Table of Contents

Compliance Overview

> Note: The “Compliance” functions are available from version 7.2.0 and onwards.

Compliance refers to the process of validating that the configuration of network devices meet your criteria. To achieve this goal the current configuration is needed AND the set of criteria that apply to it.

NCCM

The first is realized by using the NetYCE NCCM function (Network Configuration and Change Managment). By retrieving and storing the configuration each time it is changed, the NCCM is the source for the Compliance. The NCCM function in itself is to serve as a repository for all device configurations that can be used for backups and restore, but also can report on the configuration changes over time. When needed, the configuration for any date within its storage limits can be retrieved and compared.

The NCCM can therefore be used with and without the use of Compliancy. But for Compliancy the NCCM needs to be in operation. The NCCM can retrieve the configuration from the device when:

- A NetYCE job changes the configuration. Every job will retrieve the configuration before and after the change. Both configurations will be incorporated in the NCCM history of that device.
- The device sends a syslog message to the NetYCE server to inform of a configuration change. The configuration is then retrieved and appended to the NCCM history.
- The device is scheduled to have its configuration periodically fetched by the NCCM poller.

In each of these cases the NCCM can detect a configuration change which will trigger the Compliance test for the device. If no configuration changes were detected, the compliance will not be triggered.

When a device signals its configuration has changed The NCCM will not immediately be triggered to retrieve its configuration. Assuming an operator using the CLI on the device made this change, we postpone scheduling the configuration retrieval by 10 minutes to allow the operator to finish his session. Then the retrieval will be scheduled within the next 5 minutes to be fetched by the NCCM. However, if the NCCM is too busy handling all requests within that 5 minute batch, the request will be re-scheduled for the next batch. And, when the NCCM completes, the Compliance policies will be scheduled in similar fashion. Al in all, allow for 15-20 minutes for the compliance results. If the configuration change was initiated by a NetYCE job, only the Compliance Policy delay should be accounted for.

Please consult the Wiki articles on NCCM on how to set-up the polling or receiving syslog events.

Policies

The set of criteria to validate a given configuration is defined in Compliance **Policies**. Each Compliance policy is associated with a number of Node-groups so that several policies can be triggered when a new configuration needs to be validated.

The idea is that a Compliance Policy is created in such a way that it tests a criterium in a generic

sense. A policy can be created independent of vendor, model and software version. The Compliance Policy should therefore test, well, a design or company “policy”. By creating a Compliance Policy for each “policy” the resulting set allows for quick updates on changed designs, new hardware or stricter guidelines as each deals with just one aspect of the configurations implementing it.

Therefore, every Compliance Policy consists of a number of **Rules**. A Rule is vendor specific which allows the Policy to be applied to all vendors involved in the design. Rules not matching the devices vendor-type will be ignored. Each Rule deals with a specific section of the configuration (or all of it) by specifying the configuration block-start and block-end identifying markers. This way one Rule may validate some aspect of all Vlan interfaces in a Cisco_IOS configuration while another Rule may validate the same aspect of the Vlan interfaces of an HP_C7 configuration.

Then, in its turn, each Rule will consist of one or more **Conditions**. A Condition defines what the configuration block should or should not contain. The various Conditions of a Rule are combined in the rule logic. This logic is applied to find the outcome of the Rule test.

For example “*(Condition-A OR Condition-B) AND Condition-C*”, but also “*IF Condition-A THEN Condition-B AND Condition-C*”. The second example shows how a Rule can be made conditional - if condition 'A' matches, only then will conditions 'B' and 'C' be validated, otherwise the rule is ignored.

The result of each Rule is a “compliant” or a “not-compliant”. If a Policy executes several Rules for the same configuration (same vendor) the results are combined where a single “not-compliant” will make the Policy fail. As each Rule will have a **Severity**, the most severe “not-compliant” Rule will determine the Policy's reported severity.

Notifications can be configured per Policy when it is executed. These notifications can take several forms (syslog, trap, email, rest-api) and can be issued on state changes or every time as desired.

A note about censored content: we filter away passwords and other sensitive data in order to prevent them from showing up in logs. If you want to disable this feature for compliance, look up the tweak 'Cmpl_censor_config' in the Nccm Lookup and set it to 0.

Dashboard

A dashboard is provided to give a one-glance overview of the compliance status of your network. In two bar graphs the devices compliance status and the compliance policies status are shown. The top bar shows the number (or percentage) of devices that are in compliance or not. Of those that are not, their severity is color coded. The bottom bar represents the various policies and their severities.

Reporting

Reports on Compliance can be defined and saved for reuse either publicly or personal. Reports are either based on Nodes (devices) or Policies, each with their specific set of filters.

Reports display all policies or nodes that match your queries. Note that any node that has no policy, or any policy that has no node, is automatically non-compliant. Also a policy that has never been run is non-compliant, same for a node.

Whether you selected nodes or policies, when you select an entry you'll get a list of all its compliance checks. For policies you'll get a list of its nodes, for nodes you'll get a list of its policies. Whether they

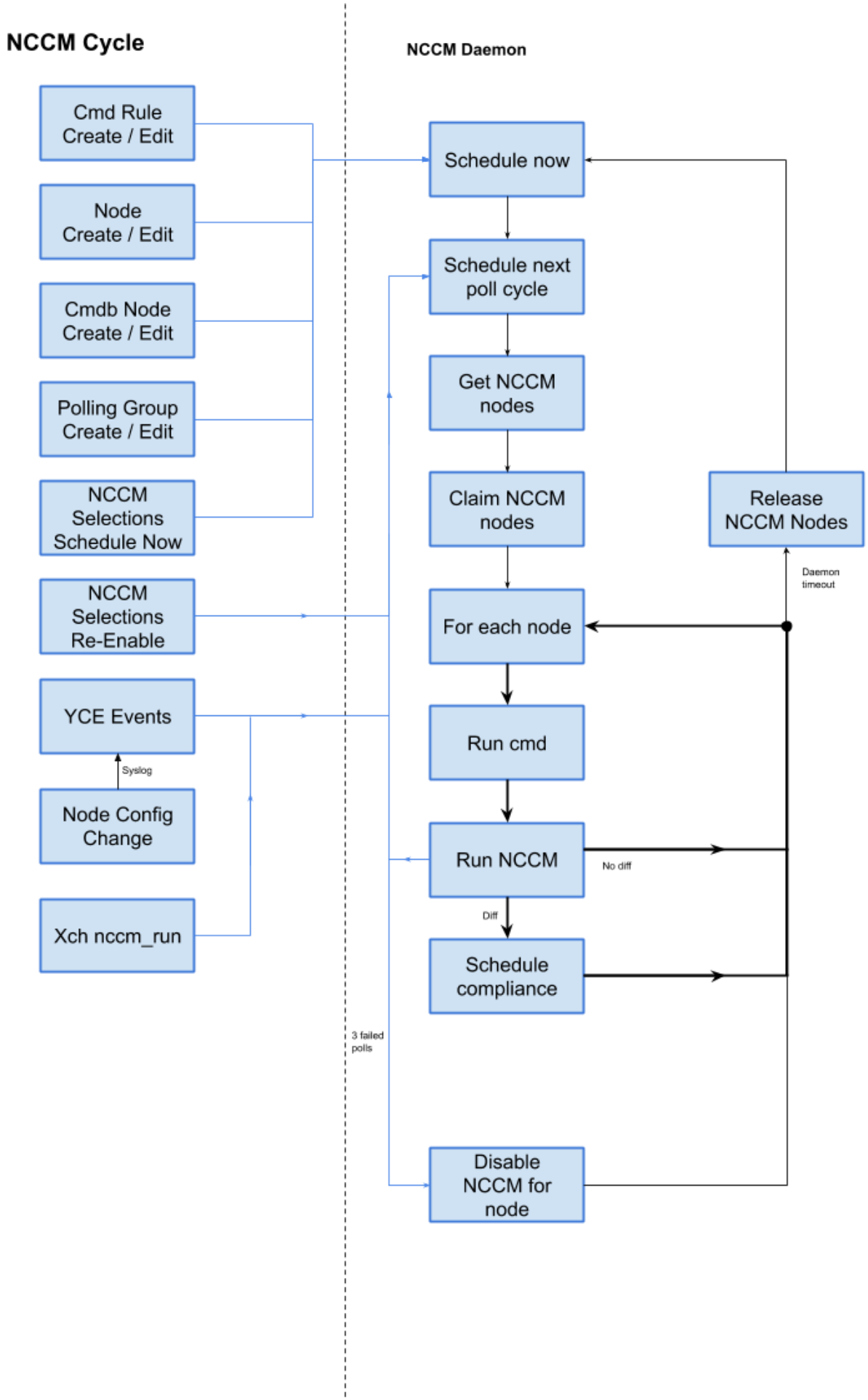
are compliant, and when their last check has been. You can also see the last time it changed compliance status. When you click on one of the entries you can see its compliance report in a new window. Reports are also downloadable.

Licensing

NetYCE uses Compliance licences that are assigned to individual devices. New devices are automatically assigned a Compliance license if available. The “Licensed nodes” compliance page allows the user to remove and re-assign the compliance licences to the devices of choice. Unlicensed nodes will not be checked for compliance. If they were licensed in the past, their results will not show up in reports or the dashboard.

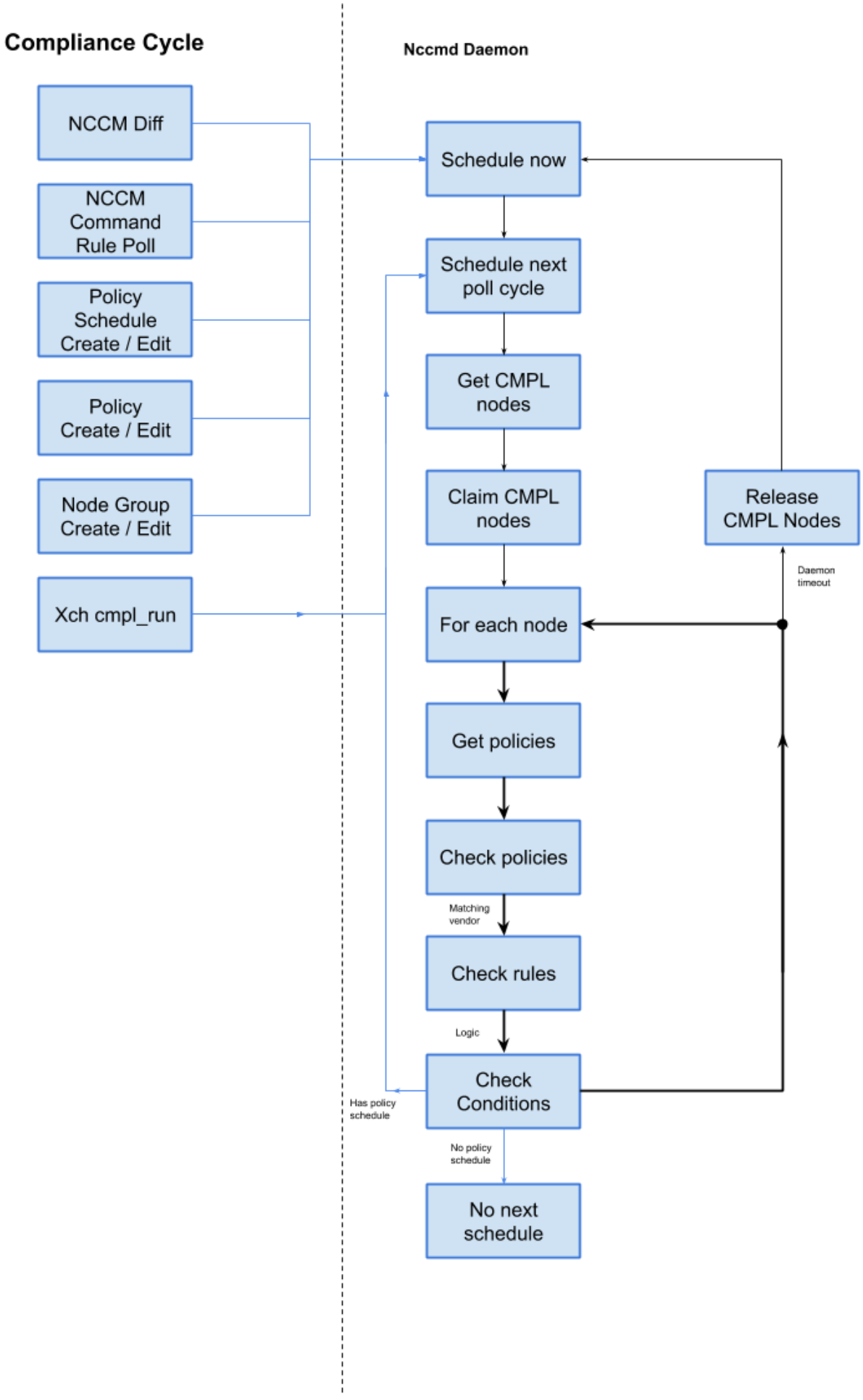
NCCM Daemon Cycle

The following schema shows a global overview of how the daemon works for the nccm. The black arrows show the process that the daemon goes through, and the blue arrows show trigger from (outside) processes outside of the main loop. Left are the processes outside of the daemon, and right happens inside the daemon.


NCCM Cycle
NCCM Daemon
Cmd Rule Create / Edit
Node Create / Edit
Cmdb Node Create / Edit
Polling Group Create / Edit
NCCM Selections Schedule Now
NCCM Selections Re-Enable
YCE Events
Syslog
Node Config Change
Xch nccm_run
Schedule now
Schedule next poll cycle
Get NCCM nodes
Claim NCCM nodes
For each node
Run cmd
Run NCCM
No diff
Diff
Schedule compliance
3 failed polls
Disable NCCM for node
Release NCCM Nodes
Daemon timeout

Compliance Daemon Cycle

The following schema shows a global overview of how the daemon works for compliance. The black arrows show the process that the daemon goes through, and the blue arrows show trigger from (outside) processes outside of the main loop. Left are the processes outside of the daemon, and right happens inside the daemon.


Compliance Cycle
Nccmd Daemon
NCCM Diff
NCCM Command Rule Poll
Policy Schedule Create / Edit
Policy Create / Edit
Node Group Create / Edit
Xch cmpl_run
Schedule now
Schedule next poll cycle
Get CMPL nodes
Claim CMPL nodes
Release CMPL Nodes
Daemon timeout
For each node
Get policies
Check policies
Matching vendor
Check rules
Logic
Check Conditions
Has policy schedule
No policy schedule
No next schedule