WHITE PAPER

Integrating the PSM in Enterprise Operations: Strategy and Benefits

PENSANDO

Contents

Pensando Policy and Services Manager Overview

This document describes the features of the Pensando Policy and Services Manager (PSM) that offer value and insights into the operation of enterprise data centers.

The Pensando **Distributed Services Platform** is built around the Distributed Services Card (DSC): a PCIe adapter that provides services and network I/O for the host. The DSC provides services that would otherwise be implemented either in software on the host CPU, or in appliances within the network. The Policy and Services Manager (PSM) delivers network, security, and telemetry policy to Pensando DSCs at scale, thus offering a single point of management and monitoring for the distributed services running on the DSCs. Moreover, the PSM offers lifecycle management of DSCs.

For fault tolerance and scale, the PSM runs as a quorum-based cluster of three VMs that execute on separate servers.

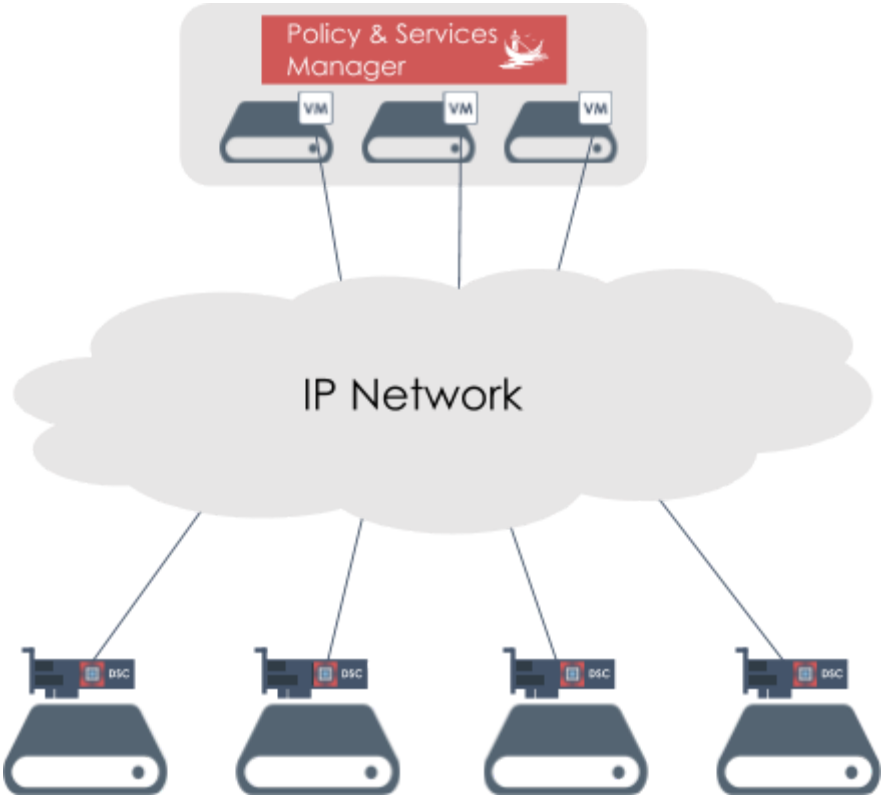

Figure 1. PSM and DSCs

The PSM is accessible through both a web browser-based Graphical User Interface (GUI), and a secure RESTful API.

All inter-cluster communication (PSM's REST API, and PSM-to-DSC communication via gRPC) is encrypted to ensure security. The PSM is intent-based: it does not require that policies are propagated and accepted at the same time by all the DSCs, as in a transactional model, but instead continuously works to reconcile the policies on the DSCs with the intent specified on the PSM.

Policies are user-configurable and intent-based. Labels can be associated to groups of objects and can be used within policies, making "administration at scale" simple and extremely effective, as a single policy can be applied to a potentially large number of objects with the same label.

This document focuses first on features related to distributed services and applications running in the data center, and then those related to the Pensando platform itself.

For detailed information on managing the PSM, including installation instructions and a description of its complete feature set, refer to the *Pensando PSM Enterprise User Guide*.

Distributed Services and Applications

All services running on the Pensando platform are designed with data center operations in mind, and thus can be monitored via the PSM or through third party tools. The PSM also provides visibility into applications running on DSC-equipped hosts and the traffic they generate.

Flow export

DSCs can collect statistics on any network flows that transit the DSC. An administrator can use the PSM to set policies that specify which flows should be monitored. Figure 2 illustrates that each flow is identified through a 5-tuple: source and destination IP address, transport protocol, source and destination transport port.

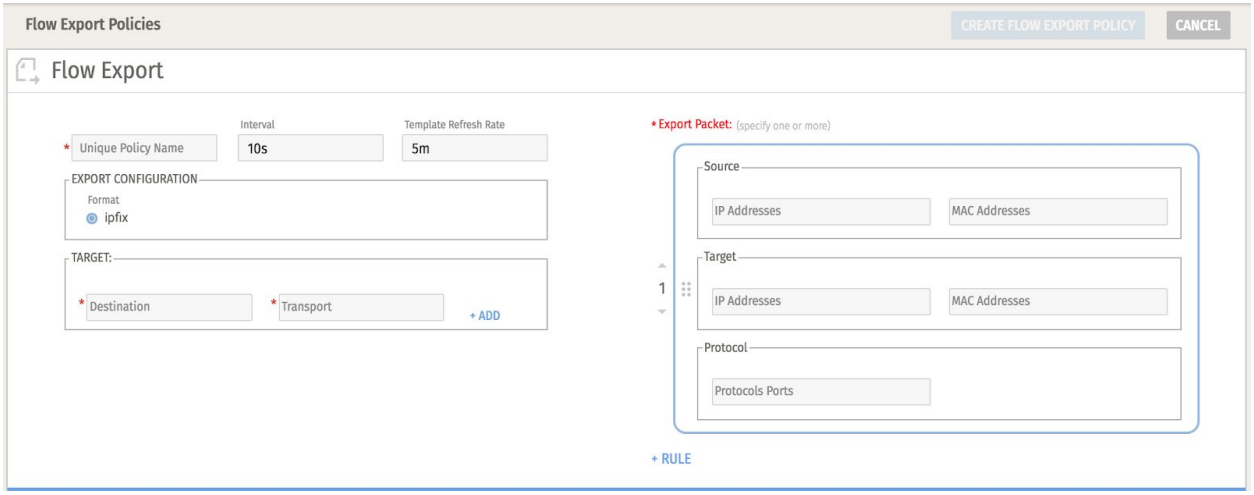

Figure 2. Configuring a Flow Export policy

The PSM administrator can then specify the collector (or target) that should receive the flow information and the transport that should be used (e.g. "udp/2055"). The flow information is sent in IPFIX format.

The PSM administrator does not have to specify which exact DSCs should be configured for flow monitoring and exporting. The Pensando platform ensures that the DSCs subscribe to all collection and export policies. Those DSCs that are involved in the flow will then collect and export any relevant information. If the workload generating a flow is moved to a different DSC (e.g. a VM is moved through vMotion to a different server), the platform continues to seamlessly monitor and collect flow information without requiring administrator intervention.

Metrics

Each DSC collects a large set of metrics ("Fields" in Figure 3) organized by various categories ("Measurement" in Figure 3).

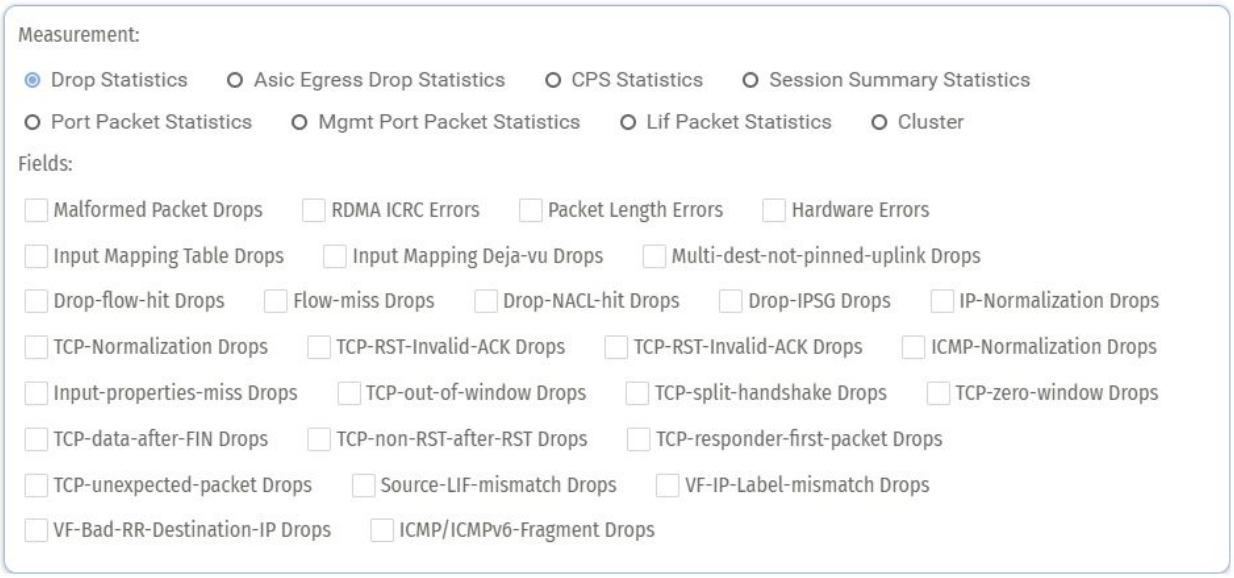

Figure 3. Selecting metrics

A subset of these metrics can be selected to create custom graphs on the PSM such as the one shown in Figure 4. Graphs can be saved by name, showing the latest metric values, hence offering a dashboard of the health and performance of the hosts, applications, and the platform itself.

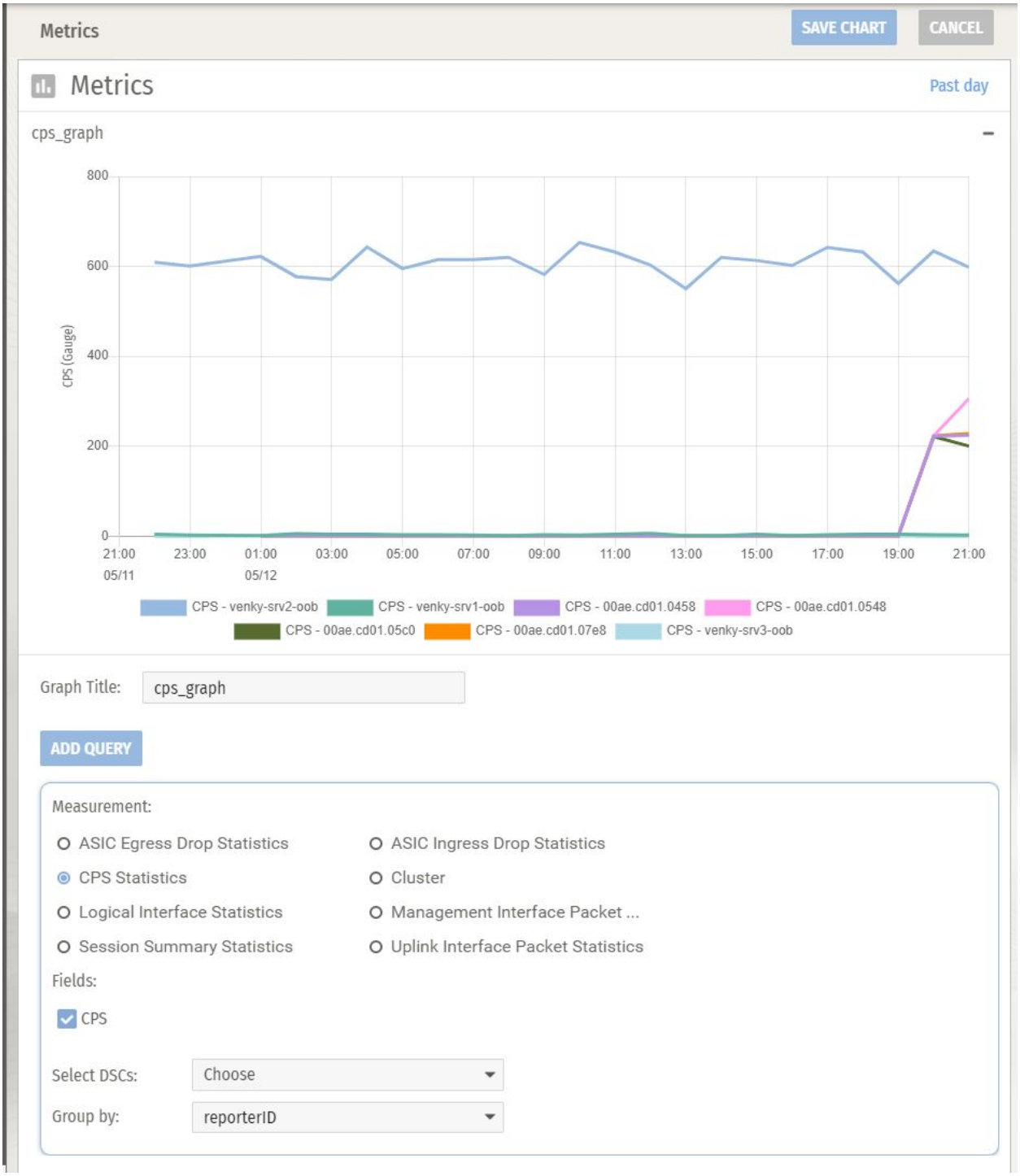

Figure 4. Creating a PSM chart

Administrators can use this powerful distributed monitoring capability to constantly observe the state of the network, identify potential performance bottlenecks, and remediate issues before they impact applications and services.

Mirror sessions

The Pensando Distributed Services Platform has the unique ability to mirror bi-directional traffic generated or received by any application or workload hosted on servers equipped with a DSC. A DSC can make a copy of each packet conforming to a given mirroring policy and send (a portion of) the packets to a collector using ERSPAN (Encapsulated Remote Switched Port Analyzer) encapsulation.

The administrator can choose whether to send all traffic that is transiting one DSC interface (called *interface-based mirroring* or *bidirectional ERSPAN*[1]), or only packets that match mirroring policies configured on the PSM. As shown Figure 5, mirroring policies can have flow-level granularity identified by a 5-tuple: source and destination IP address, transport protocol, source and destination transport port.

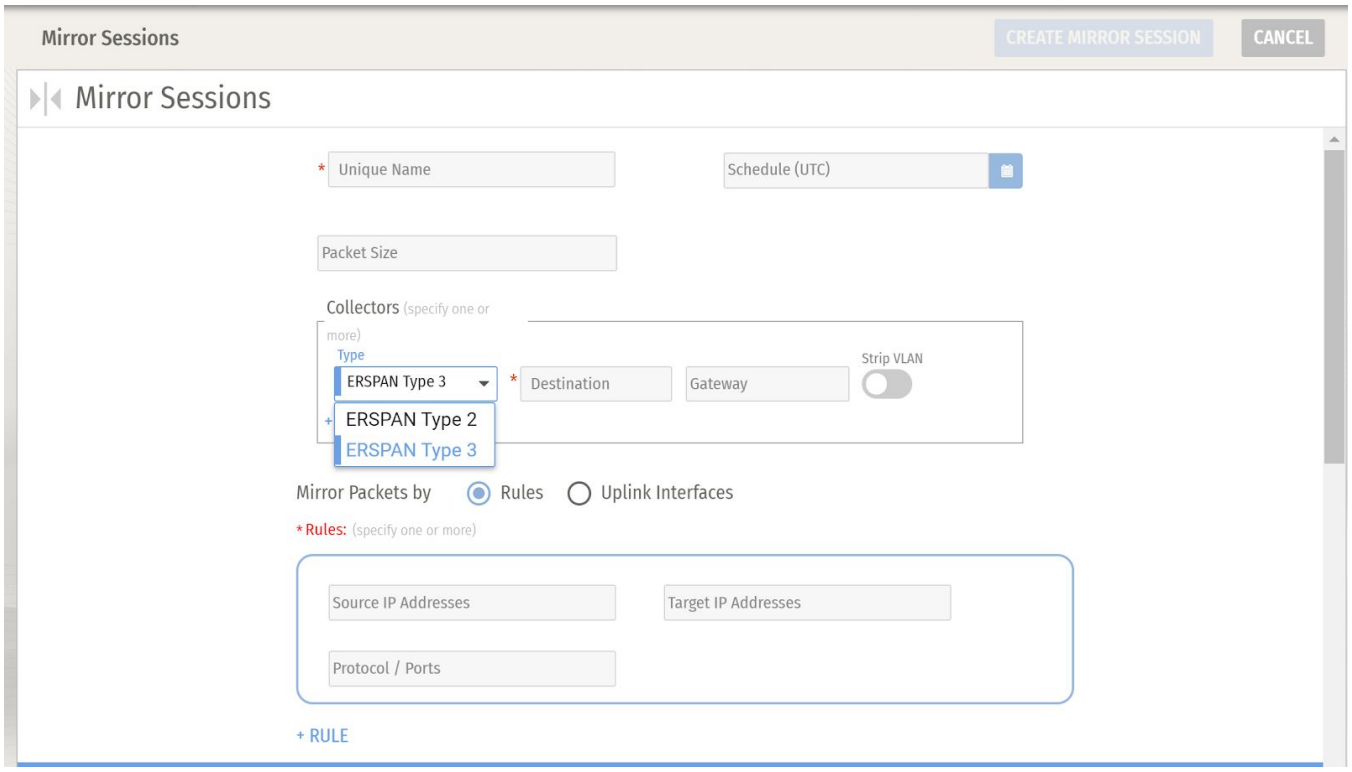

Figure 5. Configuring mirror sessions

With the Pensando platform, administrators have the visibility needed to troubleshoot traffic issues as they arise, without an expensive parallel tap and traffic-brokering infrastructure.

[1] If ERSPAN were instead enabled via the Top-of-Rack switch, only one of the traffic directions would be captured and mirrored, whereas the DSC has the unique ability to capture and mirror in *both* directions while maintaining the temporal relationship between captured packets.

Distributed stateful firewall logs

The Pensando platform offers a distributed stateful firewall to protect data center East-West traffic, which traditional firewall appliances are not well-positioned to analyze. The network administrator gains full visibility of firewall operations by exporting the firewall logs from the DSCs enforcing the firewall policies directly to "syslog" collectors.

The administrator can specify a single collector for all logs, or distribute the logs to different collectors based on the action being logged (allow, deny, reject, etc.).

PSM Administration

Operation of the Platform itself is simplified by its built-in features, including logging events and alerts related to system state and configuration, saving and restoring global configurations, and managing upgrades in a completely automated way.

AAA

The PSM offers a complete solution for Authentication, Authorization, and Accounting (AAA).

Authentication

The PSM supports several authentication policies, as shown in Figure 6.

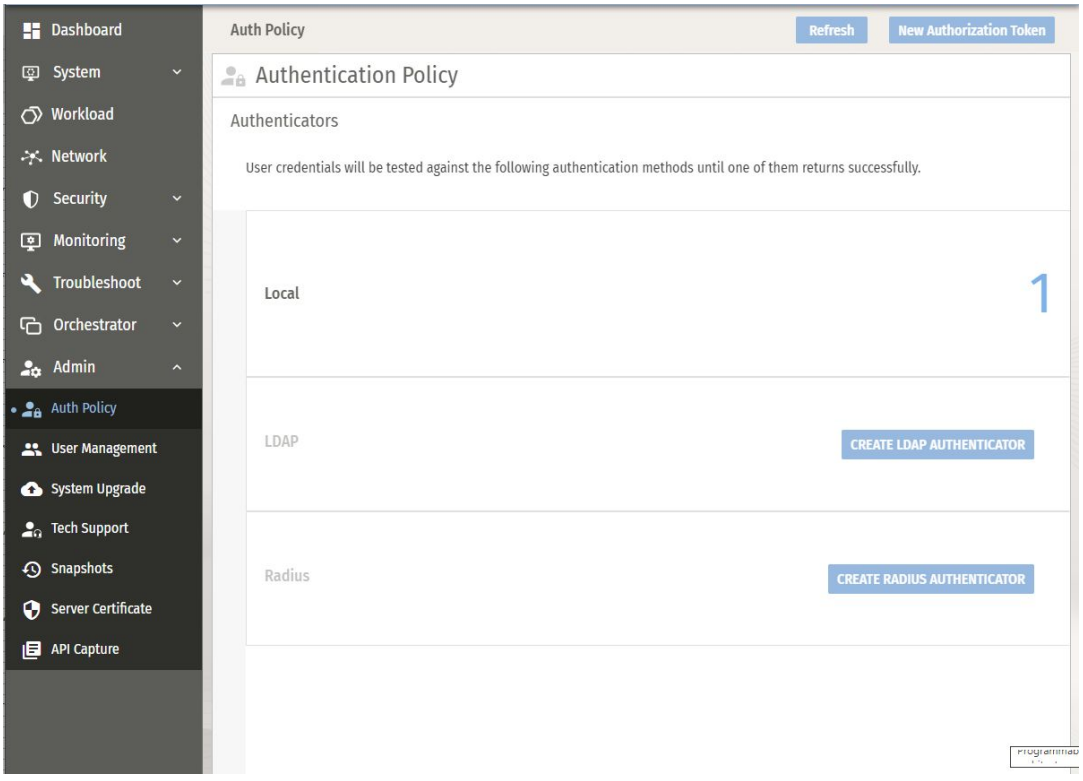

Figure 6. Authorization Policy screen

Authentication Policy should be established early in the system setup process with Authentication Policies that can be reordered dynamically.

Local users

Local users can be created via the User Management menu, clicking on the Add User button, and filling out the form shown in Figure 7:

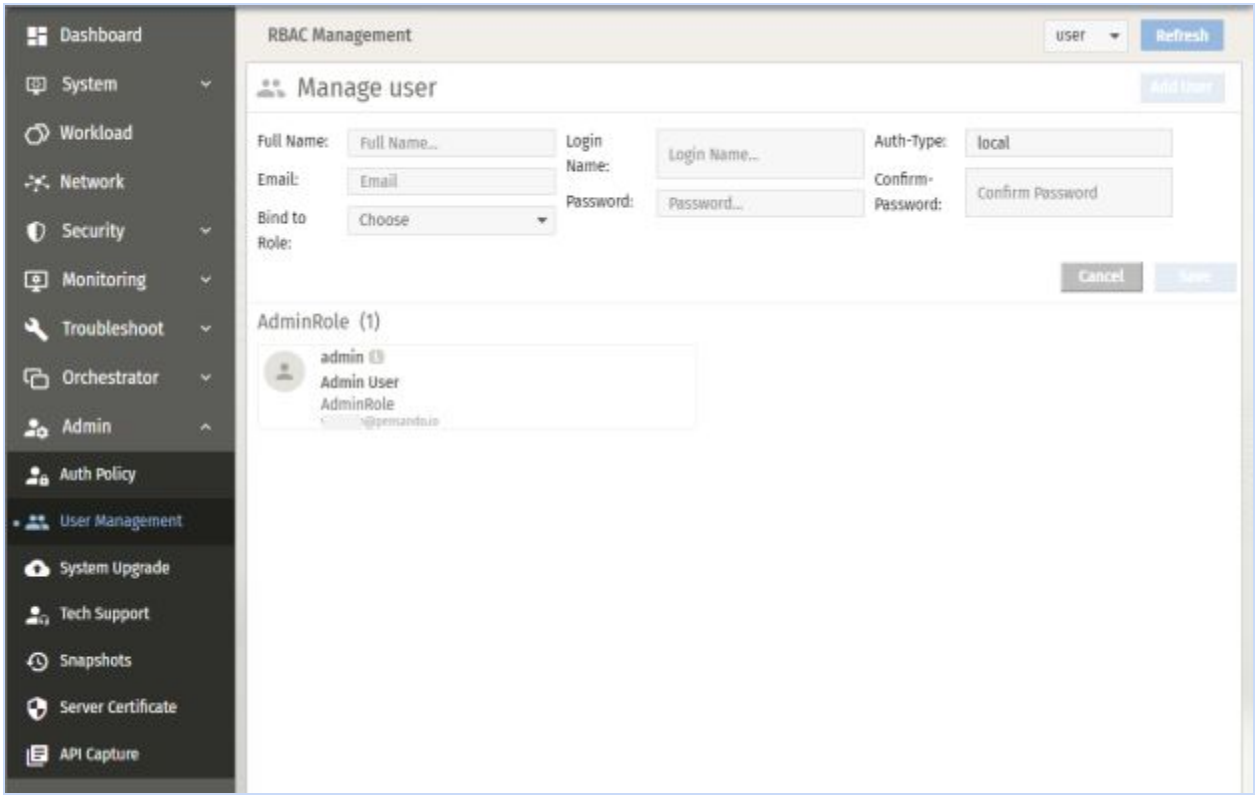

Figure 7. Creating a local user

LDAP and Active Directory (AD)

To create an LDAP (Lightweight Directory Access Protocol) Authorization Policy, click the "CREATE LDAP AUTHENTICATOR" button in the Admin view, shown in Figure 6 above. Active Directory (AD) and OpenLDAP providers are supported.

Configure the **Credentials**, **Scope**, and **Attribute** Mapping as appropriate, ensuring all required (*) fields are properly filled, as in Figure 8:

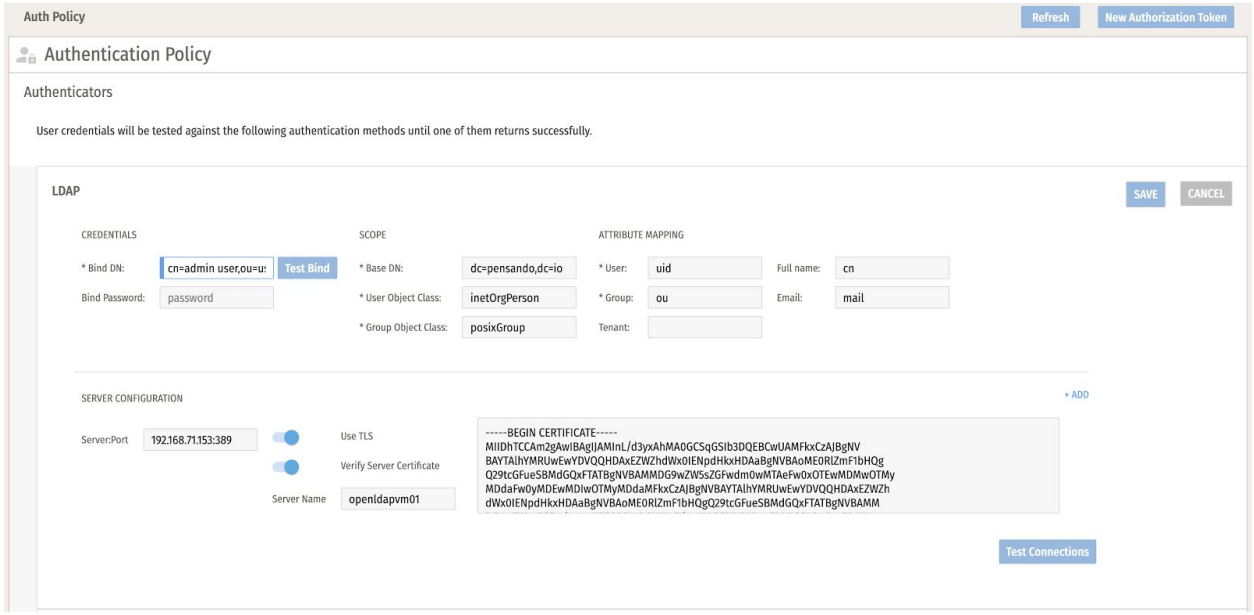

Figure 8. Authentication fields

Once saved, the values should be visible, as in Figure 9:

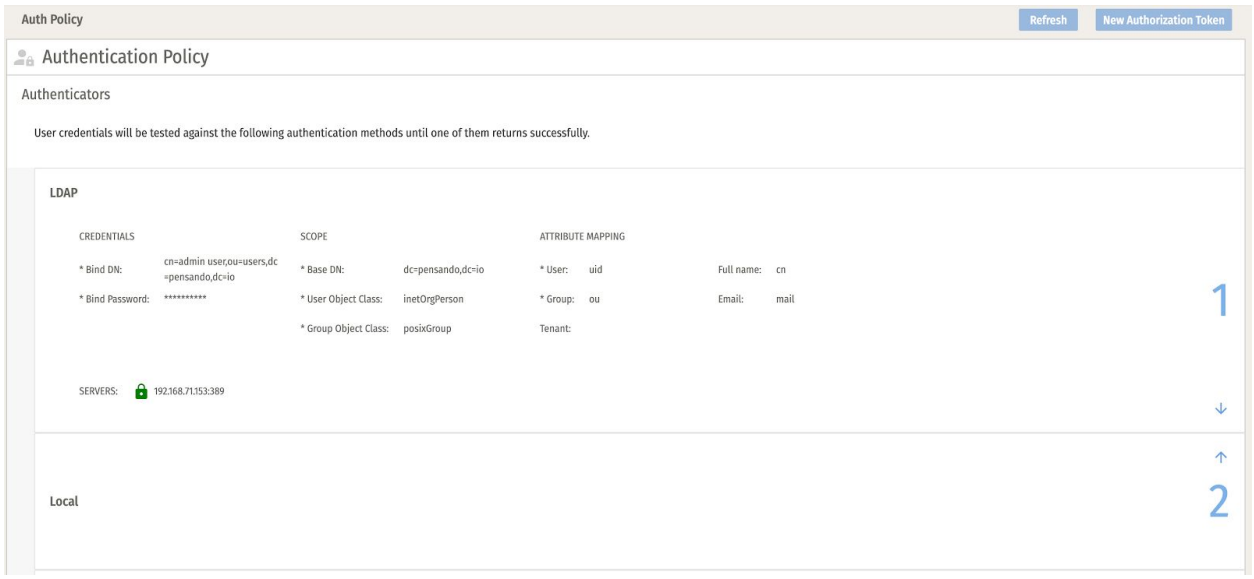

Figure 9. LDAP settings

Create or Update the RoleBinding with the "User Groups" string as below. This string is the "Group" attribute value configured in the LDAP policy "Credentials" section, taken from the LDAP server configuration for the corresponding LDAP user(s).

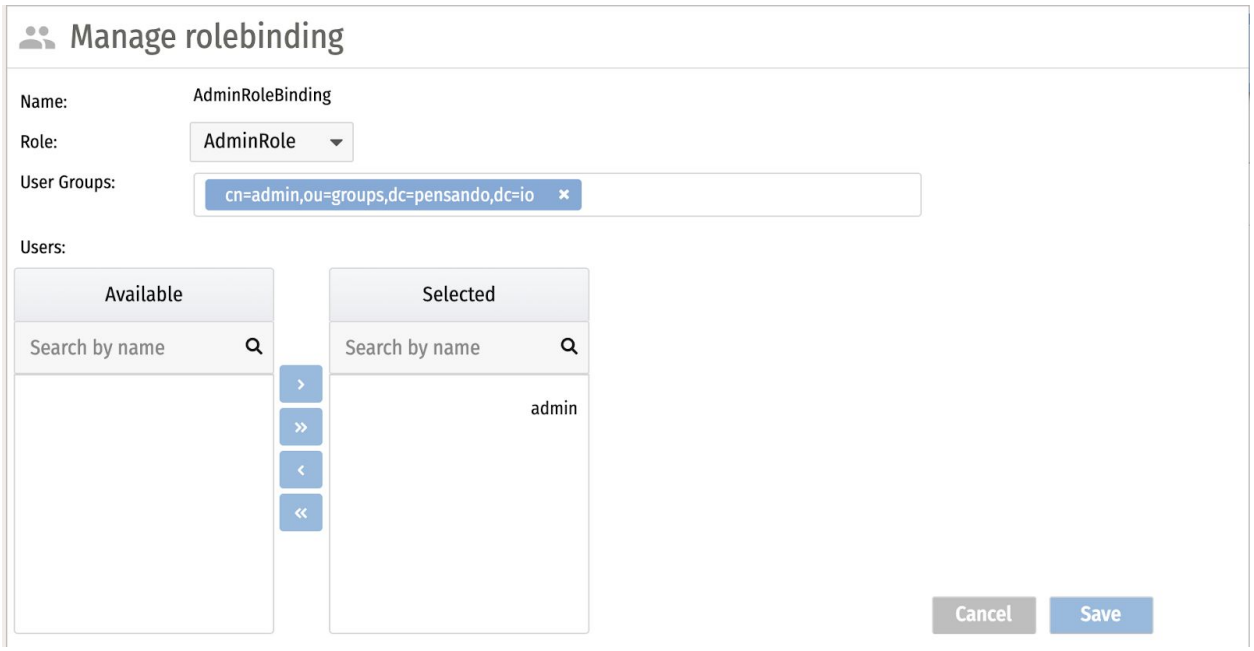

Figure 10. Rolebinding

User Management

User Management, Roles, Role Bindings and Authentication Policy settings can be configured in PSM in User Management under the Admin Menu.

The recommended sequence for User Management is to first create one or more Roles, followed by one or more Users. The Role, Rolebinding and User objects can all be created from the dropdown User Management Menu:

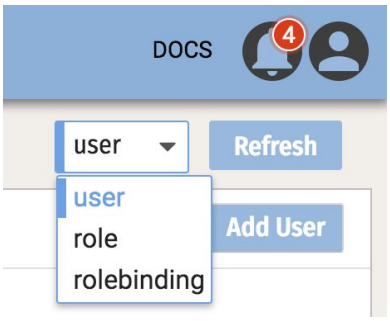

Figure 11. User Management menu

Role / Rolebinding

Create a Role to control access classes for users. Roles can have scope over various "Groups" (i.e. management aspects) including:

- Auth
- Cluster
- Diagnostics
- Monitoring
- Network
- Objstore
- Rollout
- Security
- Staging
- Workload

For a given Group, Action Access can be further granted or limited to:

- Create
- Delete
- Read
- Update

Once a Role is created, a corresponding "Role Binding" is created implicitly.

User Creation

Creating a User will allow you to bind the User to any previously created Rolebinding.

Audit logs

The PSM collects Audit Events that, as shown in Figure 12, log configuration changes to the platform and the distributed services running on it.

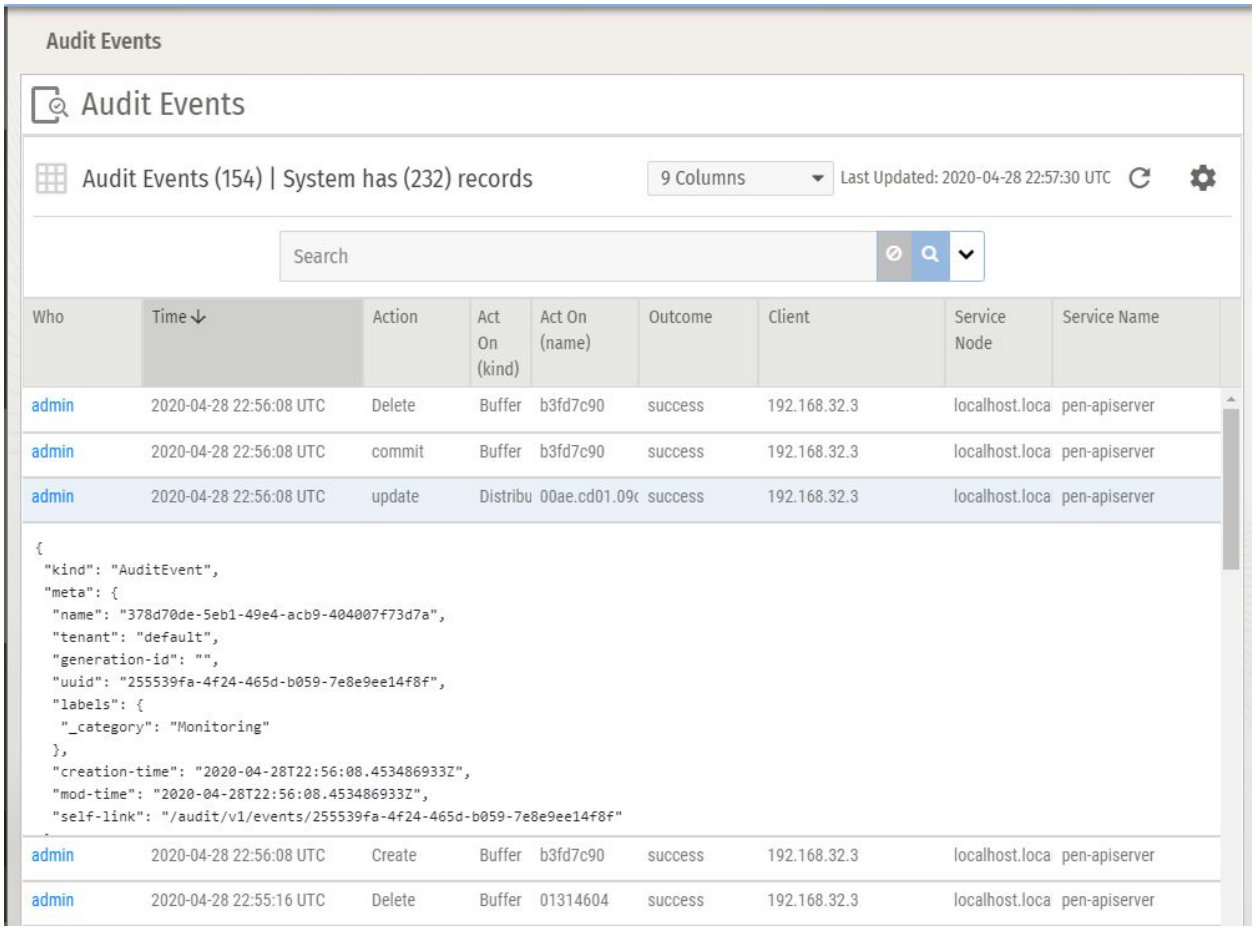

Figure 12. Audit configuration

System logging

The PSM collects events and alerts related to the platform. The administrator can define policies to specify which such events should be logged and whether they should be sent to an external "syslog" collector.

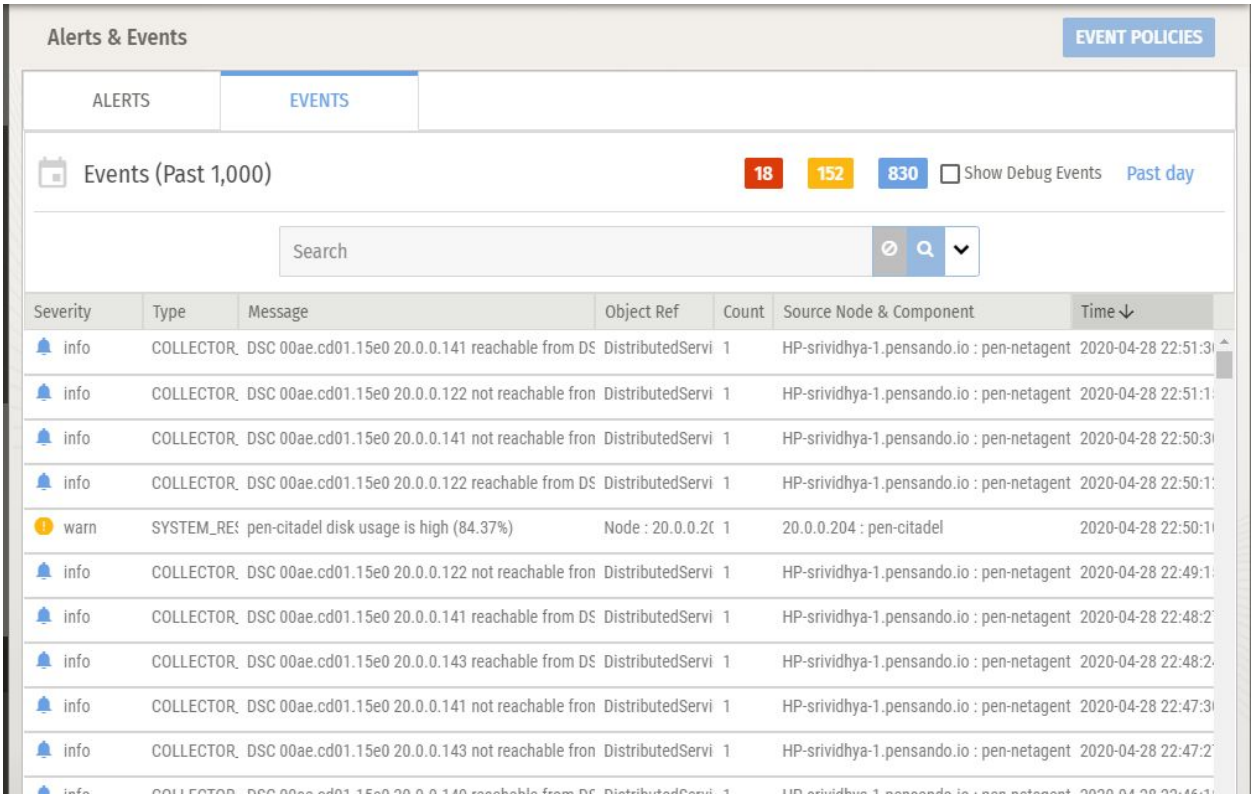

Figure 13. Logged Events

Figure 13 above shows a sample display of events, classified as informational, warning or errors. Typical events include PSM level information (such as a disk getting full or a user logging onto the PSM), DSC lifecycle events (such as a DSC being admitted to the PSM), or a "syslog" collector not being reachable.

The administrator also has the capability to select a subset of alerts and events to be collected into a downloadable archive.

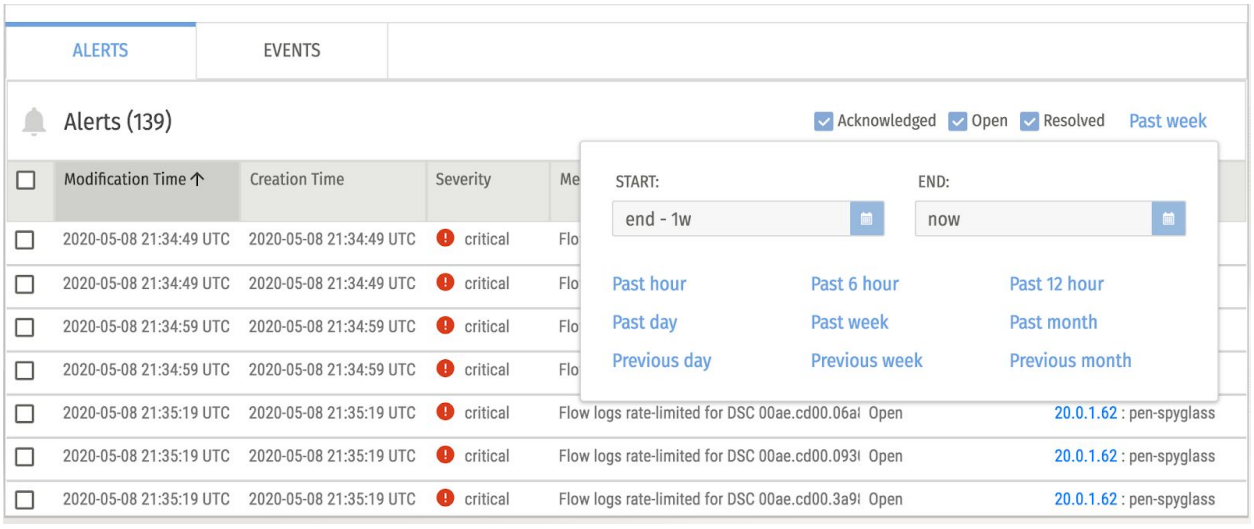

Figure 14. Selecting specific events

The screenshot in Figure 14 above shows sample alerts that are classified as critical. Administrators can filter based on disposition ("Acknowledged", "Open", "Resolved"), and limit the search to a specific time period.

Configuration Snapshots

The PSM can capture a snapshot of its configuration, which includes the feature sets activated and policies installed on each DSC. Snapshots are stored on the PSM and can be restored when necessary.

This lets the administrator save configurations that are known to work properly, and experiment with changes knowing that the entire platform can be easily rolled back to a known, working state.

Upgrades

The PSM provides a centralized, simplified system for managing DSC software and firmware upgrades. The PSM also provides easy, reliable management for upgrading the Virtual Machines (VMs) that compose the PSM cluster itself.

Once a new software release is selected and the upgrade is started, the PSM is upgraded first, one VM at a time. Then each DSC is upgraded.

Upgrading a 3-node PSM cluster takes about 15 minutes, while the upgrade of each DSC takes about 3 minutes. During the upgrade, services are not disrupted; packet forwarding is halted for a short time on each DSC, but no state information is lost and after a brief pause, packets resume flowing normally. The overall time required to complete the upgrade of an entire platform depends on the upgrade strategy adopted and the maximum number of DSCs that are allowed to be upgraded in parallel. For example, it is possible to schedule the upgrade to be performed at a future time and to specify that DSCs are upgraded only the next time their host is rebooted. The PSM provides a view of the status of the upgrade process.

Third-party Integration

The Pensando Distributed Services Platform is designed to integrate with third party tools and systems to simplify the role of the network administrator, facilitate the deployment of the Pensando platform in pre-existing environments, and leverage functionality not directly provided by the Pensando solution. Some examples are given below:

Custom Orchestrators and Automation

In addition to the Graphical User Interface (GUI) as seen in examples abovet, the PSM offers a REST (REpresentational State Transfer) API (Application Programming Interface), allowing for programmatic access to all the features offered by the Pensando platform. This API enables sophisticated integration of the network and visibility services offered by the Pensando platform with existing data center environments, such as an orchestrator used by an enterprise for the automation of their data center. Since the API design and documentation is based on Swagger, it is particularly easy to create Python and Ansible scripts to automate PSM operations.

Custom Controllers

If an enterprise has developed their own controller for their services and prefers to use it instead of the PSM, this is easy to do as all communication between the PSM and DSCs takes place via a well-defined interface based on gRPC (gRPC Remote Procedure Call). Since the protobuf (Protocol Buffer) message definition understood by the DSC is documented, DSCs can be controlled directly from a custom enterprise controller.

Telemetry Collectors and Analytics

As previously discussed, DSCs offer a wide array of telemetry data and even the capability of exporting captured packets. Since standard formats and protocols such as IPFIX, syslogs, and ERSPAN are used for this purpose, various third-party tools and platforms can be used to collect and analyze this data. For example, interoperability has been verified with solutions such as Wireshark, Corvil, Extrahop, Splunk, and ELK.

About Pensando

Founded in 2017, Pensando Systems is the company pioneering distributed computing designed for the New Edge, powering software-defined cloud, compute, networking, storage and security services to transform existing architectures into the secure, ultra-fast environments demanded by next generation applications. The Pensando platform, a first of its kind, was developed in collaboration with the world's largest cloud, enterprise, storage, and telecommunications leaders and is supported by partnerships with HPE, NetApp, Oracle, IBM, Equinix, and multiple Fortune 500 customers. Pensando is led by Silicon Valley's legendary "MPLS" team – Mario Mazzola, Prem Jain, Luca Cafiero, Soni Jiandani and Randy Pond – holding an unmatched track record of disruptive innovation having already built $8Bn/year businesses across storage, switching, routing, wireless, voice/video/data, & software-defined networking. The company is backed by investors that include Goldman Sachs and JC2 Ventures. For more information, please visit www.pensando.io

DOCUMENT REVISIONS

Pub Date	Exp/Review Date	Description
31-Nov-2020	1-Dec-2021	Initial release.