assesses the server capabilities and resources, then generating the different configuration files for tis components and copying to the target locations. Finally, many of the background processes (daemons) are restarted to load the new configurations.

```
New setup:
devel7a.netyce.org (*)
  | IP-address  | IPv4            | IPv6
  |  users      |  172.17.10.24   |  3001::24
  | Database    | Primary         | Secondary
  |  id=1       |  devel7a (*)    |  devel7b
devel7b.netyce.org
  | IP-address  | IPv4            | IPv6
  |  users      |  172.17.10.25   |  3001::25
  | Database    | Primary         | Secondary
  |  id=2       |  devel7b        |  devel7a (*)
devel7c.netyce.org
  | IP-address  | IPv4            | IPv6
  |  users      |  172.17.10.26   |  3001::26
  | Database    | Primary         | Secondary
  |  -          |  devel7a (*)    |  devel7b
  local server is marked with (*)

-- Create and activate configuration files
   Create configuration for local server 'devel7a'? [yes]
```

When invoking the `yce_setup.pl` script with the `-r` option to “regenerate”, the config generation and restarting is the only action it performs.

```
   Create configuration for local server 'devel7a'? [yes]
-- Creating configs for server 'devel7a'
-- Yce: /opt/yce/etc/devel7a_yce.conf
-- Retrieving file-transfer configurations...
     can support 'sftp'
     can support 'scp'
     can support 'ftp'
     can support 'tftp'
-- Mojo: /opt/yce/htdocs/angular/app/host.js
     mojo url set to 'https://devel7a.netyce.org:8080/'
     wiki url set to 'http://wiki.netyce.com/'
-- Yce_psmon: /opt/yce/etc/devel7a_psmon.conf
-- Crontab: /opt/yce/etc/devel7a_crontab.conf
-- Httpd: /opt/yce/etc/devel7a_httpd.conf
-- Mysql: /opt/yce/etc/devel7a_mysql.conf
     mysql version is '10.2.36'
     mysql key_buffer set to '376M'
     mysql tmpdir set to '/var/tmp'
-- SSL certificate found. Run 'mk_ssl_cert.pl' to re-create when desired
-- Updating 'devel7a' menu-tree (C)
     Creating menus for the role(s): "frontend","database"
     Renewed the menu tree using the default
     Updating 'devel7a' encryption keys
     Updating scenario syntax highlighting file
-- Renewing NMS table permissions
-- Checking database replication
     replication local: 172.17.10.24, remote: 172.17.10.25
```

```
-- Updating config-sync setup
     located '55' config-files in '6' groups
     updated config_sync.conf has '28' entries
-- Relaunching NetYCE daemons...
-- yce_psmon: 28227
     stop: /usr/bin/sudo /usr/bin/systemctl stop yce_psmon.service
     wait stop 'yce_psmon':
     start: /usr/bin/sudo /usr/bin/systemctl start yce_psmon.service
     wait start 'yce_psmon': 10766
-- yce_netmon: 2220
     stop: /opt/yce/system/init/yce_netmon stop
     wait stop 'yce_netmon':
     start: /opt/yce/system/init/yce_netmon start
     wait start 'yce_netmon': 10846
-- yce_cramer:
     # disabled
-- yce_tftpd: 28351
     stop: /usr/bin/sudo /opt/yce/system/init/yce_tftpd stop
     wait stop 'yce_tftpd':
     start: /usr/bin/sudo /opt/yce/system/init/yce_tftpd start
     wait start 'yce_tftpd': 10890
-- yce_skulker: 28374
     stop: /opt/yce/system/init/yce_skulker stop
     wait stop 'yce_skulker': 28374
     wait stop 'yce_skulker':
     start: /opt/yce/system/init/yce_skulker start
     wait start 'yce_skulker': 10913
-- yce_sched: 28406
     stop: /opt/yce/system/init/yce_sched stop
     wait stop 'yce_sched':
     start: /opt/yce/system/init/yce_sched start
     wait start 'yce_sched': 10943
-- yce_nccmd: 28430
     stop: /opt/yce/system/init/yce_nccmd stop
     wait stop 'yce_nccmd':
     start: /opt/yce/system/init/yce_nccmd start
     wait start 'yce_nccmd': 10967
-- yce_ibd:
     # disabled
-- morbo:
     # disabled
-- mojo: 5798 8363 8364 28440 28472 28473 28475
     mojo hot-deploy on pid 28440
     running 'mojo': 5798 8363 8364 28440 28472 28473 28475
-- yce_xch: 28500
     stop: /opt/yce/system/init/yce_xch stop
     wait stop 'yce_xch':
     start: /opt/yce/system/init/yce_xch start
     wait start 'yce_xch': 11039
-- Completed
```