NETMOD Working Group
Internet-Draft
Intended status: Informational
Expires: July 7, 2016

K. Watsen
Juniper Networks
T. Nadeau
Brocade Networks

January 4, 2016

Terminology and Requirements for Enhanced Operational State Visibility and Control
draft-ietf-netmod-opstate-reqs-02

Abstract

This document discusses the difference between intended configuration and applied configuration of a device and how intended and applied configuration relate to the operational state of a device. The document defines the necessary terminology and identifies requirements enabling visibility into the difference of intended configuration and applied configuration.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 7, 2016.

Table of Contents

1. Introduction

This document discusses the difference between intended configuration and applied configuration of a device and how intended and applied configuration relate to the operational state of a device. The document defines the necessary terminology and identifies requirements enabling visibility into the difference of intended configuration and applied configuration.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

The term "client" is used throughout this document to refer to what is many times known as the "application" or "network management system". This definition is intended to be consistent with the term "client" defined in [RFC6241], Section 1.1, but independent of any association to a particular protocol.

The term "server" is used throughout this document to refer to what is many times known as the "device", "system", or "network element". This definition is intended to be consistent with the term "server" defined in [RFC6241], Section 1.1, but independent of any association to a particular protocol.

This document defines the following terms:

Applied Configuration: This data represents the configuration state that the server is actually in. That is, the configuration state which is currently being used by server components (e.g., control plane daemons, operating system kernels, line cards). With respect to NETCONF architecture, the applied configuration resides in the "system software component" box listed on page 15 of [RFC6244]

NOTE: The server's ability to report applied configuration accurately may be limited in some cases, such as when the configuration goes through an intermediate layer without an ability to inspect the lower layer.

Asynchronous Configuration Operation: A configuration request to update the running configuration of a server that is applied asynchronously with respect to the client request. The server MUST update its intended configuration (see term) before replying to the client indicating whether the request will be processed. This reply to the client only indicates whether there are any errors in the original request. The server's applied configuration state (see term) is updated after the configuration change has been fully effected to all impacted components in the server. Once applied, there MUST be a mechanism for the client to determine when the request has completed processing and whether the intended config is now fully effective or there are any errors from applying the configuration change, which could be from an asynchronous notification or via a client operation.

Derived State: This data represents information which is generated as part of the server's own interactions. For example, derived state may consist of the results of protocol interactions (the negotiated duplex state of an Ethernet link), statistics (such as message queue depth), or counters (such as packet input or output bytes).

Intended Configuration: This data represents the configuration state that the network operator intends the server to be in, and that has been accepted by the server as valid configuration. With respect to NETCONF architecture, the intended configuration is captured by the "config database" box listed on page 15 of [RFC6244]

Operational State: Operational State is the current state of the system as known to the various components of the system (e.g., control plane daemons, operating system kernels, line cards). The operational state includes both applied configuration and derived state.

Synchronous Configuration Operation: A configuration request to update the running configuration of a server that is applied synchronously with respect to the client request (i.e. a blocking call). The server MUST fully attempt to apply the configuration change to all impacted components in the server, updating both the server's intended and applied configuration (see terms), before replying to the client. The reply to the client indicates whether there are any errors in the request or errors from applying the configuration change.

3. Backwards Compatibility

Any solution satisfying the requirements specified in this document MUST ensure backwards compatibility with regards to existing deployments. Specifically, it MUST be possible to upgrade a server to one that supports the solution without breaking existing/legacy clients. Likewise, it MUST be possible for a client that has been coded to support the solution to interoperate appropriately with existing/legacy servers.

4. Requirements

1. Ability to interact with both intended and applied configuration

   A. The ability to ask the operational components of a server (e.g., line cards) for the configuration that they are currently using. This is the applied configuration (see term).

   B. Applied configuration is read-only

   C. The data model for the applied configuration is the same as the data model for the intended configuration (same leaves)

   D. When a configuration change for any intended configuration node has been successfully applied to the server (e.g. not failed, nor deferred due to absent hardware) then the existence and value of the corresponding applied configuration node must match the intended configuration node.

2. Support for both synchronous and asynchronous configuration operations (see terms)

   A. A server may support only synchronous configuration operations, or only asynchronous configuration operations, or both synchronous and asynchronous configuration operations on a client-specified per-operation basis.

B. Servers that support asynchronous configuration operations MAY also provide a verify operation that a client can request from the server to return information regarding the difference between the intended and applied configurations.

C. The configuration protocol MUST specify how configuration errors are handled. Errors MAY be handled by semantics similar to NETCONF's error-options for the <edit-config> operation (stop-on-error, continue-on-error, rollback-on-error), as described in Section 7.2 in [RFC6241], but extended to incorporate both the intended and applied configurations. Support for "rollback on error" semantics SHOULD be provided.

3. Separation of the applied configuration and derived state aspects of operational state; ability to retrieve them independently and together

A. Be able to retrieve only the applied configuration aspects of operational state

B. Be able to retrieve only the derived state aspects of operational state

C. Be able to retrieve both the applied configuration and derived state aspects of operational state together

4. Ability to relate configuration with its corresponding operational state

A. Ability to map intended config nodes to corresponding applied config nodes

B. Ability to map intended config nodes to associated derived state nodes

C. The mappings needs to be programmatically consumable

5. Security Considerations

It is understood that the intended and applied configurations will differ while synchronization is in progress. During the synchronization process, the server will be in an inconsistent state from the client's perspective. Implementations need to take care to ensure that this inconsistency minimizes gaps in the application of security policy (e.g., replacing a firewall policy in a single step). Implementations additionally need to ensure that any gaps in security

policies or not dependent on external input that an attacker might be able to control or prevent access to.

6. IANA Considerations

None

7. Acknowledgements

The authors would like to thank the following for contributing to this document (in alphabetic order): Acee Lindem, Andy Bierman, Anees Shaikh, Benoit Claise, Carl Moberg, Dan Romascanu, Dean Bogdanovic, Gert Grammel, Jonathan Hansford, Juergen Schoenwaelder, Lou Berger, Mahesh Jethanandani, Martin Bjorklund, Phil Shafer, Randy Presuhn, Rob Shakir, Robert Wilton, Sterne, Jason.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

8.2. Informative References

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <http://www.rfc-editor.org/info/rfc6241>.

[RFC6244] Shafer, P., "An Architecture for Network Management Using NETCONF and YANG", RFC 6244, DOI 10.17487/RFC6244, June 2011, <http://www.rfc-editor.org/info/rfc6244>.

Authors' Addresses

Kent Watsen
Juniper Networks

EMail: kwatsen@juniper.net

Thomas Nadeau
Brocade Networks

EMail: tnadeau@lucidvision.com