JichenDai_CS524_HW#5

1. Answer:

Motivation: The objective of the framework is to describe the execution of policy-based control over the QoS admission control decisions, with the primary focus on the RSVP protocol as an example

Network providers wanted to have a mechanism that would enable granting a resource based on a set of policy rules. The decision on whether to grant the resource takes into account information about the user, the requested service, and the network itself. Employing SNMP for this purpose was not straightforward, and so the IETF developed a new protocol, for communications between the network element and the *Policy Decision Point* (*PDP*)—where the policy-based decisions were made. The protocol is called *Common Open Policy Service* (*COPS*)

goals: The goals of the framework are support for pre-emption, various policy styles, monitoring, and accounting.

Cited textbook page 264 and 317

2. Answer: Something intrinsically new about COPS—as compared with SNMP or CMIP—is that COPS employs a *stateful* client–server model, which is different from that of the remote procedure call. As in any client–server model, the PEP (client) sends *requests* to the remote PDP (server), and the PDP responds with the *decisions*. But all the requests from the client PEP are *installed* and remembered by the remote PDP until they are explicitly deleted by the PEP. The decisions can come in the form of a series of notifications to a single request. This, in fact, introduces a new behavior: two identical requests may result in different responses because the states of the system when the first and second of these requests arrive may be different—depending on which states had been installed. Another stateful feature of COPS is that PDP may "push" the configuration information to the client and later remove it

Cited textbook page 319

3. Answer:

a. The SNMP transactional model and the protocol constraints make it more complex to implement MIBs. A logical operation on a MIB can turn into a sequence of SNMP interactions where the implementation has to maintain state until the operation is complete, or until a failure has been determined. In case of a failure, a robust implementation must be smart enough to roll the device back into a consistent state.

b. One part of the problem is that it is not easy to identify configuration objects. Another part of the problem is that the naming system is very specific and physical device re-configurations can thus break the capability to play back a previous configuration.

c. Operator requiremnets:

1. Ease of use is a key requirement for any network management technology from the operators point of view.

2. It is necessary to make a clear distinction between configuration data, data that describes operational state and statistics. Some devices make it very hard to determine which parameters were administratively configured and which were obtained via other mechanisms such as routing protocols.

3. It is required to be able to fetch separately configuration data, operational state data, and statistics from devices, and to be able to compare these between devices.

4. It is necessary to enable operators to concentrate on the configuration of the network as a whole rather than individual devices.

5. Support for configuration transactions across a number of devices would significantly simplify network configuration management.

6. Given configuration A and configuration B, it should be possible to generate the operations necessary to get from A to B with minimal state changes and effects on network and systems. It is important to minimize the impact caused by configuration changes.

7. A mechanism to dump and restore configurations is a primitive operation needed by operators. Standards for pulling and pushing configurations from/to devices are desirable.

8. It must be easy to do consistency checks of configurations over time and between the ends of a link in order to determine the changes between two configurations and whether those configurations are consistent.

9. Network wide configurations are typically stored in central master databases and transformed into formats that can be pushed to devices, either by generating sequences of CLI commands or complete configuration files that are pushed to devices. There is no common database schema for network configuration, although the models used by various operators are probably very similar. It is desirable to extract, document, and standardize the common parts of these network wide configuration database schemas.

10. It is highly desirable that text processing tools such as diff, and version management tools such as RCS or CVS, can be used to process configurations, which implies that devices should not arbitrarily reorder data such as access control lists.

11. The granularity of access control needed on management interfaces needs to match operational needs. Typical requirements are a role-based access control model and the

principle of least privilege, where a user can be given only the minimum access necessary to perform a required task.

12. It must be possible to do consistency checks of access control lists across devices.

13. It is important to distinguish between the distribution of configurations and the activation of a certain configuration. Devices should be able to hold multiple configurations.

14. SNMP access control is data-oriented, while CLI access control is usually command (task) oriented. Depending on the management function, sometimes data-oriented or task-oriented access control makes more sense. As such, it is a requirement to support both data-oriented and task-oriented access control.

Cited RFC 3535

4. Answer: No.

5. Answer: **YANG Data Model** is the de-facto modeling language for NETCONF.

It is specified in **RFC 6020**

YIN is the XML-based representation of YANG.

Cited textbook page 323

6. Answer: There are seven steps:

1. Defining the workload
2. Provisioning cloud resources
3. Establishing a connectivity bridge
4. Deploying the workload
5. Ensuring seamless two-way access
6. Testing and validating
7. Discontinuing the old service

Cited www.interxion.com/whitepapers/practical-guide-to-cloud-onboarding#pardot

7. Answer:

a. Three actors: Cloud service provider, the Cloud service developer, and the Cloud service consumer.

b. Offering is augmented with the constrains, costs, policies, and SLA.

Cited textbook page 269

8. Answer: Communications among daemons are carried out via the ***Advanced Message Queuing Protocol*** **(*AMQP*)**.

Cited textbook page 280